
international risk governance center

Not for circulation

BACKGROUND PAPER

# Governing Cyber Security Risks and Benefits of the Internet of Things: Application to Connected Vehicles and Medical Devices

## Creating trust in connectivity: confidentiality, integrity, and availability

This paper is to support discussions at the expert workshop on 15-16 Nov 2016, organised by IRGC with support from Swiss Re & AXA Technology Services, and hosted by the Swiss Re Centre for Global Dialogue. It describes the context in which presentations and discussions at the workshop will be organised and provides background elements for each session and suggests questions for discussion. The paper does not intend to constrain the topics that will be addressed in the workshop.

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

international risk governance center

# Preface

The development of the Internet of Things (IoT) implies a range of cyber security issues. As this background paper illustrates, this is specifically the case for connected vehicles, which are connected to the Internet and location services. This is also the case in the field of connected implantable or wearable medical devices, because most of these also require some form of connection to external networks.

It is important to address those issues, otherwise the trust of the public – in this case, car and road users or patients – can be eroded. When trust is lacking, opportunities that IoT-related technologies offer cannot be fully exhausted, and benefits to society and the economy will be suboptimal.

Cyber security risks in the IoT are worth exploring in-depth because of their particular nature as adversarial risks with a deliberate intention to cause harm, which is outside of the scope of standard risks. When a cyber risk has negative consequences on a person's health, integrity or even life, or causes breaches to privacy, the stakes are quite different from when the loss is financial or reputational. Vulnerabilities can also extend to other systems. Thus, the implications of relying on insecure connectivity for the IoT, involving devices and communication channels, are wide ranging.

What is not clear is what type of risk management can be implemented, on top of security measures. Can cyber security concerns be dealt with through technical means only, i.e. cyber security *solutions*, which industry can implement because they make sense in economic and business terms? Are new or revised standards needed, with appropriate certification schemes? Which other arrangements, such as public regulation or insurance incentives and schemes must be put in place?

Ultimately, it is society that decides on whether or not it wants to adopt disruptive technologies such as those involved in the IoT with increased internet access and other forms of connectivity.

- Society may decide based on its evaluation of *expected benefits* such as performance, convenience or comfort; or
- especially if a serious *accident* happens, society may conclude that, in its opinion, the risks exceed the benefits; or
- it may decide based on a complete analysis of the *trade-offs* between various risks and benefits, or prepare to revise its decision as the IoT develops

IRGC recommends that actors in this field engage into a complete analysis of the trade-offs involved, so that society makes the best possible informed decision. IRGC will provide a space for discussion about various ways to govern cyber security risks during a multi-disciplinary expert workshop on 15-16 November 2016.

# Contents

## Introduction

The Internet of Things (IoT) drastically changes how individuals interact with objects, wherever those may be located. It creates significant opportunities for more efficiency, convenience and comfort and can improve performance and reduce inefficiencies in numerous sectors. Specific promising gains and applications include traffic efficiency thanks to connectivity between vehicles and with infrastructure (towards autonomous vehicles), the provision of personal health care (mHealth or eHealth[1]) through implantable or wearable connected medical devices including apps (Software as a Medical Device), smart homes and buildings, smart factories and supply chains, smart cities, and smart grids. IoT technologies include specific infrastructure with sensors and processors for wired and wireless applications, and a range of connectivity and security solutions.

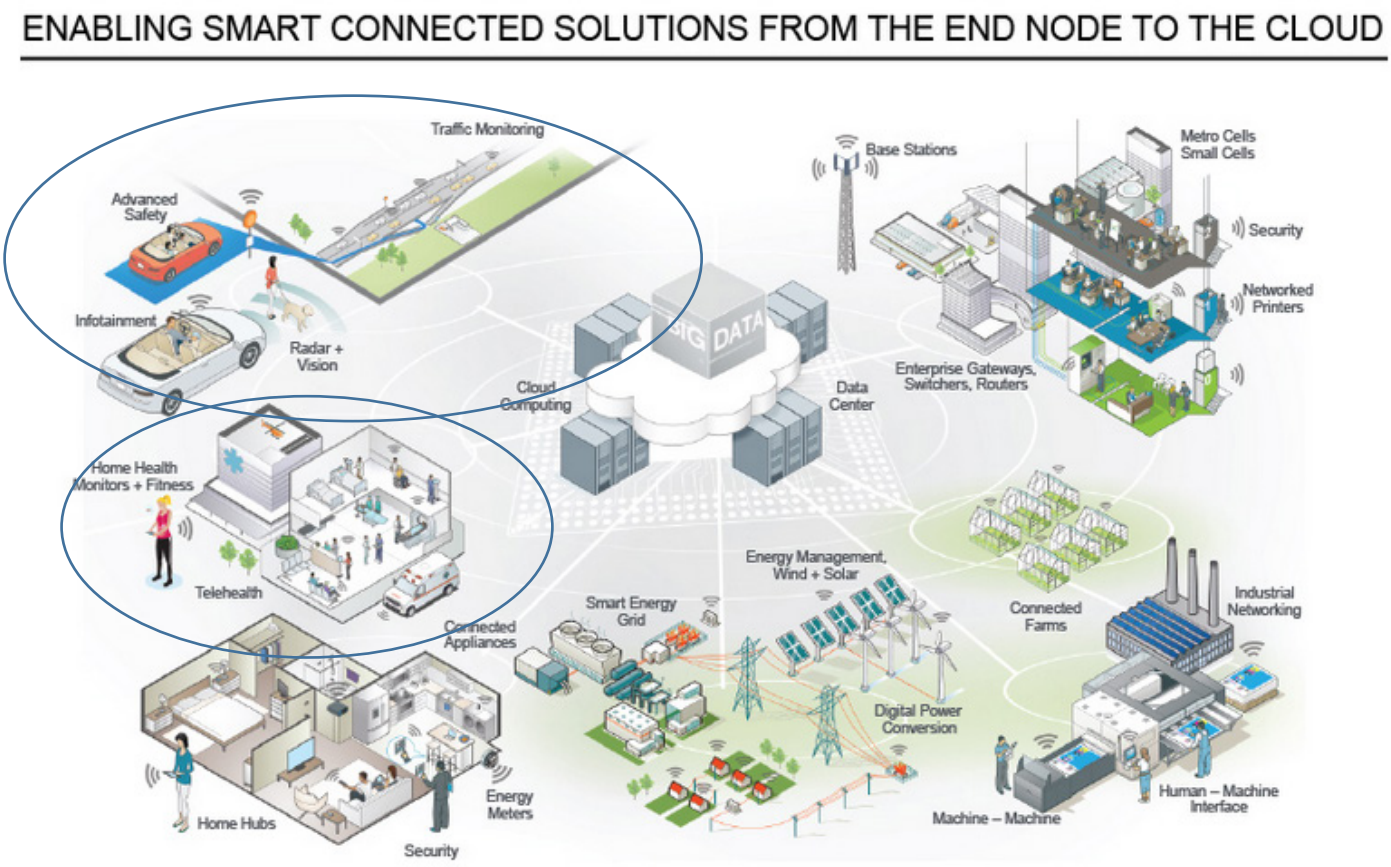


*Figure 1: Smart Solutions for the IoT.*
*Courtesy from NXP - Available at: http://www.nxp.com/applications/solutions-for-the-iot-and-adas/smart-connected-solutions-for-the-iot:SMART-CONNECTED-SOLUTIONS*

The safe and secure use of IoT is concerned with cyber security issues and vulnerabilities. These issues associated with connected vehicles and with connected medical devices are similar to other applications of the IoT. However, what makes these applications and their networked environment special is the potential direct negative impact on the physical safety and the security of road users and patients, if cyber security vulnerabilities are exploited. The IoT has the potential to play a transformational role in transportation and in health care, but could also directly expose road users, patients and health care organisations to new safety and security risks. Unintended consequences of increased connectivity and

automation in car driving and of the digitalisation of health care include the risk of being hacked, being infected with malware and being vulnerable to unauthorised access, which may trigger risk of a physical car accident or adverse health outcomes. It also includes a risk of accident caused by unintended error or negligence, because of the increasing complexity of the cyber-physical systems.

Those issues will be addressed in the expert workshop.

The workshop will:

- Explore the extent to which cyber security is a true concern for connected cars and medical devices (implantable or wearable)
- Review what technological solutions exist or are needed, and what types of new governance arrangements would be necessary
- Aim to elaborate practical guidelines or recommendations for improving cyber security and creating trust in connectivity of the IoT

**Defining the context**

In the context of high expectations and promises of the Internet of Things (IoT), this paper focuses on:

- Connected vehicles (CVs), in which connectivity between vehicles (V2V) or with infrastructure (V2I) is needed for advanced levels of autonomy.

- Implantable or wearable medical devices that are connected to a network (NMDs). We include implantable medical devices such as insulin pumps, pacemakers or defibrillators as well as wearable devices for medical monitoring for better health outcome, when there is a connection between a patient and his healthcare provider, whether in a hospital setting (infusion pumps, ICU monitoring) and home/mobile monitoring equipment. Wearable devices for healthy lifestyle monitoring are included to the extent that they represent vulnerable entry points to healthcare or other critical systems, such as in the October 2016 Dyn attack in the US[a].

