OECDpublishing

DIGITAL SECURITY AND RESILIENCE IN CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES

OECD DIGITAL ECONOMY PAPERS

April 2019 **No. 281**

OECD
BETTER POLICIES FOR BETTER LIVES

This paper was reviewed by written procedure by the Committee on Digital Economy Policy (CDEP), Committee on Public Governance (PGC) and International Energy Agency (IEA), and approved and declassified by the Committee on Digital Economy Policy (CDEP) on 14 November 2018 and prepared for publication by the OECD Secretariat.

This publication is a contribution to the OECD Going Digital Project, which aims to provide policymakers with the tools they need to help their economies and societieise prosper in an increasingly digital and data-driven world.

For more information, visit www.oecd.org/going-digital

#GoingDigital

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/GD(2018)14/FINAL

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Foreword

This document brings together material from the OECD Going Digital Workshop on Digital Security and Resilience in Critical Infrastructure and Essential services, held on 14-15 February 2018 at the OECD Conference Centre in Paris.

Since the adoption of its first "Security Guidelines" in 1992, the OECD has been the only international organisation addressing digital security policy making from the economic and social perspective. Over the last 25 years, the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) and its parent body, the Committee on Digital Economy Policy (CDEP), have provided a unique international venue for dialogue and exchange of good practice in this area, and for the development of analytical work and policy recommendations.

As a horizontal exercise cutting across a vast array of the OECD's areas of work, the Going Digital project provided the opportunity to explore digital security issues in a more multidisciplinary manner by leveraging expertise across the organisation. Six OECD directorates and programmes brought their knowledge and networks together to organise a collaborative project in this area, consisting primarily of a Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services. Participants discussed digital security from different sectors (finance, energy, transports, government services) and perspectives (SMEs, civil society, academia, etc.).

This document brings together key messages from the workshop, an issues paper prepared to help develop the agenda, the workshop agenda (Annex A) and the proceedings from the discussions (Annex B).

The project benefitted from a financial contribution from the government of Korea.

The Secretariat wishes to thank the speakers and participants for their active engagement and lively discussions.

The project was co-led by the OECD Directorate for Science, Technology and Innovation (STI: Laurent Bernat and Suguru Iwaya), Directorate for Public Governance (GOV: Jack Radisch), and the International Energy Agency (IEA: Jan Bartos, George Kamiya and Jesse Scott). The initiative also involved the Directorate for Financial and Enterprise Affairs (DAF: Gert Wehinger and Leigh Wolfrom), the International Transport Forum (ITF: Tom Voege) and the Centre for Entrepreneurship, SMEs, Regions and Cities (CFE: Lucia Cusmano and Marco Bianchini). Benjamin Dean, consultant to the OECD, was the workshop rapporteur and helped prepare this document.

Speakers' bios and presentations are available at www.oecd.org/going-digital/digital-security-in-critical-infrastructure/.

Table of contents

GOING DIGITAL WORKSHOP ON DIGITAL SECURITY AND RESILIENCE IN CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES

KEY MESSAGES

On 15-16 February 2018 the Organisation for Economic Co-operation and Development (OECD) hosted a Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services. The workshop brought together over 120 participants to discuss the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructure. Over 25 experts discussed digital security in the financial, energy and transport sectors, in relation to the delivery of public sector services, and from the digital security public policy making perspective. Issues faced by SMEs were also addressed throughout the event (the agenda is available in Annex A).

This section reflects key cross-cutting high-level policy messages from the workshop. A more detailed account of discussions in each session can be found in the workshop proceedings section.

Digital transformation exacerbates digital security risk in critical infrastructure (CI) and essential services across sectors.

Many aspects of digital security risk are shared across sectors…

The adoption of common digital technologies (e.g. operating systems) and shared service providers (e.g. cloud providers), combined with the hyper-connectivity they involve, create digital dependencies across sectors and borders.

Digital transformation is blurring the lines between information technology and operational technology. The need to detect, prevent and respond to digital attacks is now a part of the risk landscape facing physical infrastructure operators in sectors such as energy and transport.

… increasing the potential for systemic, catastrophic disruptions…

If vulnerabilities in these common technologies are exploited or service providers experience disruptions, the impacts can be felt simultaneously across sectors. For instance, the NotPetya ransomware disabled many business computers through the exploitation of a common flaw in operating systems, affecting global logistics companies (e.g. Maersk) and interrupting supply chains in essential sectors such as health (e.g. Merck).

Moreover, digital disruptions to stakeholders in particular sectors (e.g. finance, energy) can cascade onto dependent stakeholders in other sectors. For instance, disruptions of retail payment systems (e.g. Visa, Mastercard) or interbank networks (e.g. Society for Worldwide Interbank Financial Telecommunication – SWIFT) could result in knock-on effects for the many financial institutions and businesses globally that rely upon these systems.

…. but there are also sector-specific differences and issues.

The pace of digital technology adoption and use varies across sectors, which is reflected in differing levels of sophistication and maturity of digital security risk management across those sectors.

In some sectors, such as energy and transport, operators of essential services use sector-specific digital technologies (e.g. smart grid or autonomous vehicles). This lowers the probability of widespread simultaneous failure but does not eliminate risk linked to sophisticated threat actors.

Digital transformation creates new risks in some sectors. For example, the vulnerabilities of new entrants, which are often SMEs (e.g. fintech), could increase uncertainty in the financial sector. The extension of electricity production to end users, by involving their information systems and networks, could also create additional weak points in energy value chains.

In the digital transformation, managing digital security risk increases the likelihood of economic and social benefits, but cannot entirely eliminate the risk.

Digital security risk is the consequence of ecosystems that are dynamic and complex …

An ecosystem is akin to a living organism. It evolves over time, has multiscale dynamics, contains interdependencies, and crosses borders. It is complex. As a consequence, it inherently contains uncertainty and risk.

Each essential sector comprises its own ecosystem of interrelated stakeholders and dynamics. It also exists within a broader ecosystem cutting across other sectors. Digital transformation amplifies the complexity, dynamism and interdependencies of such ecosystems.

… which precludes static or simplistic policy formulation.

Conventional thinking about digital security assumes that it is possible to create a “safe and secure” digital environment and seeks to attain control at the expense of potential benefits.

Yet digital ecosystems are constantly evolving due to technological change, threat adaptation, etc. Moreover, it is impossible to prevent all possible incidents over time with limited resources. This precludes an approach based on “silver bullets” with the goal of total safety and security.

Instead, digital security risk should be assessed and reduced to an acceptable level, aiming for enhanced resilience and preparedness.

Digital security risk cannot be eliminated but it is manageable. If handled effectively, the benefits of digital transformation to CI and essential services can be realised with minimal disruption and cost.

Given that widespread disruptions to critical infrastructures are possible, policies should aim at ensuring crisis preparedness and enhancing resilience. The application of general resilience principles (i.e. diversity, reserves, and modular open interfaces) can help to minimise negative impacts in the event of systemic disruption.

Risk assessment should include continual re-evaluation of what is deemed "critical"

Criticality can vary depending on the organisation in question (i.e. what part of the organisation is critical to what?); the part of a system or process in question (e.g. what part of election infrastructure is critical to what?); and at different points in time. Digital transformation requires to continuously re-evaluate what is deemed critical. The OECD's revision of its *2008 Council Recommendation on the Protection of Critical Information Infrastructure* is an opportunity to explore this concept in-depth.

Achieving resilience through risk management requires a whole-of-government, co-operative, and agile approach to policy.

Digital security risk is multidisciplinary…

Managing digital security risk, including assessing the impacts of CI failure, requires understanding of economic, social and technical dimensions. This includes sectoral specificities, competitive dynamics, incentive structures and public-private regulatory interplays. As a facilitator of cross-sectoral international dialogue, the OECD is well placed to play a role in this area.

… which requires the marshalling of multiple domains of expertise across government.

A whole-of-government approach facilitates the integration of digital security risk into national risk management. It brings together the required knowledge and understanding that may reside only within sector-specific or functionally-specific public organisations.

Co-operation and partnerships across many stakeholders are needed to effectively manage risks.

Operating effectively in a multi-disciplinary domain requires the involvement of many stakeholders across the ecosystem rather than siloed models. Relevant stakeholders include operators of CI and essential services; SMEs and startups; government regulatory agencies; digital products and services providers; standards making bodies; academia; and civil society.

Flexible and agile - rather than rigid and prescriptive - public policy is the best response to dynamic digital security risk.

The policy process has to incorporate differences of perspectives and situations among stakeholders. For instance, determination of what is "critical", as opposed to what is simply "important", differs depending on who is involved and under what conditions.

Stakeholders are ultimately responsible for managing their own risks. In the event certain risks are not adequately managed, a flexible and agile approach ensures that incentives – such as voluntary or mandatory measures – are implemented and adjusted appropriately.

Partnership-based policies can make concrete contributions to awareness raising, improved information sharing, and skills acquisition.

Collaboration and information sharing between public authorities and private sector operators are vital.

Mechanisms are needed to allow for risk-related information to flow across public-private sector boundaries, between large and small firms, along value chains, across sectors, across borders, etc.

There are many obstacles to sharing information between operators and the government, particularly internationally and at scale. These include lack of trust and perception of unbalanced reciprocity, fear of further exposure and legal liability due to incident reporting.

Policies can play a key role to remove these obstacles and create the conditions for trust as well as learning from failures. For example, ensuring two-way information sharing benefits all players through mechanisms such as Information Sharing and Analysis Centers (ISACs). ISACs function best when encouraged and supported by public policy that encourages private sector many-to-many information sharing and collaboration.

Policies can play a direct and indirect role in bolstering awareness and skills.

To some extent**,** awareness of digital security risk increases naturally as stakeholders gain experience, particularly when faced with incidents. However, policy can and does play a direct and indirect role in additionally raising awareness.

Improvements in digital security risk management practices can be triggered by policies in adjacent domains e.g. privacy protection with the implementation of the General Data Protection Regulation (GDPR).

Greater awareness has exposed deficits in digital security risk management skills (“digital security gap”) across stakeholders (particularly SMEs). These gaps appear at a general technical level, at a sector-specific level and in specific functional lines within organisations.

Policy can play a role in raising skill levels through vocational training that reflects the needs of the private sector; collaborative training schemes between public universities and the private sector; and the updating of primary/high school curriculums to ensure minimum levels of technological literacy.

Issues Paper

This draft issues paper aimed to support discussions at the OECD Going Digital Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services, which was held on 15-16 February 2018. Following the introduction below, it discusses digital security and resilience for the delivery of critical financial, energy, transport and government services. It then introduces the perspective of whole-of-government digital security public policy. Each individual section concludes with a list of questions for discussion at the workshop.

Introduction

The ongoing digital transformation of the economy and society promises to spur innovation, generate efficiencies and improve services. In doing so he hope is that it will support more inclusive and sustainable growth as well as enhance well-being. At the same time, new challenges are emerging. Foremost among them is the digital security and resilience of critical infrastructure and services, which are essential for the functioning of our economies and societies. These include financial services, energy (notably electric power) supply, and transportation systems, as well as key government services. While critical infrastructure often involves large operators, many small and medium-sized enterprises (SMEs) are reliant upon these infrastructures and/or digitally interconnected with essential services' value and supply chains. A holistic view across enterprise sizes is therefore necessary to properly appreciate and respond to risks introduced by digital transformation.

Digital security is not a new issue for critical infrastructure and essential services operators. Most of them began to adopt digital technologies several decades ago and, at various paces, have migrated from centralised, closed and isolated systems to open and globally interconnected digital networks. In doing so, they increased their exposure to new threats and vulnerabilities that cross organisational and jurisdictional boundaries. Over the same time period, threats have likewise evolved and vulnerabilities have both persisted and multiplied to a point where they now present unique challenges to organisations and governments around the globe.

Recent high impact incidents have increased general awareness of digital security challenges. Recent examples include the Wannacry and NotPetya attacks in May and June 2017, which caused temporary production shutdowns in many SMEs, at several global companies and government services (e.g. parts of the UK National Health Service) (Hern, 2017). Such widespread and visible consequences from this incident has transformed what may previously have been thought of as an abstract or hypothetical risk into a tangible and concrete risk across stakeholders.

While many companies remain silent about the damages incurred from digital security incidents, perhaps to protect their reputation or shield against legal liability, the scale of the economic impact from this particular set of incidents has led to information disclosures in some companies' quarterly financial statements. For example, the US pharmaceutical company Merck revealed a reduction in the company's third-quarter sales by USD 240 million after NotPetya disrupted the production of its GARDASIL 9 vaccine, which is used to prevent certain cancers and other diseases caused by the Human Papillomavirus 9. (Merck, 2017). European logistics company, A.P. Møller-Mærsk (2017), claimed in its interim Q2 2017 report that NotPetya resulted in EUR 200-300 million in negative financial impact.

Another striking example of possible large-scale impacts from a digital security incident is the December 2015 attack against the electric grid in Ukraine. This incident caused a black-out of up to six hours for approximately 225 000 customers thereby demonstrating the potential for significant disruption from a digital security attack on a critical infrastructure (Tuptuk and Hailes, 2016). For decades the potential for such incidents has been largely hypothetical (see for instance Clarke & Knake [2010] or Koppel [2015]). Yet again, recent events have concretely manifested what were previously hypothetical risks.

Three technological developments are driving digital transformation

As more and more countries around the globe become digitally-enabled and join the digital economy, we have reached an inflection point with respect to the use of digital technologies throughout society (i.e. 'digital transformation'). For example, within households, the number of connected devices in households in OECD countries is expected to be 14 billion by 2022 — up from around 1.4 billion in 2012, or to put it differently from 10 connected devices in a household with two teenagers to 50 in ten years' time (OECD, 2014). Within manufacturing and industrial facilities, use of sensors and semi-autonomous 'cobots' increases in the search for efficiency and safety gains (Holinger, 2016). At a city-level, efforts are underway in many OECD countries to integrate information systems around power and water production so as to reduce waste and costs (Jan Top, 2010; OECD, 2015a). At all levels of society these changes are being seen – benefits are being realised - and risks introduced.

