Cybersecurity and the auto industry: The growing challenges presented by connected cars

Morris, D., Madzudzo, G. & Garcia-Perez, A.

Original citation & hyperlink:
Morris, D, Madzudzo, G & Garcia-Perez, A 2018, 'Cybersecurity and the auto industry: The growing challenges presented by connected cars' International Journal of Automotive Technology and Management, vol. 18, no. 2, pp. 105-118. https://dx.doi.org/10.1504/IJATM.2018.092187

DOI 10.1504/IJATM.2018.092187
ISSN 1470-9511
ESSN 1741-5012

Publisher: Inderscience

Cybersecurity and the auto industry: the growing challenges presented by connected cars.

September 2017

Abstract

The term "connected cars" embraces all private passenger vehicles which are connected to the internet in some way. Whilst most modern road vehicles, including buses and trucks, are now complex computer-laden devices attached to the "internet of things" (IoT), this article concentrates on cars where, arguably, the greatest cyber security challenges occur as a consequence of the number of vehicles involved, the potential disincentives to invest in cybersecurity, the range of user threats greater and overall risks the highest. Despite the magnitude and potential impacts of cybersecurity issues, there are very few academic contributions to the debate which focus on the wider social, economic and behavioural aspects rather than the technological. This article discusses cybersecurity issues with the objective informing the agenda for the developing debate and identifying areas for potential action.

Key words:

Cybersecurity; connected cars; automotive electronics; ICT; vehicle software; technical complexity; supply networks; knowledge sharing.

Introduction

The automotive industry is built on a foundation of engineering and process rigour. However, this professional legacy has established an overriding culture of conservatism which is only now beginning to break down as vehicles enter the realm of connectivity and cybersecurity. Clark et al. (2014) define cybersecurity as

a globally-interconnected digital information and communications infrastructure that supports the functionality of almost every system in the modern world.

Cybersecurity measures are associated with managing risks, patching vulnerabilities and improving system resilience. In the context of road vehicles, the (US) National Highway Traffic Safety Administration (NHTSA), defines automotive cybersecurity as

the protection of automotive electronic systems, communication networks, control algorithms, software, users and underlying data from malicious attacks, damage, unauthorised access, or manipulation.

Vehicle development is continually evolving from familiar mechanical systems to electromechanical constructs with highly integrated hardware and software subsystems forming in-vehicle computer networks (Checkoway et al., 2011), which are, in turn, connected to an expanding array of other networks. OEMs are beginning to contemplate the strategic shift from being carmakers to becoming mobility service providers; modern cars now embody a bundle of services which go beyond transportation per se. However, the major auto manufacturers will not be able to deal with these shifts by themselves or in their traditional way. Long development cycles, incremental change and arms' length supplier relationships will no longer work. The constant addition of new connected services and features embodying unfamiliar technologies will require OEMs to become part of a complex ecosystem of traditional suppliers, ICT giants such as Apple and Google, telecoms providers, technology start-ups, aftermarket service providers and infrastructure designers.

As cars increasingly incorporate in-vehicle computer systems to improve vehicle safety, security, comfort and performance, the threat of cybersecurity vulnerabilities increases. The creation of a new product in the automobile industry is a complex task,

characterised by uncertainty and variability. The rapid development of connected cars further emphasises these challenges. Cooperation of OEMs and their suppliers in the form of knowledge sharing is an important aspect in developing cybersecurity vulnerability solutions. A compelling reason for focusing on connected cars as a category is that cybersecurity issues form a major and increasingly exposed part of the current automotive industry agenda and, arguably, present in an extreme form in connected cars. "Extreme" embraces the complexity of the issues, the range of levels (individual to global) impacted by cybersecurity failures, the very high costs (social, reputational, policing as well as financial) of cybercrime in the sector, the level of investment being made by auto manufacturers in smart technology innovations to their products, the global structure of the industry, and the highly pervasive and mobile nature of the product.

