CYBER SECURITY
AND INTELLIGENT MOBILITY

November 2016

CATAPULT
Transport Systems

CONTENTS

ACKNOWLEDGMENTS

This report is the result of collaboration between leading cyber security and transport professionals. Transport Systems Catapult expresses its thanks and appreciation to each of the external members of the project team for their input, guidance, and expertise.

EXECUTIVE SUMMARY

The world of mobility is undergoing significant change. This new world also brings a fresh challenge to the mobility space: cyber security. As with any sector undergoing rapid, impactful change, intelligent mobility is facing technological threats to its evolution. The exploration of these threats, as well as trends and observations, has led to recommendations on the next steps to a way forward – for the UK to lead as a secure intelligent mobility market.

INTELLIGENT MOBILITY: A NEW CYBER SECURITY PROPOSITION

This report is a research and analysis piece that set out to understand the implications of the interactions between the evolving cyber security and intelligent mobility landscapes over the next 10 years. By understanding the key trends, messages and challenges that frame this future space from over 70 sources of secondary data and UK-based thought leader interviews, new opportunities and recommended actions were determined.

The intelligent mobility cyber security proposition will be defined by the following:

- **Deep levels of integration across all mobility sectors and new forms of mobility.** Service offerings that will gain advantage in this space will be offerings that integrate several aspects of different systems to deliver a whole mobility offering. This is not just a single offering, but data and system providers will benefit, and expect, to benefit from the insight and analysis of these offerings. The technological relationship between infrastructure providers, service operators, and technology solutions will become deeper, further strengthening the requirement to understand security implications at a whole mobility system level.

- **Decentralised control of customer and operational choices.** The convergence of internet of things technologies, autonomous control of networks, and personalised mobility services will mean that control of travel choices and operations will increasingly become decentralised. Single points of control of highway networks and even scheduling of services will be slowly replaced decentralised systems of control and coordination through increasingly complex relationships between many providers.

- **Autonomy as standard, but with humans.** Autonomous vehicles are progressing towards commercial offering at an accelerating pace. Vehicle manufactures are increasingly taking the mindset of designing future vehicles with future autonomy in mind. This thinking is also being applied to network operations and technology systems, with autonomy supporting human decision making. Protecting of safety-critical systems is the manifestation of an increasingly cyber-physical challenge.

- **New business models and services emerging.** New technologies are increasingly challenging established business models in all mobility sectors. Technologies are enabling new services that customers increasingly demand, and expect. This is in addition to new market entrants increasingly challenging the established companies. For cyber security companies it will change who their customers are, and what they will expect.

- **The digital and the physical becoming a singular, whole mobility experience.** Like other sectors of the economy, the mobility sector is experiencing the increasing convergence of the digital and physical experience. Cloud-based services are simplifying processes and integrating physical and digital service channels and operations. This in turn is driving opportunities to personalise and tailor mobility services and operations, further decentralising cyber security requirements.

A UNIQUE SECTOR: OBSERVATIONS AND TRENDS

With increasingly sophisticated mobility systems, complex and interconnected networks across sectors and services, there are unique challenges for security in intelligent mobility. Analysis of literature and interview findings highlighted eight key drivers of change for intelligent mobility and cyber security:

- **Technology is becoming more integral to mobility experience.** The next 10 years will see a paradigm shift as the demand for a better user experience, driven by technology. This will shift the transport sector away from supply-led to a demand-led service offering, as companies seek to exploit a £900bn global opportunity by 2025.

- **Technological innovation in cyber security is accelerating.** To meet a rising threat from cyber attacks, companies and governments are investing significantly in developing cyber security capability, with £1.9 billion in planned investment by the UK Government until 2021. But as technological innovation accelerates, so does the capability to exploit this technology for criminal purposes.

- **Internet connectivity is expected – and everywhere.** Transport will be a critical element of the Internet of Things, with 250 million connected vehicles to be on the roads globally by 2020. Consumers and companies are moving from connectivity as desirable to expecting connectivity as standard.

- **An industry-wide approach is shaping up.** All parts of the traditional transport sectors realise that cyber security is a risk affecting their industry, and they need to work collaboratively to tackle the issue. But the maturity of capability is variable, and there is little evidence of an intelligent mobility approach to cyber security.

- **Transport is a critical national infrastructure.** Disruption to the UK transport network has significant impacts on national defence, security, and the operation of the state. This critical infrastructure is managed and maintained by a complex set of actors, each of whom tackle cyber security differently.

- **Sector vulnerability and cyber threats are evolving.** Just like the technology changes, the threat landscape facing those in the intelligent mobility space is also changing. Cyber criminals are rapidly adopting new technologies, and are refining the cyber crime business model. Attacks in this connected world will be possible from anywhere, at any time.

- **Safety and security are two sides of the same coin.** The cyber security threat is increasingly becoming cyber-physical, as vehicles, infrastructure, and control systems become increasingly connected. Accordingly, physical safety – an established practice across transport sectors – and cyber security will become one and the same. This necessitates a significant shift in industry culture.

- **Privacy will be an ongoing consumer debate, and opportunity.** Significant steps have been taken recently, notably at the European level, to protect the data and privacy of citizens. Additionally, privacy is increasingly being promoted as a selling point for technology products, with 35% of consumers having made purchasing decisions based upon privacy concerns.

While the UK faces considerable challenges progressing the intelligent mobility market in a secure way, it is well placed to be a global leader. Analysing themes and trends from expert interview research revealed four fundamentals of this unique emerging sector:

£2.4 MILLION
THE AVERAGE ANNUALISED COST OF CYBER CRIME TO TRANSPORT COMPANIES ON THE UK[1].

• **The rapidly changing security and mobility landscape is likely to mean more cyber-attacks, more often, and potentially with more severe consequences.** The cost and number of cyber-attacks is likely to increase. Fuelled by 20.8 billion things being connected to the internet by 2020[2] and an increasing number of these systems exercising a physical function, such as controlling traffic, the implications of a successful cyber-attack are much more severe.

• **Understanding the nature of the existing issue is still a challenge.** All sectors of mobility realise that cyber security is a significant issue affecting operations and services. But this understanding is still not equivalent to the scale of the issue at hand. This also poses a challenge for delivering new, innovative cyber security solutions into the mobility sector.

• **The UK is well positioned to respond to the challenge as it already has strong capability in cyber security.** The UK is one of the leading nations globally for cyber security, with the Government's new cyber security strategy reaffirming its commitment to not only defend the nation, but to exploit cyber security as an economic asset. Combined with the UK's leading capability in intelligent mobility, this presents a significant opportunity.

• **The technology the UK needs is not an issue – secure intelligent mobility requires a robust strategy and cultural focus.** New cyber security strategies will be accelerated regardless of the conditions of the intelligent mobility market. But their impacts will be greatest where effective strategy to accelerate these technologies into intelligent mobility exist, and where industry culture enables it to do so.

THE CORE CHALLENGES TO A SECURE INTELLIGENT MOBILITY FUTURE

The UK has the potential to be a global leader in secure intelligent mobility because it has capabilities that can be applied to the sector, it has supportive government policy on innovation and cyber security, and its Internet of Things environment and consumer views on privacy are enablers for secure long-term solutions. In order to build on this potential, it must address three key challenges:

1. Creating solid foundations such as an improved understanding of the complexities of the cyber security and transport markets, establishing sound security principles and balanced regulation.

2. Developing a security proposition with progressive governance structures, a clear strategy, shared intelligence and solutions, as well as by encouraging innovation.

3. Delivering the value of intelligent mobility securely with new value chains including Mobility as a Service, as well as smart data that is focused on new business models and by viewing consumer privacy as an opportunity.

[1] Ponemon Institute (2015) 2015 Cost of Cyber Crime Study. Ponemon Institute

[2] Gartner (2016) Gartner Says 6.4 billion Connected Will Be in Use by 2016, Up 30% from 2015. URL: http://www.gartner.com/newsroom/id/3165317

RECOMMENDATIONS FOR ACTION: SECURING FUTURE SPACE

As the UK has evidenced capability and technology that supports a secure intelligent mobility future, and this report has clearly identified key trends, challenges and opportunities, a strategic view and approach is required. A focused cyber security and intelligent mobility strategy would provide a clear path that begins with five critical steps.

STEP 1
Principles for securing intelligent mobility. The unique challenge of securing intelligent mobility necessitates a review of the suitability of established security principles for this future in the context of intelligent mobility. This acts as a basis for securing the future of mobility.

STEP 2
Technology and research roadmaps for securing intelligent mobility. Technology and Research Roadmaps need to be accelerated and adopted for securing all aspects of intelligent mobility. Such roadmaps should have a particular emphasis on the convergence with other mobility technologies.

STEP 3
Upskilling the mobility sector workforcey. Cyber security should be positioned as an essential skill for those working in intelligent mobility. This needs to be supported by backing for skills development, provision of funding, and development of appropriate courses.

STEP 4
Transparency as standard across mobility domains. Transparency and knowledge exchange across mobility sectors needs to be standard practice, as well as the coordination of actions and research. Cyber security is not an automotive or aviation problem. It is a problem for all of mobility.

STEP 5
Accelerate cyber security innovation for intelligent mobility. Building upon established innovation capability in cyber security, there needs to be a concerted focus on innovating in cyber security in intelligent mobility.

INTRODUCTION
THE NEW WORLD: TRANSPORT, TECHNOLOGY, AND SECURITY

Today's pace of technological advancement presents both opportunities and threats to the landscape of transport, both in the UK and globally. With the proliferation of systems and digital connectivity, the consumer's experience of transportation is fast moving and ever changing. And as the consumer's expectations of mobility progress with their ever-changing experience of it, the pressure to evolve secure data, systems and wider digital solutions in this sector increases.

While today's transportation integrates digital developments such as traffic management, entertainment and booking systems, tomorrow's mobility will be far more evolved. With sophisticated, connected and innovative tech solutions driving change, new business and operational models will radically redefine transport.

UK travellers see the advantages of a new approach to transport. The Traveller Needs and Capability Study in the UK (2015) revealed 57% would not mind sharing their data for services and 39% would use driverless cars today. The desire for improved consumer experience, along with the need to progress efficiency, safety and integration, means a revolution in transportation is taking shape.

> " Intelligent Mobility is the future of transport. It is about harnessing innovation and emerging technologies to create more integrated, efficient and sustainable transport systems. It marks an exciting meeting point between traditional transport and the new products and services that are emerging as we start to exploit vast amounts of multi-layered data.
>
> Transport Systems Catapult (2016) Technology Strategy for Intelligent Mobility

Growing digital capabilities demonstrate this is not far away: there is already a distinct shift away from traditional transport toward intelligent mobility. With the UK's ambitious plans to dominate the intelligent mobility market, the transport and technology sectors have some exciting new opportunities ahead. And as with any digital advancement, there are also challenges and threats for transportation and technology leaders in the UK to address.

Indeed, there is due cause for concern for senior leaders in both sectors. As the capacity and frequency of hacks and cyber attacks increase, there is more evidence to support the need for a careful review, analysis and exploration of online, data and information security.

Cyber security is inextricably linked to the success of digital progress, transport in general and, specifically, intelligent mobility. Without the safe and secure use of networks, infrastructure and devices, there will be problems for everyone involved in transport and information technology. These will likely begin with consumer cautiousness and slow adoption of services, and continue through to organisational cost, resource and development.

So, how will technological change affect cyber security in intelligent mobility over the next 10 years? And what challenges does the intelligent mobility sector face in managing this change? From careful, detailed research into current and trending practices in transport, the unique needs of the emerging intelligent mobility sector were obvious. And following a review of the unique challenges that intelligent mobility has with cyber security, it is apparent that there are eight drivers determining its future security. These drivers are framing the future of the transport and cyber security sectors, and have the capacity to make or break the UK's success in both.

> " Cyber security is a collection of tools, policies, security safeguards, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets... The general security objectives comprise confidentiality, integrity, and availability.
>
> United Nations Information Technology Unit (2016) Definition of cyber security

METHODOLOGY
THE LINK BETWEEN TECHNOLOGY, INTELLIGENT MOBILITY AND CYBER SECURITY

In order to explore the link between technology, intelligent mobility and cyber security, there must be a clear picture of the near future, as well as the longer-term threats and opportunities. This requires understanding of:

• Current UK cyber security (academic and industry) capability, practices and research, both within the cyber security market and more broadly in the transport sector

• Current strategy globally to tackle cyber security issues, and the capability within the transport sector to deal with these issues

• The nature of the cyber security threats relevant to transport systems

• Future changes in technology likely to impact the transport sector, and the cyber security implications of this technology

• The requirements for the transport sector to meet the emerging cyber security challenges

INSIGHT FROM LITERATURE AND INTERVIEWS

Evidence was gathered across an in-depth review of reports, white papers, policy documents and academic research, along with interviews and workshops with key stakeholders and thought leaders.

The evidence that underpins this report pulls on secondary data, sources and research from over 70 sources, including technical publications, white papers, and articles. It is supported by interviews and a workshop that captured the insight of 70 UK-based cyber security and transport thought leaders. Expert observation, experience and identification of trends that connect cyber security and intelligent mobility were captured on the following key areas:

Priority areas for action

The most critical issue for the future

Current practice in all mobility sectors – automotive, aviation, maritime, public transport

Key technologies affecting both the cyber security and intelligent mobility in the next 10 years

Analysis that followed was based on the PESTLE Framework, which frames the political, economic, social, technological, legal and environmental aspects. This analysis delved into the immediate future (the next five years), and the further future (six to 10 years). Once trends were ranked by relevance and impact, a Futures Wheel[3] methodology was used to organise and understand the implications of change. This presented an understanding of the critical trends, challenges and opportunities that will shape the future of intelligent mobility and cyber security will interact. It also helped to identify the uniqueness of intelligent mobility's security needs and challenges.