Three key interrelated technological developments, among many others, are at the core of digital transformation:

- open hyperconnectivity through high-speed fixed and wireless broadband which enables data to flow globally, across jurisdictional and organisational boundaries and along global value chains;
- "Internet of Things" (IoT) technologies that bridge the physical and the digital worlds through sensors and actuators; as well as robots that enable the delivery of new services in the physical world; and
- data analytics and artificial intelligence, which facilitate the extraction of meaning and value from massive amounts of data to enable data-driven innovation.

The combination of these technologies enables the transformation of entire business activities, which can unleash new opportunities, lead to the development of new business models and create new sources of growth. Digital transformation integrates digital technologies into the core of all business functions, making it more difficult to separate or distinguish the digital from the non-digital in the value chain. This represents an evolution from previous decades during which Information and Communication Technologies (ICTs) were separated from operational technologies and primarily used to improve separate business processes in terms of increased productivity, reduced cost and/or enhanced quality.

Ultimately, entire sectors are expected to be transformed: automated vehicles will drive the evolution of the transport sector towards mobility services. This will in turn impact other areas such as insurance, urban planning and environmental protection. The decentralisation of electricity systems enabled by smart real time energy trading systems will deeply transform the energy sector. Innovations in financial technology, or Fintech, including mobile payments, are already shaking up the financial sector, with implications for the future role of banks and central banks. These innovations are often based on distributed ledger (DLT) or blockchain technology that have applications beyond finance and involve the transfer of rights, values or information without the need for a trusted third party.

Yet placing data, open networks and IoT devices – which often come along with increased digital security vulnerabilities – at the core of essential services' business models also expands considerably these services' exposure to operational risks and risks regarding integrity and confidentiality of information.

The consequences of such risks, if they materialise, can rapidly affect the core of business operations, as well as organisations' reputation, in addition to their competitiveness, ability to grow and innovate. As a result, digital security can no longer be viewed as only a technical matter but should rather be approached as an economic and social risk that should be managed in light of the economic and social activity supported by the digital technologies (OECD, 2015b).

For risk management in firms and governments, as well as for regulation, the challenge is to balance reaping the benefits of digital transformation against reducing the concomitant digital security risk. In many sectors, such as those that primarily process tangible assets (e.g. electricity or transportation), a significant cultural and organisational change is required.

The proliferation of connected devices, machines and structures; their reliance upon critical infrastructure and essential service operators to function; and the emergence of new and potentially systemic risks such as those outlined above, pose profound questions to operators as well as the government authorities under whose jurisdiction they fall. These include:

- Does digital transformation elevate the importance of public policy for the protection of critical information infrastructure?
- Is digital transformation changing how digital security and resilience are approached by critical infrastructure and essential services operators?
- How should digital transformation affect related public policies?
- Should whole-of-government policies aiming to make digital transformation work for the economy and society take into account digital security and resilience in critical infrastructure and essential services, or should this area be approached separately from the other challenges raised by digital transformation?
- Are operators in the financial sector better equipped to manage digital security risk than in the energy and transport sectors where digital transformation is perhaps a more recent phenomenon?
- To what extent are the threats they face and the mitigation measures they should take similar or different?

To answer these questions, and many others, it is necessary to better understand the commonalities and differences across critical infrastructure and essential services with respect to digital security in the age of digital transformation.

Small businesses play a role in innovating to manage digital security risks but also introducing their own

One important challenge of digital transformation across the finance, energy, and transportation sectors is the increasing role taken by SMEs in supply and value chains. While the attack surface of a smaller organisation may be lower, these organisations may have relatively fewer resources to dedicate toward the appropriate management of their digital security risk.

Within essential services' value chains, SMEs can be viewed by large central players, such as banks or electricity companies, as weak links within a digitally interconnected ecosystem. In this way, SMEs introduce risk outside of the traditional perimeter of larger organisations, which necessitates new collaborative and information sharing efforts than those used in the past.

At the same time, SMEs also include start-ups, some of which offer innovative services that can transform and sometimes disrupt essential services. These include payments, energy trading, or mobility services in the area of transport. Uncertainty around the impacts and future trajectory of these innovations introduce risk by their very nature, which requires organisations to revise their existing risk management plans to adapt to the changes. In all cases, the ability of SMEs to embed digital security risk management at the core of their innovations and operations is likely to become increasingly important into the future.

In this respect, raising awareness about digital security and strengthening workers' and managers' skills are especially important SMEs where the adoption of appropriate risk management strategies and practices may be required but underdeveloped. Training at all levels of the organisation – from the board and owners to managers and staff– will be key for digital security to be understood at a strategic level - including integration of consideration of the resilience of the business model against attacks or shocks – as well as operationalised in day-to-day activities.

The digital dependencies of all essential sectors raise new digital security risk management challenges

Digital security and resilience in critical infrastructure and essential services also requires consideration of dependencies and their effect on risk management. Different types of dependencies can cut across sectors and borders, which makes the development and implementation of policies challenging.

The first kind of dependency is one that is linked to widespread use of common digital infrastructure components. For example, a vulnerability affecting a digital component, on which many organisations and individuals depend, could be exploited. The disruption caused by exploitation could subsequently cause massive chaos and damages simultaneously across several if not all sectors that are dependent on that organisation. Such vulnerabilities could for example affect software, as in the aforementioned Wannacry and NotPetya attacks; microprocessors or other hardware components, as illustrated by "Spectre" and "Meltdown"; or essential elements of the core Internet, such as the Domain Name System, Internet Exchange Points or large Certificate Authorities. Although it did not affect critical infrastructures directly, the 2016 massive Denial of Service attack against the domain name provider Dyn took down access to numerous popular websites for a number of hours. This incident gives a glimpse as to the potential impact of large-scale interruption of Internet operations on economic activities.

Another type of digital dependency is when a digital security threat to an operator of critical infrastructure or essential service successfully propagates to other operators, within the same or in different sectors, eventually causing damages to a large range of services. This has led to recognition of the concept of "critical *information* infrastructure protection" (CIIP). A striking illustration of this possibility is the famous Stuxnet worm, discovered in 2010, which was initially designed to specifically target a nuclear enrichment facility in Iran and infected approximately 100 000 hosts in over 155 countries[1]. Fortunately, this occurred without resulting in damages beyond its intended target. Dependencies such as these suggest there is a need for co-ordination across sectors for example in the sharing of information on threats, vulnerabilities, incidents, risk management practice, and operational incident response.

A third category of dependency is the effect that disruption of an essential service in one sector - due to a digital security incident - might have on the delivery of an essential service in another sector. For example, a digital security incident that causes an electricity outage could result in disruptions of transport systems and hospitals in the outage's geographic area. This could in turn disrupt other essential services. In this case, the digital security incident would act as the root cause of knock-on effects – propagating a disaster along a chain of interdependent essential services. However, the digital security incident itself would not directly affect the second-level services. This dependency points to a need to integrate critical *information* infrastructure protection (CIIP) within the broader critical infrastructure protection (CIP) policy framework.

Lastly, the globally interconnected nature of digital technologies creates dependencies across borders, which may arise in combination with the aforementioned dependencies across sectors. The Denial of Service attack on Dyn, which is physically based on the United States East Coast, demonstrated this kind of dependency, as access to sites from Europe was affected by the incident. Given the possibility of these incidents, co-ordination at the domestic level should be complemented by regional and international co-operation both at the policy and operational levels (e.g. incident response, information sharing, etc.).

Cross-cutting issues

A number of cross-cutting questions also emerge given the numerous sectors, stakeholders and international nature of digital transformation in critical infrastructure and essential services. These include:

- **To what extent is digital transformation changing the protection of critical information infrastructures and the management of digital security risk?** How is the risk evolving along the value chain, including beyond/across sectors? Are "hybrid threats" as well as threats against confidentiality and privacy becoming increasingly challenging in relation to the protection of critical infrastructures and essential services against digital security risks? What is the role of individuals?
- **To what extent are cross-border and cross-sector dependencies addressed?** How can stakeholders take into account globally distributed digital infrastructures (e.g. Cloud computing) as well as potential systemic risk from widespread vulnerabilities (e.g. Meltdown and Spectre)?

[1] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

- **What are good policy practices to encourage digital security risk management by all organisations, including SMEs?** What is the right balance between mandatory and voluntary policy measures to protect critical infrastructures and essential services? What should be the respective roles of digital security agencies, public safety departments and sectoral regulators? Are SMEs a weak link in essential services' value chains?
- **How can governments foster trust in and between private operators to enable information sharing on threats, vulnerabilities and incidents?** How can they encourage information sharing between operators competing in the same sector? How can SMEs be included in trust frameworks?

Digital security risk in the financial sector

The financial system is responsible for managing, safeguarding and transferring ownership of financial assets within and across borders. The digital resilience of this system is therefore crucial for financial and economic stability throughout OECD countries. Digital transformation has led to many benefits, particularly in the payments space, including efficiency gains for financial institutions and added convenience for customers. New entrants to the market (e.g. SMEs) have in many cases driven these changes. However, these entrants also add new vulnerabilities to the financial system. Given the financial system’s inherent role in financial flows, digital attacks against financial service providers are persistent and sophisticated. Moreover, high-profile and systemic digital security incidents, whether caused intentionally or accidentally, could undermine public trust, which underpins the entire financial system. Policy has a challenging task in balancing the benefits from innovation due to digital transformation against the need to maintain stability, certainty and trust.

The disruptive effect of innovation in financial technology, or FinTech, is generating many benefits in the financial sector. In the payments space particularly, benefits to customers can include a superior and seamless customer experience, a wider range of products and services at a lower cost and potential for access to financial services for underserved customers (potentially some SMEs) or the underbanked.

Additional benefits from digital transformation can be seen in efficiency gains for financial institutions by "cutting out the middle man". Increased digitalisation has also opened up interconnections of financial institutions to external parties, such as through cloud computing or Application Programming Interfaces (APIs), and to FinTech providers that may be outside the regulatory perimeter.

A new wave of efficiency gains may be seen with the integration of blockchains, or distributed ledger technology (DLT) more generally, into existing processes within and between stakeholders in the financial sector. Moreover, many start-ups and SMEs are offering innovative blockchain-based payment services. These services promise faster, cheaper and more secure transfer of value, which is creating pressure on established financial institutions to consider adopting variations of this technology as well.

Finally, new value creation is likely to occur in Europe with the Revised Payment Service Directive (PSD2) recently coming into force. This will enable third-parties (not only small FinTech start-ups but potentially also large technology companies such as Facebook and Google) to build financial services on top of banks’ data and infrastructure. This should enable bank customers, both consumers and businesses, to use these third-party providers to make payments and manage and analyse their finances more generally. Banks who are obliged by this Directive to provide third-party providers with access to their customers' accounts through open APIs have raised security concerns, leading to a delay in the Directive's implementation until these issues are resolved.

While disruption in the financial sector brings benefits, it also amplifies some existing risks and creates a variety of new risks. These risks can be linked to malicious attacks or the accidental failure of digital technologies. They can also result in large-scale but localised impacts as well as systemic and global impacts.

While functional separation, through cloud computing, and outsourcing may be good from a competition and efficiency standpoint, they also poses new challenges. With digitalisation introducing many new interlinkages between organisations, vulnerabilities often exist outside of any specific organisation's own network perimeter. For instance, opening up information via APIs multiplies entry points and thus vulnerabilities that could be exploited. These vulnerabilities may be particularly acute in relatively smaller organisations that form part of the supply or value chain (e.g. data aggregators or intermediaries).

The increasing collection of personally-identifiable data, public display of personal data and use of common credentials across platforms by organisations outside of the financial sector have also created new risks to financial institutions. In the event that data are stolen then sold on 'darknet' markets and misused, it is financial institutions that must bear the cost of fortifying their systems against penetration and replacing/resetting stolen credentials. Depending on the circumstances surrounding some instances of fraud, such as credit card fraud, it is either the payment provider, bank and/or merchant that shares the potentially large cost of this fraud.

In the context of crypto-currency transactions, while security may be enhanced as transactions are performed among peers in a 'trustless' way, this changed configuration also brings risks. Many successful digital security attacks have affected nascent blockchain start-ups (e.g. The Distributed Autonomous Organisation [DAO] attack in 2016). Crypto-currency exchanges commonly find themselves either as the target of attack (e.g the Coincheck hack in 2018) or as malicious parties themselves (e.g. Mt Gox incident in 2014). This suggests that digital security risks are not yet appropriately managed across many stakeholders in the emerging crypto-currency ecosystem.

At a systemic level, the interconnectedness of financial institutions allows for speedy and efficient cross-border and cross-sector transactions but also creates systemic risks. The systemic importance of certain financial institutions, and the effects of rapidly eroded trust in those institutions, was fully exhibited during 2007-08. A variety of past digital attacks on financial institutions, such as a series of Denial of Service attacks against American banks from 2011-13, indicate that these risks are not hypothetical. Moreover, the networks that bind together financial institutions can also be disrupted in ways that could erode trust. A recent example of such an incident afflicted the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network and involved the attempted theft of up to USD 1 billion from Bangladesh Bank in 2017. As the frequency of digital attacks increases and the nature of these attacks changes, so too the probability and potential impact of systemically important incidents rises.

Given the inextricable relationship between stakeholders in the financial sector and various regulatory authorities across OECD countries, policy can play numerous roles in encouraging practices that lead to greater resilience amongst stakeholders in the financial system.

Facilitating information sharing (e.g. via platforms/hubs or bilaterally between companies and their key stakeholders) is a particularly important part of digital security response initiatives. However, sharing can be hampered by a lack of trust among participating organisations due potential legal liability exposure; concerns about the ability to ensure that shared information is not subsequently breached; and/or due to a lack of comfort in revealing or legal ability to reveal business information to potential competitors., among other possible reasons Moreover, impediments to information sharing may also arise from new privacy laws such as the EU General Data Protection Regulation (GDPR) which leave companies unclear about what information what can be shared and how.

