
Transatlantic cyber-insecurity and cybercrime

Economic impact and
future prospects



STUDY

Perspectives on transatlantic cooperation

Transatlantic cyber-insecurity and cybercrime: Economic impact and future prospects

Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has also enabled costly new forms of crime, and created systemic risks to transatlantic and national critical infrastructure, threatening economic growth and development.

The transnational nature of these phenomena make it very difficult for effective policy solutions to be implemented unilaterally by any one jurisdiction. Cooperation between stakeholders in both the EU and US is required in the development and implementation of policies to increase the security of digital technologies and increase societal resilience to the cybersecurity risks associated with critical infrastructure. Although there is a great deal of congruence between the stated policy goals in both the EU and US, obstacles to effective cooperation impede effective transatlantic policy development and implementation in some areas.

This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues that policy-makers on either side of the Atlantic could work together on, and explains where effective cooperation is sometimes impeded.

AUTHOR

Benjamin C. Dean, Iconoclast Tech

Foreword by Patryk Pawlak, formerly of EPRS, now of EU Institute for Security Studies

To contact the authors, please email: EPRS@ep.europa.eu

ADMINISTRATOR RESPONSIBLE

Elena Lazarou, Members' Research Service, EPRS

ABOUT THE PUBLISHER

This is an abridged version of a paper commissioned by the Members' Research Service, within the Directorate-General for Parliamentary Research Services of the Secretariat of the European Parliament.

LINGUISTIC VERSIONS

Original: EN

This document is available online at:

<http://www.eprs.ep.parl.union.eu> (intranet)

<http://www.europarl.europa.eu/thinktank> (internet)

<http://epthinktank.eu> (blog)

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Original manuscript completed in May 2017.

Brussels © European Union, 2017.

Photo credits: © jijomathai / Fotolia.

PE 603.948

ISBN 978-92-846-1087-7

doi:10.2861/023034

QA-04-17-514-EN-N

1. FOREWORD

Reports of high profile cyber-attacks and malicious cyber operations are becoming more common, including the use of ransomware for financial gain and of stolen data to interfere with political processes. Consequently, digital risks, if unmitigated, are not only damaging to the economy but may also destabilise the political system of a state, weaken trust within a society, undermine economic freedom, and increase the risks of conflict. In order to protect the positive impact of the internet on stimulating growth and job creation, there is recognition on both sides of the Atlantic of the urgent need to strengthen cooperation on eradicating safe havens, and on building capacities to improve resilience of systems and societies to threats posed by other states and criminal networks, such as cyber-espionage and attacks on critical infrastructure. As the potential gains from attacks increase (whether for common cybercriminals or state-sponsored groups) and the threshold for access to cyber-tools decreases (primarily due to the development of the 'malware as a service' and 'ransom as a service' business models), the threat to the European Union and United States grows. This trend is accelerated by limited human, legal and institutional capacities in some regions of the world – in particular in Africa and eastern Europe – which facilitates the emergence of safe havens, from which criminal networks can harm citizens and businesses operating in the EU and the US. Consequently, addressing cybercrime and building more robust cybersecurity is desirable to further unlock the benefits of the digital economy and to ensure the free and open nature of cyberspace in the transatlantic area and beyond. At the same time, the increasing number of politically motivated attacks by states, state-affiliated groups, and non-state actors, committed as part of hybrid operations, suggests that the need to protect strategic interests and values is no longer limited to the physical world but is increasingly also necessary for the cyber domain.

Threat landscape: financial, security and political nature of attacks

Intelligence and threat assessment reports show that state-sponsored operations from countries like Russia, China and Turkey no longer focus exclusively on cyber-espionage but also undertake critical infrastructure vulnerability scanning, disruptive attacks, and propaganda and disinformation campaigns. Consequently, transatlantic efforts to build cyber-resilience are not focused just on domestic efforts but increasingly may reflect the needs of strategic partners and allies, with regard to several dimensions.

Protection of critical information infrastructure

Attacks on critical infrastructure are particularly common as a tactic in ongoing conflicts, risking possible escalation. For instance, pro-Russian groups like Sprut, Beregini or the Sandworm gang, often working in tandem, have conducted several attacks against the Ukrainian energy grid. The attack against the Ukrainian energy provider *Ukrenergo* in December 2016 resulted in an outage of over an hour in the northern part of Kyiv. Hacktivist groups from Ukraine, too, have orchestrated attacks against Russian targets, such as the Russian airline *Komiaviatrans* as part of the campaign #OpRussia in protest against Russian involvement in Ukraine and the Syrian conflict. In Iran, the National Centre for Cyberspace is considered responsible for the preparation of a 'cultural war' between Iran and its designated enemies.