RESEARCH ❯

- Over 100 publications, white papers, and articles
- Academic and technical
- Sourced from UK and international practice
- Identified capability, challenges, and opportunities

ENGAGEMENT ❯

- 70 experts in cyber security and transport
- Interviews and workshop with specialists from industry, academia, and government
- Verified research findings
- Identified future trends

ANALYSIS ❯

- Trends grouped into a PESTLE Framework
- Trends mapped using Future Wheels methodology
- Trends ranked by anticipated scale of impact

THEME OF QUESTIONS ASKED ABOUT NOW AND THE FUTURE

	NOW	FIVE YEARS	TEN YEARS
PRACTICE	Automotive	Emerging	Conceptual
	Public Transport		
	Aviation		
	Maritime		
MARKET CHANGE	Transport	>	Intelligent Mobility
TECHNOLOGICAL CHANGE	Cyber Security	>	Future Technologies
	Transport	>	
KEY ISSUES	Need Action Now	Research Now	Prepare for Now
PRIORITY ACTION AREAS	Immediate Market Failures	Implications of Connectivity	Implications of Intelligent Mobility

[3] Glenn, J. (2009) Futures Wheel. Futures Research Methodology Version 3.0. Millennium Project.

FINDINGS

INTELLIGENT MOBILITY HAS UNIQUE CYBER SECURITY NEEDS

A comprehensive assessment of transport, cyber security and intelligent mobility literature, as well as interviews with thought leaders revealed the uniqueness of this emerging sector when it comes to delivering safe, secure platforms and technology.

Because mobility systems are increasingly sophisticated, with complex and interconnected networks that work across sectors and services, intelligent mobility requires comprehensive security solutions. There are three main areas that make intelligent mobility unique in its security challenges:

1. AUTOMATION

2. NEW MOBILITY MODELS

3. SMART ECOSYSTEMS

AUTOMATION

Perhaps one of the most significant developments in intelligent mobility, automation has the potential to greatly reduce human error. However, it also offers the opportunity to greatly increase the impact of cyber attacks and system responses that endanger lives, particularly in cyber-physical systems.

As an area that's receiving significant investment, automation is being explored in every sector, from automotive to shipping. Because of the possibility of it being such a wide-reaching attribute, and one with the opportunity to connect cooperative systems for self-managed responses in real time, it is critical that it operates in a safe and secure way.

There have been extensive academic discussions about the security implications of autonomous vehicles. And research is also underway for the security of connected systems. This has seen some action embedded – for instance, the European Commission has recommended a common technical framework for the deployment of autonomous vehicles in a connected environment.[5]

76
MILLION

THE NUMBER OF VEHICLES WITH SOME
DEGREE OF AUTONOMY EXPECTED
TO BE SOLD GLOBALLY BY **2035**[4]

80%
OF SECURITY AND MOBILITY
PROFESSIONALS

WE INTERVIEWED IDENTIFIED AUTONOMOUS
VEHICLES AS A MAJOR CYBER SECURITY ISSUE
FACING BOTH SECTORS OVER THE NEXT 10 YEARS

[4] IHS Automotive (2016) IHS clarifies autonomous vehicle sales forecast. URL: http://press.ihs.com/press-release/automotive/autonomous-vehicle-sales-set-reach-21-million-globally-2035-ihs-says.
Date Site Accessed: 9/6/2016.

[5] C-ITS Platform (2016) C-ITS Platform – Final Report. European Commission. http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

DAY 1 SERVICES

- Slow or stationary vehicles
- Traffic ahead warning
- Road works warning
- Weather conditions
- Emergency brake light
- Emergency vehicle approaching
- Other hazards
- In-vehicle signage
- In-vehicle speed limits
- Signal violation / intersection safety
- Traffic signal priority requests
- Green Light Optimal Speed Advisory
- Probe vehicle data
- Shockwave dampening

DAY 1.5 SERVICES

- Fuelling and charging stations
- Vulnerable road user protection
- On street parking management and information
- Off street parking information
- Park and ride information
- Connected & cooperative navigation
- Smart routing for autonomous vehicles

STANDARDISED TRUST MODEL AND EU CERTIFICATE POLICY	
Technical capability	Regulatory framework

'Security for connected and autonomous networks – a technical framework for a Connected Intelligent Transport System Platform' [6]

Autonomous systems will also require detection, identification and resolution within seconds to prevent potentially serious safety breaches. While critical to the success of automation, any safety intervention needs to be balanced with user experience. For instance, it is unlikely that travellers will tolerate a stop-start journey because the vehicle's system detects safety breaches.

This safety challenge extends to liability and insurance. Research into the possible risk factors and insurance models present trials for those shaping business models, standards and legislation for multi-national organisations.[7]

Insurers can also act as regulators of practice. For example, Lloyd's Register has significant influence on the marine industry, while payment mechanisms and certification requirements are directly influenced by insurance.[8]

---

[6] C-ITS Platform (2016) C-ITS Platform – Final Report. European Commission. http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[7] Lloyd's (2014) Autonomous Vehicles – Handing Over Control: Opportunities and Risks for Insurance.

[8] National Highway Traffic Safety Administration (2014) A Summary of Cybersecurity Best Practices. US Department of Transportation.

NEW MOBILITY MODELS

With the rapid development of the intelligent mobility sector, new solutions and models are emerging – and will succeed or fail just as quickly as their launches. New concepts such as Mobility as a Service and ride sharing are rapidly becoming a reality as customers increasingly satisfy their mobility needs in new ways.

These new mobility experiences are adding complications to system security. Third party integration of mobility services is a desirable and necessary precursor to delivering these new forms of mobility. This additional layer of cross-party complexity on top of existing systems introduces new security concerns.

$1 TRILLION

VALUE OF THE GLOBAL MOBILITY AS A SERVICE MARKET IN **2030**[9]
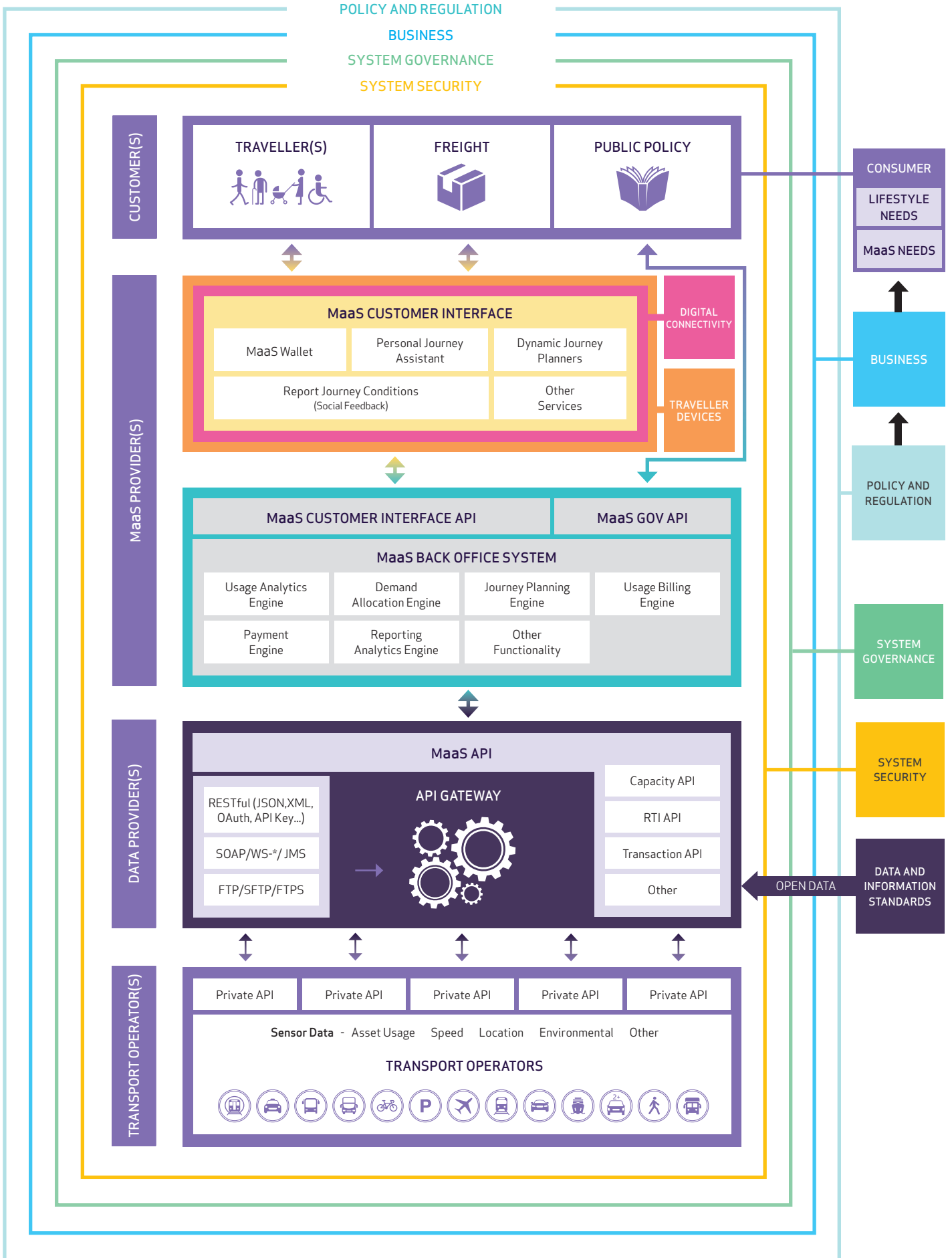
Mobility as a Service is defined as using a digital interface to source and manage the provision of transport-related services, which meet the mobility requirements of a customer.

Transport Systems Catapult (2016) Mobility as a Service –
Exploring the opportunity for Mobility as a Service in the UK

[9] ABI Research (2016) Mobility as a Service. ABI Research

MaaS reference architecture[10]

POLICY AND REGULATION
BUSINESS
SYSTEM GOVERNANCE
SYSTEM SECURITY

CUSTOMER(S)

| TRAVELLER(S) | FREIGHT | PUBLIC POLICY |

CONSUMER
LIFESTYLE NEEDS
MaaS NEEDS

MaaS PROVIDER(S)

MaaS CUSTOMER INTERFACE

| MaaS Wallet | Personal Journey Assistant | Dynamic Journey Planners |
| Report Journey Conditions (Social Feedback) | | Other Services |

DIGITAL CONNECTIVITY

TRAVELLER DEVICES

BUSINESS

| MaaS CUSTOMER INTERFACE API | MaaS GOV API |

MaaS BACK OFFICE SYSTEM

| Usage Analytics Engine | Demand Allocation Engine | Journey Planning Engine | Usage Billing Engine |
| Payment Engine | Reporting Analytics Engine | Other Functionality | |

POLICY AND REGULATION

SYSTEM GOVERNANCE

DATA PROVIDER(S)

MaaS API

RESTful (JSON, XML, OAuth, API Key...)	API GATEWAY	Capacity API
SOAP/WS-*/ JMS		RTI API
FTP/SFTP/FTPS		Transaction API
		Other

SYSTEM SECURITY

DATA AND INFORMATION STANDARDS

OPEN DATA

TRANSPORT OPERATOR(S)

| Private API | Private API | Private API | Private API | Private API |

Sensor Data - Asset Usage   Speed   Location   Environmental   Other

TRANSPORT OPERATORS

[10] Transport Systems Catapult (2016) Mobility as a Service: Exploring the Opportunity for Mobility as a Service in the UK. Transport Systems Catapult.

These new models of mobility are data based, and driven by a demand for service – and less on transport as a product. On top of existing issues associated with payments and timetabling, there are added security implications for these new models. Namely, privacy of consumers and companies, and the security of open data. While some data is highly regulated, and new laws are defining personal data ownership, more commercial incentives need to be in place to ensure the protection of personal data.

Some of these challenges are not new. The linking of new, complex datasets across third parties will be critical to generating value[11] from mobility models. This is because the adoption of security does not only apply to the opening of these data sources[12], but also to setting standards and protocol for assessing the value of this data. Indeed, collecting data (especially personal data) just in case it may be useful could be viewed as dangerous and makes it a 'toxic asset'.[13]

SMART ECOSYSTEMS

As the transport sector evolves and the intelligent mobility sector grows, its traffic management, ports, airports and logistics handling becomes more intuitive and efficient. And with its increasingly complex and wide-reaching connecting systems, mobility will integrate technology more effectively than it has ever been before. The result will be a variety of smart ecosystems operating across different industries and through different organisations.

Single authorities investing in capability development and partnerships have pioneered this smart ecosystem concept.[15] New and improved security frameworks will be required for smart ecosystems. This will require collaboration that is highly evolved – and far more progressive than traditional multi-stakeholder governance models. New cross-sector trusted partnerships will be essential to secure these networks and establish sustainable innovation ecosystems.[16]

> "We're going to have to be smart and efficient and focus on what each sector does best, and then do it together.

President Barack Obama at Cybersecurity and Consumer Protection Summit, February 2016

$757.74 BILLION
IS THE VALUE OF THE SMART CITIES MARKET GLOBALLY BY 2020[14]

[11] Royal Academy of Engineering and The Institution of Engineering and Technology (2015). Connecting Data – Driving Productivity and Innovation. Royal Academy of Engineering.

[12] CPNI (2015) Open Data: Adopting a Security-Minded Approach. CPNI.

[13] Schneier, B. (2016) Data is a toxic asset. Schneier on Security. URL: https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html

[14] Markets and Markets (2015) Smart Cities Market worth 757.74bn USD by 2020. URL: http://www.marketsandmarkets.com/PressReleases/smart-cities.asp

[15] Carrudo, C. (2015) An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. IOActive.