When connected to the Internet, these 'things' are vulnerable to cyber security threats and consequently pose additional risks. Serious connectivity malfunctioning could affect the critical services provided by the IoT.

[a] The October 2016 Dyn cyberattack took place on October 21, 2016, and involved multiple denial-of-service (DoS) attacks targeting systems operated by Domain Name System (DNS) provider Dyn which made major Internet platforms and services unavailable to large swaths of users in Europe and North America. The groups Anonymous and New World Hackers claimed responsibility for the attack.(...) Dyn disclosed that (...) the attack was a botnet coordinated through a large number of Internet of things-enabled (IoT) devices, including cameras, home routers, and baby monitors, that had been infected with Mirai malware. October 2016 Dyn cyberattack. (2016, October 26). In Wikipedia, The Free Encyclopedia. Retrieved 06:45, October 26, 2016, from https://en.wikipedia.org/w/index.php?title=October_2016_Dyn_cyberattack&oldid=746252416

**Promises and associated issues**

The IoT promises to deliver significant improvement to the quality of life and efficiency gains across a wide range of sectors. To make this happen, policymakers, regulators and other stakeholders work to establish a regulatory context that facilitates the IoT, but also deals with key physical safety, economic and legal issues, including data privacy and data security, intellectual property rights, legal liability (who is responsible in case of incident, product liability and tort liability). It also addresses issues such as the possibility that greater automation displaces certain manual work, and the risk that social and economic impact and inequalities will increase and exclude certain groups from the benefits.

Manufacturers routinely rely on smart sensors and sensor data to optimise the operation of devices, for example in supply chains. What is new is that the data is used not only for monitoring, detection and control, but increasingly for management: optimisation and prediction. IT systems, and progressively artificial intelligence, analyse the data and make autonomous decisions about management actions. If the data is missing or compromised, as a result of either unintentional user error, defect or intentional intrusion in the system, the output may have catastrophic consequences. Also, widespread sensor placement, network connectivity and sophisticated data analytics now enable applications that aggregate large amounts of data generated by devices connected to the IoT, which are often private. This data may belong to an individual who may decide or be obliged by law to share them with other people, in exchange for expected benefits. As individuals let others have access to the data, they may or may not be aware that they expose themselves to risks that they may be unable to control. Consequently, if things turn out negatively, they may not be able to stop, reverse or modify the process.

**Applications to connected vehicles and medical devices, cyber security concerns**

There is a large variety of applications that use the IoT. Some are primarily for convenience, leisure and comfort, while others involve physical safety, privacy and personal data.

- **Autonomous vehicles (AVs)**
  When autonomous vehicles are connected to other vehicles or to infrastructure, it enables more efficient driving: vehicles communicate and cooperate with each other and with infrastructure. More efficient driving is linked to numerous benefits, including reducing traffic congestion, air pollution, $CO_2$ emissions and new mobility services. GPS navigation is only available if cars are connected to mapping services, based on maps elaborated by private or public entities, which deliver information that must be trusted by car users.
  The automotive industry uses the IoT for connecting cars, as part of the move towards autonomous driving. In the Chrysler Jeep Hack in 2014[2], key systems such as engine management and braking systems were shown to be accessible using an external cellular connection. In March 2016, the US computer emergency readiness team (US-CERT) issued a warning through a joint FBI, Department of Transportation and NHTSA Public Service Announcement that vehicles are increasingly vulnerable to remote exploits.[3]

- **Networked medical devices (NMDs)**
  The medical sector also uses the IoT for connecting medical devices. When someone's pacemaker or insulin pump is connected through wireless connectivity, the patient's health is monitored for improved medical care. Personal data is transmitted from and to the device. The broad medical sector and the population became publicly alerted to this potential risk when US vice-president Dick Cheney revealed in 2013 his fear that his pacemaker could be hacked because of its wireless functionality[4]. US FDA recognises that cyber security threats to medical devices are a growing concern and that the exploitation of cyber security vulnerabilities presents a potential risk to the safety and effectiveness of medical devices. FDA recommends that manufacturers incorporate controls in the design of their new products to help prevent these risks, but also that they consider improvements throughout the entire lifecycle of a device. "*All medical devices that use software and are connected to hospital and health care organisations' networks have vulnerabilities—some we can proactively protect against, while others require vigilant monitoring and timely remediation*".[5]

Neither the conventional automotive industry (i.e. excluding new entrants in the sector such as Google or Tesla that have a different approach to the marketing of autonomous driving) nor the medical sector have established routine risk management frameworks that include *both* traditional safety aspects and cyber security aspects. Many IT specialists and risk managers are not used to dealing with risks from adversaries, with deliberate attention to cause harm, who exploit weak entry points as vulnerabilities to enter in the system, and seek money, data or power. Information security risk (particularly intentional threats) is a relatively new field for service providers, manufacturers and regulators, embedded in the new role of chief information security officers (CISOs).

- Road and car safety regulators are not familiar with cyber security issues and it is not clear how conventional regulators like UNECE or NHTSA will address these risks in their regulations.
- The medical sector and biomedical technicians in hospitals do not routinely include in their risk management frameworks risks involved in the use of NMD, which are primarily handled by IT specialists or chief digital officers (DGOs).

The term **cyber security risk** is used to describe a large variety of context-specific adversarial challenges. Overall, it entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption. In this workshop, we may also include risks that derive from **unintentional important failures or deficiencies in the connectivity function**, as they would result from inappropriate security design.

Device or data security, and the lack of clarity of purpose or understanding of the benefits of the IoT are often cited as causes for concern.[6] We need to worry about how the IoT connects devices, using mainstream computer platforms, PCs, tablets, smartphones, and software that are susceptible to unintentional failures, as well as malware and intentional hacking. Software needs to be properly designed, configured and regularly updated or patched to protect data. On their side, consumers are required to observe good cyber security "hygiene" to prevent cyber security risk from materialising.

Attacks on the IoT and its associated infrastructure are potentially very serious[7]. There is some speculation as to the severity and scope of such threats, and to what extent privacy or life can be threatened. However, if not addressed early and comprehensively, cyber security risk may hinder trust in specific applications of the IoT, such as those that can be life critical or threatening[8].

This paper introduces discussions about cyber security aspects of the IoT, in critical sectors where individual lives could be put at risk if the IoT is dysfunctional. **Questions** include:

- The IoT develops new opportunities through technological development, but what are the risks that come with this?
- What are we protecting and for what purpose?
- Is there a way to connect all those "things" without creating new risks that are not manageable?
- To what extent can new technologies and IT science help mitigate the risks?
- Can we make better use of existing standards, controls, and solutions?
- Are general rules needed? New or revised regulations and standards?

More regulation may impose content controls, diminish intellectual property rights, or make other requirements that could hinder innovation. If regulation is needed, it should be after a careful and evidence-based risk assessment that evaluates and balances the benefits and the risks from network connectivity, and a review of current and anticipated technical ways to manage the risks.

## 1. How does science, research and technology help deal with cyber security issues and other potential failures in connectivity, confidentiality, integrity and availability?

Protecting data in the IoT requires securing the hardware itself (and having the right checks in place from the design stage) as well as the software (and the ability to maintain and upgrade it).[9]
In general, the following principles can be recommended:

- **Security by design and by default**. It is very important to consider security right from the start when a new product is designed and not as on top of an existing product. Devices connected to the IoT must be protected to be made intrinsically secure from the ground up, and the default configuration settings should be the most secure settings possible. However, security should be thought of as a process rather than an end-product.
- **Privacy by design and by default**. Each service or business process that makes use of personal data must take the protection of such data into consideration. It is very important to consider data protection and privacy right from the start when a new product is designed. The strictest privacy settings should automatically apply. Privacy is safeguarded by law and regulation as well as by technology. However, privacy should be thought of as a process rather than an end-product only.
- **Need to know principle** (principle of least privilege). Access to the information may be restricted to what is strictly necessary. Each connected entity can only communicate to the IoT the data that is absolutely necessary for its application. Allocating access rights is equally important.
- **Testing**. Connection testing and integration of devices (hardware) and software are a major issue for medical devices, before being deployed in the market. But testing techniques only cover very specific types of weaknesses. Penetration testing is needed to assess the real-world security of a system from the viewpoint of an attacker, by discovering the vulnerabilities and by actively trying to exploit them (assessing security controls).
- **Maintenance**. IoT devices have to be able to receive security updates throughout their whole lifespan to fix vulnerabilities discovered by manufacturers or third parties. Manufacturers should furthermore follow best practices in security which include actively engaging in discovery of said security vulnerabilities.