Fight against cybercrime

Many countries in Eastern Europe, as well as former Soviet republics, are either attractive targets or safe havens for cybercriminals. In November 2016, a Russian

darknet forum (*WWH-Club*) served as a venue for the auction of full packages of medical data stolen from a medical facility in the United States. Some of these groups are suspected of ties to national law enforcement. Two major darknet markets in Russia – *AlphaBay Market* and *SilkRoad 3.0* – prohibit sales of personal data belonging to Russian citizens, to avoid engagement with Russian law enforcement. The pro-China group, the *Honker Union of China*, responsible for attacks against US and East Asian organisations has admitted links to the Chinese state. International criminal infrastructure such as *Avalanche* – which was dismantled in November 2016 thanks to a joint operation by Germany, the US, Europol and Eurojust – are used by cybercriminals to conduct phishing, malware distribution campaigns and money mule schemes.

Support for political stability

The cyber-domain is also a theatre in which disinformation and interference are used to influence political processes in individual countries. For instance, the pro-Russian group *Cyberberkut* was responsible for a series of attacks against the Ukrainian government as well as Organization for Security and Co-operation in Europe (OSCE) and United Nations (UN) missions. In 2016, a group known as *Guccifer 2.0* suggested that the results of the then-forthcoming elections in the United States might be falsified, and claimed to have gained access to the network of the Federal Election Commission to monitor the elections as an independent observer. External intervention in national electoral campaigns was also seen recently in Montenegro, in an effort to change the country's pro-Western course.

Curbing terrorist use of the internet

Although the offensive cyber-capacities of groups such as ISIL/Da'esh are very limited, as far as we know, the cyber-domain is not only used as a space for recruitment, fundraising and propaganda but increasingly as a platform to recommend best practices or new ways to maintain secure communications on the internet, for instance through a new encrypted application, *Signal*. *Electronic Horizons Foundation* – a pro-ISIL/Da'esh technical support group – has published a tutorial on the 'Invisible Internet Project'. Other outlets such as *Kybernetiq* (in German) not only provide tutorials but also explain how to pay for services anonymously using Bitcoin. At the same time, pro-ISIL/Da'esh collectives such as the *United Cyber Caliphate* and *Cyber Khilafah* are engaged in the physical domain. The former has offered a US\$5 000 cash reward for the execution of Saudi citizens and members of security services whose names appear on their own kill lists.

Defending human rights and rule of law

Building cyber-resilience goes beyond narrowly defined security measures. It also includes a focus on the protection of human rights online and offline. Organisations such as the Freedom Online Coalition and AccessNow have pointed to a growing trend of intentional internet shutdowns – more than 50 times, by some 25 governments, on almost every continent in 2016 – which not only undermine the freedoms of expression, association, and peaceful assembly online but also damage the socio-economic development of societies. The criticism of such practices by the EU and the US has only exposed them to attacks from various hacktivist groups from the countries concerned. For instance, the Turkish, pro-government Lion Soldiers Team (*Aslam Neferler Tim*) targets organisations seen as insulting national pride, the Islamic faith, or Turkey's leaders. Since 2015, the group has claimed responsibility for attacks on the Ministry of Foreign Affairs and national parliament in Austria, the Central Bank of Greece and Germany, and the European Parliament.

Supporting the multi-stakeholder model of internet governance

The goal of building resilient states and societies is not interpreted in the same way around the globe. Rapid shifts in online demographics – currently 2.5 billion internet users live in developing countries, compared to just 1 billion in the developed world – and the distribution of digital resources, result in a global competition for influence, often in contradiction to European discourse. Russia and China, for instance, are the main drivers behind the proposal for the International Code of Conduct presented to the United Nations by the Shanghai Cooperation Organisation – an initiative that the European Union has often criticised for its insufficient guarantees for the protection of human rights online and the multi-stakeholder model of the cyber-domain. At the same time, as a possible solution to the increasing vulnerability of digital infrastructure, prompted by the unchecked proliferation of the Internet of Things, the International Telecommunication Union (ITU) is promoting a new universal identifier known as 'Digital Object Architecture'. However, should this technology be applied universally, governments may gain access to an unprecedented breadth of information on citizens, undermining their right to privacy and potentially other civil liberties.

A transatlantic perspective on building cyber resilience

There is universal understanding that increasing internet connectivity contributes to economic growth – between 1 % and 2 % GDP growth for every 10 % increase in the connected population.¹ At the same time, there is still limited acknowledgment of the fact that cyber-insecurity constitutes an indirect tax on growth estimated at around 1 % of GDP.² That means that, as the size of the 'digital economy cake' gets smaller due to data breaches or attacks on critical infrastructure, so does the share of EU and US citizens who could potentially benefit from it. The analysis of challenges – and opportunities – to possible EU-US cooperation in building cyber-resilience suggests three main axes of cooperation: the fight against cybercrime, building resilient critical infrastructure, and countering threats to national security through international cooperation.

