Workshop Highlights

As part of an on-going workshop series and project work on cybersecurity and in line with its mission to bridge the gap between science and policy, IRGC organised a one-day expert workshop on Governing Cybersecurity Risks and Benefits in the Internet of Things (IoT), applied to connected vehicles and medical devices - **Creating trust in connectivity: confidentiality, integrity and availability**.

With the support of Swiss Re and AXA Technology Services, the invitation-only multidisciplinary workshop, held on 15 – 16 November 2016 at the Swiss Re Centre for Global Dialogue in Rüschlikon, Switzerland, brought together 30 experts from research, technology, industry, regulation, insurance and other stakeholder groups in an open, facilitated roundtable discussion under Chatham House Rule.

The workshop discussed **cyber security challenges in the IoT**, with focus on two different sectors:

- **Connected cars** (connectivity between vehicles and between vehicles and infrastructure is necessary for automation and autonomy)
- **Implantable and wearable medical devices** (many of them are connected via unsecured communication).

In those sectors, connectivity improves both safety and vulnerability, and cyber security failures can be life-critical or -threatening. The cyber vulnerability of connected cars and medical devices has drawn much media attention in the past few months, emphasising both the potential for severe accident, and that there is little information about the probability of harm due to cyber risk. It is thus important to not distract attention from the true benefits, in particular to safety and efficiency.

Workshop participants discussed technical security solutions (very different in both sectors, but similar principles), risk management options (trade-offs between patients' or drivers' physical *safety*, *privacy* and data protection, other cyber *security* concerns, and *cost*), standards and certification, regulation, liability and insurability issues (insurance may be the final enabler in a regulated environment).

Key points from the workshop discussions included:

1. **Cybersecurity risk poses a considerable challenge in both the automotive and the medical device sectors**. Failures ('risk of a really bad scenario') could certainly hinder innovation and development, especially as some companies may try to ignore the risk or fail to communicate about known risks. Technology is moving fast to keep up, yet it is not clear whether the industry applies the best techniques available (security by design and by default, encryption, integration of secure elements, software update, etc.). This is because of potential technical

difficulties, the costs involved and the lack of incentives and requirements by standard setting organisations, regulators and insurers.

2. **The traditional way of increasing security by isolating systems is outdated**. Attempting to isolate a critical system, which must be protected from a potentially insecure external system, is probably no longer the most effective method of protection. Moreover, cybersecurity cannot be fixed just with a technical solution certified by an authority. Technical solutions are important, but cybersecurity must be dynamic and holistic; it is the outcome of continuous improvement within an ecosystem of collaborating actors.

3. **The benefit-risk balance is changing because the innovators are not those who take the risk**. The asymmetry of information is obvious and there is little transparency about this issue. Much of the attention is focused on comfort, convenience and performance. In the event of a failure, it is very difficult to identify who is responsible and therefore liable. Clear attribution of legal liability is absent and would be needed, notably in the case of software defects.

4. **In both sectors, if consumers (patients, drivers) have to choose, they choose physical safety (to avoid the risk of a health or car accident) over cybersecurity and privacy.** When prompted, or in an emergency situation, people are inclined to give up on privacy (they give access to their private data) in exchange for increased safety, comfort and convenience. When one looks at how people behave in reality, it is clear that the notion of privacy is changing. Prioritising physical safety over cybersecurity also implies that IoT connected devices may remain vulnerable entry points into interconnected networks (e.g. medical records in health care systems, location tracking in cars). Regulators are advised to consider customer behaviour when they regulate about cybersecurity and privacy. Moreover, trade-offs between privacy and security often have to be made at the individual level; but the choice that an individual makes at any given moment may not be the best choice for society or for that individual later in life. Therefore, the development and use of methods that would enhance both privacy *and* security (such as with 'usable security' where the default option is both privacy and security and the consumer does not have to make a choice) should be encouraged.

5. **Collaboration between actors is still ill-developed.** Important actors in the dialogue to develop a common understanding of the cybersecurity challenge include governments and regulators, certification agencies, data protection agencies, industry (manufacturers), technology and security companies, service providers, telecom operators, insurance and user associations. Although compulsory incident reporting schemes in other sectors have demonstrated their effectiveness in contributing to raising awareness, thus encouraging the development of both technical and governance solutions, the medical and automotive industries are not keen on sharing information on cybersecurity incidents with others (whether regulators, insurers, the public, or even with those in the same industry). From 2018 data privacy breach reporting will become mandatory under the 2016 EU Global Data Protection Regulation (GDPR) and, for some sectors, the 2016 Network Information Security Directive. This reporting is primarily to regulators, but the GDPR also includes an obligation to notify affected individuals in certain cases. Cybersecurity may hence become a question of trust between manufacturers and their customer. Reputation matters.

6. **Cybersecurity is a challenge for standard-setting and certifying organisations, as well as public regulation**. Regulation has to adapt to a fast evolving field. If it is too strict it will hinder

innovation and incentivise free riders. It may be that it is not possible to certify the cybersecurity of connected devices. Both standardisation and regulation may have to move towards recommending or requiring the adoption of certain principles and processes towards improvement, rather than a certain 'level' which manufacturers will aim to hit, but not exceed.

7. **The insurance of cybersecurity risk is a challenge**. Through interconnected supply chains and contracts, the risk of accumulation is considerable to insurers. However, if insurers cannot provide the necessary cover for cybersecurity risk, this will create gaps in the risk transfer chain, with threats to business and consumers. As insurance is a key actor to enable or constrain an innovation in coming to market in a regulated sector, their role in the IoT is critical. Cyber insurance for extraordinary events may eventually look like terrorism or natural catastrophe insurance, with governments providing coverage above a certain limit.
8. **Self-regulation by industry should not be neglected.** Public regulators are advised to create incentives for codes of conducts among manufacturers, thus fostering self-regulation and perhaps self-certification. Prior-approval types of regulation are not dynamic by default and do not allow the type of maintenance and updates that cybersecurity challenges require. Voluntary industry-level initiatives may provide a positive way forward if the industry can create and maintain trust with consumers and regulators. In this respect, it is up to industry to act. Self-regulation is accompanied by **liability regimes,** which are yet to be refined to address specific cybersecurity risks.

The IoT will continue to develop because many consumers, the industry and public institutions (e.g. in the health care sector or in public transport) are convinced that its benefits will exceed the cybersecurity risks. However, the possible occurrence of serious cybersecurity incidents may lead regulators to tighten product authorisation.