[16] Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., and Oliveira, A. (2011) Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. Future Internet Assembly.

Interactions between stakeholders and operators in Smart Cities[17]
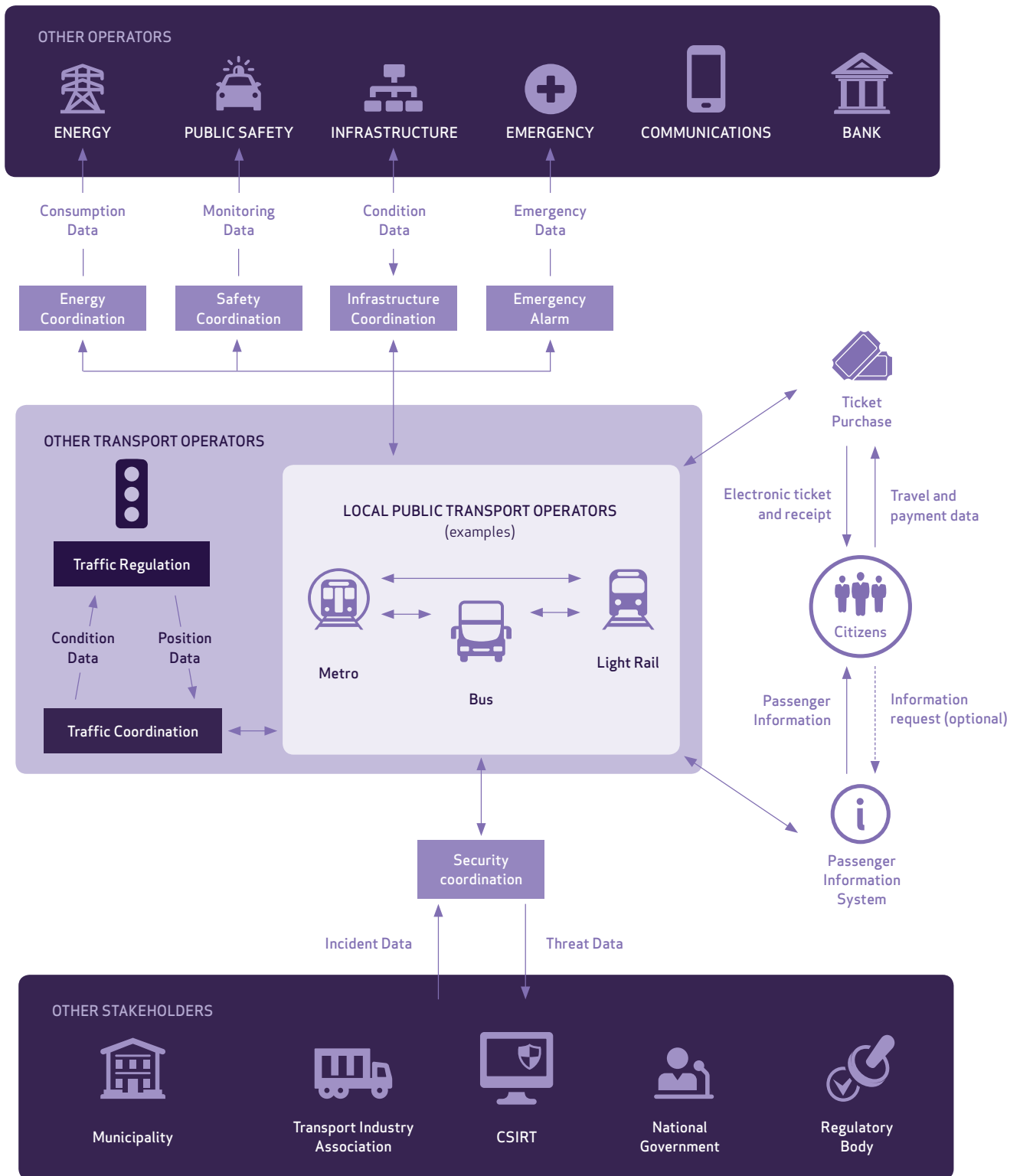
While this requires significant thought and investment, much of the operational principles and practices of smart ecosystems are already well established in security. The work of the Jericho Forum, for instance, extensively covers the "de-perimeterization" of security in a world dominated by connected systems. These established commandments for security were necessary to deliver such a vision.[18.] Leveraging such change requires conscious change in the architecture, and subsequently the security, of systems.

The convergence of the three defines the intelligent mobility cyber security proposition

Automation, new mobility models, and smart ecosystems are three unique attributes with significant security challenges on their own. The future will see a convergence of the consumer and operational offerings of each space into a single consumer offering, utilising the technologies of all three. This convergence constitutes the intelligent mobility cyber security proposition.

The development of security protocols and technologies in isolation may in some cases be desirable, for instance a highly specialised technology for sensitive cargo manifests. But where value will be added is in how these distinct offerings relate to each other, and combine as part of new offerings to customers in intelligent mobility. This intelligent mobility cyber security proposition will be defined by the following:

- **Deep levels of integration across all mobility sectors and new forms of mobility.** Service offerings that will gain advantage in this space will be offerings that integrate several aspects of different systems to deliver a whole mobility offering. This is not just a single offering, but data and system providers will benefit, and expect, to benefit from the insight and analysis of these offerings. For instance, transport application developers work closely with Transport for London to not only benefit from their universal open data feeds, but also to provide them with insights on travel behaviour. The technological relationship between infrastructure providers, service operators, and technology solutions will become deeper.

- **Deep levels of integration across all mobility sectors and new forms of mobility.** Service offerings that will gain advantage in this space will be offerings that integrate several aspects of different systems to deliver a whole mobility offering. This is not just a single offering, but data and system providers will benefit, and expect, to benefit from the insight and analysis of these offerings. For instance, transport application developers work closely with Transport for London to not only benefit from their universal open data feeds, but also to provide them with insights on travel behaviour. The technological relationship between infrastructure providers, service operators, and technology solutions will become deeper.

- **Autonomy as standard, but with humans.** Autonomous vehicles are progressing towards commercial offering at an accelerating pace. Whilst the widespread autonomisation of the vehicle fleet may still be many years away, vehicle manufactures are increasingly taking the mindset of designing future vehicles with future autonomy in mind. This thinking is also being applied to network operations and technology systems, with autonomy supporting human decision making.

- **New business models and services emerging.** New technologies are increasingly challenging established business models in all mobility sectors. Far from simply integrating new technologies into existing ways of working, companies are increasingly looking at technologies as offering new services that customers increasingly demand, and expect. For instance, airlines are increasingly offering whole trip services as integrated travel deals, and infrastructure operators are looking at ways the technologies they have developed can be exploited. This is in addition to new market entrants increasingly challenging the established companies. For cyber security, this radically changes it consumer market, changing who their customers are, and what they will expect.

- **The digital and the physical becoming a singular, whole mobility experience.** Like other sectors of the economy, the mobility sector is experiencing the increasing convergence of the digital and physical experience. Cloud-based services are simplifying processes and integrating physical and digital service channels and operations. This in turn is driving opportunities to personalise and tailor mobility services and operations, further decentralising cyber security requirements.

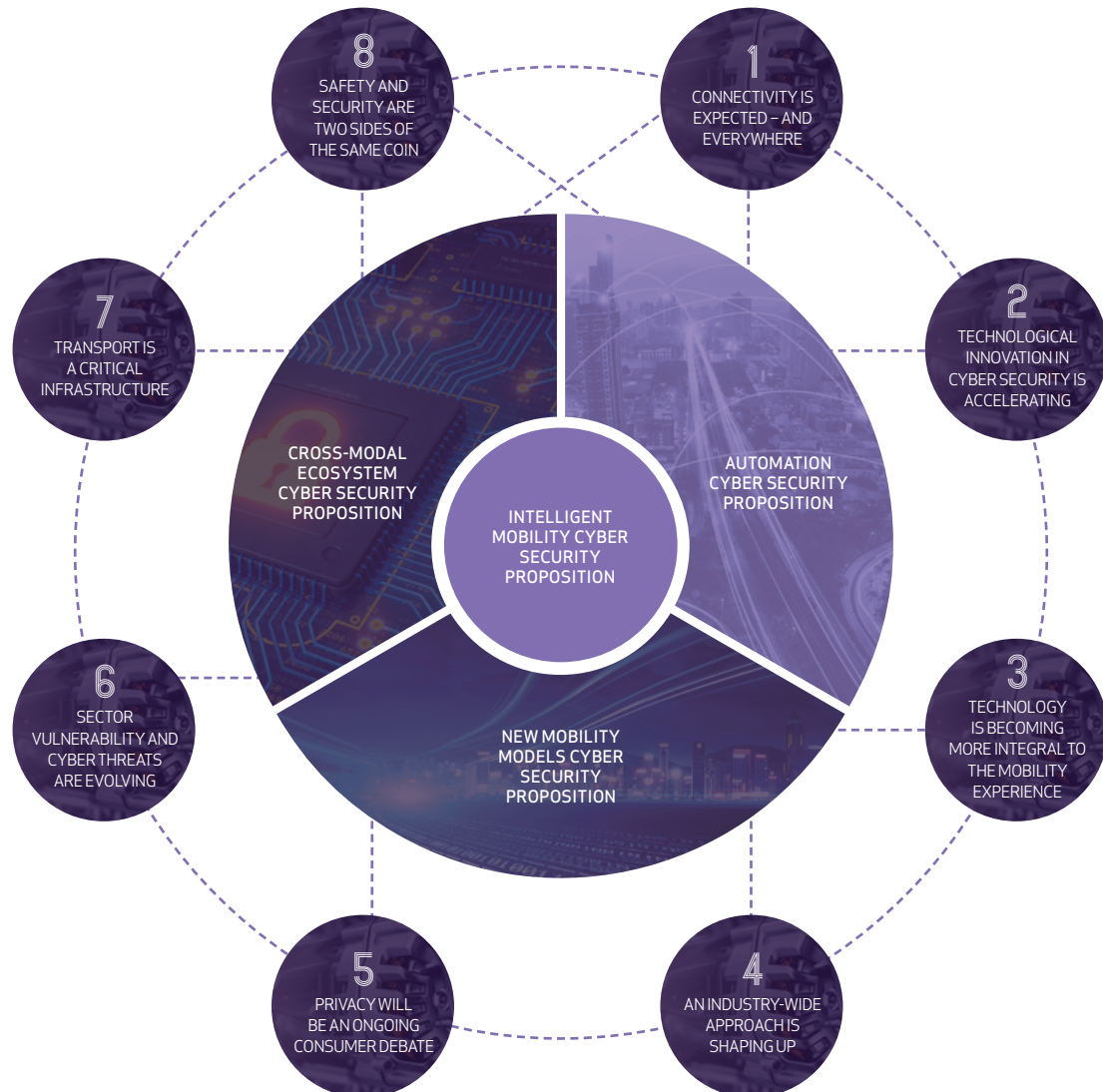[18] Jericho Forum (2007) Jericho Forum Commandments. Jericho Forum

The development of security protocols and technologies in isolation may in some cases be desirable, for instance a highly specialised technology for sensitive cargo manifests. And those of value need to consider the intelligent mobility context. From these three unique attributes and the evidence closely linked to them, the intelligent mobility sector raises distinctive challenges for cyber security.

Further analysis has led to a high-level view of the key trends, or drivers of change, in intelligent mobility and cyber security. These technological, social, industry and contextual trends are creating challenges and opportunities not only for solution providers, they are doing so for all involved in transport, technology and cyber security.

While this requires attention, thought and development time, these valuable cyber security insights from intelligent mobility present opportunities for the wider transport industry. With the development of security across new business models, autonomy, smart ecosystems and other technological spaces, learnings and progress can be shared and adopted elsewhere.

THE KEY DRIVERS OF CHANGE

While each transport sector will witness differences and the operational environment may be unique to them, analysis of literature and interview findings highlighted eight key drivers of change linking intelligent mobility and cyber security.

8 SAFETY AND SECURITY ARE TWO SIDES OF THE SAME COIN

1 CONNECTIVITY IS EXPECTED – AND EVERYWHERE

7 TRANSPORT IS A CRITICAL INFRASTRUCTURE

2 TECHNOLOGICAL INNOVATION IN CYBER SECURITY IS ACCELERATING

6 SECTOR VULNERABILITY AND CYBER THREATS ARE EVOLVING

3 TECHNOLOGY IS BECOMING MORE INTEGRAL TO THE MOBILITY EXPERIENCE

5 PRIVACY WILL BE AN ONGOING CONSUMER DEBATE

4 AN INDUSTRY-WIDE APPROACH IS SHAPING UP

CROSS-MODAL ECOSYSTEM CYBER SECURITY PROPOSITION

INTELLIGENT MOBILITY CYBER SECURITY PROPOSITION

AUTOMATION CYBER SECURITY PROPOSITION

NEW MOBILITY MODELS CYBER SECURITY PROPOSITION

CONNECTIVITY IS EXPECTED – AND EVERYWHERE

The next 10 years will see internet connectivity everywhere. With multi-faceted improvements to connectivity, it is expected that the transport and mobility sector will significantly contribute to the growth of the Internet of Things over the next decade.

> The internet of things (IoT) describes a world in which objects that form part of our everyday lives contain microchips that can communicate through various networks. This technology will help us to socialise, navigate and interact with the world in ways that we can barely imagine.