Policymakers have to consider ways how these numerous obstacles to effective information sharing might be overcome when crafting policy related to information sharing. Governments in some OECD countries have taken an active role as a repository for incident reporting and distributor of synthesised threat intelligence to financial sector stakeholders. Others have taken an approach that seeks to enable financial sector stakeholders to share information on their own terms through mechanisms like Information Sharing and Analysis Centres (ISACs). The suitability of any approach is largely determined by the specific context in question. Therefore, policymakers should undertake a needs assessment, with the involvement of key stakeholders, so as to develop relevant and effective policy in this space.

At an international level, policymakers have recognised the importance of digital security threats and the need to address them. Initiatives have been seen even at the G20 level with Finance Ministers agreeing at the 2017 German summit in Baden-Baden to, “promote the resilience of financial services and institutions in G20 jurisdictions against malicious use of information and communication technologies, including from countries outside the G20” (G20, 2017). Moreover, authorities across the globe have taken regulatory and supervisory steps designed to facilitate both the mitigation of digital security risk by financial institutions, and their effective response to, and recovery from, digital security incidents.

Policy makers provide the rules and frameworks in which digital security resilience can be established. They can also coordinate across jurisdictions via international regulatory bodies and standard-setters, which is important for addressing cross-border issues. For instance, a stocktake report by the Financial Stability Board (FSB) on “Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices”, was released in October 2017. It found that FSB member jurisdictions have been active in addressing cybersecurity. All member jurisdictions have released regulations or guidance that address cybersecurity for the financial sector.

With specific relevance for payment systems, regulators and supervisors gathering in the Committee on Payments and Market Infrastructures (CPMI) have also been active in addressing issues of digital security and resilience. A ‘*Guidance on cyber resilience for financial market infrastructures’* was released in conjunction with International Organization of Securities Commissions (IOSCO) in November 2015. This guidance highlighted the importance of governance, identification, protection, detection, and response and recovery for risk management. Overarching components included: testing, situational awareness and learning and evolving.

Long-standing standards exist in the payments sector such as the Payment Card Industry Data Security (PCI) Standard, which is a mandatory set of controls that payment providers require of merchants that store, process and transmit cardholder data. A challenge for policymakers in developing other mandatory standards is ensuring that the burden of compliance with mandatory controls is not unnecessarily excessive to smaller organisations.

In this context, so-called ‘regulatory sandboxes’ may provide a means by which to allow for technological experimentation at a small scale in an environment with lower compliance requirements. The United Kingdom Financial Conduct Authority (FCA, 2015) defines a sandbox as, “a ‘safe space’ in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question.”

Policymakers contending with the risks associated with crypto-currency exchanges, particularly the tendency for such exchanges to suffer accidental or intentional loss of customer funds, may consider bringing such exchanges under existing stock exchange rules and regulations or financial sector digital security requirements. For instance, to respond to the risk of money laundering and tax evasion, regulators might consider imposing anti-money laundering/know-your-customer (AML/KYC) requirements on fiat-to-cryptocurrency gateways and crypto-currency exchanges.

Capacity building, in terms of increasing digital security skills and awareness, is important in assuring resilience of the financial system. In 2017, approximately 10% of successful digital security incidents in the financial and insurance sector involved error as a causal event (Verizon, 2018), which can be linked back to lack of awareness and staff skills. As a result, awareness raising and training related to digital security risks is important at many levels within organisations (e.g. from employees through to the board level). Reflecting this importance, in its 2018 CISO Cybersecurity Trends survey, the Financial Services ISAC’s found that employee training was the top priority for improving security amongst 35% of respondent Chief Information Security Officers, “because employees serve as the first line of defense” (FS-ISAC, 2018). Policymakers may consider ways in which to foster the alignment of skills taught in the curriculums of education providers with the skills requirements in industry.

Questions for discussion

1. Which new challenges in terms of digital security risks and resilience is your business, and the industry more broadly, facing in light of digital transformation? What are the benefits of blockchain technology in terms of enhancing digital security and efficiency especially of payments? Can start-ups propose new methods and processes that can benefit the financial industry at large?
2. Have new approaches and players in payment capture created risks for system integrity? How do you assess the benefits and risks of Europe’s Revised Payment Service Directive (PSD2)? What needs to be done to reduce its risks while allowing appropriate competition from third party providers? Should regulators pursue similar opening efforts in other jurisdictions?
3. Are current information sharing arrangements about digital security attacks within companies as well as with their peers, regulators and supervisors appropriate and sufficient? Which sharing platforms or other options do exist, should be enhanced or should be created? How do you assess the benefits of sharing threat intelligence, versus possible trade-offs in terms of perhaps unwanted revelation of business information or enhanced supervisory and regulatory scrutiny?

4. How can policy makers help in improving risk management and information sharing? Is the level of cooperation between industry and government sufficient to address digital resilience challenges, and how should it be improved? How should cross-border cooperation on oversight of cross-border systems be improved? How can regulators and supervisors build capacity to keep up with technological advances and increased sophistication of digital security attacks?
5. What, in your view, are key policy recommendations to improve digital security and resilience that one should take away from this discussion?

Digital security risks to energy infrastructure: electricity

Digital technologies promise to make energy systems more connected, intelligent, efficient, reliable and sustainable. While digital transformation can generate many benefits for operators in the energy sector and to energy consumers, it also creates new and amplifies some existing risks to energy security. These risks are linked to natural hazards (e.g. geomagnetic storms), unintended digital security incidents and intentional digital security attacks. As maintaining a stable supply of energy is critical to the smooth functioning of many aspects of modern economies and societies, digital security incidents involving energy infrastructure can be particularly disruptive.

Technological innovation has always been at the core of power sector development, starting with early competition between alternating current and direct current (IEA, 2017). This tradition continues with the energy sector being a relatively early adopter of digital technologies. For instance, electricity utilities were using early digital technologies to facilitate grid management and operation in the 1970s and have continued to do so until the present day.

Current application of the data and analytics components of digitalisation to the structure and operation of power systems can provide a series of improvements in at least four ways: by reducing O&M costs; improving power plant and network efficiency; reducing unplanned outages and downtime; and extending the operational lifetime of assets (IEA, 2017). The connectivity component of digitalisation also has the potential to reshape the power sector by connecting power supply with key demand sectors such as transport, buildings and industry (IEA, 2017).

Digital security attacks themselves sometimes target operational technology (OT): the computers, software and networks used to control, monitor, manage and protect energy delivery systems. Other attacks might target only the IT business systems of energy companies that do not control the physical process of energy delivery but instead result in administrative interruptions (IEA, 2017). These attacks can target personnel, products (both data and physical infrastructure) and/or processes (system data flow). They seek to compromise the integrity, availability and/or confidentiality of information or networks both within the organisation in question and in its supply chains.

The probability of success of these attacks, and the potential range of their impact, is increasing due to a couple of trends. First, increasing connectivity and automation, a shift to cloud computing, and the replacement of energy-specific IT by sophisticated open-protocol industry standards have resulted in newer systems with greater functionality. However, their relative openness potentially reduces the level of specialised energy system knowledge needed for attack. Second, the potential “attack surface” in energy systems is also increasing. The rapid growth in connected devices, combined with the diversification and decentralisation of energy technologies, will link millions of new small-scale prosumers and billions of devices into the electricity system. Industry forecasts vary but one estimate places the total number of connected IoT devices at more than over 20 billion by 2020 (Gartner, 2015). If there is one vulnerable device at the edge of a network, this can be a weak point for the whole system, and the number of endpoints keeps increasing non-linearly.

Additionally, unintentional digital security incidents can occur given that a great deal of legacy technology exists in the energy sector. Early applications often relied on proprietary or vendor-specific information technology (IT) and operational technology (OT), with electricity substations using several generations of equipment, assembled piecemeal over time. The complexity of these "systems of systems" is increasing as many layers of IT and OT – sometimes termed the 'cyber-physical nexus' – are combined and layered upon one another. While older infrastructure often pre-dates embedded security standards, which means it may benefit from "security by obscurity[2]", it also increases the probability of inadvertent incidents such as when an update in one type of equipment causes malfunctions in other equipment (IEA, 2017).

Disruptions to energy systems caused by digital security incidents and attacks have so far been relatively limited when compared to more "traditional" causes (e.g. extreme weather). However, some notable examples do exist. For example, digital disruption to an electricity grid was witnessed in the Ukraine in 2017 (Tuptuk and Hailes, 2017). Incidents such as these can have knock-on effects throughout society given the essential nature of power to almost all activities. Such incidents raise the spectre of low-probability, high-risk scenarios where the entire electricity grid of a major economic region could be shut down for a period of days or even weeks due to one or a string of digital security incident(s). One such scenario, undertaken by Lloyds of London and the Cambridge Centre for Risk Studies, pegged the range of potential loss from such an outage on the US east coast in the hundreds of billions of dollars (Lloyds, 2015).

Full prevention of such incidents is impossible, particularly given finite resources and budgets. However, their impact can be limited if countries and companies adopt effective risk management practices with the goal of maintaining resilience in response to incidents.

Resilience involves designing, operating and managing systems in a way that allows them to withstand shocks and to be able to quickly recover in the event of an incident. Building system-wide resilience depends on all actors and stakeholders (including SMEs) being aware of the risks, maintaining proper cyber hygiene and incorporation of security objectives into their research and design processes.

Clarity about the division of responsibilities for security, preparedness and response among market players and governing bodies, is therefore critical. With sufficient preparation, a company or local operator is likely to be able to handle the majority of attacks by botnets or amateurs (e.g. the "script kiddie" teenage hacker) but will have difficulty adequately managing sophisticated attacks and/or incidents, particularly though resulting from systemic risks.

Unlike most IT systems, electricity OT systems must operate in real-time, which means patches of updates cannot be simply installed, or systems cannot be shut down and rebooted, as is common when responding to digital security failures in other sectors. Security models for such systems are therefore very different to those more commonly

[2] i.e. specialised knowledge is required for successful attacks.

experienced by those operating in the traditional digital security domain. Assuring resilience therefore requires cross-domain expertise and associated training as well.

In terms of solutions to risks introduced by digital transformation, blockchain, or distributed ledger technologies more broadly, might hold some promise at the grid edge. For example, if these technologies are developed then deployed to validate whether a device is running up-to-date firmware and has not been tampered with. Such solutions are currently being developed, often by start-ups and SMEs whose business models involve rethinking existing processes and services. However, these technical solutions will bring new risks of their own, or amplify some existing risks, which will require continued revision of digital security risk management practices so as to remain relevant in light of continued technological change.

Moreover, the trend toward microgrid electricity networks also present opportunities for risk reduction. Microgrids are small electric grid systems linking a number of households or other consumers together rather than connecting them to a centralised entity. Their decentralised structure means that portions of the network can be islanded, or temporarily segregated from the rest of the grid, which reduces the may reduce the probability of large-scale, systemic incidents.

Depending on the country in question, electricity utilities may be restricted in the amount that they can invest in digital security measures given restrictions on the prices they can levy on consumers. Adjustments to regulatory requirements might help ensure necessary investments are made in digital security measures given that uncertainty about risks makes it difficult to justify large expenditures on staff or on cyber-insurance policies. Adding digital security criteria to the base rate for electricity grids, for example, might be one way in which to incentivise greater investment in security measures.

A mixed picture emerges as to the role of standards in encouraging the adoption of security measures. The International Electrotechnical Commission (IEC) develops worldwide standards and conformity assessments for equipment and business processes. So far it has identified around 650 electrotechnical standards from 40 different standard-setting organisations that have applicability to cybersecurity (IEA, 2017). At the same time, compliance with standards at an international or national level does not guarantee infrastructure will be secure over time. This is partly because regulatory standards may struggle to keep up with rapid technological changes, the introduction of new vulnerabilities or the evolution of threat actors.

Governments and energy companies therefore need to also be proactive and adaptive in finding then sharing digital security risk management practices. These may include establishing cooperative and collaborative groups beyond regulatory requirements so as to save costs, pool resources and expertise or conduct joint exercises. The Information Sharing and Analysis Centre model, first developed and adopted in the United States then adopted in many other OECD counties (e.g. Japan, the Netherlands), is one way in which to facilitate information sharing and collaboration between industry players at a national and international level. International cooperation, which can be facilitated through such arrangements or in international standard development, is particularly important due to the global and instant nature of the Internet.

Another key element is promoting proper digital security hygiene, or a basic set of precautions and monitoring that all digital technology users should undertake. Reinforcing a security-conscious culture in all relevant levels of technology users as well as promoting simple operating rules, such as keeping software up to date or not sharing access rights, can greatly increase overall security levels. This is especially relevant for SMEs that cannot afford to hire or train digital security specialists.

Finally, research and development plays an important role in developing measures to increase security and reduce risk. Security objectives and standards should be incorporated at the outset of the research and design process for digital technologies, rather than being added ex-post, as has been the case in the design and manufacture of many systems that have been in place for some time. Funding might be provided for research and development, as has been done through the European Union's Horizon 2020 programme.

Questions for discussion

1. What are the greatest digital security risks to energy systems today, and how are they evolving and changing in different parts of the energy sector? How can risks be appropriately identified, assessed, and prioritised? What gaps or barriers are creating challenges in identifying and raising awareness of these risks?
2. What are leading governments and companies doing to enhance digital resilience? How can digital resilience be integrated into wider critical infrastructure resilience? How can best practices be transferred across the sector, to other sectors, and to other regions?
3. In building resilient energy systems, what are the appropriate roles, responsibilities and actions of different actors such as international organisations, national governments, large energy companies, SMEs, device manufacturers, and individual users? What can be done to ensure that all actors dedicate adequate resources to conduct proper threat assessments, monitoring, and updating?
4. What are the appropriate roles and responsibilities of different relevant government agencies and ministries within a country in enhancing digital resilience of energy? How can governments ensure adequate cooperation and coordination among these agencies, including developing clear and accepted standards and definitions?
5. How can governments ensure good, relevant and adaptive regulation in face of the rapidly changing environment? What can they do to ensure proper implementation of regulations? What are the advantages and disadvantages of different regulatory approaches in different legislations – e.g. centralised vs. decentralised? Should there be international coordination of rules and norms?
6. How can new digital technologies, such as blockchain, help to enhance or improve security and resilience of energy systems and networks? How can different actors, including start-ups and SMEs, help to mainstream digital security objectives and standards into research and development, and ensure that new systems are from the onset secure by design?
7. What, in your view, are key policy recommendations to improve digital security and resilience that one should take away from this discussion?