The wider context is set out in the policy document *"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"* (EC, 2013). This firmly locates cybersecurity strategy within the EU's core values. Parallel policy imperatives are set out by the US and UK among other countries. Whilst there are no specific references to connected cars per se, the overarching principles of ensuring that digital interactions are open to all, democratically governed and provided and conducted safely in a positive environment of shared responsibility are the guiding principles for future action.

The auto industry, in common with many others, for example financial services and ICT, is ill-prepared to meet the new challenges. Among the many concerns are weak integration of component supply chains in critical electronics areas, poor component integration strategies, inadequate understandings of vulnerabilities at component interfaces, the secondary attention paid to cybersecurity issues, the lack of incentives and mechanisms to share intelligence on cybersecurity breaches and the asymmetric advantages enjoyed by cybersecurity attackers over defenders. The business models of automotive OEMs will need to evolve and adapt to meet these challenges. In the meantime, connected cars might be the site of the perfect cybersecurity storm.

A new landscape for the auto industry

There are three major areas of development in the auto industry which will result in a fundamental reconfiguration of its technological, competitive, regulatory and cooperative existence. In broad terms these are the introduction and take-up of new engine systems to provide energy to vehicles, notably the spread of EVs, the development of autonomous vehicles (AVs) and the enhancement of services available to increasingly connected cars. Whilst these avenues of development could exist without each other, they have a synergy and interdependency which cannot be ignored. The important feature is connectedness. “Connected cars” include autonomous (“driverless”) cars and ones employing ADAS, Advanced Driver Assistance Systems. Connectedness enables and promotes different degrees and dimensions of driving autonomy, rather than the opposite, that is the desire for autonomy in vehicles being the stimulus to develop connected cars. The move towards connected cars is promoting major realignment within the automotive industry (Beiker et al., 2016). Perhaps, for the first time, the key technological developments which will drive industry innovation, individual firm competitiveness and consumer choice lie outside the ambit of automotive manufacturers’ core historical competencies.

The potential costs of vehicle cybersecurity attacks and their prevention measures need to be weighed up against the undoubted benefits which technological benefits in connected cars may bring. A useful way of viewing connected cars is to see them as a collection of functionality bundles. These build on the familiar bundle of transport services to add driver assistance, passenger safety, vehicle security, improved mobility, entertainment, office and communication services, navigation and so on. The inclusion of software in automotive design architectures has paved the way for improving the driving experience and everyday life (Charette, 2009; Onishi, 2012). In very brief terms connected car positives include

- Improved safety through better road infrastructure, on-board safety systems, automatic “Smart SOS” emergency services’ calling (for example, eCall)
- Improved vehicle security through more sophisticated access systems
- Better use of road infrastructure to reduce congestion, enable smart parking, and spread journeys through time

- Safer and more accessible driving for those whose driving abilities are physically compromised enhancing employment and leisure opportunities
- Greener driving through reduced emissions
- User and usage based, including driving style and habits, insurance premiums providing an incentive for safer driving
- Improved vehicle maintenance and reliability
- The improvement of air quality
- Opportunities for passengers to use the time spent on car journeys in more interesting and/or productive ways
- More enjoyable car travel
- Greater competition in the vehicle servicing, updating and repair industry resulting in greater consumer choice and potentially lower costs (the "right to repair")
- Improved payment services for fuel (including e-car battery charging), pay-as-you-drive insurance, parking charges and other car-related mobility services

Estimates of the likely number of connected cars abound; about one in five cars on the road will have some sort of wireless connection by 2020, that is a quarter of a billion vehicles. The value of the 2020 connected car market is estimated at €42bn. The (UK) Society of Motor Manufacturers and Traders, SMMT (2016) estimates that the annual economic benefit of connected vehicles to the UK will grow to €65bn by 2030. A study by Telefonica of more than 5,000 people found that 70% were already using or would, in the future, use connected car services. The World Economic Forum estimates that the digital transformation of the automotive industry will generate $67 billion in value for that sector and $3.1 trillion in societal benefits (West, 2016).