Government Office for Science, Internet of things review, 1 September 2014

There are already substantial investments in aviation[19], maritime[20] and public transport[21] for the Internet of Things. For connected vehicles alone, it is estimated that in excess of 250 million will be on the roads globally by 2020.[22] This investment is being driven by consumer demand and internal organisational requirements, and is enabled by reduced costs of hardware, internet connections and cloud computing power. For example, the cost of cloud computing power is predicted to fall by 14% by 2020.[23]

Connecting previously unconnected devices to internet and cloud enabled services means incorporating and integrating legacy systems for connectivity. One example of this is traffic management systems. This obviously requires IT infrastructure investment – especially because cloud computing offers opportunity to upscale.

Connectivity will be the basis upon which new mobility services are delivered, and the possibilities of new technologies will be exploited [24]. And while cyber security professionals accept the Internet of Things presents a security challenge, there is much debate about how it will manifest. For example, 48.8% of security professionals believe the Internet of Things will have the same level of security problems, though they will appear in other applications and systems.[25]

Our interviews illustrated that the security of the Internet of Things is a major issue currently challenging security professionals, with over 90% of persons who we interviewed identifying the security implications of the Internet of Things as a major challenge for the next 10 years. Comments from those interviewed indicated concerns over current device security, the significant potential for disruption enabled by connected infrastructure. Where systems are to be integrated with others as part of an ecosystem (for instance smart cities) organisations have to be increasingly mindful of threats from outside of their company, and industry. Because not many companies can currently invest in internet-enabled platforms, systems architectures are beginning to centralise at an infrastructure level and on to a handful of hardware and software platforms. This centralisation also enables even more devices to be connected to, and theoretically controlled by, by Internet of Things systems.

> The shortened timescales from product development to being available for public beta means that many IoT products are being released without even basic security protocols in place. This is less so on safety critical systems, but the issue is how such systems can be accessed through these new, unsecured, devices.

> I worry about the security of connected vehicles purely because of the potential impacts of a successful cyber attack on them. A rogue actor seizing control of a fleet of vehicles does not bear thinking about.

> Current smart city investment is focussed on improving efficiency of services, of which highways is one. But this is based on a security assumption that the attacks will be direct. The ecosystem being built means that such attacks will be through other services and your supply chain. In fact increasingly so.

> Whilst the long term future is likely to progress to more decentralised control networks – enabled by technologies like distributed ledgers – in the medium term systems architectures will centralise on cloud platforms. Thus, the power of malicious attacks will also be concentrated.

Research highlighted ongoing issues with authentication, vulnerabilities, privacy and the integrity of control systems, along with many more concerns. However, as the culture and practice within the transport sector is consistent, the inevitable change that the future brings could likely be consistently managed.

[19] CPNI (2012) Cyber Security in Civil Aviation. CPNI.

[20] ENISA (2011) Analysis of Cyber Security Aspects in the Marine Sector. ENISA.

[21] ENISA (2015) Cyber Security and the Resilience of Intelligent Public Transport. ENISA.

[22] Gartner (2015) Gartner says that by 2020 a Quarter Billion Internet Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities.
URL: http://www.gartner.com/newsroom/id/2970017

[23] Tariff Consultancy Ltd. (2016) Pricing the Cloud 2 – 2016 to 2020. TCL.

[24] The Institution of Engineering and Technology and the Knowledge Transfer Network (2015) Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles.

[25] Pescatore, J. (2014) Securing the "Internet of Things" Survey. SANS.

TECHNOLOGICAL INNOVATION IN CYBER SECURITY IS ACCELERATING

In the cyber security sector, new technologies are being accelerated to market to counter established and emerging threats, with many being adopted in the mobility sector. This is being driven by a significant cyber security market opportunity more generally, with a total of $1 trillion anticipated to be spent globally on all cyber security products from 2017 to 2021.[26] Major companies have significantly boosted their budgets for cyber defence – averaging between 7% and 9% year on year. The main spending areas are access and authentication, advanced malware protection, and endpoint protection.[27]

Accelerating this innovation is also being enabled by significant government intervention. The UK government is rapidly accelerating investment by diversifying the innovation offer in the cyber space domain with £1.9 billion investment planned between 2016 and 2021. The UK government is not on its own. For instance, the US government will increase cyber security investment by 35% between 2016 and 2017.[28]

Whilst defence technologies are being rapidly accelerated, many emerging technologies are also being exploited for cyber-attacks. Common consensus is that even with this significant acceleration in innovation and technological development, analysts will be unable to keep pace with a rapid rise in cyber-crime when forecasting.

Potential applications of technological developments in cyber security for the mobility sector include advanced encryption techniques, advanced threat detection and high security wireless communications. Respectively, this could mean mobility services using cloud-based analytics, detection and protection against network attacks and consumer wireless in vehicles.

[26] Cybersecurity Ventures (2016) Cyber Security Market Report. URL: http://cybersecurityventures.com/cybersecurity-market-report/
[27] Filkins, B. (2016) IT Security Spending Trends. SANS
[28] The White House (2016) FACT SHEET: Cybersecurity National Action Plan. URL: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

SELECTED CYBER SECURITY TECHNOLOGIES AND THEIR LIKELY ADOPTION TIMELINE IN THE MOBILITY SECTOR [29]

TECHNOLOGY	DESCRIPTION	ANTICIPATED PROGRESS IN THE MOBILITY SECTOR BY		
		NOW	2021	2026
ADVANCED THREAT DETECTION	A set of technologies that are used to aid the detection of computer network intrusions that are part of targeted attacks.	Early Adoption	Widespread Use	Widespread Use
DIGITAL FORENSICS	A branch of forensic science encompassing the recovery and investigation of material found in digital devices.	Early Adoption	Widespread Use	Widespread Use
NANOCOMPUTING	Nano-computing is the class of extremely small and low cost computer devices for boundary defence and secure network engineering	Early Adoption	Widespread Use	Widespread Use
NEAR FIELD COMMUNICATIONS	A short-range high frequency wireless communication technology used for controlled access	Early Adoption	Widespread Use	Widespread Use
NEXT GENERATION FIREWALLS	Augment the capabilities of traditional firewalls through the ability to identify the user as well as the IP address, inspecting encrypted traffic, and conducting intrusion prevention.	Early Adoption	Widespread Use	Widespread Use
PENETRATION TESTING TOOLS	Involve the use of multi-step attack scenarios to find vulnerabilities in computer systems	Early Adoption	Widespread Use	Widespread Use
PREDICTIVE ANALYTICS	A range of analytical and statistical techniques that can be applied to data to determine potential future events or behaviours	Early Adoption	Widespread Use	Widespread Use
BIG DATA ANALYTICS NETWORK MONITORING	Analysis of significant and dispersed datasets for intelligence gathering, user profiling, and intrusion detection.	Prototype	Early Adoption	Widespread Use
CLOUD SECURITY	Defence of cloud computing platforms, where users share resources to achieve economies of scale	Prototype	Early Adoption	Widespread Use
CONTEXT-AWARE	Delivery of personalised information to the user	Prototype	Early Adoption	Widespread Use
COMPUTING	Based on their identity, previous interactions and preferences, including controlled access			
CRYPTOCURRENCIES	An electronic based medium of exchange that is created, transferred, verified and stored electronically	Prototype	Early Adoption	Widespread Use
DISTRIBUTED LEDGER TECHNOLOGIES	Cryptographically stored records of transactions stored, verified and synchronised in a distributed manner	Prototype	Early Adoption	Widespread Use
HIGH SECURITY WIRELESS NETWORKS	Enhanced security protocols for Wireless communications for civilian use	Prototype	Early Adoption	Widespread Use
HOMOMORPHIC ENCRYPTION	Processing data while it is still encrypted, without the need to decrypt the data	Prototype	Early Adoption	Widespread Use
CRYPTOGRAPHY	Technologies for the secure transfer and sharing of data and functions.	Prototype	Early Adoption	Widespread Use
ARTIFICIAL INTELLIGENCE	Use of artificial learning and insights systems for the purpose of user monitoring and security incident detection and response.	Concept	Prototype	Early Adoption
AFFECTIVE COMPUTING	Systems and devices that can recognise, interpret, process, and simulate human affect	Concept	Concept	Prototype
POST-QUANTUM CRYPTOGRAPHY	Cryptographic algorithms secure against an attack by a quantum computer	Concept	Concept	Prototype
SMART MACHINES	Use of machine learning techniques to perform or augment traditional human tasks	Concept	Concept	Prototype
SOFTWARE-DEFINED NETWORKS	Separates the network control from the actual forwarding functions, allowing network control to be centralised in software and not devices	Concept	Concept	Prototype
WIRELESS MESH NETWORKS	Communications networks that use a mesh topology	Concept	Concept	Prototype

TECHNOLOGY IS BECOMING MORE INTEGRAL TO MOBILITY EXPERIENCE

Since its inception, technology has always played a pivotal role in the operation, management and experience of transport. The next 10 years will see a paradigm shift. As demand for information and user experience increases, so does the demand for their connectivity. While this demand will also be driven by supply, consumer experience and expectation is crucial.
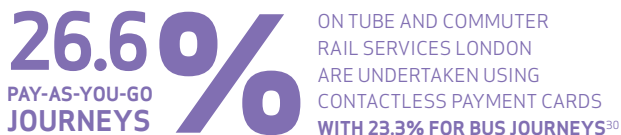
HIGHWAY TRAFFIC MANAGEMENT SYSTEMS:

550 MILES OF MOTORWAY TO BE MANAGED OR SMART MOTORWAYS IN THE UK **BY 2023**

RAILWAY SIGNALLING:

£644 MILLION SPEND ON RAILWAY SIGNALLING RENEWALS BY NETWORK RAIL IN 2014/15

PUBLIC TRANSPORT TICKETING SYSTEMS:

26.6% **PAY-AS-YOU-GO JOURNEYS** ON TUBE AND COMMUTER RAIL SERVICES LONDON ARE UNDERTAKEN USING CONTACTLESS PAYMENT CARDS **WITH 23.3% FOR BUS JOURNEYS**[30]

AIR TRAFFIC CONTROL:

£10 MILLION THE **ESTIMATED SAVING BY 2019** FROM THE DELIVERY OF DEPARTURE PLANNING INFORMATION TO **7 UK AIRPORTS**[31]

MARITIME SERVICES SECTOR:

£22.2 BILLION IS THE GROSS ADDED VALUE FROM THE UK MARITIME SERVICES SECTOR IN 2013[32]

MOBILITY APPLICATIONS:

54% OF UK TRAVELLERS CONSIDER THEIR SMARTPHONE TO BE ESSENTIAL TO THE TRAVEL EXPERIENCE[33]

Technology has quickly become a key part of the transport experience. Companies shipping goods want to know where their shipments are – in real time. Consumers, both individuals and organisations, are using technology to tailor their experience of mobility to their needs. This makes an important shift in the sector: away from supply-led and toward demand-led service, or the emergence of Mobility as a Service. It represents a move from personally owned transport modes to mobility solutions that are delivered as a service. As data becomes more available, and technology continues to advance, consumer behaviour adapts and supports this Mobility as a Service expectation.

[29] TSC own analysis.
[30] Transport for London (2016) Commissioner's Report – 3rd February 2016. URL: http://content.tfl.gov.uk/board-160203-item05-commissioners-report-v2.pdf.
[31] TSC own analysis.
[32] Oxford Economics (2015) The economic impact of the UK maritime services sector. Oxford Economics.
[33] Transport Systems Catapult (2015) Traveller Needs and UK Capability Study. Transport Systems Catapult.

AN INDUSTRY-WIDE APPROACH IS SHAPING UP

It is widely acknowledged across the transport sector that cyber threats are a major risk to operations and the industry in general – and that an industry-wide response is required to deal with this. While this shared thinking is reassuring, there are different technological standards and approaches to cyber security being taken across mobility, which highlights a clear need to manage security principles holistically

> " The effort being put into secure systems has significantly increased over the last few years. But our security practice needs to be as pervasive as the threat we face. Not just as an industry, but as a society we are nowhere near that level.

With an anticipated increase in the number and complexity of cyber attacks across all areas of transport, there are well-documented studies on the financial implications and reputational damage. For UK business, this is estimated to be worth £2.9 million.[34] A holistic view is not just desirable, but is essential.

This holistic view to security has been established in the security profession for a long time. The adoption of common security standards and principles of security has aided in this. But owing to the scale of threat faced, this holistic view needs to be reflected across the mobility sectors, and not just by technology professionals.

The next 10 years will necessitate a proactive move towards addressing cyber security as a cross-mobility issue. There are already signs that a significant shift is taking place within the mobility sector. Globally, the number of board of directors participating in information security has increased significantly[35], an essential first step for organisations to tackle this issue holistically. The automotive and critical infrastructure sectors are significantly increasing their investment in developing their cyber security capabilities.[36]

Most encouragingly, there are signs that specific sectors are developing common strategies and coordinating actions. Guidelines on such coordination have been published by organisations such as the International Maritime Organization[37], IATA's Cyber Security Toolkit[38], and the European Agenda in Security.[39] In the UK, the Automotive Council is actively considering cyber security as an issue, and the Railway Safety and Standards Board is undertaking work to develop a cyber security strategy for the railways.

Underpinned by significant government initiatives and risk-based frameworks such as the US National Institute of Standards and Technology's Cyber Security Framework, the emerging signs are encouraging. However, to meet the intelligent mobility cyber security proposition, more work needs to be undertaken to take this coordination to the next level of cross-mobility coordination. This is a task not just for security professionals, but all of mobility working collaboratively.

[34] Oxford Economics (2014) Cyber-attacks: Effects on UK Companies. CPNI.