Digital security risks to transport infrastructure: automated vehicles

Transport infrastructure is a critical enabler for public services (e.g. emergency services, law enforcement, waste disposal); trade-related activities such as freight transport and logistics; as well as various means of mobility required in a modern, globalised society. The underlying physical infrastructure is increasingly digitalised, which holds the promise of improved performance, efficiency and safety of transport as well as various second-order benefits to employment, trade and the environment. Increasing digitalisation can also be seen in the automation of vehicles (e.g. cars, trains, ships) as well as growing interconnectivity between the vehicles themselves.

Digital transformation of transport infrastructure brings benefits but also new risks, particularly given the systemically important role that transport infrastructure plays in the economy and the trend toward greater interconnection within and between entities. Effective management of these risks will necessitate a multi-level approach that takes into account risks at the vehicle-level, adjustment of laws and regulations at a national level and the development of standards and agreements at an international-level, among other measures.

The development and implementation of new digital technologies that has occurred gradually over the past decade is now triggering fundamental changes to transport and mobility. Adoption has primarily been driven by a desire for improved performance, efficiency, safety, fluidity, etc. of existing transport means and systems. High-level political commitments may also have played a role such as the major global agreements of 2015 and 2016 on sustainable development, climate change and the New Urban Agenda.

Adoption has occurred at differing speeds across various modes of transport. For instance, though e-tickets on the mobile phone have become broadly accepted in civil aviation, electronic signature in freight transport is still not widespread. Moreover, the pace and intensity of digital technology uptake also differs across OECD countries in line broadly with level of economic development.

Innovative uses of digital technologies have also given birth to completely new mobility services (e.g. car and ride sharing platforms). These services are sometimes perceived as being disruptive not just to incumbents within the transport sector but also to existing public policy in these sectors. However, they stand to potentially reduce traffic congestion in urban areas and reduce prices to end-users.

Digital technologies have also increased the capacity for real time information services on traffic, vehicle and cargo. Such ‘Intelligent Transport Systems’ have already made it technologically possible to redesign infrastructure pricing and to implement the “user-pay” principle. This and other implementations may result in reduced costs to logistics companies, increased employment to data and service providers as well as price reductions in the event that cost-reductions due to efficiency gains are passed-on to end-users.

Developments in vehicle automation and progress towards autonomous vehicles are recent and major trends driven by digital technologies. Road transport automation (e.g. cars, trucks), particularly when combined with car-sharing and e-hailing, but possibly also with urban freight delivery, is likely to see the first use cases of vehicle automation. Safety benefits are likely to be the most visible positive impacts of increasing automation though at the expense of gross employment in sectors affected in the short to medium term.

Digital transformation also creates various risks to transport infrastructure. The risks exist at different levels of the infrastructure (e.g. vehicle, between-vehicle, vehicle to network and at all levels of the internet architecture [application, protocol and infrastructure]). Complicating the picture even further is the multitude of different sectors involved (e.g. cars, trains, ships), the numerous stakeholders that each involves and the interaction between these various stakeholders across borders (which are precisely the kind of new interactions facilitated by digital technologies).

Over many decades software has gradually been integrated into different kinds of vehicles to perform various tasks. For example, in cars software is used in the course of braking, cruise control and the functioning of entertainment systems (Motovalli, 2010). All software has bugs and, with millions of lines of code in the standard automobile, the potential exists for software failure leading to injury or property damage (Dean, 2017). The lack of clear standards around software quality in vehicles, coupled with the continuing trend to integrate more software and internet connectivity into these vehicles, creates new digital security risks at a vehicle-level.

The trend toward vehicle-to-vehicle connectivity is driven by the continued development and adoption of autonomous capabilities in these vehicles. Between levels 2 and 3 of autonomy there is a need for vehicles to communicate with one another (Evans, 2017). Once vehicles need to communicate with one another, a means for communications is needed, and this means of communication introduces new risks particularly in the presence of an internet connection. Measures to reduce these risks – whether due to connectivity malfunction and/or malicious hacking by an outside party – will be required.

Increasing use of software for functions within vehicles (whether cars, trucks, trains or ships) requires the patching of software over time, which in turn may require internet connectivity. Moreover, some form of internet connectivity is required if autonomous functioning of vehicles is desired. Introduction of network-level connectivity (e.g., internet service providers, wireless providers, and IP protocol), transport-level connectivity (e.g., protocols such as TCP/UDP and the Domain Name System), and application-level connectivity (e.g., protocols such as SSL/TLS, HTTP/HTTPS, etc.) all create new digital security risks.

At each of these levels of connectivity, some form of systemic risk is introduced. For instance, were internet connectivity to be disrupted, as was the case when Dyn suffered a denial-of-service attack in late 2016, occasioning disruption of internet connectivity on the US East Coast and Western Europe, there is a non-zero probability of disruption of the functioning of all vehicles reliant upon that connectivity. The presence of bugs common to a protocol, such as Heartbleed, which affected the OpenSSL cryptographic library, point to the possibility of incidents due to exploitation of the common bug affecting multiple vehicles at the same time. Given the scale of transport networks, the size of some vehicles and their cargo, as well as the inherently physical nature of transportation, any systemic disruption holds the potential for serious impacts.

New policies and considerable institutional changes will be necessary to reap the full benefits of digital transformation, to unleash the business and transport benefits, and to address emerging risks related to personal data protection, digital security and resilience. The multi-sectoral scope of transport infrastructure and services as well as the multi-national reach of digital technologies require adaptation in policy development and approach.

As individual vehicle owners/users are increasingly unable to identify and thus manage the digital security risks they face due to integration of digital technologies, responsibility and associated liability may shift from the end user to perhaps producers and/or manufacturers. For example, in the context of automobiles, users cannot inspect/repair components lest they lose their warranty due to tampering with their devices. This requires policymakers to craft legal and regulatory frameworks that allocate liability to those parties best placed to bear and manage the associated risks. To provide one such example, policymakers in Japan have already taken steps to allocate liability in a way that differentiates between layers of autonomy and the presence of defects (Nikkei, 2018).

The policy and regulatory framework related to the transport sector requires fundamental rethinking of urban and national transport policies. A whole-of-government approach will be required given that traditional authorities responsible for transportation policy (e.g. motor or maritime safety authorities) are unlikely to possess staff with the requisite skills to effectively identify/understand digital security risks and, in turn, develop appropriate and effectively policy responses.

Closer policy and regulatory cooperation as well as information sharing will be required between stakeholders within the various transport sectors, the telecommunication sector, digital technology companies as well as government regulatory agencies. One instance where the need for such cooperation and sharing can already be seen is in the context of incident investigations related to autonomous vehicles e.g. the data stored on Tesla vehicles, which have autonomous capabilities, are in a proprietary format that cannot be accessed by non-authorised parties (Levin, 2018). Information sharing and collaboration between industry and government may be pursued through mechanisms such as the Automotive Information Sharing and Analysis Center (Auto-ISAC).

Finally, given the international scope of digital technologies, international coordination, development and revision of globally agreed regulations and standards will be crucial to ensure compatibility and interoperability of digital technologies. Knowledge sharing in this field has been growing in the framework of the United Nations (ITU; UNECE Inland Transport Committee and its Inland Transport Security Forum) and the G20.

The OECD and the International Transport Forum have embarked on work to explore the safety and security issues surrounding overall road network safety and system-wide security vulnerabilities that may come with more automated driving. This work will investigate impacts of early-stage crashes and incidents on consumer sensitivity and vehicle adoption rates as well as issues relating to security and privacy of the cyber-physical system of connected and highly automated vehicles (ITF, 2018). Prior roundtables have also explored in-depth issues such as co-operative systems of automobile-based mobility and automated driving as well as commercial vehicle on-board safety systems.

Questions for discussion

1. Who is responsible for ensuring digital security and resilience and under what conditions? i.e. governmental authorities, businesses (including OEMs, IT and software companies, insurance sector, etc.), international organisations?
2. What are the new vulnerabilities introduced by digital transformation at various levels? E.g. infrastructure and traffic management covering all modes; vehicle, passenger/ driver/ cargo (including dangerous goods, explosives, and other sensitive cargo); the special case of highly automated vehicles; increased vulnerability due to new technology and new ways of achieving mobility (shared vehicles, ride haling)?
3. What changes are needed in the insurance sector and in its regulatory framework in light of risks introduced due to digital security attacks and automation?
4. What changes may be needed to international governance models and frameworks developed in the past so as to meet the requirements of digital technologies?
5. Who will pay, and how, for sound digital security measures put in place at an infrastructure level (e.g. should road user charges include earmarked revenues for digital security)?

6. What, in your view, are key policy recommendations to improve digital security and resilience that one should take away from this discussion?

Digital security risks to Government and public services

Digital transformation is a high priority for all governments that value the improvement of public sector productivity and increasing access to, and the quality of, their public services. The high rate of government spending as a share of GDP, which in 2015 ranged from 28.7% to 57%, is among reasons driving adoption of digital technologies in public service delivery (OECD, 2018).

Digital technologies present opportunities for public administration to make efficiency gains that improve the national competitiveness of their economy just as is the case with business enterprises. Perhaps the greatest similarity between governments and the private sector when it comes to digital transformation is that both gather and store massive amounts of highly sensitive data on citizens and customers, which could be lucrative in the hands of criminals.

As governments have shifted the delivery of public services to digital platforms, they also have had to contend with digital security risk. In the 2018 Verizon Data Breach Investigation Report, 14% of reported breaches in the prior year involved public sector entities. The challenges specifically facing governments in this area are numerous. Some personal data must sometimes be kept for use over longer periods than is common in the private sector. This sometimes leads to it being kept on older, more vulnerable systems. Government agencies are regularly targeted not just by opportunistic criminals, but also by teams funded and trained by governments. Approximately half of the incidents affecting public sector entities reported in Verizon’s 2018 report were attributed to State affiliated actors. Moreover, even as government agencies try to protect themselves from hostile intruders, citizens want the customer experience that they have become accustomed to in their interactions with enterprise. A trend to expect in future is that citizens will more frequently and more openly use online platforms to evaluate public service delivery. Customer relations management (CRM) platforms are already pervasive in the private sector, and citizen relations management platforms are likely to follow in future.

Governments undergoing digital transformation are finding digital security a major challenge, particularly given that any disruption to the functioning of essential services can seriously erode public trust. Data breaches can have high stakes in terms of public health, public safety and national security. Successful digital security attacks have revealed vulnerabilities in government information management systems essential to the functioning of early warning and alert systems for natural hazards, CCTV networks and public health services.

In 2017 the “Wannacry” and “NotPetya” global ransomware attacks demonstrated the broad reach of extortion and damage due to wiper malware. Europol estimated that around 200 000 computers were infected across 150 countries, including networks of several central and local government agencies. When a computer is infected with ransomware, documents and files are encrypted and a message appears to demand payment of a ransom, typically in a digital currency, in exchange for a digital key to unlock the files. If victims do not have a recent backup of the files, they must either pay the ransom or face the risk of losing permanent access to all the files. Networks of hospitals in the National Health Services of England and Scotland were amongst those affected, and reports emerged of patients having surgeries rescheduled as a result. Other examples of ransomware attacks on governments involve the targeting of data stored by local police agencies. While any data could be targeted, the recurrent modus operandi appears to focus on data that is critical to an organisation’s mission and for which recovery is time sensitive. Many governments have since issued guidance to agencies on what to do to prepare for ransomware attacks as well as what to in case they become a victim.

"Cyberespionage" has become a major means for stealing State secrets such as designs for defense technologies, negotiation strategies in international trade and the personal information of civil servants. Armed with such stolen information, adversaries may improve their own defense capacities, adapt their strategies on external commerce and seek to intimidate, corrupt or harm specific public authorities. In June 2015, the United States Office of Personnel Management (OPM) announced that hackers had managed to exfiltrate sensitive government files containing personal data of more than 22 million individuals, including present, past and prospective federal government employees. Information targeted in the breach included the names, dates and places of birth of persons, their addresses, as well as their “social security numbers”, which is a unique identifier for citizens and residents of the United States.

In light of the constant and growing digital security risks facing government administrations and delivery of public services, a key challenge is to hire, train and retain a workforce of public employees with the necessary digital security skills and capabilities. A key aspect of this challenge is the inability of many governments to compete with the private sector for a shortage of supply in talented human resources.

Governments can take various steps to improve the digital security workforce, including initiatives to promote digital security training and skills and developing guidance to address digital security workforce challenges. In New Zealand, a Cyber Security Skills Taskforce was established to address a shortage of digital security professionals. It was established in recognition that not enough New Zealanders were entering digital security professions at a sub-degree level, and to create a pathway for junior analysts to develop skills with academia and industry supported internships. It is not designed, however, to directly produce highly qualified digital security professionals.

Governments have improved efforts to recruit qualified digital security professionals by identifying them both in public and private employment according to a standardised set of capacities. The National Initiative for Cybersecurity Education (NICE) is a partnership in the United States among government, academia, and the private sector to increase the number of skilled digital security professionals. Specific measures to standardize competencies and accelerate hiring processes could follow its lead and include the development of a framework to consistently define and describe digital security work at any public or private organisation. Governments can assign multi-digit employment codes for each digital security work category and specialty area they identify and use these codes to identify digital security positions in personnel and payroll systems across a large pool of organisations and companies.