The growing cybersecurity threat

The automotive industry is facing an increase in the number of cybersecurity incidents. In March 2012, over 300,00 touch screens fitted to the Edge, Focus, Explorer and Lincoln MKX models malfunctioned, prompting Ford to send out software updates installed on flash drives. In July 2015, Fiat Chrysler recalled 1.4 million vehicles due to concerns about the cars' software and possible remote manipulation. Software coding errors enabled the Nissan Leaf to be hacked via the

NissanConnect EV application. The error permitted hackers to remotely control in-car systems and view drivers' identity data.

Connected vehicles house vast amounts of personal data in their in-car networks and carry-in devices connected to them. Connected vehicles lack security mechanisms for real-time tracking, detection, analysis and mitigation techniques targeting cybersecurity incidents. The lack of security mechanisms in in-vehicle networks was demonstrated by Koscher et al. (2016) who conducted experiments on two cars within a test environment. They demonstrated how to adversarially access and take control of a wide range of critical automotive functions and cause them to ignore driver input and the means to infiltrate virtually any car Electronic Control Unit (ECU) after bypassing their rudimentary network security protections.

Modern connected vehicles now contain over 60 ECUs (Koscher et al. 2010; Studnia et al.; 2013; Loukas, 2015). These ECUs are tasked with controlling and monitoring the internal car network and its various subsystems interconnected through several gateways (Durrani, 2012). Automobile internal networks have historically adopted an isolated closed loop structure; the continuing path of software and ECU development in automotive manufacture has seen these networks transition to a more open system structure. Connected cars are not usefully thought of as "ICT + cars"; the relationship is not a simple additive one. Nor are connected cars likely to be just "smarter" existing cars or more sophisticated "intelligent cars", although they will embody many features of them. Connected cars are fully-fledged nodes on the "Internet of Things" (IoT), that is the web of physical objects, including cars, embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data. Connected cars consume, create, supplement, direct and share digital information with other vehicles, transport infrastructure (Kleberger et al., 2011) and a host of other physical devices. Cars become entertainment centres, communications hubs, mobile offices, learning spaces, virtual shopping malls and whatever else our collective imaginations can dream up. But cars cannot be seen simply as "things"; they are prized possessions, highly mobile, dangerous in the wrong hands or at the wrong time, and potentially very attractive targets for a wide variety of criminal activity, increasingly including cybercrime.

Vehicular evolution ushered in by computerised control has paved the way to an array of potential cybersecurity incidents. Increased vehicle-to-infrastructure (V2I) connectivity through infotainment, navigation and telematics systems dramatically increases the risk of security breaches (Checkoway et al., 2011; Weimerskirch et al., 2012). In addition, the deployment of highly sophisticated software increases the potential for coding errors and software defects (Onishi, 2012; Trim et al., 2014). Research has been aimed at identifying different attack vectors with the capability of compromising connected vehicles and exposing their networks. Areas covered include infotainment, telematics, on-board diagnostics, in-vehicle communication protocols (Koscher et al., 2010; Hoppe et al., 2011). Researchers have identified and documented numerous vulnerabilities in connected cars, for example remote exploitation of in-car systems (Miller et al., 2014), vehicle sabotage, electronic tuning, theft and car viruses (Nilsson, 2008; Studnia et al., 2013). However, little research effort has been directed towards the creation of an infrastructure for collecting, processing, and managing cybersecurity incident data that can be used to develop cybersecurity incident management strategies.

One special area of concern is the rise of V2G (vehicle to grid) technology, that is, the integration of EVs into "smart" electric grids. By using V2G technologies, utility providers can let electricity flow from car batteries to power lines and back, creating a new market for utility companies and savings on home electricity bills for EV owners. However, there are fears that malevolent hackers or terrorists could inflict substantial damage to either the electrical grid or in the transportation infrastructure through use of unforeseen security holes. As a recent commentator suggested:

a malicious attack on the electric vehicle cyber infrastructure could potentially result in brownouts or stranded vehicles, and any failure in smart charging systems could strike a huge blow to utilities as well as consumer confidence in the reliability and viability of electric vehicles as a preferred mode of transportation (Pike Research, 2013).