Cryptography is one of the core technologies routinely used to provide confidentiality, integrity, and authenticity in digital (communications) systems. However, in addition to following cryptography best practices, there are other important technologies that should also be considered to secure the IoT, including:

- **Secure decentralised systems**. Topics here include private and anonymous communication technologies, Internet architecture, and secure operating systems.[10] [11]
- **Robust and transparent software update mechanisms**. As has been shown countless times in the past, software update mechanisms are often one of the most security-

critical components in software-dependent systems and therefore very lucrative and frequently attacked targets. Novel techniques promise to help to defend against, or at least help unveiling, backdoored or otherwise malicious updates. [12]

- **New approaches to privacy and data protection**. There is ongoing research to lay the foundations and develop mechanisms to protect privacy and security in tomorrow's hyper-connected world, with an emphasis on mobile/wireless network.[13] Other work includes protection against fingerprinting of traffic between devices. [14]
- **Smart contracts, distributing trust with blockchains** to redefine cyber security and defend the IoT.[15] [16] [17]
- **Verified software**. There are a few examples of non-trivial software systems that have been fully verified (proven correct).[18] These systems can eliminate quite many potential attacks and other software faults, which is or should be a requirement for building a safety-critical system.
- **Avionics software**. Airplanes rely on high-quality software. The vendors have very strict processes and have to be certified at a very high level. Critical IoT systems would be advised to look at the way software is done in avionics, and use it as a starting point.

**Questions for discussion:**

- What will future IoT technology look like?
- How can IoT-devices be designed, deployed, and maintained in ways that satisfy current security standards?
- What are the main areas of research in computer science and specific IT instruments currently in development for securing the IoT?
- Are manufacturers and IoT operators familiar with these instruments? Do they use them?
- Are manufacturers and tech companies embracing “Security by Design (SbD)” and “Privacy by Design (PbD)” as part of their product development lifecycle and Quality approach?
- To what extent are cyber security issues different for open source vs. proprietary software?
- What are the limiting factors, e.g. power, processing, and storage capacity?
- Could there be a ‘code of conduct’ for manufacturers of IoT devices? For medical devices? For autonomous vehicles? What should it include?

## 2. Connected vehicles (CVs)

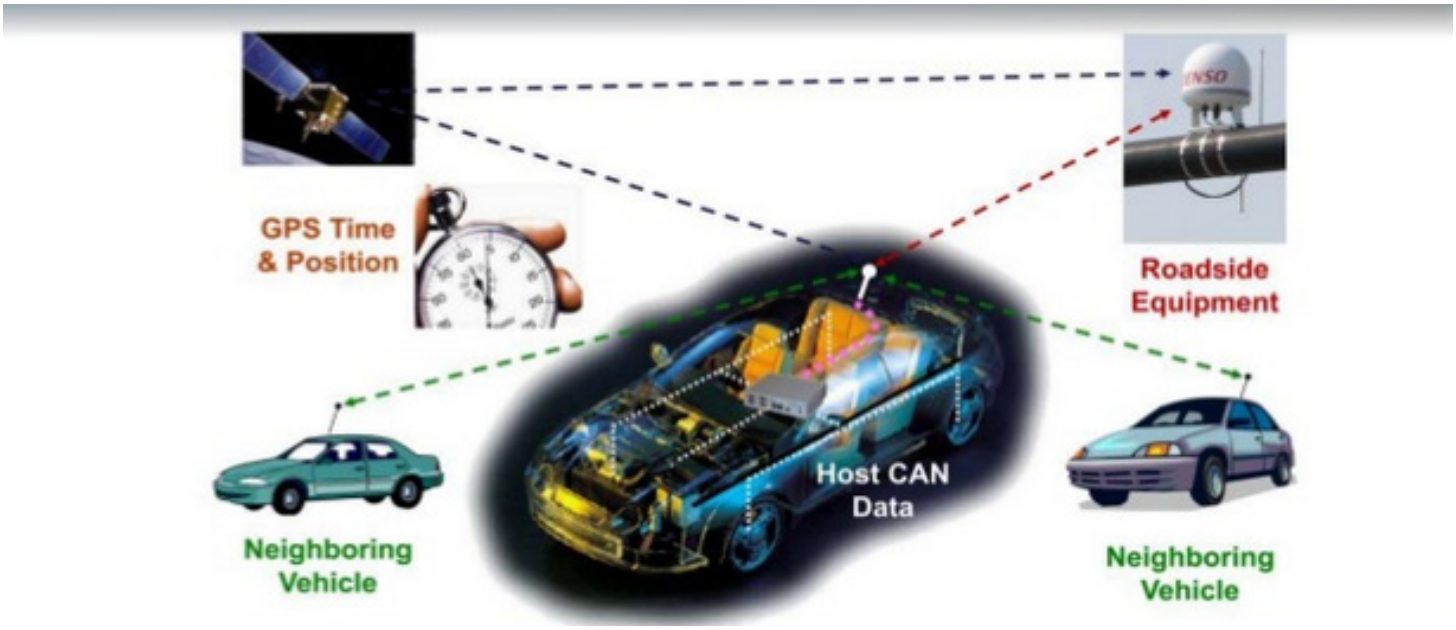


*Figure 2: Connected cars.*
*Courtesy from CAN connected. Available on http://www.slideshare.net/spukale/connected-cars-iotmum-org*

The security challenges involved in the development of connected vehicles (which is instrumental to the success of autonomous vehicles) is closely linked to that of the entire IoT environment. Current automotive platforms do *not* have default security features as applied in other sectors such as the IT industry and the banking sector. However, the automotive sector *must* include security and privacy protection in today's automotive components, systems and platforms where different communication paradigms are embedded in[19]. An acceptable level of performance and reliability in security, safety, privacy-protection for fully connected vehicles will be required before users trust them and regulators authorise them.

The **vulnerability** of connected cars has been demonstrated in numerous cases.[20] Malicious actors can exploit vulnerabilities ranging from unauthorised entry to commandeering the vehicle's operation. The opportunities for compromise will increase together with consumer demand for more features, some for convenience and comfort only.

**Risk of manipulation, intrusion or cyber threats in general are due to:**

- Complexity, which makes securing systems very difficult. For example: there are approximately 100 million lines of codes in a vehicle; vehicles must communicate with many networks, via many Engine Control Units (ECUs), which have to communicate with them; and in-vehicle systems are highly heterogeneous, with some for critical functions, and others for leisure or convenience.
- Connectivity, with the development of wireless communication interfaces and networks. These interfaces serve to connect the vehicle to the IoT and extend functionality, but also make the vehicle more exposed, accessible and attractive to cyber attacks.

- The value of the content information that can be stolen: personal information such as identity or data.

With a growing number of connected vehicles on the roads, their value to attackers and subsequent potential gain will increase. What is unclear is what will be the (main) **motivations** for hackers and the vectors of attacks. Security experts have produced comprehensive analyses of attack surface, type of hacks and specific threats that they pose, and anatomy of attacks.[21] Bluetooth, for instance, is considered to be one of the biggest attack surfaces, due to the complexity of the protocol and underlying data.

The **potential threats** that may be of highest concern include[22]:

- Unauthorised physical access to vehicles; deliberate manipulation of a vehicle's operation: door unlocking, remote start, acceleration, steering, braking.
- Theft of personally identifiable information from manufacturer or third-party storage systems
- Extortion enabled by ransomware that renders vehicles inoperable until a ransom is paid.
  The risk of ransomware has so far affected ordinary individuals, hospitals, and other institutions. Vehicle's increased connectivity, ever-expanding attack surface, and high upfront cost make them attractive ransomware targets. Also, vehicles are more likely susceptible to ransomware attacks when their disablement can cause knock-on effects.
- Hijacking vehicle systems to enable malicious cyber activity: if vehicular systems are/would be used as command and control infrastructure for illicit cyber activity.
- Connectedness dependency, both to the vehicle's function and the social implications.

**Cyber security risk in Intelligent Public Transport**

The European Union Agency for Network and Information Security (ENISA) is an EU agency that works with EU member states, as the centre of expertise for cyber security in Europe. In 2015 it published the results of a survey about threats, risks, challenges and gaps facing cyber security within Intelligent Public Transport (IPT) [23]
Challenges:

1. Difficulty to integrate security for safety
2. Inadequate importance and spending being afforded to cyber security
3. Inadequate checking for countermeasures
4. Unwillingness to collaborate and exchange information on cyber security
5. Slow phasing out of legacy systems
6. Inadequate data exchange between IPT and smart cities operators
7. Weak situational awareness of cyber threats
8. Resistance to security adoption

After summarising existing technical, policy, standards, organisational and human good practices, the report provides a gap analysis:

1. Lack of a common EU approach to IPT security
2. No integration of security in current EU guidelines for IPT

3. Lack of common definitions and formalised cyber security policies
4. Lack of corporate governance of IPT security
5. No specific security standards for IPT
6. Lack of advanced interdependent analysis tools
7. Lack of advanced risk assessment tools
8. Lack of advanced real-time and multi-stakeholder-enabled security technologies

Recommendations include:

Institutions and decision makers should:

- Promote public/private collaboration on IPT cyber security
- Promote and facilitate the development of a common EU approach to IPT security
- Develop a comprehensive EU strategy and framework for cyber security in IPT
- Integrate and converge security efforts made in other sectors of activity
- Foster the development of harmonised cyber security standards for IPT