Amongst the public services that have been targeted by digital attacks are components of the electoral system, which in some OECD Members has been designated a critical infrastructure sector. The digital security of voter rolls, voting machines and databases of tallied results are paramount to the integrity of the overall electoral process, which goes to the heart of democracy. In countries where election systems are centralised vulnerability is at greater risk by design compared to a distributed system where elections are fully administered at different levels of government. Amongst the measures considered to ensure the continuity and integrity of elections are the use of paper ballots and ensuring redundant capacity for machine based voting in case their functionalities are attacked on the day of an election.

Governments are keenly aware of digital security attacks that aim to steal, destroy and distort data, and have developed an array of policies, tools and partnerships to mitigate these risks. However other insidious forms of threats which do not necessarily breach the digital security of information systems and data have recently appeared in the digital age such as the widespread use of digital platforms to manipulate public opinion in the attempt to destabilise democratic institutions, create distrust of the media and scientific communities of experts, enflame social tensions and cast doubt on the integrity of elections and the character of candidates.

“Fake news” campaigns and “organised trolling” on social media platforms demonstrate the power of such “hybrid threats” to intensify conflicts within societies, and to erode the conditions for civil debate and social cohesion. These deceptive campaigns illustrate the heightened susceptibility of a digital society to disinformation tactics that have long been used to influence public opinion, due to a step change in their scope, frequency and rapidity. The digital environment enables adversaries to use such tactics from a distance, with near anonymity and at low cost (Zarate, 2017). The economic impact of this form of “hybrid threat” has not been closely studied, but their social and political disruption is clear to see. Ignoring the problem plays into the hands of adversaries. Many OECD Members have begun to consider what a comprehensive strategic approach would entail. The European Union has formulated a “Joint Framework on countering hybrid threats - A European Union Response”, which places situational awareness, resilience and response at the heart of its comprehensive strategy (European Commission, 2017). The Joint Framework recognises digital security attacks on critical infrastructure as one type of hybrid threat used in conjunction with disinformation campaigns and counter intelligence to cause serious harm and spread instability. Its aim is to improve capacity to detect and understand malicious hybrid activities early and to enhance the resilience of critical infrastructure (e.g. transport, communications, energy, space and finance) and institutions that are fundamental to withstand and recover from attacks.

Among the defensive steps that OECD Members could take to complement digital security measures focused on information systems and networks, are: improving understanding of the tools used to conduct digital disinformation campaigns, raising public awareness that a specific act is taking place, pushing back against fake stories as they occur with facts, and identifying and discrediting the source of fake stories. Australia has established a multi-agency Electoral Integrity Task Force to guard against digital security attacks and interference in elections, amid concerns foreign powers are meddling in domestic affairs and ahead of elections. This effort to identify and address risks to Australia’s electoral process was most recently strengthened in June 2018 by comprehensive legislation aimed at preventing foreign interference.

How to identify fake news and what to do about it present difficult challenges for policy makers, including how to determine truth and validity of stories as distinct from “fake news”, and how to avoid unacceptable limits to freedom of speech. The effort of governments to identify fake news inevitably requires partnerships with private sector media and social media companies, including the major social media platforms that have been abused in foreign influence campaigns. To their credit, these businesses recognise a strong common interest in preserving the integrity of democratic electoral processes and are working closely with many OECD Members to understand the threats, identify and flag false news and validate stories and information. Among the concrete forms of action that these major platforms take are:

- Monitoring elections proactively across countries for foreign interference from any country. Platform operators can monitor suspicious accounts of foreign origin for civic related content and notify their security teams to manually review whether it violates the terms of service.
- Closing fake user accounts using machine learning and artificial intelligence to protect against the creation of fake accounts, and to uncover coordinated behaviour that is abusive and counter to their Community Standards.
- Making advertising more transparent so that the public understands more about who is creating content on their platforms.
- Reducing the distribution of fake news by prioritizing informative posts and down ranking hoaxes and fake news flagged by third parties.
- Supporting an informed user community by helping people connect with political candidates and learn about policy issues that are important to them
- Establishing a mechanism for authorisation of political ads that requires advertisers to: submit a copy of their government issued ID and the last four digits of a social security number; provide a physical mailing address in the country; the platform will confirm each address by mailing a postcard with a unique access code. Advertisers who have successfully undergone this verification process can then fulfil disclosure requirements by indicating when an ad they place is political in nature and declaring the ad's funding source.

Questions for discussion

1. What are the greatest digital risks of concern to governments today, and what are governments doing to prepare for them in advance? How can risks to government continuity be appropriately identified, assessed, and prioritised? What vulnerabilities do governments consider the Internet of Things to expose public institutions to?
2. What are governments doing to enhance digital resilience in critical infrastructures that they depend upon for their own functions as government to be carried out? In what situations, if any, should governments have direct regulatory control over operators of critical infrastructure? What can they do to ensure proper implementation of regulations?
3. In building resilient governments, what are the appropriate roles, responsibilities and actions of public / private partnerships to combine efforts across different actors? How can best practices be transferred from the private sector to government agencies? How can governments compete for digital security talent with the private sector? Should governments adopt secondment policies that foster secondments from and to the private sector?
4. How can governments make sure that the administration of institutional structures does not preserve stovepipes around the digital and physical domains that get in the way of a holistic approach to risk management?

5. Are governments paying sufficient attention to the cross-border dimensions of the challenge, for example by sharing good practices?
6. How can governments partner with the private sector to build resilience against digital hostilities aimed at sewing social discord and undermining the democratic electoral process?

Whole-of-Government Approaches to Digital Security in Critical Infrastructure and Essential Services

Faced with ongoing digital transformation, governments are struggling to create the conditions for higher levels of digital security and resilience in essential services and critical infrastructures. After decades of long-standing market failures (e.g. information asymmetry, negative externalities, moral hazard) in what was once called the "ICT sector" has led to chronic deficiency in the level of security of digital technologies that are now driving digital transformation. Moreover, many of the risks that characterise these technologies do not manifest themselves for some time (i.e. once use of technologies occurs at scale), which means that accurate perception and management of risk early-on can be impeded. This difficulty is compounded by the concomitant rapid pace of digital technological change.

Many digital security risks and risk management practices are similar across sectors. These similarities are due to different kinds of dependencies. The first kind of dependency is one that is linked to widespread use of common digital infrastructure components. Another type of digital dependency is when a digital security threat to an operator of critical infrastructure or essential service successfully propagates to other operators, within the same or in different sectors, eventually causing damages to a large range of services. A third category of dependency is the effect that disruption of an essential service in one sector - due to a digital security incident - might have on the delivery of an essential service in another sector. Some risks, however, are sector-specific. These differences might be due to use of domain-specific technical equipment, particular market characteristics (e.g. value chain structure), regulatory requirements (e.g. minimum service requirements), among other reasons.

In response, governments are increasingly adopting whole-of-government frameworks to better understand and manage risk from a national perspective (national risk management); to enable cross-cutting measures such as training, information sharing, and incident response; and to increase sector-specific digital security risk management expertise and practices. A whole-of-government approach involves collaboratively development and implementation of policies by Ministries, public administrations and public agencies in order to provide a unified and multi-faceted set of solutions to a particular policy problem or issue. Such an approach requires appropriate balancing of the complementary, and sometimes also competing, objectives of economic and social prosperity and national security.

Public policies for Critical Information Infrastructure Protection (CIIP) initiated in the mid-2000s generally had the aim of providing a whole-of-government framework. Based partly on this experience, in 2008, the OECD Council adopted the *Recommendation on the Protection of Critical Information Infrastructure* (OECD CIIP Recommendation). This is a set of high-level principles to guide the development of policies at the domestic level and across borders. The Recommendation's goal is to protect, "those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy”.

Since then, many important policy actions were taken at national, regional and international levels to encourage critical infrastructure operators to adopt appropriate measures to manage new threats and vulnerabilities. These include Canada's Action Plan for Critical Infrastructure, the United States 2016 Cybersecurity National Action Plan, NIST Cybersecurity Framework and C^3 voluntary programme; Japan's adoption of its 4th programme for Critical Information Infrastructure Protection; and the European Union's adoption of its Directive on Security of Network and Information Systems (NIS Directive) in 2016. At an international level, the Meridian Process, created in 2005, is an example of an international initiative that gathers senior CIIP policy makers every year to exchange ideas and initiate actions for the cooperation of governmental bodies on CIIP issues globally. Another initiative is the “Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers”, which was developed in 2016 by Meridian and the Global Forum on Cyber Expertise (GFCE).

The 2008 OECD CIIP Recommendation is presently under review. The goal of this review is to to align it with the *2015 Recommendation on digital security risk management for economic and social prosperity*. Preliminary results of a policy questionnaire circulated to OECD members for the review indicate that CIIP policies are generally developed on the basis of both a critical infrastructure protection (CIP) policy framework and a national digital security strategy. In fact, CIP and national digital security frameworks can be viewed as "parent" frameworks for CIIP policies.

Countries are at various stages of CIIP policy making maturity. Some adopted a framework over a decade ago and are updating it in light of recent policy and technical developments as well as experience gained from previous iterations. Others are currently building or considering building their approach from the ground up.

CIIP policy frameworks across OECD countries share a number of common characteristics. These include a recent trend towards policies that encourage the adoption of better digital security risk management practice by operators of essential services. However, the means by which governments incentivise operators vary from mandatory regulatory requirements to voluntary measures.

One example of a compliance approach is the 2016 NIS Directive. The Directive lays out the approach by which EU member states, "shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations". The Directive also states that Member States shall ensure that the competent government authorities, "have the necessary powers and means to assess the compliance of operators of essential services with their obligations". This includes an obligation to notify relevant authorities of incidents that have had or are likely to have a significant impact on the continuity of the essential services they provide. EU members have until May 2018 to adopt appropriate laws and regulations to comply with the directive. Some countries, such as France and Germany, have already adopted legislative and regulatory measures in this area.

In contrast, some other countries, such as Japan, consider flexible policy measures that incentivise operators and encourage information sharing to be more effective than the introduction of new digital security regulations. Another example can be seen in the United States which tasked the National Institute of Standards and Technology (NIST) to work with the private sector to collaboratively develop a "Cybersecurity Framework". This framework, operators are encouraged to voluntarily adopt, helps organisations plan and document their digital security risk management practices. Moreover, voluntary information sharing between the public and private sector is encouraged through, for example, partial funding for information sharing and analysis centres/organisations.

Almost all countries place public-private co-operation at the centre of the development and implementation of CIIP policy. Such an approach is necessary given how much critical infrastructure and digital technology is developed and used by private operators or enterprises. For example, France and Germany have established voluntary public-private partnerships (PPP) to draft the details of regulations or specific security standards with the private sector. These PPPs aim to take into account operators' expectations and constraints to avoid creating unnecessarily burdensome requirements. They also aim to build trust among participants by establishing reciprocal benefits whereby the government gains a better understanding of the field and improved relationships with operators, and operators help develop pragmatic regulation that better fits their needs. Furthermore, such PPPs can also provide a venue for discussions among operators, and other government actors such as sectoral regulators. The extent to which SMEs participate in these public-private partnerships can be unclear though.

Information sharing about threats, vulnerabilities, incidents and risk management practice is generally at the core of efforts to strengthen the protection of critical information infrastructure. A key area for public policy is therefore the creation of appropriate enabling conditions for the development and maintenance of trust among stakeholders. However, risk-related information disclosure is often extremely sensitive as it can increase the risk faced by organisations, for example by exposing their reputation or the organisation itself to legal liability when releasing information about incidents. It could also facilitate the task of potential attackers particularly when linked to the disclosure of details about vulnerabilities or protection measures. Although information exchange between organisations in the same sector might be carried-out in the general interest, companies may be reluctant to share information on their vulnerabilities with competitors. Such information sharing might also fall foul of competition/anti-trust legislation. Finally, information sharing with governments can also be challenging as governments might be perceived by some operators as possible threat actors. This challenge in doing so is even greater for cross-border information sharing given the potential sensitivities related to national security between some countries.

Questions for discussion

- On digital security risk management:
  1. What are the most important characteristics of or good practice for digital security risk management essential service operators? Are they the same across sectors? What are the main challenges faced by operators to implement such good practice and how can policies best encourage them to do so?
  2. How should SMEs that are part of essential services value chains improve their digital security risk management practices?
  3. What parts of the Internet could be particularly protected in light of their critical role as supporting essential services?
- On policy development and implementation:

4. How can policies to enhance digital security of critical infrastructure and essential services' operators strike the right balance between digital innovation and digital security? How can they best take into account operators' need to innovate in an era of digital transformation?
5. How can government implement a whole-of-government perspective when managing digital security risks to critical infrastructure and essential services?
6. How can coordination between sectoral, digital security and other government agencies at national and local levels be best organised? Do these actors have enough resources and expertise?
7. What are the conditions to establish trust among stakeholders in order to encourage information exchange on threats, vulnerabilities and incidents? How can information sharing be encouraged including between competitors, public-private actors, SMEs and large operators? How can we reconcile privacy concerns with the need for confidentiality when sharing sensitive information between critical infrastructure operators?
8. What are the best avenues to enhance regional and international co-operation?
9. What, in your view, are key policy recommendations to improve digital security and resilience that one should take away from this discussion?