The development of vehicle-to-cloud-to-everything networks results in even greater potential vulnerabilities. These challenges not only affect auto designers, developers and producers, but also have major repercussions for other sectors, for example the insurance industry and regulatory bodies. Even though modern cars are pervasively

computerized and open to remote compromise from many attack vectors (Checkoway et al., 2011), the protection of automotive control systems against manipulation has only very recently prompted major concern.

Developing issues

Software complexity

Complexity entails non-linearity. It is important to distinguish between complex systems and complicated systems. Complicated systems may have high dynamism and convoluted behaviour patterns, but they still exhibit linearity and causal consistency. Complex cybersecurity systems do neither. Non-linearity means that technical and human behavioural influences on cybersecurity issues cannot be separated. Cyber systems, given their high degree of non-linearity and variability in actor behaviour, cannot be explained or threats measured in traditional risk theory terms. It is likely that cybersecurity decision makers are under-equipped to gauge the magnitude and form of threats.

A major challenge is thus developing given the growing complexity of the software code in use. With most of this code still being hand-written, despite there being tools that can be used to generate complex code, the probability of errors in code is high (Axelrod et al., 2014). With most of the coding carried out by suppliers, integration issues arise and expose some systems to remote exploitation (Checkoway et al., 2011; Thomas et al., 2013; Amin et al., 2015). Coding errors may, in part, be attributable to the shortage of personnel with the required skills and expertise (Assante et al., 2011; Axelrod et al. 2014).

Advances in artificial intelligence (software that applies advanced computing to problem-solving) and deep learning (software analytics that learn from experience) allow on-board computers connected to cloud processing platforms to integrate data instantly. With the emergence of 5G networks and the Internet of Things, these trends are firmly embedded in the new era of vehicle development. Advanced software enables cars to learn from the experiences of other vehicles and adjust their guidance systems as weather, driving or road conditions shift. On-board systems can learn from other vehicles on the road through machine-to-machine communications. Autonomous cars depend on vehicle-to-vehicle (V2V)

communications and vehicle-to-infrastructure (V2I) connections. It is crucial to maintain security in each of these pathways as well as in the personal electronic communications that passengers transmit via email, phone calls, texting, Internet surfing, and location data. “Cyber-presence” is generally shaped by the interaction between software developers, system architects and engineers, managerial initiatives, partners in the industry ecosystem and end-users. Delimiting the “cyber perimeter”, and therefore policing it, can be difficult, as vulnerabilities can emerge from sources which are conventionally outside the organisation’s familiar visibility span.

Inadequate infrastructure

Infrastructure problems plague many countries. In India, for example, highways and roads represent a major challenge. Nearly 38 percent of the country’s roads are unpaved, compared to about 16 percent in China. Poor highways pose challenges for autonomous vehicles. Such cars need predictable surfaces and clearly defined traffic lanes. To the extent that roads are poorly marked or engineered, it is difficult for either semi-autonomous or fully-autonomous vehicles to traverse such routes. The risk of accidents increases and there is a grave danger that computerized algorithms will lead to poor decisions.

Inadequate spectrum availability is a major barrier in many countries. Finding dedicated frequency ranges is key to supporting connected cars. They need specific bands that perform well regardless of weather or traffic conditions. In practice this means mid-range spectrum below 6 GHz to achieve a workable balance between connection speed and reliability. Demand and competition for such frequencies is high and current capacity is unable to satisfy the additional demands generated by a widespread adoption of AVs.

Talent shortages

A lack of skilled cybersecurity professionals has contributed to the growth of cybersecurity incidents. Trim et al. (2014) highlight the lack of skilled cybersecurity professionals including managers with the ability and awareness to understand the technical gaps and the human deficiencies. Assante et al. (2011) point out that cybersecurity attackers and defenders are people and successful cybersecurity solutions require talent identification and recruitment, and continued development and conditioning of security professionals. Identifying and developing talent to address

the cybersecurity human resource deficit has become a priority for governments, higher education and many other organisations (Assante et al., 2011; Axelrod et al., 2014; Dark et al., 2015).