[35] PwC (2016) The Global State of Information Security Survey 2016 – Key Themes. URL: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html

[36] Global Industry Analysts (2016) Critical Infrastructure Protection Market Trends. URL: http://www.strategyr.com/MarketResearch/Critical_Infrastructure_Protection_CIP_Market_Trends.asp

[37] International Maritime Organization (2016) Maritime Safety Committee (MSC), 96th session, 11-20 May 2016. URL: http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-96th- session.aspx

[38] IATA (2016) Aviation Cyber Security Toolkit – 2nd edition. URL: http://www.iata.org/publications/Pages/cyber-security.aspx

[39] European Commission (2016).

PRIVACY WILL BE AN ONGOING CONSUMER DEBATE

Since its inception, technology has always played a pivotal role in the operation, management and experience of transport. The next 10 years will see a paradigm shift. As demand for information and user experience increases, so does the demand for their connectivity. While this demand will also be driven by supply, consumer experience and expectation is crucial.
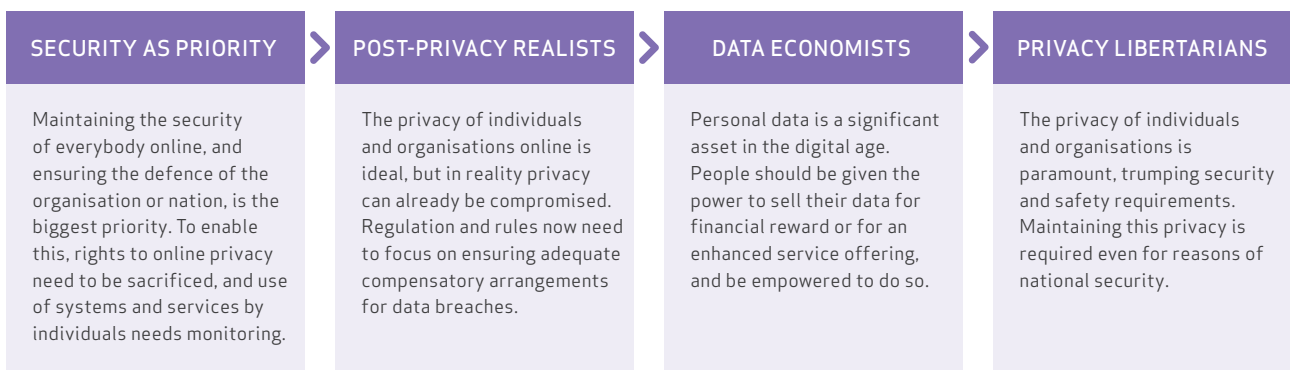
Today's privacy debate focuses on encryption and anonymity. This has progressed from early national security concerns, and looks set to evolve yet again. As the internet becomes even more pervasive, and consumer relationships with data change, the debate develops in a more complex way.[41] At the crux of this is consumer awareness of the way systems work, how they are secured and the implications of their actions on data and privacy. Most transport systems users are not experts, so interpretations and understanding varies. However, behavioural evidence suggests that this does not yet translate into an application of online activity.[42]

Our research identified several key influencing groups in the privacy and security debate, ranging from those with security as an absolute priority, to those with priorities on privacy. Our interviews incorporate perspectives from across this spectrum. These views are likely coalesce around both business opportunities, and wider social debates about privacy and security.

35%

OF CONSUMERS HAVE MADE PURCHASING CHOICE DECISIONS BASED UPON PRIVACY CONCERNS[40]

SECURITY AS PRIORITY	POST-PRIVACY REALISTS	DATA ECONOMISTS	PRIVACY LIBERTARIANS
Maintaining the security of everybody online, and ensuring the defence of the organisation or nation, is the biggest priority. To enable this, rights to online privacy need to be sacrificed, and use of systems and services by individuals needs monitoring.	The privacy of individuals and organisations online is ideal, but in reality privacy can already be compromised. Regulation and rules now need to focus on ensuring adequate compensatory arrangements for data breaches.	Personal data is a significant asset in the digital age. People should be given the power to sell their data for financial reward or for an enhanced service offering, and be empowered to do so.	The privacy of individuals and organisations is paramount, trumping security and safety requirements. Maintaining this privacy is required even for reasons of national security.

The privacy and security debate will continue to be central to an increasingly connected future. Meanwhile, the complexity of these issues has led to little action beyond compliance and general principles. Notable exceptions to this can be seen in market leaders such as Apple, who uses enhanced consumer data protection through encryption as a marketing opportunity.[43]

Nonetheless, as the World Economic Form argues, establishing global norms is difficult.[44] The fragmented privacy and security requirements of different nations and regions of the world, along with different approaches to security, data jurisdiction, legal enforcement (especially across borders), makes for a complex situation. Securing the privacy of organisational and consumer data, and complying with different cyber security requirements, is an ongoing challenge for those providing services at a global scale.

[41] Bott, E. (2014) In 2014, the debate over online privacy has become more muddled than ever. URL: http://www.zdnet.com/article/in-2014-the-debate-over-online-privacy-is-more-muddled-than-ever/

[42] Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S. (2015) "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. 2015 Symposium of Usable Privacy and Security.

[43] Poulsen, K. (2014) Apple's iPhone encryption is a godsend, even if cops hate it. URL: https://www.wired.com/2014/10/golden-key/

[44] World Economic Forum (2016) Resilience Insights. World Economic Forum.

SECTOR VULNERABILITY AND CYBER THREATS ARE EVOLVING

Whether deliberate or accidental, there are many known threats to the transport sector. For intelligent mobility, two new and ongoing issues will continue over the next 10 years. Firstly, market pressure for rapid innovation means security considerations are often subordinate if principles are not designed and established. With 99.9% of vulnerabilities compromised within year, even adequate security patching will not prevent exploitation.[46] Secondly, deliberate or intentional perpetrators can become rapid innovators. The relative risk posed by these individual threats is difficult to predict.

Our research indicates there are 5 key themes that define the changing nature of the cyber threat. The net result of these key themes is that the number and complexity of future cyber attacks is likely to increase. What makes this especially pertinent to transport is the cyber-physical and open nature of the systems operation. Given significant lag times in investment, these fundamental system properties are unlikely to change significantly. This means transport – and intelligent mobility – must carefully integrate security and safety into its culture.

> " Only amateurs attack machines; professionals target people.
>
> Bruce Schneier[45]

1. POTENTIAL ATTACKS ON TRANSPORT SYSTEMS WILL CONTINUE TO BE POSSIBLE – FROM ANYWHERE AND AT ANY TIME.

In the last two years, cyber attacks have become more targeted, and operations are bearing the hallmarks of organised and criminal operations.[47] They are, however, more difficult to detect.

2. MOTIVATIONS FOR INTENTIONAL CYBER ATTACKS ARE STILL LIKELY TO BE FOR FINANCIAL GAIN.

Interviews with thought leaders indicated a great focus on the cyber-physical element of securing transport systems. The most commonly attacked parts of the transport networks handled financial transactions, payment systems and conduits. And a new emerging threat was also identified: politically motivated attacks.

3. THE CYBER CRIME BUSINESS MODEL IS LIKELY TO BE MORE REFINED IN COMING YEARS.

Cyber attack models are often based on tried and tested exploits, coding and methodologies such as social engineering.[48] Instead of random attacks, cyber crime is turning towards a service model with a primary motivation of financial gain. Loose coalitions of hackavists, criminality and nation state sponsors are taking advantage of this to coordinate targeted attacks.

4. CYBER CRIMINALS ARE PREDICTED TO CONTINUE TO BE AMONG THE FIRST ADAPTORS OF NEW TECHNOLOGIES.

Thanks to intense competition, cyber criminals are testing and bringing new technological advances into their organisations at a pace that surpasses business, academia, and government. During 2014, groups of advanced hackers targeted five out of six large companies, a figure up 40% on the previous year.[49] Similarly, the cost of investigating, managing, and containing cyber crime activity will continue to rise as these alliances grow more complex, and the demands on regulators increases.[50]

5. THE INSIDER THREAT WILL HAVE MORE OPPORTUNITY TO CAUSE DAMAGE, WHETHER INTENTIONAL OR NOT.

A significant source of security incidents is still likely to be ones internal to mobility organisations. 76% of network intrusions originate from weak user credentials, and whilst the source of the attack may be external, taking advantage of poor internal user cyber hygiene and stolen credentials is a significant attack vector.[51]

[45] Schneier, B. (2000) Crypto-Gram. URL: https://www.schneier.com/crypto-gram/archives/2000/1015.html

[46] Verizon (2015) 2015 Data Breach Investigations Report.

[47] Trustwave (2016) Trustwave Global Security Report. URL: https://www2.trustwave.com/rs/815-RFM- 693/images/2016%20Trustwave%20Global%20Security%20Report.pdf
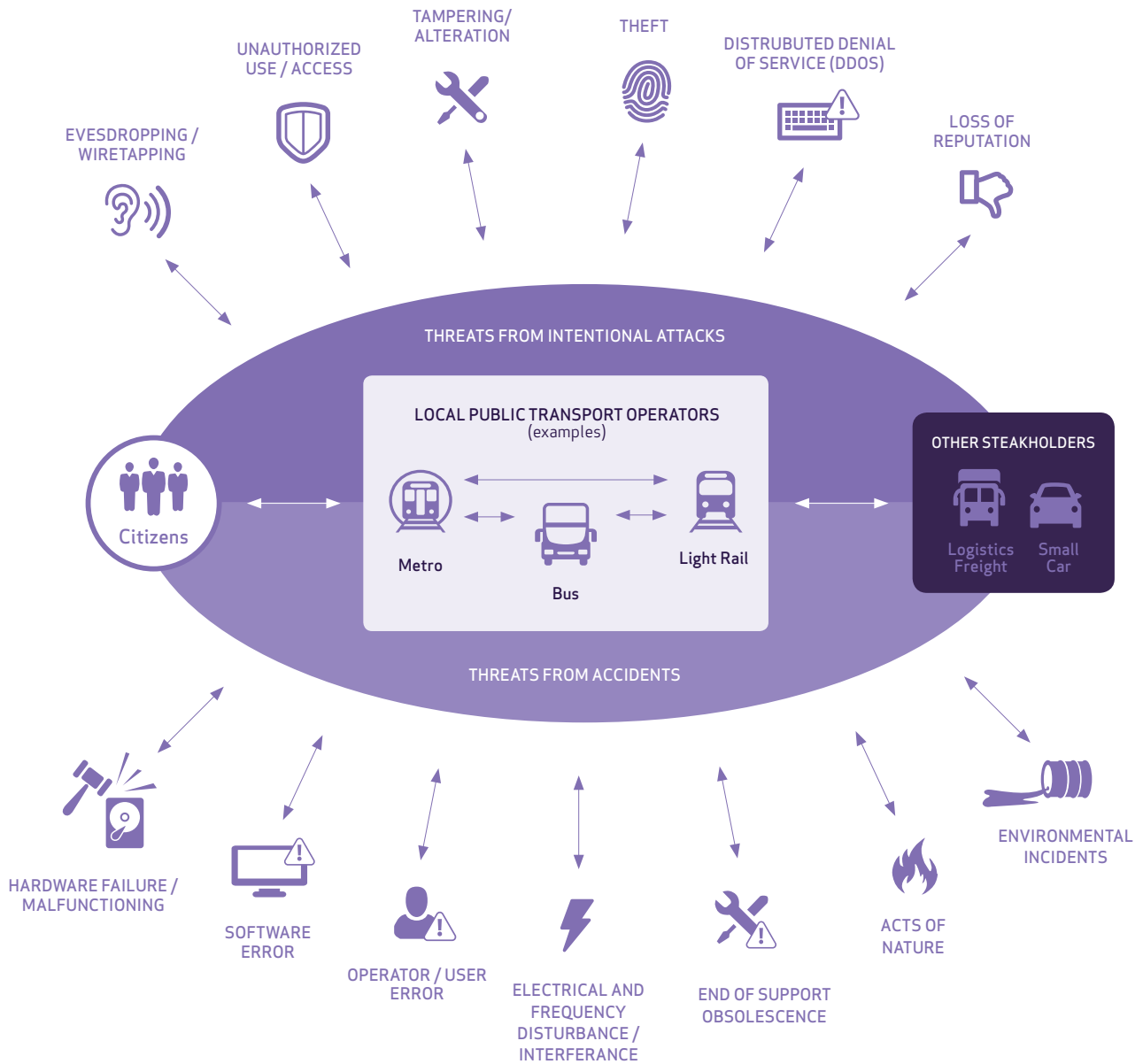
[48] Europol (2015) The Internet Organised Crime Threat Assessment 2015. URL: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

[49] Kuchler, H. (2015) Cyber criminals lead race to innovate. Financial Times. URL: http://www.ft.com/cms/s/0/94dcee3a-e21a-11e4-9995-00144feab7de.html#axzz4AJZlAztz

[50] Durbin, S. (2014) Cybercrime: The Next Entrepreneurial Growth Business? Wired. URL: http://www.wired.com/insights/2014/10/cybercrime-growth-business/

[51] Verizon (2016) 2016 Data Breach Investigations Report. Verizon.

ENISA'S KEY THREATS TO INTELLIGENT PUBLIC TRANSPORT SYSTEMS

EVESDROPPING / WIRETAPPING

UNAUTHORIZED USE / ACCESS

TAMPERING/ ALTERATION

THEFT

DISTRUBUTED DENIAL OF SERVICE (DDOS)

LOSS OF REPUTATION

THREATS FROM INTENTIONAL ATTACKS

LOCAL PUBLIC TRANSPORT OPERATORS
(examples)

Metro

Bus

Light Rail

Citizens

OTHER STEAKHOLDERS

Logistics Freight

Small Car

THREATS FROM ACCIDENTS

HARDWARE FAILURE / MALFUNCTIONING

SOFTWARE ERROR

OPERATOR / USER ERROR

ELECTRICAL AND FREQUENCY DISTURBANCE / INTERFERANCE

END OF SUPPORT OBSOLESCENCE

ACTS OF NATURE

ENVIRONMENTAL INCIDENTS

TRANSPORT IS A CRITICAL INFRASTRUCTURE

The UK government has classified its transport network as one of its 13 critical national infrastructures.[52] The loss or compromise of this infrastructure could have detrimental results on the UK's national security, defence, or the functioning of the state.[53] By coordinating action and establishing leadership across government departments, there is practical work taking place within the transport industry to develop its security capability.