Transport operators should:

- Integrate cyber security in their corporate governance
- Develop and implement an integrated corporate strategy addressing holistically cyber security and safety risks
- Implement risk management for cyber security in multi-stakeholder environments including external contractors and dependencies
- Clearly and routinely specify their cyber security requirements
- Annually review organisational cyber security processes, practices and infrastructures

Manufacturers and solution providers should:

- Create products / solutions that match the cyber security requirements of IPT end-users
- Collaborate in the development of IPT-specific standards and apply them to IPT solutions
- Develop a trusted information sharing platform on risks and vulnerabilities
- Provide security guidance for systems, products and solutions

*Box 1: ENISA Cyber Security and Resilience of Intelligent Transport Systems*

**Cyber security is a new challenge and a new field for car manufacturers**

The cyber security of connected vehicles is among the major challenges that car manufacturers and others in the supply chain are facing, primarily because this is new to them. The mitigation of cyber security is a new field of research, testing and implementation.[b]

The field of automotive cyber security is emerging. It is different from the field of automotive safety, because safety is probabilistic. The individual risk of accident can be calculated and kept within acceptable boundaries aligned to a set of protective measures. The residual risk can be transferred to insurance. In contrast, cyber risk can hardly be calculated because of the malicious nature of hackers, who cause intentional and accidental

[b] Other challenges (which the workshop will not discuss) include the technology of sensors, radars, cameras and LIDARs that enable to a car to sense its environment, and with data fusion that enables the car ECU to interpret the data and make decisions.

harm. More research is needed about the cyber security of connected cars, to assess and characterise the risk, and develop methods for predicting it, preventing it and reducing its negatives consequences. A particular difficulty is that this must be done throughout the lifetime of the vehicle, which requires maintenance and updates, both physical and over-the-air.

Successful remote and safety-critical attacks on vehicles are not only "cyber". They are "**cyber-physical**" attacks. They require that attackers can have a remote access to an internal automotive network, that they are able to communicate with the network by sending messages to the vehicle's internal communication bus, to control the target ECU, and that they can instruct the ECU to take control of the physical parts of the vehicle, by interacting with other ECUs, such as those for braking, steering or accelerating.

Like for any cyber-physical system, it is difficult to determine ex-ante whether a car is safe. First, one must examine how it behaves in many different circumstances, user contexts and driving styles. Testing safety features and behaviour is an activity that car manufacturers are familiar with, but assessing the absence of insecure behaviour, or the lack of vulnerability, is much harder. Vehicles are made to be safe. This is an intention. But whether an autonomous car behaves safely is different. Hackers do not look at the beauty of the systems architecture, but at the bugs and weak points of entry. Program testers look at the presence of bugs, not their absence.

Suggestions for building cyber security in connected vehicles, and end-to-end security and privacy will probably be based on the following principles[24]:

- Security and privacy frameworks, implementation on the basis of security and privacy by default
- (Open) platform principles and architectures that utilise trust components and trusted intra- and extra-vehicular networks, the seamless cooperation of different communication paradigms and high data-rate sensor-networking
- Trusted cloud services for diagnostic, prognostics, monitoring and upgrading
- Safety, comfort and cooperative mobility services, which also maintain privacy
- Good practices, policies and standards, organisational processes (see suggestions provided by ENISA in "Cyber Security and Resilience of Intelligent Public Transport Systems" in Box 1 and forthcoming publication on securing smart cars).[25]

**Standards**

There are numerous complementary and perhaps overlapping international standards that address car safety, security and connectivity. The proliferation of standards is a sign that industry is aware and working to improve the situation, but some simplification or harmonisation may be needed, especially to address issues of interoperability. Among the ISO working groups and standards that are relevant to cyber security issues:

- ISO TC 22 road vehicles / SC 32 Electronical and electronic components and general systems aspects and ISO 26262 deal with in-vehicle transport information and control systems.

- ISO TC 204 Intelligent Transport Systems is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work programme in this field including the schedule for standards development, taking into account the work of existing international standardisation bodies.
  ISO 15638 "Intelligent transport systems" provides a framework for cooperative telematics applications for regulated vehicles[26], and the basis for future development of cooperative telematics applications for regulated commercial freight vehicles, allowing for a platform for highly cost-effective delivery of a range of telematics applications. It provides a business architecture based on a (multiple) service provider-oriented approaches, and addresses legal and regulatory aspects for the approval and auditing of service providers.
- Other standards may apply, although not specific to the automotive industry. For example, software for mobile phones used to connect a car to the Internet.

**Insurance and liability considerations**

- What is the situation with regards to how the consequences / costs of cyber security risk are covered by insurance?
- In the case of a cyber security breach involving a connected car, what is covered, and by whom or which or whose insurance?
- Are specific insurance products for that already available or being developed? What is different in the US and in Europe?
- What is the insurance situation if an automated braking (or steering) system is manipulated as a result of a cyber security breach, and this causes an accident?
- If the breach lets the hacker have access to data that is protected by law who is responsible?

**Generating trust in connected cars**

Beyond technical security, it is the generation of public confidence that will ultimately determine whether connected vehicles are viewed as secure by their users. People want to trust the secure systems developed for these vehicles, as it is these systems that will ensure that their car is safe and their private data well protected. However, since perfect safety is not achievable, users' decisions (to buy or use an autonomous car, to turn features on or off) will be based on their own perception, appreciation and trade-offs between two relative perceptions of safety or security, balancing convenience, utility, safety and security. The user's configurable interface in itself can cause significant problems with many configuration combinations which adds to the complexity of testing. One issue here is that the software and security measures are likely to be proprietary to the manufacturers and therefore users will be limited to marketing hype when making decisions on safety.

In the context of governance, two initiatives are worth mentioning here:

- The US-based grassroots organisation "I am the Cavalry" urges carmakers to acknowledge that vehicle safety issues can be caused by cyber security issues, and embraces security researchers as willing allies to preserve safety. It proposes five foundational capabilities to improve the visibility of car safety programmes: safety by

design, third party collaboration, evidence capture, security updates, and segmentation and isolation.[c]

- The European Commission DG Move C-ITS platform to promote Intelligent Transport Systems in Europe delivered its final report in January 2016. C-ITS addressed the main technical and legal issues (such as liability, data protection and privacy), and provided policy recommendations and proposals for action.[d]

**Questions for discussion:**

- To what extent are current vehicles at risk of being hacked? Are the existing vulnerabilities being exploited? How much do we know in reality?
- To what extent can the risk impact the safety of car drivers, passengers and other road users?
- What available cyber security solutions exist today?
- Where is short- medium- or long-term research needed?
- In the case of an accident or incident, what is the ability for self-correction or resilience?
- What is the perception of the drivers / users? Is there too much hype? Or not enough attention?
- Where is there a need for more or different standards and regulation?
- How to build and implement a comprehensive cyber security strategy?
- Is there a risk that too much attention on risk hinders innovation?
- What is the role of insurers? What are they concerned about? What solutions do they consider?
- Is there a problem of trust?

[c] https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf

[d] http://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

## 3. Implantable, wearable, networked medical and health devices (NMDs)

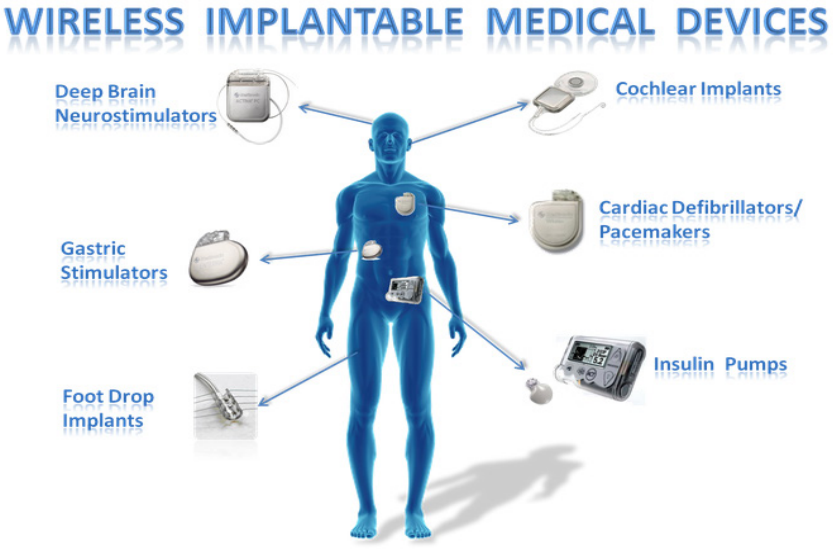


*Figure 4: Wireless implantable medical devices.*
*MIT CSAIL. Courtesy of / available from http://groups.csail.mit.edu/netmit/IMDShield/*


*Figure 3: Wearable health devices.*
*Cisco. Courtesy of / available from http://blogs.cisco.com/digital/the-future-of-mobility-wearables-healthcare*

Wireless interfaces and computer software systems have now become routinely used in modern medical devices. Implantable medical devices (IMDs), including insulin and other drug infusion pumps, neurostimulators, pacemakers or cardiac defibrillators, feature wireless connectivity for the remote control and monitoring of patients' vital signs, to improve the ability of healthcare care providers to deliver timely treatment. Patients lead more normal and healthy lives. Wearable devices for healthy lifestyle monitoring can also be used as vulnerable entry points to healthcare or other critical systems.