Weak or ineffective recruitment and training methods have also contributed to the constantly depleting supply of skilled cyber-aware professionals. Axelrod et al. (2014) argue that a lack of skilled cybersecurity experts is encouraged by some academic processes. IT security firm Cybrary indicated in 2015 that there is a global shortage of skilled cybersecurity professionals and this could be one of the reasons that has contributed to the rise of cybersecurity incidents in connected vehicles (Cybrary, 2015). Their survey of 435 senior technology professionals revealed some of the obstacles that most employers encounter in employing skilled cybersecurity personnel. The reasons given by 80% of respondents included lack of skilled cybersecurity talent, limited resources to locate and entice suitable talent, lack of certification and professional standards and salary levels. There is a very high demand for personnel with cybersecurity skills that greatly out-weighs supply in most industrial sectors and not just the automotive industry. The ability of IT professionals has been outpaced by sophisticated technology and tactics employed by criminals rendering cybersecurity a major business problem as well as a technical one.

Supply network configurations

Traditionally, OEMs focused on stability and performance of their supply chains, increasingly devising means to maintain and gain a competitive edge within the sector. ICT driven transformation, technological developments, component out-sourcing, the growing influences of cybersecurity, increased customer demand, proliferation of models and model variants have collectively induced far-reaching changes in the automotive supply chain. The new competitive forces faced by the industry render the simple tiered structure unsuitable. Growing software system complexity and highly integrated IT sub-systems have paved the way for the emergence of new suppliers. The new entrants provide services, particularly in design and engineering, rather than physical products (Loukas, 2015). These firms have a huge global presence and have located local plants close to OEMs forming supplier parks, taking responsibility for designing and assembling whole modules or systems of a vehicle. However, physical proximity of major suppliers and OEMs may have

fewer benefits where the “components” being supplied take the form of computer software and associated hardware.

Rather than thinking of major critical suppliers as being in Tier 1, it is helpful to identify them in terms of their new roles. System integrators have sophisticated capabilities in design and component integration. They integrate sub-systems into complete system modules prior to being shipped directly to the OEMs. Most automotive manufacturers place design and development responsibilities for systems, sub-systems, multi-technology products and components on system integrators (Amin et al. 2015) reflecting the relative unfamiliarity of the new technologies embodied in connected cars to incumbent OEMs. Global standardisers, a subset of system integrators, set the standards for a component or system on a global basis. These companies are capable of designing, developing and manufacturing complex systems or multi-technology products.

System manufacturers design systems and components from functional specifications and performance factors provided by automotive OEMs; however, at times, system manufacturers make design decisions without OEM input. System manufacturers supply components to the system integrators or directly to the OEMs. Component specialists design and manufacturer specific components or sub-systems for a given car or platform. These companies are often suppliers to system integrators and system manufacturers. They design systems and multi-technology products from functional specifications and performance factors provided by OEMs.

Complex digital systems and sub-systems are manufactured by a plethora of globally dispersed suppliers within the supply network. This multi-supplier structure permits design and development outsourcing, reduces development lead times, improves responses to strict deadlines, enables product proliferation at lower cost and encourages the production of quality products. However, it also creates knowledge-sharing challenges and may reduce the participation of OEMs in the design and development of vital components, software systems and multi-technology products. Yet, it is still OEMs who are responsible for the safety, quality and security of the products which bear their name.

Information and cost asymmetries

Cybersecurity is a secondary task within most business models; it provides limited opportunities for monetisation and value creation in a highly profit-oriented market environment. This results in security thinking being framed as a secondary function in many automotive OEMs and their major suppliers.