Despite this focus, governance is currently a blend of public, private, and non-governmental models with different scales, rules and approaches. Future focus must go beyond traditional stakeholder models, and move towards flexible, collaborative and trusted cross-sector relationships for evolved governance.[54] For instance, the varying governance structures in the marine sector were identified as a risk – workers at sea could have greater allegiance to an information-rich society, instead of to employers or states.[55]

Similarly, there is no one-size-fits-all approach that can be applied to governing the cyber security space. Different industries are at different maturity levels, and cyber security is defined by a fast-changing, ever-innovating and present threat.

> UK Government, working with the Devolved Administrations and other responsible authorities where appropriate, will ensure that the UK's most important organisations and companies, including the critical national infrastructures, are sufficiently secure and resilient in the face of cyber attack. Neither the Government nor other public bodies will take on the responsibility to manage this risk for the private sector, which rightly sits with boards, owners and operators. But the Government will provide support and assurance proportionate both to the threat these companies and organisations face, and to the consequences of their being attacked.

The National Cyber Security Strategy 2016 to 2021

EMERGENCY SERVICES · CHEMICALS · COMMUNICATIONS · DEFENCE · ENERGY · FINANCIAL SERVICES · FOOD · GOVERNMENT · HEALTH · CIVIL NUCLEAR · SPACE · TRANSPORT · WATER
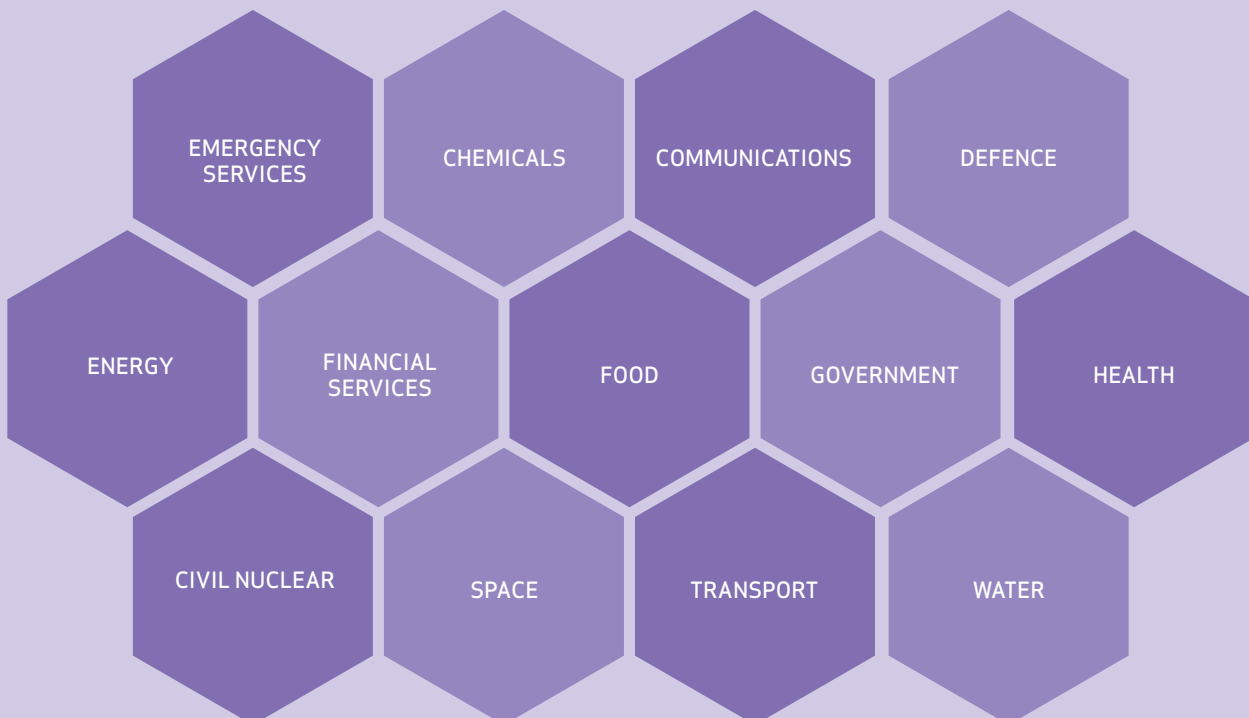
[52] Cabinet Office (2010) Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Cabinet Office

[53] Centre for the Protection of National Infrastructure (2016) About CPNI – The national infrastructure. URL: http://www.cpni.gov.uk/about/cni/

[54] Verhulst, S.G., Noveck, B.S., Raines, J., and Declercq, A. (2014) Innovations in Global Governance: Towards a Distributed Internet Governance Ecosystem. URL: https://www.cigionline.org/sites/default/files/gcig_paper_no5.pdf

[55] Fitton, M., Prince, D., Germond, B., and Lacy, M. (2014) The Future of Maritime Cyber Security.

The UK Government's National Cyber Security Strategy identifies that the National Cyber Security Centre, in partnership with government departments and regulators, will provide a number of services to support the most important organisations and companies. These include:

- Share threat information that only Government can obtain, providing intelligence against attacks which these organisations can defend themselves against;

- Define what good cyber security looks like – in partnership with industry and academia – and provide appropriate guidance and support;

- Stimulate the introduction of high-end security needed to protect the critical national infrastructure, and;

- Conduct exercises with critical national infrastructure organisations to test their capabilities, and help manage their vulnerabilities.

SAFETY AND SECURITY ARE TWO SIDES OF THE SAME COIN

This emerging and evolving threat landscape also poses another challenge to the mobility sector, and onbe that was commented on by many of those who we interviewed. The increasing potential for cyber attacks to do physical damage and harm means that safety and security will increasingly be seen as a whole, not as separate activities.

Modern transport systems fuse physical and digital assets in complex network architectures. Control systems are prone to threats like natural hazards, accidental and intentional damage, and physical wear and tear. These systems can cross locations of great distance (for example railway lines) or cause considerable disruption if tampered with (for example busy highway junctions).

As legacy transport systems become more connected, securing the information communication technology (ICT) infrastructure becomes an art form for physical and information security. The physical operation of ICT-enabled vehicles or other assets, cyber security and physical safety become more interdependent on one another.

CHALLENGES POSED BY INTELLIGENT MOBILITY

Cyber Security poses many significant current challenges to the transport sector. These are well known, identified, and to some degree are being tackled. While our research indicates that these issues need to be addressed, the focus of this paper is the future, and intelligent mobility. As a result, these challenges affect the UK's realisation of a secure intelligent mobility vision.

These challenges have been grouped and defined by the following headings:

•   **Setting solid foundations upon which a secure intelligent mobility should be based**

•   **Developing intelligent mobility's cyber security proposition**

•   **Delivering the value of intelligent mobility securely**

The grouping of these challenges reflects a level of urgency of action to enable a secure future for intelligent mobility. This is not to dictate timescales, as all challenges need to be met to fully realise the future of intelligent mobility.
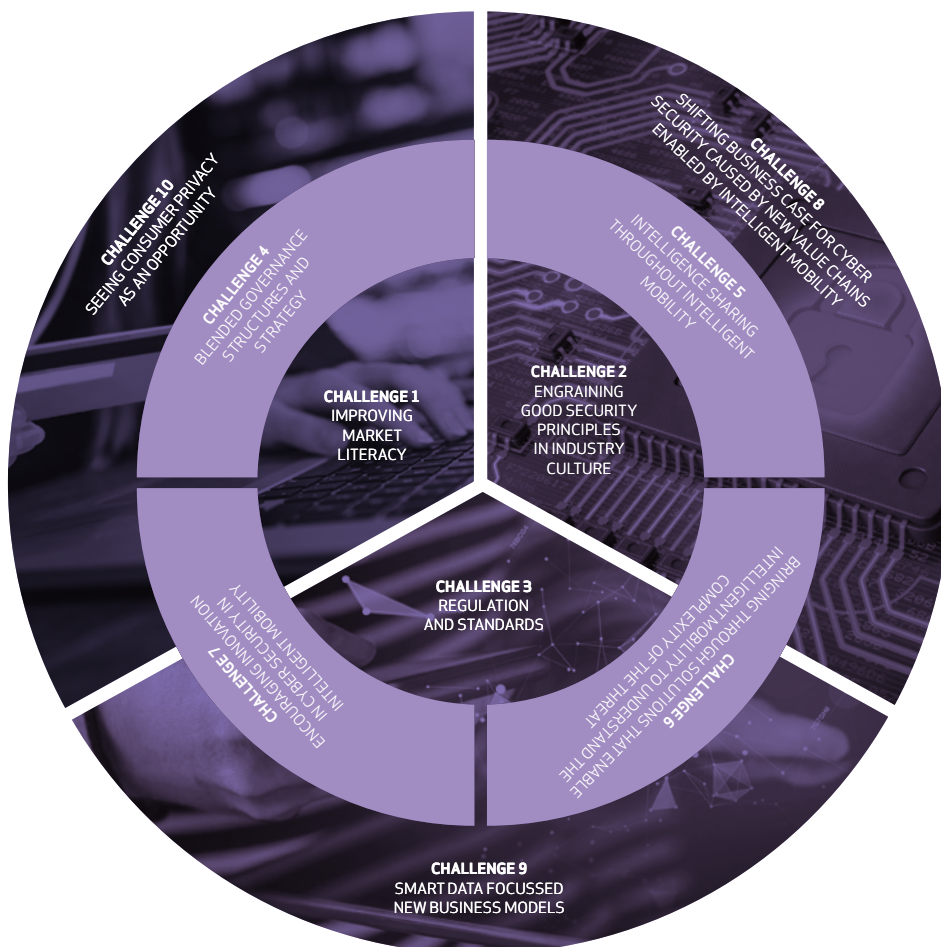
SETTING SOLID FOUNDATIONS

Challenge 1 – Improving market literacy

The UK has significant cyber security capability – particularly in the defence and financial sectors – and yet a common message from our interview was the current lack of understanding of the cyber security and transport markets. From the cyber security market, common issues reported are: Who is responsible for what? Who is my potential customer for my technology? What standards do I have to meet to have my product approved in a particular market?

Similarly, transport providers reported that a common approach to purchasing is to either embed security risks into big tenders, or approach a major software or security vendor. This reduces opportunities for SMEs and innovative products to be delivered to market.

This is not to say that both parties are not aware of cyber risks, but there is a significant difference between awareness and literacy.[57] Part of this issue is about understanding the nature of the risk on both sides. The cyber security industry understands the cyber risk, but is unsure where liability for cyber security lies within transport industries. This perpetuates an issue of racing to tackle current issues, as opposed to the issues presented by intelligent mobility.

85% OF BUSINESS EXECUTIVES

CONSIDER THEIR BOARD OF DIRECTORS' CYBER SECURITY LITERACY TO BE GOOD OR EXCELLENT, COMPARED TO **54% OF IT PROFESSIONALS**[56]

Challenge 2 – Engraining good security principles in industry culture

A critical challenge for this is skills. Globally, the supply of relevant skills struggles to keep pace with demand for it, with all industries claiming they have a problematic shortage of skills. The UK government has already committed to taking action to embedding cyber security expertise in new STEM graduates.[59] Analysis undertaken as part the Intelligent Mobility Skills Strategy indicates that intelligent mobility is likely to place further demand on such cyber capability.

However, this is not just about ensuring there is a core capability, it is also about a much wider issue of cyber security literacy. Transport prides itself on its safety culture. A mix of awareness-raising, training and leadership, and making the safe thing do the easiest thing to do, has created a culture where any preventable incident is unacceptable. A similar approach to cyber security also needs to be part of the industry's culture if it is to tackle the cyber threat in a world of intelligent mobility.

75% OF IT PROFESSIONALS

SAY THERE IS A SHORTAGE OF CYBER SECURITY PROFESSIONALS IN THE UK[58]

Challenge 3 – Regulation and standards

Our research indicated that in relation to the protection of critical national infrastructure, regulation is expected. In relation to safety-critical systems, regulation was desired by some of our respondents, although this needs to be balanced against potentially reducing innovation investment and raising barriers to entry.

But what was most desired is clarity over standards relating to specific aspects of intelligent mobility – notably autonomous cars – and cyber security. The complexity of the standards landscape was a common comment, and whilst work has been undertaken in specific areas in this space – notably standard J3061 on Cybersecurity for Cyber-Physical Vehicle Systems – the many technologies and systems in the whole intelligent mobility space necessitates clarity to aid delivery.

[56] TripWire (2015) The Cyber Security Literacy Confidence Gap. TripWire

[57] TripWire (2015) The Cyber Security Literacy Confidence Gap. TripWire

[58] Intel Security and Center for Strategic and International Studies (2016) Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills. Intel Security

[59] Department for Business, Innovation, and Skills (2014) Cyber Security Skills – Business Perspectives and Government's next steps. HMSO

[60] European Commission (2016) Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber threats. URL: http://europa.eu/rapid/press-release_IP-16-2321_en.htm

DEVELOPING INTELLIGENT MOBILITY'S SECURITY PROPOSITION

Challenge 4 – Blended governance structures and strategy

Current industry governance models with responsibilities for tackling cyber threats are siloed in operation, are heavily reliant on government to mandate change, and have little overarching strategy for coordinating work amongst industry players. In a connected future, such governance models will be unsustainable if intelligent mobility wishes to adequately tackle the level of cyber threat posed to it.