**Vulnerabilities of networked medical devices**

Interconnectivity makes medical devices vulnerable to security breaches, in the same way as most networked computing systems are vulnerable. We ought to be concerned that **the connectivity of medical devices has the potential to directly affect clinical care, patient safety, and the protection of patients' private data**. Medical devices are no longer isolated. Their connection to a network raises tensions between safety and security which will require both technical mitigation strategies and a revision of current governance arrangement between stakeholders.[27] Similarly, there is concern regarding the vulnerability that the devices themselves create to a hospital or other medical IT network by their presence on it.

Internet security experts have been warning for years that implantable medical devices such as pacemakers are open to data theft and remote control by a hacker. According to an article published in January 2015 in Science[28] "*Medical devices such as insulin pumps, continuous glucose monitors, and pacemakers or defibrillators have become increasingly small and wearable in recent years. They often connect with a hand-held controller over*

*short distances using Bluetooth. Often, either the controller or the device itself is connected to the Internet by means of Wi-Fi so that data can be sent directly to clinicians. But security experts have demonstrated that with easily available hardware, a user manual, and the device's PIN number, they can take control of a device or monitor the data it sends*."

The Computer Science Department at the University of Massachusetts, the CSAIL group at MIT[29] and others have shown that wireless connectivity can be exploited to compromise the confidentiality of the data transmitted by the device or to send to the device unauthorised commands, some with the potential to be life threatening. Recent hacks or threats continue to raise concerns.[30]

Innovation in the field derives from progress in medicine, computer engineering and science, and other sciences. But medical device software is not always trustworthy, leading to shortfalls in properties such as safety, effectiveness, dependability, reliability, usability, security, and privacy. This is caused by the **increasing complexity and a lack of attention to security aspects in the early development of medical devices**, due to the costs and older architectures, together with the long development processes and approval/certification for medical devices These become vulnerable and can be compromised, their behaviour can become unpredictable or manipulated.[31] Wireless connectivity is thus convenient, but raises the risk of malicious access to an IMD that can potentially infringe patients' privacy and even endanger their life.[32] The secondary impact on patient safety means that we need to consider what we are protecting against in the context of use both inside and outside the network.

Vulnerabilities include possible breaches in:

- Confidentiality, which can be compromised when poor access control measures leads to unauthorised access
- Integrity, which can be affected by data corruption or unauthorised manipulation of data, possibly impacting the patient safety. This can result from either unintentional failure (when incorrect clinical decision is taken based on corrupted data) or intentional attack (when an attacker remotely operates the device)
- Availability, which causes loss of data from or to the device. Disruption in accession important or critical data can affect the functioning of the device and clinical decisions. If alerts are not received, the patient life may be at risk.

These vulnerabilities increase:

- With legacy devices, operating systems and software. In particular, older devices run proprietary operating systems, that are not recognised by standard cyber security vulnerability detection products
- When software is not updated or patched
- When unprotected web services are used to interface with the network
- If compromised medical devices are used to enter in a health care network, where further damage will be caused
- In general, when there is a lack of awareness or a lack of concern (by professionals and the public) and poor security practices.

**Motivations** of attackers include a range of reasons, similar to other IoT applications[33]. Those considered as of utmost concerns are:

- Financial gain (ransomware)
- State-sponsored espionage (primarily to obtain access to confidential information)
- Cyber terrorism or hacktivism (to make a political statement)

Attackers can be individuals both inside and outside the organisation. This includes disaffected insiders with legitimate access.

**Technical aspects: what could be done, specific challenges of securing connectivity of NMDs**

Embedding cyber security solutions is complicated because of:

- Legacy: millions of people already have wireless IMDs in the US, which can last up to 10 years. Replacing an IMD requires surgery. Incorporating cryptographic mechanisms into existing IMDs may be infeasible because of limited device memory and power, and the need to recall hundreds of thousands of insecure devices. Consideration must be given to the risk to an individual patient balanced with the clinical risk on not using a device.
- Accessibility: need to have immediate access in the case of an emergency. Health care professionals must have immediate access to an implanted device. If cryptographic methods are embedded in the IMD itself, the device shall deny unauthorised access. Sharing credentials within a network of hospitals, if the patient is unconscious, or if the cryptographic key storage is damaged or unreachable will result in the weakening of the protection that the cryptographic method provides.
- Maintainability: software failure and bugs are frequent. For medical devices, they may require device recalls, which are costly. In addition, the problem is exacerbated by the logistics of managing software testing and updates in a hospital environment where the number of devices can be in the thousands, of which most will be in use.

How can NMDs be protected?

- Obvious approaches, such as passwords and certificates are not workable at large scale, given the lack of central authority and frequent emergencies. IMDs are constrained in their power consumption and computational capabilities. A trade-off must be made between security and utility.[34]
- Among other research groups, the Archimedes Ann Harbour Research Center for Medical Device Security based at the University of Michigan[35] produces multidisciplinary research focused on improving the cyber security of medical devices. Much of the research pertains to low-power and trustworthy computing for medical devices. Archimedes focuses on a protection of IMDs based on security mechanisms that are entirely on an external device. This approach enhances the security of IMDs for patients who already have them. It also empowers medical personnel to access a protected IMD by removing the external device or powering it off, and does not in itself increase the risk of IMD recalls.

- NMDs cannot be considered in isolation of the networks in which they are deployed. Given the gravity of the impact of adverse events on patient safety, comprehensive, integrated and well maintained organisational network security is essential.

**Standards and certification**

There are numerous international standards, including those of the technical committee (TC) 215 (health informatics): ISO/IEC 62304 (medical device software, ISO/IEC 82304 (health software), and ISO/IEC 80001 (Application of risk management for IT-networks incorporating medical device); and those of TC 210 (quality management for medical devices): **ISO/ANSI/AAMI 14971** (for the application of risk management to medical devices), or ISO 80002 (medical device software). But there seems a lack of focus on the specificity required for cyber security. These standards provide good practice in software development and lifecycle, but do not provide the much-needed guidance for cyber security protection of networked medical devices. Currently, **ISO/ANSI/AAMI/IEC 80001** is under redevelopment and will include consideration of cyber security, in addition to the specific ISO/IEC 80001-2-9 which specifies cyber security controls.

Recognising the lack of guidance for conducting cyber security risk assessment of medical devices, the Association for the Advancement of Medical Instrumentation (AAMI) published in June 2016 its "Principles for medical device security – risk management" that "provides guidance on methods to perform information security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971". The principles incorporate the expanded view of risk management from IEC 80001-1 by incorporating the key properties of safety, effectiveness, data security and systems security. It proposes recommendations to medical device manufacturers for managing "risks from security threats that could impact the confidentiality, integrity, and/or availability of the device or the information processed by the device".[36]

In April 2016, Underwriters Laboratories (UL) launched a Cybersecurity Assurance Program. The new UL 2900 series of standards offers to vendors testable cyber security criteria for network-connectable products and systems, to assess software vulnerabilities and weaknesses, minimise exploitation, address known malware, review security controls and increase security awareness. UK 2900-2 provides particular requirements for networked connectable components of healthcare systems.[37]

Regarding **certification**, the question will be to what extent certification provides necessary confidence in cyber security protection. Security is an emergent property of a system, so the security of a device must be considered in the broad context of the system of which it is a part, that is, its operating environment. No manufacturer will be able to ensure aspects of the operating environment that are outside of its control. Security can only result from a collaboration between manufacturers and health care organisations, taking into consideration technical, organisational and human factor aspects.

**Regulation**

The medical sector is heavily regulated... But this may turn against cyber security. One of the reasons for which medical devices do not get regular security updates, like smartphones and computers, is because changes to their software could require recertification by regulators

like the U.S. Food and Drug Administration (FDA). The FDA focuses on reliability, user safety, and ease of use. Until recently, it was not overly concerned with protection against malicious attacks. However, European regulators seem to be even less concerned than their US counterparts. See Boxes 2 and 3 below.

**US FDA concerns, approach, initiatives and recommendations concerning cyber security matters since 2013**

In a Safety Communication issued in 2013, the agency said that it "[we] *are not aware of any patient injuries or deaths associated with these cyber-related) incidents nor do we have any indication that any specific devices or systems in clinical use have been purposely targeted at this time.*" However, FDA was adding that it "*expects medical device manufacturers to take appropriate steps*" to protect devices. Manufacturers then began to employ security experts to tighten up their systems. But observers noted that unless such steps become compulsory, it would take a fatal attack on a prominent person for the security gap to be closed.[38]

In October 2014, FDA issued its *pre-market* cyber security guidance.[39] Key principles are:
- Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
- Address cyber security during the design and development of the medical device
- Establish design inputs for device related to cyber security, and establish a cyber security vulnerability and management approach as part of the required software validation and risk analysis.