Informational asymmetry between attackers and defenders embodies an advantage to attackers. The adversarial macro-dynamics of the contested cybersecurity relationship are shared with all competitive strategy; however, the role of information is distinct in cybersecurity as breaches generally rely on an information imbalance. Attackers aim to get advantageous information on potential vulnerabilities and the appeal of different targets; defence entails anticipation of possible, or at least likely, threats. This asymmetry is amplified by the opportunity for attackers to empirically validate their assumptions and dedicate their full energies to finding attack vectors. In addition, the costs of unsuccessful attacks are generally low, unsuccessful defence can result in major disruption and challenges to operational sustainability. The link between knowledge information limitations and the ineffectiveness of many cybersecurity defence techniques results in an overuse of intuition, reliance on static and generic knowledge and inadequate cyber presence governance (Julisch, 2013).

The human "component"

In generic terms, many of the main cybersecurity threats facing us today derive not from ICTs themselves but from human error. As a major consultancy firm expressed it:

Cyber security isn't just about technology, it's also about psychology and sociology. It's easy for engineers to believe that the most important solution is the thing with the most flashing lights, but in the world of cyber security, it's often the behaviour of people that actually determines the outcome (PWC, 2014).

The most serious cybersecurity breaches are the product of multiple failings in people, processes, procedures and technology. In the haste to adopt and exploit new technology for the potential benefit of us all, there can be a tendency to overlook the inherent risks and underestimate and, consequently, effectively manage the downside through effective security measures. Users can be the source of cybersecurity risks

through, for example, V2D interactions, such as using smartphones as the interface of choice to connected car technology. The potential need for, and costs of, user education to help prevent cybersecurity breaches in connected cars remains unexplored except for some pioneering work in the autonomous vehicle sector (Center for Automotive Research, 2016).

Possible responses

Existing approaches to ensuring cybersecurity in connected cars are inadequate (Bordonali et al., 2017). Cybersecurity knowledge sharing efforts between OEMs have been focused on providing security for communication systems and user data. This has led to several attempts to create alliances between OEMs in a bid to swap cybersecurity data and to keep abreast of the latest hacking threats targeting connected vehicles. For example, the (US) AAM (Alliance of Automobile Manufacturers), an industry trade and advocacy group comprising twelve of the major global OEMs, has created the ISAC (Information Sharing and Analysis Centre). ISAC data is available for automakers worldwide; however, the lack of economic incentives to participate and share effective and useful information has limited its success (Vanian, 2015).

The automotive industry can, and must, learn from the computing domain where standards and initiatives have developed to facilitate cybersecurity information and knowledge sharing, but in the knowledge that the computing domain itself is struggling to come to grips with cybersecurity vulnerabilities. One cause is the complexity inherent in warding off attacks that are continually being adapted and evolved to exploit system weaknesses, especially given that such weaknesses are often caused by careless design and integration flaws. Dandurand et al. (2013) argue that there is a strong requirement for improved information sharing and automation in the cybersecurity domain. Brown (2015) notes the fundamental barriers exist in the field of cybersecurity information sharing, such as those raised in protecting privacy and a legal regime inherited from a pre-cybersecurity era, which require further research.

Different economic tools, both qualitative and quantitative, embody different cybersecurity representations. Tools based on economic knowledge can highlight

cybersecurity's operational aspects and provide a valuable input into developing effective policy. Economic tools link the development and operation of technologies and inform decision-making processes across a wide spectrum. Combining social, technical, organisational and economic aspects of cybersecurity highlights the economics that shape cyberspace and vice versa. Cyberactors, including consumers, providers and public agencies, have different responsibilities and exposures to emerging threats. Economic insights help us to understand how different actors are positioned in cyberspace. Given the secondary role of cybersecurity in organisations' value creation, cybersecurity performance relies on the local manifestation of threats, the organisations' adaptive capacity and system learning, as well as on its ability to develop, sustain and adapt inferential procedures, and act on the resulting insights.

The growth and success of damaging cybersecurity incidents is promoted by the lack of research evidence to inform the development of technology regulations, policies and profit structures. It follows that, to mitigate the threat of cybersecurity, coordinated research and development strategies must be developed. Axelrod et al. (2014) contend that cross-disciplinary research in implementing security into control systems will be needed to provide the solutions necessary to combat cybersecurity incidents.