REFERENCES

Møller-Mærsk A.P. (2017), “Q2 2017 Interim Results”, http://files.shareholder.com/downloads/ABEA-3GG91Y/5010261826x0x954061/7EB88BAD-F1AE-4E86-9B95-FF32017D31F9/APMM_Interim_Report_Q2_2017.pdf

Clarke R. and Knake R. (2010*), Cyber War: The next threat to national security and what to do about it*, HarperCollins Publishers, ISBN: 9780061962233

Dean B. (2017), “Three core security and privacy issues of connected vehicles”, Center for Democracy and Technology. https://cdt.org/blog/three-core-security-privacy-issues-of-connected-vehicles/

European Commission (2017), “Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response”, JOIN(2017) 30 final. https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf

Evans B. (2017), “Steps to autonomy”. www.ben-evans.com/benedictevans/2018/3/26/steps-to-autonomy

Financial Conduct Authority, Regulatory sandbox, November 2015. www.fca.org.uk/publications/documents/regulatory-sandbox

FS-ISAC (2018), FS-ISAC Unveils 2018 Cybersecurity Trends According to Top Financial CISOs. www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

Gartner (2015), Press Release: “Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015”. https://www.gartner.com/newsroom/id/3165317

Global Forum on Cyber Expertise and Meridian (2017), The GFCE-MERIDIAN Good Practice Guide

On Critical Information Infrastructure Protection for governmental policy-makers. www.meridianprocess.org/siteassets/tno-jrv161031-02_hr.pdf

Global Forum on Cyber Expertise and Meridian (2017), Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. www.meridianprocess.org/siteassets/17-9241---707059-a5-gpg-ciip-2.pdf

G20 (2017), Communique: G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany, 17-18 March 2017. www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20

communique.pdf;jsessionid=B3B06E17EB814580F50DF0D1387F67B6?__blob=publicationFile&v=3

Hern A. (2017), “WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017”, *The Guardian*. www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

Hollinger P. (2016), “Meet the cobots: Humans and robots togerher on the factory floor”, *Financial Times* and *National Geographic*. https://news.nationalgeographic.com/2016/05/financial-times-meet-the-cobots-humans-robots-factories/

International Transport Forum (2018), “Safety and Security on the Road to Automated Transport: The Good, the Uncertain and the Necessary”. www.itf-oecd.org/safety-security-automated-transport

International Energy Agency (2017), “Digitalization and Energy”. http://www.iea.org/digital/

Jan Top H. (2010), “Smart grids and smart water metering in the Netherlands”, presentation to the European Commission ICT for Water Management event, Accenture. http://ec.europa.eu/information_society/activities/sustainable_growth/docs/water_cons/henk-jan-top_presentation.pdf

Koppel T. (2015), Lights out: A cyberattack, a nation unprepared, surviving the aftermath, Crown Publishers, ISBN: 055341996X

Levin A (2018), “Teslas don’t have black boxes, making U.S. crash probes harder”, Bloomberg Technology. www.bloomberg.com/news/articles/2018-04-03/teslas-don-t-have-black-boxes-making-u-s-crash-probes-harder

Lloyds of London (2015), “Business Blackout: the insurance implications of a cyber attack on the US energy grid”, report in conjunction with Cambridge Centre for Risk Studies. www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf

Merck (2017), “Press release: Merck announces third-quarter 2017 financial results”. http://investors.merck.com/news/press-release-details/2017/Merck-Announces-Third-Quarter-2017-Financial-Results/default.aspx

Motavalli J. (2010), “The dozens of computers that make cars go (and stop)”, New York Times, 4 February 2010. www.nytimes.com/2010/02/05/technology/05electronics.html

Nikkei Asian Review (2018), “Japan to place liability on self-driving car owners”, 31 March 2018. https://asia.nikkei.com/Japan-Update/Japan-to-place-accident-liability-on-self-driving-car-owners?n_cid=NARAN012

OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures. http://oe.cd/dsrm.

OECD (2014), OECD Technology Foresight Forum 2014 – Internet of Things. www.oecd.org/internet/ieconomy/technology-foresight-forum-2014.htm

OECD (2015a), The Internet of Things: Seizing the benefits and addressing the challenges, Background report for Ministerial panel 2.2. Working Party on Communication Infrastructures and Services Policy. www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En

OECD (2015b), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. http://oe.cd/dsrm.

OECD (2018), National Account at a Glance (Database). https://stats.oecd.org/Index.aspx?DataSetCode=NAAG.

Tuptuk N. and Hailes S. (2016), 'The cyberattack on Ukraine's power grid is a warning of what's to come', Phys.org, available from: http://phys.org/news/2016-01-cyberattack-ukraine-power-grid.html (accessed 16 September 2016).

Verizon (2018), "2018 Data Breach Investigations Report: 11th edition", www.verizonenterprise.com/verizon-insights-lab/dbir/

Zarate, J. (2017), The cyber-attacks on democracy, www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html

Annex A. WORKSHOP AGENDA

OECD Going Digital Project:
Making the Transformation Work for Growth and Well-Being

Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services

Digital Security in Energy, Transport, Finance, Government, and SMEs

15-16 February 2018

OECD Conference Centre, 2 rue André Pascal, Paris, France

OECD Going Digital Collaborative Project co-organised by:

OECD Directorates for Science Technology and Innovation (STI), Public Governance (GOV), Financial and Enterprise Affairs (DAF) - International Energy Agency (IEA) - International Transport Forum (ITF) - OECD Centre for Entrepreneurship, SMEs, Local Development and Tourism

The workshop will discuss the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructure. It will explore cross-sector dependencies and avenues for coordination among stakeholders within countries as well as across borders.

It will also discuss how an integrated whole-of-government approach to digital transformation of the economy and society can best help address the protection of critical infrastructure and essential services against digital security risk.

To this end, the workshop will bring together experts from several policy communities focusing on digital security, energy, finance, transports, national risk management and SME in a collaborative discussion, cutting across silos of expertise, with a view to identifying common high-level policy messages for the *OECD Going Digital project*.

The ongoing digital transformation of the economy and society holds many promises to spur innovation, generate efficiencies, and improve services, and in doing so boost more inclusive and sustainable growth as well as enhance well-being.

Highly automated processes enabled by big data and artificial intelligence, distributed in the cloud, and combined with technologies bridging the digital and physical worlds (Internet of Things) are enabling digital transformation of critical infrastructure and essential services. Smart grids, Fintech, and automated vehicles for example are unleashing new opportunities for innovation and growth, environmental protection and other important global challenges, while transforming business processes and markets. Digital technologies also improve how governments manage critical risks and crises and how they build resilience in society.

But these benefits go hand-in-hand with disruptions. Our interactions with one another and with society more broadly are being transformed, as are the nature and structure of organisations and markets, raising important issues such as around jobs and skills and how to ensure that technological changes benefit society as a whole, among others.

A key challenge for policymakers is to identify the policy mix that will enable their economies to maximise the benefits of an increasingly digitalised global economy and adequately address the related challenges. Only a coherent and comprehensive policy approach will have the scope to harness the benefits of the digital transformation for stronger and more inclusive growth.

To chart the road ahead, the OECD has launched a multidisciplinary project on ***Going Digital: Making the Transformation Work for Growth and Well-Being***. It aims to help policymakers in all relevant policy areas better understand the digital revolution taking place across all economic sectors and in the society as a whole.

This project brings a whole-of-OECD perspective through the involvement of 14 OECD committees and 9 directorates. It will articulate recommendations for pro-active policies that will help to drive greater growth and societal well-being and address the challenges of slow productivity growth, high unemployment and growing inequality in many countries. It will also develop an integrated whole-of-government policy framework to guide governments in adopting the range of policies needed to ensure a holistic and coherent policy approach in the digital age.

One important issue inherent to digital transformation is the need for resilience and better security to mitigate possible disruption of economic and social activities by digital security incidents. Traditionally understood as breaches of availability, integrity and confidentiality of ICTs and data, digital security incidents are increasingly frequent and sophisticated. They can take advantage of the global nature of the Internet to rapidly propagate across jurisdictional, organisational and sectoral boundaries, as demonstrated by the recent Wannacry, notPetya, and Dyn attacks. Digital security incidents can generate financial, reputational as well as physical damage as demonstrated by interruptions of electricity grids in 2015 and 2016.

Higher dependency on digital technologies increases the potential for security vulnerabilities along value chains and the exposure to security threats which can create disruptions in the activities of businesses, including SMEs, governments and individuals. Such security incidents could evolve into large scale crisis affecting infrastructures critical to the functioning of the economy and society such as essential energy, transports, finance, or government services. In addition to such catastrophic scenarios, digital security incidents affecting critical infrastructures and essential services can also have subtle but long-term negative effects by limiting innovation, slowing down adoption of new technologies, undermining trust in the digital environment as well as hampering the digital transformation and its related benefits.

Objectives of the workshop

The workshop will discuss the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructures. It will explore cross-sector dependencies and avenues for co-ordination among stakeholders within countries as well as across borders.

It will also discuss how an integrated whole-of-government approach to digital transformation of the economy and society can best help address the protection of critical infrastructures and essential services against digital security risk.

To this end, the workshop will bring together experts from several policy communities focusing on digital security, energy, finance, transports, national risk management and SME in a collaborative discussion, cutting across silos of expertise, with a view to identifying common high-level policy messages for the *OECD Going Digital project*.

Issues and challenges to be discussed include in particular:

- **To what extent is digital transformation changing the protection of critical information infrastructures and the management of digital security risk?** How is the risk evolving along the value chain, including beyond/across sectors? Are "hybrid threats" as well as threats against confidentiality and privacy becoming increasingly challenging in relation to the protection of critical infrastructures and essential services against digital security risks? What is the role of individuals?
- **To what extent are cross-border and cross-sector interdependencies addressed**? How can stakeholders take into account globally distributed digital infrastructures (e.g. Cloud computing) as well as potential systemic risk from widespread vulnerabilities (e.g. Meltdown and Spectre)?
- **What are good policy practices to encourage digital security risk management by all organisations, including SMEs?** What is the right balance between mandatory and voluntary policy measures to protect critical infrastructures and essential services? What should be the respective roles of digital security agencies, public safety departments and sectoral regulators? Are SMEs a weak link in essential services' value chains?
- **How can governments foster trust with and among private operators** to enable information sharing on threats, vulnerabilities and incidents? How can they encourage information sharing between operators competing in the same sector? How can SMEs be included in trust frameworks?

In each session, panellists and workshop participants will address the above issues and challenges and share related good practice with respect to a different policy area, with the exception of the SME policy perspective which will be addressed in each session. Sessions' moderators will then gather in a final session to identify and discuss the key policy messages to be delivered from the workshop to the broader Going Digital Project.

Participants include representatives from:

- Government bodies in charge of digital security, energy, finance and transports policy and regulation, as well as ministries and agencies in charge of critical risk and crisis management policy;
- Business and industry, including SMEs, in particular operators of critical infrastructures and essential services, as well as digital security firms;

- Civil society, academia and the technical community.

Draft Agenda

DAY 1 - 15 February 2018

14:00 - 14:15	**Welcome / opening: Digital security of critical infrastructure and essential services within the OECD Going Digital project**

These opening remarks will introduce the broader OECD Going Digital project and explain how the workshop will contribute to its objectives.

Opening remarks: Masamichi KONO, Deputy Secretary-General, OECD

14:15 - 15:45	**Session 1. Digital security risks in the financial sector**

As a custodian of financial assets with a significant dependence on digital technologies, the financial sector has been a major target of cybercrimes and has been working to address digital security risks for many years. The sector is also internationalised with significant cross-border infrastructure to manage cross-border payment, inter-bank transfer and foreign exchange settlement systems.

As a result, financial regulators have placed increasing attention on digital security risks at the institutions they oversee, and implemented a number of international coordination initiatives to share experience and ensure the integrity of the common systems on which they depend.

At the same time, policymakers and regulators have an interest in ensuring an efficient and innovative financial system that meets the needs of its users, creating an effort to balance the need for high security standards to maintain the integrity of the financial systems while ensuring sufficient openness to new innovation.

This session will explore these issues with a focus on the payment capture and settlement systems, which has seen significant innovation as the result of new technologies for making and capturing payments. It will examine how new entrants (e.g. fostered by EU's Revised Payment Service Directive (PSD2)) and traditional infrastructure providers manage the potentially competing objectives of openness to innovation and the need to maintain integrity.

Format: Panel discussion with short introductory statements or presentations followed by an open discussion among panellists and with other workshop participants

Moderator*:* Martin KYLE, Chief Information Security Officer, Payments Canada

Panellists*:*

- Nikolai BOECKX, Head of SWIFT oversight, National Bank of Belgium
- Edward DOWLING, Security Product Manager, TransferWise
- Sameer ISMAIL, Chief Compliance and Risk Officer, Coinify

- Leo PUNT, Deputy Chief Executive EMEA, SWIFT
- John M. SALOMON, Regional Director (EMEA), Financial Services ISAC
- JoAnn STONIER, EVP/Chief Data Officer, Mastercard

Coffee Break 15:45 – 16:00

16:00 - 17:30 Session 2. Digital security risks to energy infrastructure: electricity

The energy sector has been an early adopter of digital technologies, which bring many opportunities but also many technical, security or regulatory challenges. Power utilities already in 1970s used emerging technologies to facilitate grid management and operation. But the growth of the IoT combined with the diversification and decentralisation of energy technologies will link millions of new small-scale prosumers and billions of devices into the electricity system. Digital technologies used in centralised energy systems are also changing, with a move from proprietary or vendor-specific solutions to newer open-protocol industry standards, more automation and a shift to cloud computing. These newer systems might have a higher general level of security and greater functionality but also more openness, potentially reducing the level of specialised energy system knowledge needed for attack. The attack surface is thus changing and vastly expanding.

While disruptions to energy systems caused by digital security incidents and attacks have so far been relatively limited when compared to more "traditional" causes such as extreme weather, notable examples do exist and energy systems can also increasingly be affected by generic attacks such as NotPetya. Credible low-probability, high-risk scenarios of attacks shutting down the entire electricity grid of a major economic region for a period of days or even weeks can be envisaged.

Building system-wide resilience depends on all actors and stakeholders being aware of the risks, maintaining proper cyber hygiene and incorporating security objectives into research and design. Full prevention of digital security attacks is impossible, systems must therefore be designed in a way to withstand shocks and be able to quickly recover, while preserving the continuity of critical infrastructure operations.