An assessment conducted in October 2015 indicated that, among those submissions that should have included cyber security information, 53% did not provide it.

In July 2015, FDA issued its first safety communication[40] : "*The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that healthcare facilities transition to alternative infusion systems, and discontinue use of these pumps*." FDA experts had assessed that the Symbiq Infusion System could be accessed remotely through a hospital's network, thus allowing an unauthorised user to control the device and change the dosage that the pump delivers, which could lead to over- or under-infusion of critical patient therapies. Recommendation to patients and health care facilities were to disconnect the pump from the network. However, warnings also included that disconnecting the device would require drug libraries to be updated manually, which could be prone to entry error.

On 15 January 2016, as part of the FDA's ongoing efforts to ensure the safety and effectiveness of medical devices, at all stages of their lifecycle in the face of potential cyber threats, FDA strengthened its cyber security recommendations for medical device manufacturers, issuing draft guidance to address *post-market* management of cyber security vulnerabilities. The draft guidance outlines important steps that medical device manufacturers should take to continually address cyber security risks to keep patients safe and better protect the public health. The draft guidance details the agency's recommendations for monitoring, identifying and addressing cyber security vulnerabilities in medical devices once they have entered the market. The draft guidance also addresses the importance of information sharing via participation in an Information Sharing Analysis Organization (ISAO), a collaborative group in which public and private-sector members

share cyber security information. The draft guidance recommends that manufacturers should implement a structured and systematic comprehensive cyber security risk management program and respond in a timely fashion to identified vulnerabilities.[41] The draft post-market guidance was released on 22 January 2016.[42]

On 20-21 January 2016, FDA organised a public workshop in collaboration with the National Health Information Sharing Analysis Center (NH-ISAC), the Department of Health and Human Services and the Department of Homeland Security. The title was "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity." The workshop brought together diverse stakeholders to discuss complex challenges in medical device cyber security that impact the medical device ecosystem. Its purpose was to highlight past collaborative efforts, increase awareness of existing maturity models (i.e. frameworks leveraged for benchmarking an organization's processes) which are used to evaluate cyber security status, standards, and tools in development, and to engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cyber security.[43]

*Box 2: US FDA guidance (medical devices)*

**European initiatives**

The EU regulatory framework for medical devices differs from that used for pharmaceutical drug development.

Under the existing regulation, medical devices are not subject to any pre-market authorisation by a regulatory authority[44] but to a conformity assessment which, for medium- and high-risk devices, involves an independent third party, known as 'notified body'. [45] Notified bodies, of which there are around 80 across Europe, are designated and monitored by the Member States and act under the control of the national authorities. Once certified, devices bear the **CE** marking which allows them to circulate freely in the EU/EFTA countries and Turkey.

European medical device regulations are under revision. The current proposal for a Regulation on medical devices (COM/2012/0542 final - 2012/0266 [46](COD) aims to overcome flaws and gaps in the existing regulation and to strengthen patient safety further. The proposal says that a robust, transparent and sustainable regulatory framework should be put in place that is 'fit for purpose'. This framework should be supportive of innovation and the competitiveness of the medical device industry and should allow rapid and cost-efficient market access for innovative medical devices, to the benefit of patients and healthcare professionals.[47] The proposal does not address specifically issues related to cyber security and the IoT.

However, the regulation of networked medical devices will also be affected by the new Regulation (2016/679) and Directive (2016/680) on Data Protection. [48]

In the course of the revision of the Data Protection Directive, the "Article 29 Data Protection Working party", an independent European advisory body on data protection and privacy, adopted in September 2014 a specific "Opinion" (8/2014) on the "recent developments on the Internet of Things" upon the consideration that IoT poses a number of significant privacy and data protection challenges, some new, some more traditional, but then amplified with regard to the exponential increase of data

processing involved in its evolution. Section 2 of the Opinion mentions in particular concerns about the lack of control and information asymmetry, the quality of the user's consent, inferences derived from data and repurposing of original processing, and security risks: security vs. efficiency (2.6).[49]

The regulation of networked medical devices will also be affected by the new Directive on Information Security (NIS). [50] Among other requirements, NIS establishes an incident reporting scheme that requires from critical infrastructure, including health care providers, the reporting of information security incidents. The scheme is organised by ENISA, which launched in July 2016 a study on cloud and eHealth, targeted at CIOs, CISOs, doctors, patients, healthcare providers and manufacturers, cloud providers, and public authorities that are involved within the healthcare sector.[51]

**ENISA**

The European Union Agency for Network and Information Security (ENISA) is an EU agency that works with EU member states, as the centre of expertise for cyber security in Europe.

Considering mobile health (mHealth), ENISA recognises[52] that it *"is a rapidly developing sub-segment of eHealth that covers medical and public health practice supported by mobile devices. [...]. It comprises a set of technologies which will bring a more innovative care access reducing healthcare costs at the same time. More specifically, mHealth includes the use of mobile communication devices for health and well-being services and information purposes as well as mobile health applications. The European Commission, having recognised the emergent role of mHealth in the transformation of healthcare, published in April 2014 a Green Paper on mHealth that considers existing barriers and issues related to mHealth deployment and analyses mHealth potential to maintain and improve patients' health and well-being and encourage their empowerment. (...)*

*At the same time, according to the EC Directive on Critical Infrastructures, healthcare services have been recognised as a critical societal sector and therefore, healthcare systems are considered as critical infrastructures that should be protected by all types of threats, including cyber security attacks. Moreover, in the proposed NIS Directive, healthcare is considered as one of the critical sectors vital for the society" (...)*

*"Healthcare systems are becoming vulnerable to cyber security incidents due to various reasons; the volume of information and the connection with patients dictates the use of automation and IT; the diverse nature of healthcare information systems enables different devices to access the Internet (even though not designed for this) thus making them easy targets; many outdated applications and systems didn't include security as a priority requiring close attention of the information security officers and finally the exponentially increasing attack surface is making systems compromise an easier task. Combining these reasons with the fact that a breach of security can impact large parts of the population16 makes eHealth a critical sector."*

*Box 3: European regulation and initiatives (medical devices)*

It should be noted that while the FDA (Box 2) cites a lack of attack evidence, this may reflect a lack of recognition or reporting of cyber security breaches by affected organisations. Further, one aspect of concern is that the pre-market submissions are based on self-assessment and do not (and potentially cannot) include a comprehensive assessment of

potential issues once connected to a network of deployment. The reality is that an insecure device may be more clinically useful than no device at all.

**Insurance and liability issues**

- What is the situation with regards to how the consequences / costs of cyber security risk are covered by insurance?
- In the case of a cyber security breach involving a connected wearable/implanted medical device, what is covered, and by whom or which or whose insurance?
- Are there already or in development specific insurance products for that?
- If a connected pacemaker is hacked, and this causes an adverse health outcome to a patient, who is responsible and what kind of insurance coverage is available?
- It a connected pacemaker is hacked and is used to enter into a health care provider systems whose data is compromised, what is the insurance situation? Who is responsible?

**At the governance level, potential solutions include:**

- Incident reporting and feedback between health care providers and MD manufacturers, to improve risk mitigation
- Developing a risk-based approach to safety and security: risk identification, risk management, incident response[53]
- Regulation from licensing authorities (regulatory compliance for patient safety) and payer agencies (rules for reimbursement of medical therapies that involved NMD), to determine basic safety and security requirements
- New, revised or harmonised standards for NMDs
- Review by insurance companies of what they insure and how, in the case of an incident.

**A complex issue: multidisciplinary and collaborative approaches are needed**

Cyber security vulnerabilities in medical devices develop in a complex environment. It is a multifaceted problem that requires a multidisciplinary perspective with the involvement of various stakeholders representing the public sectors (regulators, health agencies, public health care operators and public payers), the private sector (manufacturers of MD, private health care providers and insurance companies) and patients.[54]

The cyber security of NMDs requires the consideration of privacy and security goals on the one hand, and health care utility and safety on the other hand. Existing NMDs do not have strong encryption and strict access control. Encryption requires a capacity for data processing and power, which are generally not available for existing NMDs. Applying solutions developed in other sectors may slow down the functioning of the devices and create new risk to patient safety, especially in the case of an emergency. In the field of health, it is safety that matters most, before cyber security requirements. Governance arrangements that could be developed should work **to close the gap between safety and security.**

The US-based grassroots organisation "I am the Cavalry" proposes a new Hippocratic Oath for Connected Medical Devices, as a symbolic attestation by physicians to the health care stakeholder communities, to provide care in the best interest of patients. The oath addresses cyber safety issues, software flaws and other negative side effects of advances in medical technology, delivered by connected medical devices. It recommends five principles: cyber safety by design, third-party collaboration, evidence capture, resilience and containment, and cyber safety updates.[e]

**Questions for discussion:**

- What is the definition of a "networked medical and health device"? Is it just the device itself? Upstream and downstream devices? Manufacturer's supporting infrastructure? Ecosystem?
- To what extent are current networked medical devices at risk? Are the existing vulnerabilities being exploited? How much do we know in reality?
- Is there a risk that too much attention on risk hinders innovation?
- What are the motivations for hacking NMDs?
- What is the perception of the patients? Is there too much hype? Or not enough attention?
- How to build and implement a comprehensive cyber security strategy?
- What are the available technologies? Are there available market solutions that are affordable in current business models?
- Where is short- medium- or long-term research needed?
- Where is there a need for more or different standards and regulation?
- What is the role of insurers? What are they concerned about? What solutions do insurers consider?
- Is there a problem of trust?
- Is there any ability for resilience and self-correction?