Connected cars contain multiple embedded software products developed by different development teams with different skill-sets, processes and tools. Software is present in most if not all vehicle components (Loukas, 2015). Each software sub-system or system is unique and offers distinct coding and integration challenges. Integration of software modules adds to the huge challenge that vehicle manufacturers face in integrating different suppliers into an automotive supply chain that ensures security and reliability.

Summary

Connected cars are embedded in a complex ecosystem, some elements of which can only be changed very slowly, including user behaviour. Ever more sophisticated cyber-security threats are emerging and cyber-criminals are learning fast. Cyber security is not a "problem" that can be "solved". It is a self-perpetuating, high stakes guerrilla war.

Despite the prominence of cybersecurity, on the one hand, as a growing and urgent issue, and the all-pervasive shift to connected cars, there is little research which combines the two areas of interest. The auto industry research agenda, largely resourced by the industry itself and often conducted by industry-related bodies, tends to stress the benefits of connected cars; cybersecurity issues are only just beginning to be given prominence. Cybersecurity research, and the literature on cybercrime, tends to stress costs and the negative impacts and there is relatively little work which relates to connected cars specifically. Discussions of cybersecurity threats, by their nature, tend to downplay the major benefits which ICT can bring to car users individually and collectively. There is a major research gap to be filled.

This paper takes a broad view of the cybersecurity challenges contingent on the development of connected cars. These challenges are economic, regulatory, industrial and infrastructural – and that is just a summary starting list. The existence of a major legacy of older ("unconnected") cars coupled with a road infrastructure built for them; the tension between the need for knowledge sharing across a wide variety of actors and the disincentives to reveal vulnerabilities and cybersecurity breaches; and the potential doubts about driver acceptance of new technologies and willingness to pay for them, are also considered. Furthermore, the sensitivity of the phenomenon does not encourage an already secretive industry to share information. The automotive industry, which is competing within resource constraints, a multitude of players in the supply chain, and insufficient cryptographic knowledge, requirements for additional hardware infrastructures, considerable processing delays and extra costs is still waking up to the emergence of cybersecurity incidents. There is a lack of understanding across the automotive industry as to how OEMs should detect and respond to cybersecurity incidents in connected vehicles. OEMs need a mechanism that allows them to respond to all forms of cybersecurity incidents in connected cars, a mechanism that informs mitigation measures that can be implemented.

The undoubted potential of ICT to be exploited for good and, on the other hand, the vulnerabilities to critical infrastructures and digital services which may result in significant negative impacts on society, need to be managed. These challenges cross all sectors, manifest themselves at all levels from the individual to the global, emerge

and mutate very rapidly and, in many cases, are still largely unknowable. And they are not only technical; as with all major changes driven by technological development, those promoted by ICT bring social, political, business and economic shifts which affect us all, now and in the future. In turn ICT-driven transformations can only be fully understood and harnessed for the undoubted benefits they can bring, if they are analysed from individual and societal perspectives in tandem with the technical.

References

Amin, M. and Tariq, Z. (2015) 'Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities'. *Technology Innovation Management Review* 5 (1)

Assante, M. J. and Tobey, D. H. (2011) 'Enhancing the Cybersecurity Workforce'. *IT Professional Magazine* 13 (1), 12

Axelrod, C. W. (ed.) (2014) *9th International Conference on Computer Simulation in Risk Analysis and Hazard Mitigation, RISK 2014*. 'Bridging the Safety-Security Software Gap'. held 4 June 2014 through 6 June 2014 at New Forerst: WITPress

Beiker, Sven; Hansson, Fredrik; Suneson, Anders and Uhl, Michael. (2016). *How the convergence of automotive and tech will create a new ecosystem*. McKinsey&Company.

Bordolani, Corrado; Ferraresi, Simone and Richter, Wolf (2017). *Shifting gears in cybersecurity for connected cars*. McKinsey&Company, April.