Format: Presentations and panel discussion followed by open discussion with workshop participants

Moderator*:* Michael APICELLI, Energy Attaché, U.S. Mission to the OECD

Panellists*:*

- Professor Tim WATSON, Director, WMG Cyber Security Centre, University of Warwick
- Richard SCHOMBERG, IEC Ambassador for Smart Energy, International Electrotechnical Commission
- Dr. Ana TRBOVICH, Co-founder, GridSingularity; Foundation Council Member, Energy Web Foundation (EWF)

- Stefano BRACCO, Knowledge Manager, EU Agency for the Cooperation of Energy Regulators (ACER)

End of Day 1

Cocktail

DAY 2 - 16 February 2018

09:00 - 10:30 Session 3. Digital security risks to Transport infrastructure: automated vehicles

The transport sector is an essential enabler for public services, freight transport and logistics, and provision of necessary mobility demand, including employment, education, trade, etc. Its underlying physical (and increasingly data-related) infrastructure is critical for a wide range of services from emergency services and law enforcement to waste disposal. Any major disruptions to transport infrastructure will thus have far reaching effects.

The wider transport sector is in the early stages of undergoing what many experts predict to be a revolution in terms of how mobility is provided. Key trends include ride-sharing platforms and vehicle automation; much of this being enabled through the emergence of big data analytics and progress in the field of data science. Here data can be seen both as a potential as well as a challenge.

The key trend of vehicle automation, particularly when combined with e-hailing, but possibly also with urban freight delivery, is likely to be among the first use cases to be implemented. In this context the enabling technology of car-to-car/-infrastructure communication needs strong data security safeguards to prevent digital security attacks on critical transport infrastructure and to ensure acceptable resilience levels in response to incidents.

Format: Presentations and panel discussion followed by open discussion with workshop participants

Moderator*:* Eva MOLNAR, former Director of the Transport Division of the United Nations Economic Commission for Europe (UNECE)

Panellists*:*

- Gereon MEYER, Head of Strategic Projects, VDI/VDE Innovation + Technik
- Sebastian ROHR, CEO, accessec GmbH
- Henrik KIERTZNER, Principal Consultant Cybersecurity, SAS
- Dimitra LIVERI, Network and Information Security Expert, ENISA

Coffee Break 10:30 – 10:45

10:45 - 12:15 Session 4. Digital security risks to Government and public services

Governments provide the apparatus for developing and administering laws and regulations to preserve public welfare and smoothly operating markets, and they also provide numerous public services, such as public safety, health, education and defence. As such, many of their facilities and agencies are critical infrastructure and providers of essential services. In recent years, governments have faced a growing deluge of threats, both targeted and untargeted, that are increasingly sophisticated, stealthy and dangerous.

Among the different forms of attacks on governments are those by cyber-criminals who hold government data for ransom; by State-sponsored actors who aim to steal State secrets (including diplomatic channels and even the personal information of civil servants); and by political activists to disrupt and deface government websites as a means to protest against policies they disagree with.

For governments, digital risk goes beyond vulnerabilities to digital security attacks. Public trust in governments per se is vulnerable to "hybrid" threats such as the use of online channels to spread disinformation campaigns that aim to influence political elections or erode social cohesion.

Many governments are still not able to mitigate advanced digital security attacks or agile enough to develop timely counter narratives to hybrid threats. This session will discuss the policies, procedures and structures to counter digital threats, in their several forms that target government.

Format: Presentations and panel discussion followed by open discussion with workshop participants

Moderator*:* Stephen DAVIES, Strategic Technology Partners, Fireye

Panellists*:*

- Steve CASAPULLA, Acting Branch Chief for International Affairs, Office of Cybersecurity and Communications, Department of Homeland Security (DHS), United States
- Chaetae IM, Senior Researcher, Korea Internet & Security Agency / Korea Internet Security Center (KISC)
- Johan RAMBI, Corporate Privacy & Security advisor, Alliander

Lunch Break 12:15 – 13:30

13:30 - 15:00 Session 5. Whole-of -Government Approaches to Digital Security in Critical Infrastructure and Essential Services

With digital transformation, governments are struggling to create the conditions for a higher level of digital security in all essential services and critical infrastructures. While many digital security risk and risk management practices are similar across sectors, some aspects are sector-specific, for example to take into account sophisticated technical equipment, particular market characteristics (e.g. value chain structure) and regulatory requirements (e.g. minimum service requirements), etc. Governments need to adopt whole-of-government frameworks to enable cross-cutting measures such as training and information sharing, as well as to increase sector-specific digital security risk management expertise and practices.

Governments' national digital security strategies and policies for Critical Information Infrastructure Protection (CIIP) generally provide such whole-of-government frameworks. This session will bring together policy experts in charge of these frameworks. It will discuss challenges they face to develop and implement them such as how to incentivise operators of essential services, which degree of regulatory requirement is appropriate, how to encourage information sharing within and across sectors, how to address cross-border and cross-sector interdependencies, etc.

Format: After a brief introduction by each panellist, the moderator will invite discussions among them and with the workshop participants.

***Moderator**:* Peter BURNETT, Meridian co-ordinator

***Panellists**:*

- Jean-Baptiste DEMAISON, Senior Advisor to the External Relations and Coordination Director, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France
- Lucy PURDON, Policy Officer, Privacy International
- George SHARKOV, Director of ESI Center Eastern Europe; Representative of the European Digital SME Alliance
- Christopher BOYER, Assistant Vice President of Global Public Policy, AT&T Services, Inc.
- Henry YOUNG, Senior Technology Policy Advisor, National Institute of Standards and Technology, US Department of Commerce

15:00 - 16:30	**Concluding session: identifying key policy messages and closing remarks**

Moderators from each session will discuss the key findings from their session and possible high-level policy messages from the workshop.

Format: After a brief summary of key discussions in each session by the rapporteur (10 min), moderators of Session 1 to 5 will be invited to discuss together and with the workshop participants, including representatives of stakeholder groups.

***Moderator**:* Jean-Baptiste DEMAISON

***Panellists**:*

- Martin KYLE: moderator of Session 1
- Michael APICELLI: moderator of Session 2
- Eva MOLNAR: moderator of Session 3
- Stephen DAVIES: moderator of Session 4
- Peter BURNETT: moderator of Session 5

Close of Workshop 16:30

Annex B. WORKSHOP PROCEEDINGS

On behalf of the OECD, Deputy Secretary General **Masamichi Kono**, welcomed participants to Paris and to the workshop. He explained the broader OECD Going Digital project and how the outcomes of the workshop's discussion would contribute to the overall project. He noted that digital transformation comes with opportunities and risks. Continued trust and confidence rest on recognition of and effective management of associated risks. He emphasised the OECD approach, grounded in the *2015 Council Recommendation for Digital Security Risk Management for Economic and Social Prosperity*, which takes into account the economic and social dimensions of digital transformation.

He noted that the OECD is in the process of reviewing its *2008 Council Recommendation for the Protection of Critical Information Infrastructure* to incorporate the implications of digital transformation on critical infrastructures in OECD countries. Turning to his aspirations for the workshop, DSG Kono expressed his hope that participants could identify insights and best practices from their cross-sectoral and global experiences, particularly given the inherently transnational nature of digital transformation.

Session 1: Digital security risks in the financial sector

The aim of this session was to explore the ramifications of digital transformation in the financial sector with a focus on payment capture and settlement systems. **Martin Kyle** of Payments Canada served as the moderator. He noted his interest in exploring the balance between the imperatives of agility and stability in the financial system and the role of policy in maintaining this balance.

Speaking as the Head of Society for Worldwide Interbank Financial Telecommunication (SWIFT) Oversight at the National Bank of Belgium, **Nikolai Boeckx** brought two perspectives to bear. First, from an operational risk perspective, he explained the challenges in ensuring reliable availability of the SWIFT service given continued changes due to digital technologies. He highlighted the constructive collaboration between Central Banks on information sharing (in the context of G20) and the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) with the goal of security and systemic resilience. Second, from a policy making perspective, he noted the difficulty in setting security standards in a way that balances security for incumbents while providing enough leniency to encourage new entrants and the benefits from innovation that they potentially create.

The second speaker in this session, **Ed Dowling** of Transferwise, explained the trend towards 'unbundling' of financial services and how this trend is driving consumer convenience and price benefits. He emphasised the balancing act that 'fintech' start-ups must contend with: ensuring that customers' funds are kept safe and their information is kept private while also providing greater convenience. To conclude he explained the challenges faced by a relatively small enterprise (i.e. with less than 1000 people) when operating in numerous different markets each of which has different verification and know-your-customer (KYC) regulatory requirements.

The next speaker, **Sameer Ismail** of Coinify, provided an overview of the unique space that the emerging crypto-currency market plays in the overall financial system, from the point of view of a "new entrant" in the industry, a Danish SME offering blockchain-based financial services. He explained that crypto-currency exists outside traditional financial markets but still relies upon parts of the financial system for customers to enter and exit any kind of crypto-currency investment. He explained that despite continued growth the market is challenged by two issues. First, the continuing trust issues linked to several large-scale incidents involving exchanges. Second, the need to manage an inherent aversion to regulation amongst the community's initial members with the need for compliance with new and existing money laundering and data protection regulations.

Leo Punt, as the Deputy Chief Executive of Europe, Middle East and Africa at SWIFT, explained measures recently developed and adopted to ensure the continued security and reliability of SWIFT's transaction messaging service. These changes were triggered by a sophisticated and large-scale incident involving compromise of the SWIFT network via Bangladesh Bank. This incident highlighted that trust in the eco-system is contingent not just on SWIFT as an organisation but also its counter-parties. SWIFT has since implemented a 'customer security program' to bolster network security, which involves three measures. First, helping customers implement a set of baseline security controls. Second, SWIFT has developed new ways to detect and respond to fraudulent transactions over their network e.g. 'next day' reporting mechanisms for incidents and 'in-flight halting/verification' of transactions. Finally, SWIFT now operates a community information sharing service for anonymised, detected incidents.

John Salomon of the Financial Services Information Sharing and Analysis Center (FS-ISAC), explained the essential role of information sharing in identifying and managing digital security risks. He outlined the ISAC model, which brings together industry communities associated with critical infrastructure sectors in a number of OECD countries (e.g. Israel, Japan, the Netherlands, the United States, etc.) to reduce systemic risk and increase resilience. The FS-ISAC is the largest such initiative, serving the global financial services industry. The FS-ISAC traditionally provided tactical and strategic information sharing, processed threat intelligence and best practices to members. It now also provides services related to fraud reduction, physical security, exercising and business resilience, and training. It participates in numerous cross-sector bodies and initiatives around the world, including the UK NCSC's Industry 100 programme, the ENISA EG-FI, and US National Council of ISACs, which allow coordination and sharing of experiences and strategies both within the financial industry and across the critical infrastructure sectors represented. Mr. Salomon concluded by emphasising the need to build common ground across a diverse membership while remaining responsive to their varied needs. He insisted that this requires engagement with governments, as well as active encouragement from public policy bodies for private-sector information sharing.

The final speaker, **JoAnn Stonier** of Mastercard, explained the role that MasterCard plays as a technology/payments company that connects financial institutions (issuers) with merchants. This requires the development and maintenance of security infrastructure so as to safeguard their reputation for safety and security of payments. She emphasised that protecting the payment system goes beyond protecting financial records. It also requires protection of identity and credentials, which are ultimately the data that give one access to financial records.

During the discussion following the session, workshop participants provided a number of responses to the moderator's list of key topics to be addressed. The responses touched on a issues such as the security implications of the move toward common set of regulatory rules (open banking); the role of standards (e.g. PCI) and cross-domain collaboration as a way to manage supply chains and the risks that reside in them; the role of regulatory 'sand boxes’ so as to provide space for new players to experiment while allowing gradual compliance over time; the positive impacts of new data protection regulation (e.g. General Data Protection Regulation) in forcing better mapping of data assets amongst stakeholders; and the potential role for government in helping to fill perceived skills gaps in digital security.

Session 2: Digital security risks to energy infrastructure: electricity

Michael Apicelli of the US Mission to the OECD moderated the second session, which focused on the digital security implications of continued digital transformation of electricity grids. He noted that disruptions to energy grids are infrequent though, when they occur, they have potentially high impacts across societies.

The first speaker, **Tim Watson** from the University of Warwick, provided a high-level approach to energy resilience and security built around three broad ideas. First, he noted that electric systems are complex, organic and adaptive systems. They function like an organic ecosystem, which precludes approaches based around the goal of system control. Second, he explained that attempts to provide resilience in such an ecosystem typically start with an attempt to list every incident that might occur, and then seek to assure continued (or partial) functioning if any of these events happen. This is 'specified resilience'. This approach can fail since unexpected shocks aren't anticipated. A more general approach involves the application of 'general resilience' principles to allow systems to cope with unknown shocks: ensuring that systems maintain sufficient diversity, reserves, modular open interfaces, and capital diversity. Finally, he insisted upon the need for a multidisciplinary/cross-functional approach and workforce to sufficiently understand the eco-system and develop effective resilience strategies.

Richard Schomberg, from the International Electrotechnical Comission, spoke about the role of development and implementation of international standards in achieving grid resilience. Utilities face challenges brought on by the blurring of lines between information technologies with operational technologies as well as the constraints imposed by the need to continually expand services while lowering costs. In response, Mr. Schomberg insisted that standards be developed by subject matter experts with the input of regulators and that preference be given to international standards. In particular, he made reference to the IEC 61850 series on intelligent electronic devices at electrical sub-stations; the IEC 61970 information exchange common module; and ISO/IEC 27001/2 for its best practice recommendations on information security.

Shifting the discussion toward innovation, **Ana Trbovich**, from Grid Singularity and the Energy Web Foundation, explained the potential of blockchain technology for security in the energy sector. Some of these benefits include potential reduction of the risk associated with single points of failure; the potential to allow certain transactions to occur without publicly revealing information; and the ability to maintain the integrity of databases. In the energy sector, Ms. Trbovich claimed two areas are likely to see implementation of blockchain technology: certificates of origin for renewables; and utility billing. These changes may require re-allocation of liability at the application level (rather than the infrastructure level) given that information posted on a blockchain at the application level cannot be removed by the infrastructure provider.