Securing intelligent mobility will necessitate a change in security governance structures in current transport sectors. This will include experimentation with new distributed and collaborative governance, which manages risk at an organisation and system level across sectors, and importantly is adaptive to a changing cyber threat landscape.

€1.8BN TO BE INVESTED IN DEVELOPING CYBER SECURITY CAPABILITY BY THE PUBLIC PRIVATE PARTNERSHIP ON CYBERSECURITY SIGNED **BETWEEN THE EU AND THE CYBERSECURITY INDUSTRY**[60]

Challenge 5 – Intelligence sharing throughout intelligent mobility

Effective collaboration for dealing with the scaling up of cyber security issues relating to intelligent mobility will require significantly more intelligence sharing amongst all organisations active in intelligent mobility. There are numerous initiatives currently in place for organisations to share intelligence about the cyber threats that they are experiencing. For instance, the Centre for the Protection of National Infrastructure facilitates a number of information exchanges to perform such a role, including the Transport Sector Information Exchange and the Aerospace and Defence Manufacturers Information Exchange.

The challenge is that current intelligence sharing is not pervasive within the transport industry, and also carries a significant time lag between detection and sharing an issue. Where multiple attacks across an industry are occurring in real time, this makes coordinating action to deal with the threat more challenging. Such joint action needs to be built upon a system of sharing trusted intelligence, in real time, with appropriate levels of information required to coordinate a response.

Challenge 6 – Bringing through solutions that enable intelligent mobility to understand the complexity of the threat

Threats to key actors in intelligent mobility are becoming increasingly complex as perpetrators of intentional attacks and technologies become more sophisticated. Those working in intelligent mobility will not only need to be more aware of the evolution of the threat facing them, they will also need to be aware of threats to other actors, who may not be within their own industry, which may in turn affect them through an increasingly connected ecosystem.

There is considerable uncertainty as to how these threats will emerge over time. New technologies are likely to be rapidly adopted by those wishing to cause harm via a cyber attack, and coalitions between threat actors are likely to become more common. Technology suppliers such as IBM, Microsoft, Kaspersky Labs, and NCC Group are investing significantly in digital forensics and other capabilities to allow customers to better understand the nature of the threat facing them.

Challenge 7 – Encouraging innovation in cyber security in intelligent mobility

Current innovation ecosystems in the UK are tailored towards developing general capability in cyber security. While intelligent mobility can benefit such ecosystems and there is considerable scope to transfer capability from sectors such as banking, a focus is required on developing intelligent mobility's innovation capability in cyber security.

Some capability is being established in specific areas of mobility. For instance, one of the areas of consideration for Innovate UK's recent Connected and Autonomous Vehicles funding call is automotive cyber security. But the combined challenge of intelligent mobility remains relatively unexplored. For the UK to be a leader in cyber security for intelligent mobility, this needs to change.

DELIVERING THE VALUE OF INTELLIGENT MOBILITY SECURELY

Challenge 8 – Shifting business case for cyber security caused by new value chains enabled by intelligent mobility

The challenge posed by intelligent mobility is that instead of generating new revenue for operators and infrastructure owners, intelligent mobility will shift existing value generated in transport, for example to Mobility as a Service providers. This will fundamentally change the business case for cyber investment for many organisations, particularly if value is shifted away from organisations with a significant cyber-physical presence, such as infrastructure operators.

£1.46
TO £3.14 MILLION

IS THE AVERAGE COST TO A LARGE ORGANISATION IN THE UK OF A DATA BREACH[57]

Challenge 9 – Smart data focussed new business models

Data is critical to generating new value in the world of intelligent mobility. One of the key balancing acts facing organisations in intelligent mobility will be to collect enough data so as to provide a useful and sustainable service and to innovate, and not so much as to be an attractive proposition for potential attackers. Intelligent mobility may be required to shift away from business models based on big data, to business models based on smart data.

Underpinning this will be robust risk and data management processes that should be an essential prerequisite for all intelligent mobility organisations.

Challenge 10 – Seeing consumer privacy as an opportunity

While the debate over security and privacy will continue over the forthcoming 10 years, it is important to realise that privacy in itself also poses a business opportunity as well as a risk that requires managing. Already many companies are identifying protecting the privacy of their customers as a unique selling point with significant potential value in a time where cyber security is becoming more a consumer concern.[63]

Domestic laws and international agreements, such as the EU-US Privacy Shield, are constantly evolving, and new solutions will need to be sensitive to this context. An emergent trend in such legislation as EU Regulation 2016/679 is around enabling citizens to access and take ownership of their personal data, as well as a right to be forgotten. These pose opportunities for mobility organisations to build privacy-based business models and to minimise opportunities for external attackers to access personal data.

European Data Protection Reform – New Rights for Citizens

• Citizens have the right to be forgotten where there are no legitimate grounds for retaining it

• It is easier for citizens to access to their own personal data

• Everyone has a right to transfer personal data from one provider to another

• Citizens can only give consent on use of their data by means of a clear, affirmative action

• Organisations being more transparent about how consumer data is handled

• Businesses and organisations must inform customers about data breaches without undue delay

• Better enforcement of data protection rights through administrative and judicial remedies

• More responsibility and accountability for those processing personal data.[62]

---

[61] HM Government (2015) 2015 Information Security Breaches Survey. HM Government

[62] Jourova, V. (2016) How does the data protection reform strengthen citizens' rights? European Commission

[63] Weaver, N. (2016) Can We Make The Internet Of Things "Secure Enough?" Backchannel. URL: https://medium.com/@nweaver/can-we-make-the-internet-of-things-secure-enough-5849dd1c29f9#.tzko76pj6

SECURING INTELLIGENT MOBILITY – A SIGNIFICANT OPPORTUNITY FOR THE UK

Securing transport systems in the future world of intelligent mobility will involve overcoming a number of significant challenges, the most notable of those identified in research were explored in the previous chapter. Despite these challenges, the UK is well placed to be a global leader in this market thanks to three key attributes.

- ● BUSINESS CLUSTERS
- ● ACCELERATORS
- ● ACADEMIC CENTRES OF EXCELLENCE

NEWCASTLE UNIVERSITY

CSIT

QUEENS UNIVERSITY BELFAST

UNIVERSITY OF LANCASTER

UNIVERSITY OF BIRMINGHAM

GCHQ

UNIVERSITY OF BRISTOL

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF OXFORD

CYLON

UNIVERSITY OF KENT

UNIVERSITY OF SOUTHAMPTON

UNIVERSITY COLLEGE LONDON

IMPERIAL COLLAGE

UNIVERSITY OF SURREY

ROYAL HOLLOWAY

1. Transferable capability

The UK is one of the leading nations globally in terms of cyber security capability. This capability has been well-established in traditional sectors such as defence and security, and the UK has a track record of transferring this capability and applying it to other sectors.

Established clusters of cyber security capability include Great Malvern, South Wales, Oxford, Reading and Bracknell, and London. Many companies in these clusters have been formed from spin-outs of government institutions (such as GCHQ and DSTL) and larger companies (such as QinetiQ). Clustering initiatives such as the Malvern Cyber Security Cluster also cooperate on awareness campaigns, and improving capability of businesses locally. The UK is also home to Europe's first cyber security accelerator, CyLon.

The academic capability in cyber security research is also very strong. This has been facilitated through initiatives such as the Cyber Security Centres of Excellence, close relationships between Universities and government, and increasingly multi-disciplinary working such as the PETRAS Research Consortium and Hub. This research capability is now being applied to the transport sector through partnerships between universities and industry, particularly in the automotive sector. Yet relative to the research capability, commercialisation of this research is lacking.[64]
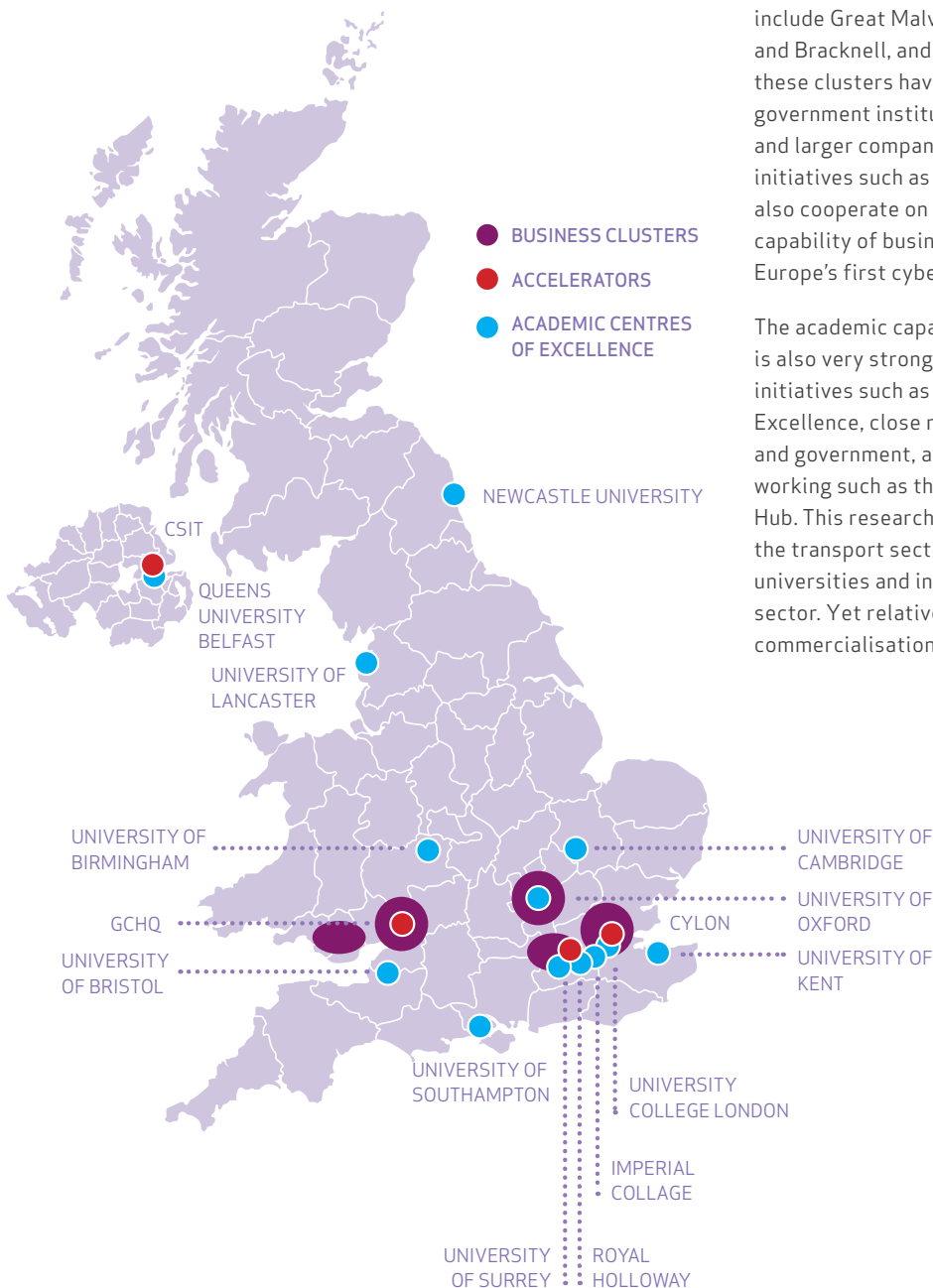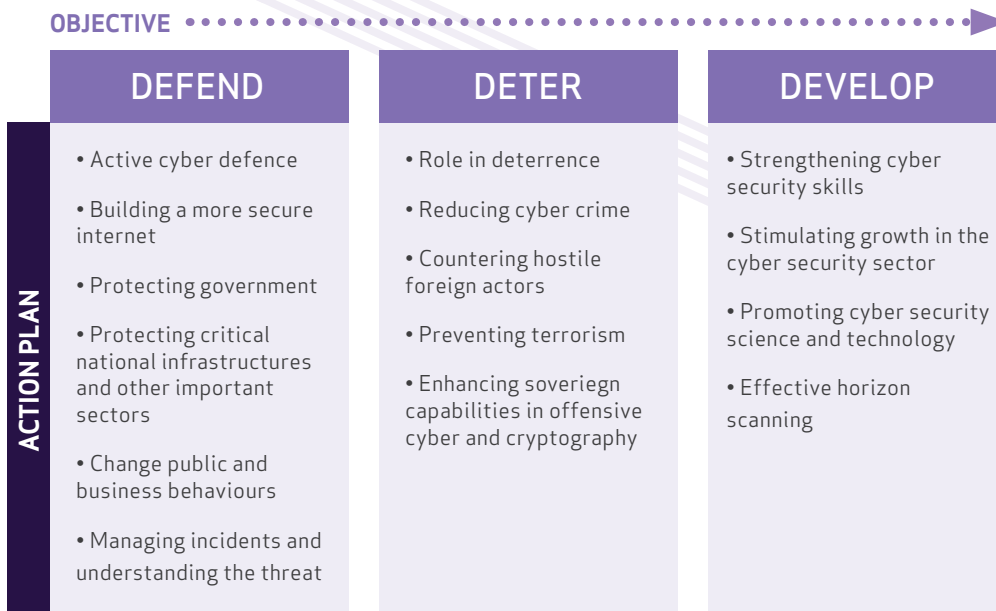
29

UK COMPANIES ARE ON CYBER VENTURES'S LIST OF 500 CYBER SECURITY COMPANIES TO WATCH IN 2016, MORE THAN ANY OTHER NATION OUTSIDE OF **THE USA**

[64] Pierre Audoin Consultants (2013) Competitive Analysis of the UK Cyber Security Sector. Department for Business, Innovation, and Skills.