[e] https://www.iamthecavalry.org/domains/medical/oath/

# 4. Collaboration among actors for cyber security risk governance: regulation, standards, interoperability, liability and insurance

Moving on, from identifying vulnerabilities and reviewing current research to developing solutions for cyber risk: What are the main principles that legislation, standards and insurance apply or are advised to apply when they regulate, certify or insure products and services that rely on the connectivity between devices and between devices and infrastructure? What are the roles of various organisations to guarantee secure connections for a safe IoT? How can collaboration among actors be organised?

- Role of policy makers, public regulators
- Role of standard setting organisations, certification.
- Role and responsibility (including liability) of various industry actors
- Role of judicial systems and litigation
- Role of affected stakeholders (e.g. road users and patients)
- Role of the insurance industry

**Regulation**

Will institutions such as the European Medicine Agency (EMA) or US-FDA for medical devices, and UNECE or NHTSA for autonomous vehicles consider specific regulation to deal with cyber security risk?

**Standards, certification and interoperability**

The IoT utilises hardware and software from many different vendors. The ability of these devices and systems to work together is critical to realise the full value of IoT applications and avoid or reduce cyber security risks. Without interoperability, many of the potential benefits of the Internet of Things will not be realised. Good collaboration between stakeholders for the development of standards is needed and will enable technological innovation. It will define and establish common foundations upon which product differentiation, innovative technology development, and performance can be developed. International standards are probably needed, so that manufacturers do not incur the additional costs associated with creating different versions of the same product for different markets.

Standards such as ISO standards in this field aim to support the commercial world with using modern and existing wireless communication technologies to enable more efficient use of commercial vehicles, medical devices and other IoT devices, safely and in controlled ways.

An indication of the immaturity of the IoT might be the proliferation of standards and protocols related to the field. At the same time, it is often the case that different devices from different manufacturers that aspire to do the same things have radically different data formats and potentially different touch-points, thus making interoperability and connection between them difficult, if not impossible.[55]

**Liability issues**

In the case of an accident resulting from negligence or breach in an IoT system, who is responsible and liable? The wide-spread adoption of technologies incurs changes in attribution of responsibility. This issue is already the topic of much discussion for autonomous cars, partly because the insurance system is concerned. In the case of an incident or accident due to a medical device being hacked, who is responsible? Are insurers concerned with this question?

In the US in particular, liability regimes and courts have an important role in structuring legal issues and responsibilities of various stakeholders. The risk of potential litigation can create powerful incentives in favour of “self-regulation". Tort liability and the potential for lost business provide a very strong incentive for US companies to design safer products.

**Insurance considerations**

Insurance can play a key role in structuring a risk market and overall improving the safety and security of insured products. It acts on two levels:

- Compensating losses in case of an accident
- Risk evaluation: the insurance industry expertise to assess risk and put on a price tag can help manufacturers improve the security of their products

Regarding cyber security risk, the question of its insurability is still uncertain, although a recent report indicates that risks "of daily life" could be insured with standard practices, whereas risks "from extreme scenarios" might require specific approaches, such as those for large natural disasters.[56]

**Conclusion: multi-stakeholder governance**

The negotiation of governance arrangements between stakeholders includes various components:

- Clear public policies about anticipated benefits of the IoT, including in the transportation and medical sectors, and appropriate strategies
- Technique: cyber security protection must be embedded in the early design and development of a product
- Awareness and perception: it is important to understand that addressing cyber security issues is not meant to hinder innovation. Industry and regulators ought to be concerned by the risk, become familiar with it, and address it seriously. It is only by understanding the key vulnerabilities that they will support dedicated research and solution development.
- Regulation and standards: much guidance is needed in this evolving, challenging and fundamental shift that is taking place in both the automotive and medical industries.
- Responsibility and liability: as new cyber security risks are impacting the business, the legal system has to determine how litigation would affect the attribution of responsibility and liability

## 5. The IoT and the digital world, resilience strategies

Creating trust in connectivity including confidentiality, integrity and availability will be key to achieving the promises of the IoT, at least in the automotive and medical sector. Assessing vulnerability, implementing and assessing security controls, designing appropriate standards and regulation as well as insurance and other governance arrangements will be critical elements. But the creation of trust may require that broader societal questions need to be addressed, including the following elements:

- **The IoT will blur the concept of privacy**
  That may be acceptable for young people who voluntarily give access to their data, but is it also acceptable that the right to privacy is ignored when cyber security risk are evaluated as being more important?[57]

- **Systemic cyber risk**
  Cyber security risks are systemic risks, with potential for cascading consequences in other systems. As illustrated by the World Economic Council in its recent report about Understanding Systemic Cyber Risk[58], there are significant gaps in cyber security resiliency related to critical healthcare information and systems. Governments and industry struggle to deal with cyber risk, although they create the risk to a certain degree by being increasingly dependent on the technology and routinely behind attackers. Managing the systemic nature of cyber risk will be necessary to create trust in the IoT.

- **Accidents will happen. We need to develop resilience**
  For complex systems that are potentially subject to unexpected failures (unexpected in the sense that prevention is not sufficient), it is commonly understood that resilience strategies must be developed. Resilience is defined by the US National Academy of Sciences (2012) as *"(t)he ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events*". Whereas risk management selects and prioritises potential protective measures to prevent or mitigate impacts to the status quo at a point in time, resilience seeks to enhance the system's inherent capacity to respond throughout the process of inevitable change - both long and short duration, thus invoking a fundamentally temporal perspective. Changes in the IoT include that software will be updated and that new versions must be installed, either over the air or during physical maintenance operations, both of which may or may not be easily feasible or recommended for medical wearable devices and connected cars. This emphasises a shift from event orientation and specific protective measures toward a capacity-centric view, stipulating four key attributes of resilient systems: robustness (withstand disruptive forces), redundancy (satisfy functional requirements with substitutable system elements), resourcefulness (effectively leverage resources to diagnose and solve problems), and rapidity (recover quickly from a disruption). In contrast with a risk-based view, which is focused on preventing intrusions (avoiding the risk) or anticipating its negative consequences, a resilience-based approach is concerned with ensuring continuity in critical functions and services with minimal disruption in the case of unexpected failure[59]. Resilience in the context of the cyber domain can be described as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources".[60]

- **Capability for graceful failures**
  Some learning could be gained from the capability for 'graceful failure' that has been implemented in industrial systems[61]. 'Graceful failure' allows the system to slow down and adapt, so that the failing system is still able to deliver the minimum services it needs to provide, and the critical functions are not affected, especially when risks are life-threatening.[62]

- **How much decision-making should we leave to machines?**
  To what extent does society want to rely on systems that are largely autonomous, for applications that can be life-critical or -threatening?
  While machines have the ability to question and use data until they have uncovered all the unexpected correlations, they still lack the personal experience or emotional intelligence to understand these relationships or act on them.

- **Autonomy of the digital world**
  Next to the natural and physical world and the human world (social system), the digital world has its own existence: its own life, rules and autonomy.[63] It is becoming autonomous, with progress in the IoT occurring in parallel to progress in robotics, smart interactive networks, machine learning, artificial intelligence[64], data sciences, deep learning or self-healing systems that are trained to learn to remedy their deficiencies. If the digital world acquires its autonomy, increasingly independent from the capacity of humans to control it, then the rules of behaviours in this world must be understood (as far as they result from emergent properties) or created (as far as organisations and individuals interact with it). Rules are needed to deal with governance issues, such as what can be done and what must not be done in this world. There is already ongoing debates about ethical issues, rights of robots, how machines such as autonomous and connected cars would decide if they are faced with a question of values or ethics.

## Acknowledgements

This paper was written by Marie-Valentine Florin (IRGC) for the purpose of informing discussion at an expert workshop to be held on 15-16 November 2016, at the Swiss Re Centre for Global Dialogue. The paper was reviewed and improved thanks to comments received from Maya Bundt, Linus Gasser, Sarbari Gupta, Russel Jones, Philipp Jovanovic and Trish Williams.

## Notes

In order to reflect the general public opinion and experts' personal opinions about the fast-moving changing field of the IoT, we cite many references to general media or websites, which are not reviewed. These should thus be viewed with caution. This may also serve as a reminder that many policy and business decisions are taken on the basis of opinions, fears or other types of non-evidence-based information.

---

[1] The term mHealth refers to the "medical and public health practice supported by *mobile* devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices" (WHO). The term eHealth is also used to emphasise the *electronic* component.