Finally, **Stefano Bracco** from the European Union Agency for the Cooperation Energy Regulators provided the historical context of digital technology in the energy sector then highlighted some challenges ahead. In the past, operators in the energy sector typically used closed, proprietary technologies. This is changing with digital transformation, which is driven by increasing competitive pressures in the industry. This transformation toward open systems and shared technologies creates greater complexity, which can be seen in terms of the number of stakeholders involved; the need to exchange information amongst these stakeholders; the number of disciplines required to maintain effective situational awareness; the cross-border operation of infrastructure; and increasing cross-sectoral dependencies. He concluded with recommendations to overcome these challenges: *i)* greater cooperation between stakeholders, *ii)* awareness campaigns for digital security risk, and *iii)* the development and implementation of acceptable baseline security standards for all stakeholders. Finally, he advocated for investments in digital security measures to be made in a way that balanced costs against benefits.

The discussion following the presentations covered on themes including: standardisation, scalability, access, fidelity of information, education, awareness, solidarity and human capital. Specific topics discussed included the need for dialogue and sharing of understanding of the overall electricity system with all relevant stakeholders; adoption of a mindset that emphasises dependability, with security as one attribute, including acceptance that 100% security is not possible (i.e. a risk management approach); identification of ways to invest in people to assist them overcome the risks/seize the opportunities presented by digital transformation; balancing the security benefits of closed-source against the lost benefits from open innovation; and ensuring that regulations support the achievement of relevant objectives and are in-line with the operational environment.

Session 3: Digital security risks to transport infrastructure: automated vehicles

Starting day two of the workshop, this session focused on the key trends and implications of digital transformation in the transport sector. The discussion focused on vehicle automation though it also touched on ride-sharing platforms and other trends. The session was moderated by **Eva Molnar**, former Director of the Transport Division at the United Nations Economic Commission for Europe (UNECE). Ms. Molnar opened by framing the discussion around a series of crises (e.g. road deaths, exhaust, etc.), which may be partially addressed using digital technologies. However, she reminded the audience that these technologies bring with them new risks, which in turn require effective management.

Dimitra Liveri, from the European Union Agency for Network and Information Security (ENISA), opened by explaining the security implications of automated vehicles. Ms. Liveri noted that the ‘smart’ cars presently being developed can be used as a means to test/refine and thereby set a foundation for more secure automated cars in the future. She explained how the Network and Information System (NIS) Directive’s security and notification requirements are likely to impact security practices in the transport sector, especially those responsible for traffic management control and operators of intelligent transport systems.

Moving the discussion toward a more technical perspective, **Gereon Meyer** of VDI/VDE Innovation + Tecknik, explained the security implications of the confluence of technologies in the automotive sector (e.g. automation, electrification, etc.). He explained how this confluence is resulting in greater complexity, which in turn creates greater uncertainty. In particular, the merger of power and data functions within automobiles render all components safety critical, which makes management of the greater uncertainty even more problematic.

Henrik Kiertzner, the Principal Cybersecurity Consultant at SAS, provided a high-level overview of the trends around risk factors (threats, vulnerabilities, incidents, etc.) in the transport sector. He explained that changes in the technical landscape have made criminal activities more profitable (e.g. wider availability of tools such as through dark web markets). As a result, the sophistication of attacks is not as closely tied to the scale of the actor as in the past. Moreover, the continuing blurring of information and operational technology risks requires manufacturers to better audit and monitor their supply chains and ensure the post-sale servicing of products (i.e. patching). Mr. Kiertzner suggested that policymakers should think very carefully about any changes to laws or regulations due to the different effects they will have on various stakeholders. In this context, he insisted that policymakers adopt approaches that enable, rather than subdue, technological innovation.

The final presentation, by **Sebastian Rohr** from accessec GmBH, returned to ‘smart’ and autonomous vehicles. He opened with an analogy based on castles to demonstrate how security is difficult to achieve over time given changes in the environment. He linked this with what is occurring in the automotive sector at the moment. The trend towards more functions and features in vehicles, which are provided with digital technologies, has increased complexity and interdependence, which in turn has led to a serious digital security situation. He posited that an absence of incentives to ensure cars are developed securely is at the root of this problem today. He suggested establishment of international minimum security requirements for autonomous vehicles as a policy measure to address the situation in the future. Mr. Rohr commended the GDPR as an impetus for greater awareness of security risks at a management and board level within corporations. At a technical level, he suggested that authentication of vehicles and their individual components, rather than personal identity, will be required in the future.

The subsequent discussion revolved principally around the implications of vehicle owners/drivers being less able to understand and tinker with their vehicles. Speakers thought that this change implies a shift in responsibility and possibly liability for the safety and security of vehicles from owners/drivers to Original Equipment Manufacturers (OEMs). Final messages from the speakers included the need for secure identities, for secure management of devices and infrastructure, as well as for “security by design” when possible.

Session 4: Digital security risks to government and public services

Stephen Davies from FireEye moderated this session on the digital security risks that inhibit governments’ ability to preserve public welfare, maintain markets and provide services. In providing these capacities, governments must now contend with a variety of different digital security risks driven by attackers with different motivations. Mr. Davies noted that mis/disinformation, while not a type of digital security attack per se, can nonetheless result in impacts such as erosion of social cohesion.

Opening the presentations, **Steve Casapulla** from the US Department of Homeland Security, explained the approach to digital security management pursued in the United States. This approach views digital security as a shared responsibility, which requires public-private collaboration in a way that does not crowd-out private sector actors. He touched on some high-profile incidents of recent years as well as specific measures that have been developed and implemented to reduce the probability of similar incidents in the future. These include a new Executive Order, which continued a process of upgrading federal agency networks; requirements for continued implementation of the NIST Cybersecurity Framework; and the operation of the EINSTEIN system for perimeter defense and development of federal government-wide situational awareness.

The second presenter, **Chaetae Im** from Korea Internet Security Agency / Korea Internet Security Center gave an overview of the Korean government's approach and measures to manage and protect critical information infrastructure. Passed in 2001, the Critical Information Infrastructure Protection (CIIP) Law laid out key definitions and government-wide responsibilities in this area. The Korean approach involves vulnerability analysis/evaluation of critical infrastructures followed by development of guidelines and incident response plans. Countermeasures are then implemented and reviewed annually to protect that infrastructure.

The final speaker, **Johan Rambi**, representing the European Energy Information Security and Analysis Centre (ISAC), explained how the ISAC brings together a diverse range of stakeholders in a way that ensures transparency and trust. Collaboration is achieved using a 'community of communities' approach, which involves groups sharing information – physically and virtually - on specific topics of interest over time. Mr. Rambi emphasised the importance of establishment of clear terms of reference at the outset in ensuring the success of this approach. He felt that one strength of the ISAC model is its ability to engage international stakeholders, which is particularly given the transnational nature of the digital world.

The discussion that ensued covered a number of topics related to the successful operationalisation of a variety of public-private partnership models at a national and international level. Given that much of the critical infrastructure is owned and/or operated by private companies, such partnerships are essential to effective digital security risk management. Speakers felt that an essential element to successful collaboration was building of trust over time. Trust provides a foundation on which efforts around information sharing and joint-development and implementation of security initiatives can be built. The notion of 'cyber poverty' was raised and was perceived to affect smaller enterprises that are the lacking resources/capacities to protect themselves. The session closed with a discussion on the potential role of government in digital security education and training.

Session 5: Whole-of-government approaches to digital security in critical infrastructure and essential services

This session was opened by moderator Peter Burnett. He briefly presented the international Meridian network, which brings together policy makers who operate below ministerial level but above the operational computer emergency response team (CERT) level. Meridian has developed a good practice guide and companion document, which can be used to transfer knowledge around critical infrastructure protection (CIP), particularly to countries where such capacity may be lacking.

The first presenter, **Jean-Baptiste Demaison** from the French National Agency for the Security of Information Systems (ANSSI), explained factors that he felt had contributed to France's successful approach in CIP. He emphasised the importance of a whole-of-government approach as a foundation for policymaking. In addition, dedicated legislation that was developed with operators ensured that policy was in line with the realities of operators. The positioning of ANSSI as an inter-ministerial agency was also helpful in that it allowed them to engage across ministries and agencies. Finally, ANSSI's role in solely defensive measures was helpful in maintaining operational focus and in building trust with operators.

Lucy Purdon from Privacy International supported the notion of whole-of-government approaches, on the condition that the over-arching goal be the protection of individuals.

She elaborated on this point with reference to countries where laws nominally intended to protect critical infrastructure or address cybercrime have been used for other ends. In particular, secrecy provisions in the critical infrastructure laws of a developing country are alleged to have been used in ways that do not live up to the spirit of the law. She noted that the definition and designation of what is 'critical infrastructure' can be problematic. No consensus has been reached internationally on a single definition. As a result, different criteria are used across different countries. This can lead to improper designation of critical infrastructure. Finally, Ms. Purdon urged for consideration of the privacy impacts of information collection initiatives to monitor and protect critical infrastructure and essential services.

Representing the European Digital SME Alliance, **George Sharkov** discussed the participation of SMEs in value and supply chains and the implications for digital security risk management. He emphasised the external dependencies that second- and third-tier enterprises, many of which are SMEs, create within complex supply chains. These dependencies can be difficult to monitor, which makes imposition of effective regulations/standards difficult in practice. He closed by suggesting that policymakers adopt a plural 'whole-of-governments' approach given that decisions can and have to be made at multiple levels to understand and manage risk effectively.

Christopher Boyer, AT&T Services Inc., provided a walkthrough of how the telecommunications sector works with the US federal government in managing digital security risk in CI. Mr. Boyer returned to the need to define what is meant by 'critical' as this designation is not always clear when, for instance, considering the composite parts of large organisations. He explained the intention and operation of the Critical Infrastructure Partnership Council (CIPAC) and Sector Coordinating Councils. He closed with an explanation of the division and allocation of responsibility for policy, planning and operations between different public and private sector stakeholders.

The final presenter, **Henry Young** of the National Institute of Standards and Technology (NIST), US Department of Commerce, explained NIST's many activities related to digital security risk. These activities include research as well as standards and guideline development (e.g. supply-chain risk management, identity management, personnel management, etc.). One notable initiative, the NIST Cybersecurity Framework, was developed with the involvement of CI operators. The framework is presently undergoing revision with their input.

The post-presentation discussion focused on the need to consider necessity, proportionality and cooperation in the development and implementation of 'hard' and 'soft' regulation to protect CI; the challenges in effective communication and supply-chain management between stakeholder groups; and the need to set clear and relevant criteria for the definitions related to CI. The participants considered if and when data might be considered as CI and concluded that this might be appropriate in certain sectors, such as the financial sector, under certain conditions.

Concluding session

This session opened with a summary of the workshop discussions by the OECD rapporteur, **Benjamin Dean**. He explained that critical infrastructure and essential services are presently at an inflection point in digital transformation. The implications of that transformation results in reallocation of costs and benefits between stakeholders. This creates various challenges for policymakers. Adopting a risk management approach can help balance competing interests involved. A whole-of-government approach can also assist policymakers in operating effectively in the multiscale, dynamic and highly complex digital security risk ecosystem.

The moderator for this session, **Jean-Baptiste Demaison**, asked participants to identify high-level messages and suggest areas where the OECD might productively engage in future work. He asked that the discussion focus on three questions: how does digital security risk cut across sectors; what are best practices to protect critical infrastructure and essential services in the present context; and, from a policy perspective, how can policymakers manage conflicting or competing interests due to digital transformation?

Martin Kyle, the moderator of the first session on the financial services sector, returned to the need to re-evaluate the concept of 'critical' in the wake of digital transformation. He reinforced the need for policymakers, and the OECD's potential role, in facilitating information sharing and collaboration at scale so as to stay one step ahead of malicious adversaries. He noted that resilience is a useful concept, particularly the related notion of redundancy. When assessing the impacts of failures of CI, he suggested going beyond economic measures to include social, environmental and other measures. He also suggested that managing weak points in supply chains, such as SMEs, may in some jurisdictions require both operator and their suppliers to meet same security requirements (e.g. PCI in the payments industry), which flow down through contractual requirements.

Michael Apicelli, moderator of session two on the electricity in the energy sector, noted the important role that international organisations such as the IEA can play in knowledge diffusion around digital security risk management. He also suggested that 'safe spaces' be created in certain critical networks as an alternative to efforts that aim to harden all components within existing networks.

Eva Molnar, the moderator of session three on the transport sector, emphasised the need to streamline awareness of digital security risk throughout organisations. She highlighted that digital transformation goes beyond borders and thus policy solutions, such as those developed in forums convened by organisations such as OECD, have likewise to go beyond national borders. She insisted that policymakers responsible for transport strategy and planning integrate resilience into their work. This would require capacity building in countries where digital security risk management maturity is relatively low.

Stephen Davies, moderator of the fourth session on digital security risks to government and public services, noted the need to work in diverse groups to overcome multi-faceted and high-scale risk factors. The OECD's expertise across Directorates could be further leveraged in this regard. He noted the difference between formal and informal information sharing arrangements and the need to build a 'circle of trust' in both cases. He suggested better incident investigations and sharing of the findings of these investigations so as to 'learn from failure'.

Peter Burnett, moderator of the fifth session on whole-of-government approaches, explained that critical infrastructure and essential service protection is an extremely important part of overall digital security in OECD countries. This is because the dependencies between CI and other stakeholder can lead to society-wide cascading effects in the event of disruptions. For this reason, he welcomed the ongoing revision of the 2008 OECD Council Recommendation on the Protection of Critical Information Infrastructures. To manage systemic risks to CI, scenario planning can be helpful as it allows stakeholders to think through and learn about what can potentially occur in the event of disruption. Mr.

Burnett suggested that policymakers look to encourage partnerships with private sector operators in areas of reciprocal benefit as opposed to mandatory requirements.