The National Cyber Security Strategy 2016-2021 vision is that "the UK is secure and resilient to cyber threats, prosperous, and confident in a digital world." This will be achieved by the following objectives:

KEY AREAS OF FOCUS IN THE NATIONAL CYBER SECURITY STRATEGY 2016-2021

OBJECTIVE ➔

DEFEND	DETER	DEVELOP
• Active cyber defence • Building a more secure internet • Protecting government • Protecting critical national infrastructures and other important sectors • Change public and business behaviours • Managing incidents and understanding the threat	• Role in deterrence • Reducing cyber crime • Countering hostile foreign actors • Preventing terrorism • Enhancing soveriegn capabilities in offensive cyber and cryptography	• Strengthening cyber security skills • Stimulating growth in the cyber security sector • Promoting cyber security science and technology • Effective horizon scanning

ACTION PLAN

2. Supportive government cyber security and innovation policy

Importantly, UK government views the developing cyber security capability as more than for defence of the nation. It has shown willingness to make strategic interventions in the cyber security market to develop cyber security as an economic asset. This includes, and is not limited to, establishing organisational standards for cyber security, establishing a cyber security innovation voucher scheme, expanding the Cyber Security Information Sharing Partnership, developing international collaboration, and partnership working on educational initiatives.[65]

As well as transport being identified as a Critical National Infrastructure, intelligent mobility is viewed by government as a significant opportunity for the UK. Government has already established an Intelligent Mobility Fund[66], and is increasingly taking an interest in the implications of cyber security for intelligent mobility. For instance, as one of its major programmes of work the Centre for Connected and Autonomous Vehicles is exploring the implications of cyber security and how that shapes the opportunity for connected and autonomous vehicles.

3. The UK can deliver secure solutions that win in the long term

Most transport networks and services, and their associated information networks, are long-term investments. Sensors, actuators, control units, and other Internet of Things infrastructure will be in operation for more than 10 years. Cyber security (across the product lifecycle) will move from what is currently an afterthought to an essential business requirement, which are similar to requirements for safety. Even if the business demand for this is lacking, there is consensus within industry that government may consider legislating for this.

57% OF UK TRAVELLERS

WOULD NOT MIND SHARING THEIR DATA IN EXCHANGE FOR BETTER SERVICES[67]

---

[65] Cabinet Office (2013) The UK Cyber Security Strategy – Our Forward Plans. Cabinet Office.

[66] Department for Business, Innovation, and Skills (2016) Eight projects have been awarded £20 million in funding to develop the next generation of autonomous vehicles.
   https://www.gov.uk/government/news/driverless-cars-technology-receives-20-million-boost

[67] Transport Systems Catapult (2015) Traveller Needs and UK Capability Study. Transport Systems Catapult.

The emergence of the Internet of Things provides not just a challenge, it also presents an opportunity to design-in security from the start. As historic computer and information networks in the transport sector and beyond reach the end of their useful life, this provides an opportunity to build security into new systems. This requirement is likely to accelerate over the next 10 years, with pervasive security at the network level feasible within 20 years.[68]

Consumers see value in sharing their personal data in return for much improved mobility service. In addition, consumers are also increasingly concerned about the impacts of data breaches. Privacy is a business opportunity, with businesses that apply the correct formula of risk and reward as part of their mobility offering are likely to win.[69]

THE WAY FORWARD

The purpose of this report is to establish the future space of secure intelligent mobility. As the first step toward addressing the key challenges and opportunities that this space presents, this report acknowledges cyber security in intelligent mobility is fast becoming a critical issue that threatens to derail the evolution of the sector. Research has highlighted five key messages that the sector can no longer afford to ignore, along with five key observations that reveal a way forward.

KEY MESSAGES

1. Intelligent mobility is a new cyber security proposition.

The intelligent mobility cyber security proposition sits at the convergence of an increasingly automated transport network with newly established models of mobility, and the emergence of smart ecosystems. Significant work has been undertaken to understand elements of this proposition, such as in connected and autonomous vehicles, and some interactions at a systems architecture level, such as journey planning requests through application programme interfaces (APIs). This alone will not be enough in the future.

Transport consumers of the future will not demand individual elements of mobility at a time, they will demand products that combine and enable automation, new mobility models, and smart ecosystems. This scaled-up demand also scales up sources and opportunities for cyber attack over and above the current industry-specific focus. As the product demand broadens and becomes more specialised, so does the perspective, scale of cooperation, and services required to effectively secure the ecosystem.

The market for intelligent mobility products and services is rapidly developing, and will continue to do so over the forthcoming years. Now is the time to begin shaping this future in a secure manner.

2. The rapidly changing security and mobility landscape is likely to mean more cyber-attacks, more often, and potentially with more severe consequences.

Recent cyber attack trends show they are becoming more frequent, extensive, and the consequences are becoming more severe and pervasive. Every expert involved in research for this report expressed concern that this trend will continue and will be exacerbated with the Internet of Things, with particularly severe consequences for an increasingly cyber-physical mobility system. This can be avoided with new practices and significant changes in technologies.

While cyber security is well-established in the defence and financial sectors, intelligent mobility is still an emerging market. In many ways, existing transport sectors are also emerging markets – with basic literacy in cyber security often lacking in some sectors and supply chains.

There is evidence that this is beginning to change. Directors are increasingly establishing cyber attacks as operational risks and are playing more active roles in managing these risks. National and inter-governmental efforts have focussed investment and provided institutional frameworks to enable the development of cyber security capability in the mobility sector. This is welcome – just as looking to the future also requires a rapid pace of acceleration.

[68] Shannon, G. (2016) Why We're So Vulnerable. MIT Technology Review.

[69] Hoffman, D. (2014) Privacy is a Business Opportunity. Harvard Business Review. URL: https://hbr.org/2014/04/privacy-is-a-business-opportunity/

3. Understanding the nature of the existing issue is still a challenge.

Despite continuing efforts, cyber security itself is a complex, and often misunderstood area of practice. Many practitioners expressed frustration at continuing misconceptions about the evolving nature of the threat, and the lack of practised basic security skills. This also means that simply securing internal systems is not enough, because all organisations providing services within the mobility space need to contribute to a collective common requirement. This will then enable a secure ecosystem.

There is a practical manifestation of this as well. If basic security literacy is lacking, there is limited opportunity for new and innovative security products delivered to the intelligent mobility market. This not only impacts organisations in terms of system vulnerabilities, it also limits the potential market for new products, with corresponding impacts on investment in new products required to defend against future threats.

Critical to tackling this is sharing information, and upskilling the mobility sectors to meet the security demands of intelligent mobility. This is starting from a more general point on global shortages in cyber security skills. Collaborative efforts on skills initiatives are therefore required.

4. The UK is well-positioned to respond to the challenge.

While the challenge of intelligent mobility is a daunting one, the UK is well-positioned compared to other nations to respond to this challenge. With a significant market opportunity available to those supplying cyber security products to the mobility markets, as well as to mobility service providers who provide secure mobility solutions, this is an opportunity that UK businesses, academia, and government cannot afford to miss.

The UK has well-established cyber security capability in the defence and financial sectors, driven by requirements for national defence and the minimisation of economic losses in a technology-rich financial sector. This is built upon close cyber security industry partnerships with government, and those industries. Cyber security practice is beginning to emerge in some fields of mobility, notably connected and autonomous vehicles.

UK government policy not only supports enhanced cyber security capability to protect critical national infrastructures and to enable defence of the nation, it is critically enabling this sector as an area of economic competitive advantage. Partnerships between government, industry, and academia to enable new solutions for acceleration to market are a fundamental pillar upon which intelligent mobility will be secured.

5. Secure intelligent mobility requires a robust strategy and cultural focus.

The most striking common research interview theme was that technology is not necessarily the issue when it comes to cyber security. Even when considering the future of intelligent mobility, there was a consistent view that technologies could be delivered to market. Strategy and cultural change is needed to effectively protect intelligent mobility and realise the economic opportunity.

Current strategies relating to protecting mobility are typically modally focussed. Some initial studies and work has been undertaken to explore how elements of intelligent mobility converge, such as work by ENISA in Public Transport in Smart Cities. Even so, a strategy reflecting the challenges for intelligent mobility is required.

Many interviewees spoke of the requirement for mobility to take a similar cultural attitude to cyber security as it has successfully done to matters of safety. This shift to a 'cyber safety' culture will require significant effort over a number of years. There are five key opportunities the UK can take advantage of to address these messages.

NEXT STEPS

Significant cyber security work is already taking place across the different sectors of mobility. While this good work should not necessarily cease, the nature of the cyber threat is broad, and not sector specific, even if it manifests itself differently in each sector. This means while building sector-specific capability is an understandable first step, it will not deliver enough to deal with the challenge of intelligent mobility.

The future of cyber security and intelligent mobility is as complex as the challenges and opportunities it poses. The UK has few concerns developing technologies in cyber security, and it needs to focus on and develop a strategy that is specific to intelligent mobility. As a means of augmenting existing work, the findings of this report support the following recommended first steps forward.

STEP 1
Principles for securing intelligent mobility

Established principles of cyber security such as the Jericho Commandments have served the security industry well for many years. Now, though, security challenges posed by the Internet of Things, and the nature of the challenge posed by intelligent mobility, suggest that the future suitability of these principles must be challenged, certainly within the context of intelligent mobility. Once these principles are established (or existing principles are reaffirmed within the context of intelligent mobility), this acts as the basis for securing this new world of mobility.

PRIMARY ACTORS
Industry, academia, government

STEP 2
Technology and research roadmaps for securing intelligent mobility

There has been progressive work on the development of technology and research roadmaps to secure some aspects of intelligent mobility, for example the Cyber Security KTN recently developed notable work with a roadmap for connected and autonomous vehicles. Similar initiatives are required in the fields of new mobility models and smart ecosystems to coordinate technology research and development across a number of different fields. Such processes should place a particular emphasis on convergence with other mobility technologies, and the challenges associated with this.

PRIMARY ACTORS
Industry, academia, government, Innovation Centres, Catapults, Knowledge Transfer Networks

STEP 3
Upskilling the mobility sector workforce

A significant proportion of cyber-attacks can be prevented through basic cyber literacy provided to members of the workforce. While many mobility companies are already training members of their workforce with Cyber Essentials, more needs to be done to bring cyber security expertise into the mobility sector, and overcome current shortages for these skills. No single intervention will overcome these issues on its own. Cyber security must be placed as an essential skill for those working in intelligent mobility, coordinated at a national level, with the according level of support for skills development, funding, and courses.

PRIMARY ACTORS
Industry, academia, government

STEP 4
Transparency as standard across mobility domains

Initial work has taken place at the level of specific sectors and industry supply chains to enable transparency in vulnerabilities of technologies and sharing threat intelligence. The Information Exchanges established by the Centre for the Protection of National Infrastructure (CPNI) are good examples of these.
To secure intelligent mobility, this transparency and information exchange must be standardised across mobility and technology sectors. In addition to evolving existing threat intelligence exchanges to the challenge of intelligent mobility, opportunities to enable transparency in vulnerabilities of technologies – while protecting valuable intellectual property – requires ongoing research, action, and above all coordination across industries.

PRIMARY ACTORS
Industry, government

STEP 5
Accelerate cyber security innovation for intelligent mobility

The UK has excellent cyber security innovation capability already established, and much of this capability is already innovating in aspects of intelligent mobility – notably autonomous vehicles. Accordingly, there are several centres of excellence for innovating in cyber security, with more being established in this crowded landscape. The challenge and opportunity of intelligent mobility necessitates a focus of its own. Accordingly, plans should be developed and accelerated to further develop cyber security innovation capability in intelligent mobility. This will require close collaboration between several organisations and institutions to leverage existing strengths and capabilities.

PRIMARY ACTORS
Industry, academia, government, Catapults, Innovation Centres

APPENDIX A – RESEARCH PARTICIPANTS

Due to the often sensitive nature of cyber security, representatives from the following organisations were interviewed as part of this research project, and did not wish to be named. Additionally, a number of cyber security professionals also provided us with their perspective on the future of cyber security and intelligent mobility in a personal capacity, and did not wish for their companies to be identified.

To all 74 of these unnamed individuals, the project team owes its gratitude for their insight and perspectives that proved so valuable in producing this report.

ADS Group	ITS-UK
Association of Train Operating Companies	Jaguar Land Rover
BAE Systems	Lloyd's Register
Boeing	Network Rail
British Transport Police	NCC Group
BSI Group	Plextek
BT	PwC
Centre for the Protection of National Infrastructure	Quinetiq
Centre for Connected and Autonomous Vehicles	Qonex
Coventry University	Queens University Belfast
Cyber Security KTN	Rolls Royce
Deloitte	Railway Safety and Standards Board
Dell	Secure Smart Cities
Department for Transport	Smile Pass
Digital Catapult	Speedcast
DSTL	Thales
ENISA	Transport for Greater Manchester
Ericsson	Transport for London
First Group	TRL Ltd
GCHQ	UK Cards Association
Go-Ahead Group	University College London
IBM	University of Aberdeen
IO Active	University of Cambridge
IoT UK	University of Lancaster
Imperial College	University of Surrey
Innovate UK	University of Warwick
IQ Payments	World Economic Forum

Transport Systems Catapult ,
The Pinnacle,
170 Midsummer Boulevard ,
Milton Keynes,
MK9 1BP,
UK

Tel: 01908 359 999

www.ts.catapult.org.uk
linkedin.com/company/transport-systems-catapult
Twitter: @TSCatapult

CATAPULT
Transport Systems