[2] https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

[3] https://www.us-cert.gov/ncas/current-activity/2016/03/17/IC3-Warns-Vehicles-Are-Increasingly-Vulnerable-Remote-Exploits / https://www.ic3.gov/media/2016/160317.aspx

[4] http://abcnews.go.com/GMA/video/dick-cheney-60-minutes-interview-reveals-fear-pacemaker-20632056

[5] Suzanne Schwartz, M.D., M.B.A., associate director for science and strategic partnerships and acting director of emergency preparedness/operations and medical countermeasures in the FDA's Center for Devices and Radiological Health.
*http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm*

[6] Computing - http://www.computing.co.uk/, from http://www.scmagazineuk.com/cyber-security-of-the-fridge-assessing-the-internet-of-things-threat/article/495675/

[7] http://www.information-age.com/technology/security/123459983/how-prevent-iot-becoming-internet-thieves

[8] http://www.information-age.com/technology/mobile-and-networking/123460168/just-paranoid-we-break-down-top-three-internet-things-conspiracy-theories

[9] http://www.information-age.com/technology/security/123459490/securing-iot-device-landscape-complete-guide-making-life-difficult-hardware-hackers

[10] Work of Prof. Bryan Ford, EPFL on decentralized systems, internet security and anonymity - AXA research programme in Information Security and Privacy Agefi 18 May 2016 -
- Decentralized witness co-signing for data protection: http://actu.epfl.ch/news/bryan-ford-the-cothority-project/

[11] Example on ongoing work: Swiss Cyber Research Initiative https://actu.epfl.ch/news/switzerland-can-and-should-develop-a-neutral-virtu/

[12] See Bryan Ford: Apple, FBI, and Software Transparency, 10 March 2016 https://freedom-to-tinker.com/2016/03/10/apple-fbi-and-software-transparency/

[13] See Prof. Jean-Pierre Hubaux, EPFL on network privacy and security, http://lca.epfl.ch/projects/privacy-mobile-pervasive/

[14] See for example Dissent project: Security Analysis of Accountable Anonymity in Dissent, Ewa Syta, Aaron Johnson, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, and Bryan Ford. ACM Transactions on Information and System Security (TISSEC), Volume 17 Issue 1, August 2014.

[15] See Prof. Ari Juels, Cornell University http://www.initc3.org/ - See: Exploring the future of smart contracts
[16] http://www.information-age.com/technology/security/123460713/how-blockchains-are-redefining-cyber-security
http://www.information-age.com/technology/security/123461443/how-blockchain-will-defend-internet-things
[17] IBM Zurich https://www.zurich.ibm.com/~cca/
[18] This includes the L4 operation systems in Australia (which is likely to play an important role in IoT systems http://ts.data61.csiro.au/, and the Certified Compiler project at INRIA http://compcert.inria.fr/
[19] http://fortune.com/2016/01/26/security-experts-hack-cars/
[20] See work and publications from the Center for Automotive Embedded Systems Security (CAESS) a collaboration between the University of California San Diego and University of Washington http://www.autosec.org/publications.html
See also the Miller & Valasek survey of remote automotive attack surfaces, available at http://illmatics.com/remote%20attack%20surfaces.pdf
[21] See for example TU-Automotive Hacks and Threats Report 2016. http://www.tu-auto.com/cybersecurity-report/ from the Cyber Security Group at the Centre for Mobility and Transport (CMT) at Coventry University http://www.coventry.ac.uk/research/areas-of-research/mobility-transport/cyber-security/
[22] See full review of the five risk scenarios by FireEye:
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf
[23] ENISA (2015). Cyber Security and Resilience of Intelligent Public Transport Systems, https://www.enisa.europa.eu/publications/good-practices-recommendations
[24] http://www.nxp.com/about/about-nxp:COMPANY_INFO_HOME
[25] See ENISA (2015) above
[26] See https://www.iso.org/obp/ui/#iso:std:iso:15638:-15:ed-1:v1:en
[27] Williams, P.A.H. & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices. *Medical Devices: Evidence and Research, 8*:305-316.
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/pdf/mder-8-305.pdf
[28] Daniel Cléry (2015). Could your pacemaker be hackable? Science 30 Jan 2015:Vol. 347, Issue 6221, pp. 499
DOI: 10.1126/science.347.6221.499 http://science.sciencemag.org/content/347/6221/499
[29] http://groups.csail.mit.edu/netmit/IMDShield/
[30] Threats on insulin pumps: http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L, http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/
[31] Kevin Fu. On the technical debt of medical device security, September 13, 2015. Available on http://cra.org/ccc/wp-content/uploads/sites/2/2015/11/Kevin-Fu-Medical-Device-Security.pdf
[32] http://sharps.org/wp-content/uploads/ROSTAMI-DAC.pdf
[33] SANS Institute report (2014). Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon, http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735
[34] Masoud Rostami, Wayne Burleson, Ari Juel and Farinaz Koushanfar (2013) Balancing security and utility in medical devices http://www.arijuels.com/wp-content/uploads/2013/09/RBJK13.pdf
[35] https://www.secure-medicine.org/
see also: The Security and Privacy Research Group at the University of Michigan, works broadly on research problems pertaining to trustworthy computing, exploring the research frontiers of computer science, electrical and computer engineering, and healthcare.
https://spqr.eecs.umich.edu/

[36] AAMI Medical Device Security Working Group (2016). Principles for medical device security—Risk management. These principles are part of a technical information report (TIR). A TIR is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board. This document is neither a standard nor a recommended practice, but it reflects a recommendation from industry for addressing a particular aspect of medical technology, in particular those where there is an underlying safety or performance issue.
[37] UL cybersecurity Assurance Program: http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/. UK 2900-2: https://standardscatalog.ul.com/standards/en/outline_2900-2-1_2
[38] Could a wireless pacemaker let hackers take control of your heart?", Science Mag, Feb 9, 2015 http://www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart
[39] http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf
[40] See: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm Coincidently, this alert was made a few days after the first alert by the National Highway Traffic Safety Administration, to recall 1.4 million Fiat Chrysler Jeep Cherokee cars to fix a hacking issue. See http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html?_r=0
[41] http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm
[42]http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf
[43] http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm474752.htm
[44] See current regulatory and procedural guidance explained by EMA: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/general/general_content_000523.jsp&mid=WC0b01ac05800267b9
[45] Such as: http://www.emergogroup.com/services/europe/ce-certification
[46]http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0542_/com_com(2012)0542_en.pdf
[47] http://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/revision_en
[48] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[49] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[50] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[51] https://www.enisa.europa.eu/news/enisa-news/join-enisa-study-on-cloud-security-and-ehealth
[52] ENISA Security and Resilience in eHealth Infrastructure and Services: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services
[53] Such as the one recommended by Deloitte Center for Health Solutions: Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives. Issue Brief (2013). http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf
[54] Williams, P.A.H. & Woodward, A. (2015). See above
[55] Read an opinion here "Internet of Things undermined by a lack of standards": http://www.computing.co.uk/ctg/news/2413874/internet-of-things-undermined-by-a-lack-of-standards-warns-pentaho-md-paul-scholey
[56] See "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class, a report from the University of St Gallen in collaboration with Swiss Re, 2016, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

[57] Read an opinion here "Get ready: the Internet of Things is the final nail in privacy's coffin" http://www.information-age.com/industry/services/123459271/get-ready-internet-things-final-nail-privacys-coffin

[58] World Economic Council (2016) Understanding Systemic Cyber Risk. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

[59] Bodeau D, Graubart R (2016). Cyber Resilience Metrics: Key Observations. Case No. 16-0779. The MITRE Corporation

[60] Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, *57*(2), 31-35.
See also: Zacharie Collier and Igor Linkov. Cyber security standards: managing risk and creating resilience, Computer ( Volume: 47, Issue: 9, Sept. 2014 )

[61] Woods DD (2012) Chapter 9: Resilience and the Ability to Anticipate. In: Pariès, M. J., Wreathall, M. J., Woods, D. D., & Hollnagel, E. (Eds.). Resilience engineering in practice: a guidebook. Ashgate Publishing, Ltd.

[62] Read an opinion here: " Does Your User Experience Deal with Connectivity Failures Gracefully?" http://www.ics.com/blog/does-your-user-experience-deal-connectivity-failures-gracefully

[63] Smirnov, A., Kashevnik, A., Shilov, N., Makklya, A., & Gusikhin, O. (2013, November). Context-aware service composition in cyber physical human system for transportation safety. In ITS Telecommunications (ITST), 2013 13th International Conference on (pp. 139-144). IEEE.
Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., & Zhao, K. (2015). Cyber-physical-social system in intelligent transportation. IEEE/CAA Journal of Automatica Sinica, 2(3), 320-333

[64] The Economist, 25 June 2016, "March of the Machine" http://www.economist.com/printedition/2016-06-25


International Risk Governance Center

École Polytechnique Fédérale de Lausanne
CM 1 517
Station 10
1015 Lausanne
Switzerland

Tel +41 21 693 82 90
Fax +41 21 693 82 95

irgc@epfl.ch
irgc.epfl.ch
irgc.org



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

international risk
governance center