Brown, Cameron S.D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9.9: 55-199

Center for Automotive Research (2016). *Impact of Automated Vehicle Technology on Driver Skills.* Report, June 2016.

Charette, R. N. (2009) 'This Car Runs on Code'. *IEEE Spectrum* 46 (3), 3

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. (eds.) (2011) *USENIX Security Symposium*. 'Comprehensive Experimental Analyses of Automotive Attack Surfaces.': San Francisco

Clark, D., Berson, T., and Lin, H. (2014) *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington DC: National Academics Press

Cybrary (2015). IT and Cyber Security Survey. Available at: https://www.cybrary.it/wp-content/uploads/pdfs/Cybrary-Survey-Presenation.pdf

Dandurand, Luc and Serrano, Oscar Serrano (2013). Towards improved cyber security information sharing. *Cyber Conflict (CyCon). 2013 5th. IEEE International Conference* , June 4-7.

Dark, M., Bishop, M., Linger, R., and Goldrich, L. (2015) *Realism in Teaching Cybersecurity Research: The Agile Research Process*.: Springer New York LLC

Hoppe, T., Kiltz, S., and Dittmann, J. (2011). Security Threats to Automotive CAN networks—Practical Examples and Selected Short-Term Countermeasures. *Reliability Engineering & System Safety* 96 (1), 11-25

Julisch, K (2013). Understanding and Overcoming Cyber Security Anti-Patterns. *Computer Networks, 57 (10): 2006-2211.*

Kleberger, P., Olovsson, T., and Jonsson, E. (eds.) (2011) *Intelligent Vehicles Symposium (IV), 2011 IEEE*. Security Aspects of the in-Vehicle Network in the Connected Car: IEEE

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., and Shacham, H. (eds.) (2010) *Security and Privacy* (SP), 2010 IEEE Symposium on Experimental Security Analysis of a Modern Automobile: IEEE

Loukas, G. (2015). Cyber Physical Attacks on Implants and Vehicles IN *CYBER-PHYSICAL ATTACKS: A Growing Invisible Threat.* ed. by AnonOxford, England: Elsevier, 82-102

McGettrick, Andrew 2013). Toward Effective Cybersecurity Education. *IEEE Security & Privacy*11(6): 66-68.

Miller, C. and Valasek, C. (2014) 'A Survey of Remote Automotive Attack Surfaces'. *Blackhat Usa*

Onishi, H. (ed.) (2012) *2012 4th International Conference on Cyber Conflict, CYCON 2012*. 'Paradigm Change of Vehicle Cyber Security'. 5-8 June 2012, Tallinn.

Pike Research (2013). *Hackers Could Use Electric Vehicle Charging Stations to Cripple Cars and Grid*. Reported by theblaze.com. April 2013

PWC (2014). *Cyber security: Building Confidence in your digital future*. Available at: www.pwc.co.uk/events/cyber-security-building-confidence-in-your-digital-future.html

SMMT (2016). *The Digitalisation of the UK Automotive Industry*. Report. November 2016

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., and Laarouchi, Y. (eds.) (2013) *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on*. 'Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks': IEEE

Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., and Woodyard, M. (2013) 'How Bad is it? –a Branching Activity Model to Estimate the Impact of Information Security Breaches'. *A Branching Activity Model to Estimate the Impact of Information Security Breaches (March 11, 2013)*

Trim, P. and Lee, Y. (2014) *Cyber Security Management: A Governance, Risk and Compliance Framework*. Surrey, England: Gower Publishing Limited

Vanian, Jonathan (2015). Automakers Unite to Prevent Cars From being Hacked. *Fortune,* July 15.

Weimerskirch, A. (ed.) (2012). *Security Considerations for Connected Vehicles*. SAE Government/Industry Meeting, Washington DC.

West, Darrell M. (2016). *Moving forward: Self-driving vehicles in China, Europe, Japan, Korea, and the United States. Brookings*: Center for Technology and Innovation. September.