Fight against criminal networks online

The potential for transatlantic cooperation and the convergence of interests is visible in the case of the fight against cybercrime. In April 2016, an international cyber-gang unleashed malware known as GozNym, that stole US\$4 million from more than 24 American and Canadian banks, credit unions and popular e-commerce platforms in just a few days. A week after launching the attack campaign in North America, GozNym's operators spread a new European configuration that attacked corporate, investment banking and consumer accounts held with major banks in Poland and Portugal. Against this background, possible avenues for EU-US law enforcement cooperation in the fight against cybercrime are being addressed in the EU-US Working Group on Cybercrime, among other fora. Specific commitments in this domain have been made over several years, and include facilitating law enforcement exchanges, including but not limited to those pertinent to child sexual abuse offences, travelling child sexual offenders and network intrusion; collaboration in fighting and disrupting

¹ <http://www.worldbank.org/en/topic/ict/overview>.

² M. Hathaway, C. Demchak, J. Kerben, J. McArdle, and F. Spidaleri (2015), *Cyber Readiness Index 2.0*, Potomac Institute. Available at: <http://www.potomacinstitute.org/academic-centers/cyber-readiness-index>.

cybercrime and enhancing cybersecurity, including through joint research; and promoting adoption of the Budapest Convention and training practitioners on its provisions. In addition, representatives from counterpart US agencies have been placed within Europol's Cybercrime Centre (EC3) and Eurojust with the aim of supporting operational cooperation. For instance, in April 2015, a multinational law enforcement operation led by the EC3 and the Joint Cybercrime Action Taskforce (J-CAT) disrupted the operations of the Beebone botnet, that had installed malware on about 12 000 computers in around 195 countries. Cooperation between Europol, law enforcement cybercrime units in Member States and technology-industry partners operating across the Atlantic helped to dismantle the botnet, known as Zeroaccess, which was responsible for infecting over 2 million computers worldwide and had cost online advertisers US\$2.7 million each month. Cooperation between law enforcement agencies from across the world, led by the FBI and supported by the EC3 at Europol, also ensured the disruption of the Gameover Zeus botnet and the seizure of computer servers crucial to the malicious software known as CryptoLocker.

Improving resilience of networks

Beyond the fight against cybercrime, the EU and US may have a strong interest in developing joint approaches – or at least ensuring close coordination and sharing best practices – with regard to protection and building resilience of their critical infrastructure networks (e.g. energy, transport and financial systems). Given the extent to which the EU and US are interconnected, the economic and social implications of such attacks on either side of the Atlantic could have a huge impact on the economy, and potentially stability, across the transatlantic area. Attacks on critical infrastructure – albeit on a small scale – are nevertheless quite common. In 2015, a report³ released by the German Federal Office for Information Security confirmed that a German steel mill suffered 'massive' damage, as a result of a cyber-attack manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down.⁴ In April 2016, multiple forms of malware were found in a German nuclear energy plant in Gundremmingen.⁵ Even though the types of malware discovered suggest an accidental infection rather than a targeted attack, the news reaffirmed the persistent vulnerability of critical infrastructure networks. Given that there is almost universal agreement on the growing risk of cyber-attacks on critical infrastructure, the EU and US may need to enhance their cooperation in preparing for a transatlantic 'cyber Katrina'. Currently, the EU-US Working Group on Cybersecurity provides a setting for discussions along several strands, including those focused on public-private partnerships and incident management, but most commentators are clear that this dialogue would possibly benefit from additional political impetus.

³ Bundesamt für Sicherheit in der Informationstechnik (2014) *Die Lage der IT-Sicherheit in Deutschland 2014*. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

⁴ K. Zetter (2015) 'A cyberattack has caused confirmed physical damage for the second time ever', *Wired*, 1 August 2015. Available at: <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>.

⁵ K. Townsend (2016) *Concerns raised over malware in German nuclear plant*, 27 April 2016. Available at: <http://www.securityweek.com/concerns-raised-over-malware-infecting-german-nuclear-plant>.

Countering threats to national security through international cooperation

Due to the fact that criminal networks often operate in several jurisdictions, or receive support from third-country governments, and that some cyber-attacks might pose a serious threat to a state's security – potentially resulting in military conflict – a transatlantic discussion about secure and safe cyberspace would necessarily involve both diplomats and military staff. Several instances illustrate that this is indeed the case. For example, in November 2015, air traffic control systems across much of Sweden were unavailable, resulting in the cancellation of multiple domestic and international flights at the airports of Arlanda, Landvetter and Bromma. Sweden reportedly suspected that a hacker group linked to Russian military intelligence service (GRU) was responsible for an attack and passed this information on to NATO members, such as neighbouring countries Norway and Denmark. Another example is a growing cyber-threat posed by terrorist groups.

Even though, to date, the attacks by jihadi groups such as ISIL/Da'esh have been limited to compromising social media accounts or defacing websites, the announcement of a new group called the 'United Cyber Caliphate' (following the merger of several groups) raises new concerns regarding ISIL/Da'esh cyber capabilities. In both cases, the need to think in broad national security terms (something which law enforcement and critical infrastructure operators are not always used to doing), and a possible response going beyond law enforcement, technical measures and national borders (which other actors are not empowered to do), may bring diplomats and 'cyber soldiers' into the picture.

With regard to international security, the EU and US generally seek greater stability and promote norms of responsible state behaviour and compliance with existing international law in cyberspace. Even though the successive reports by the United Nations Governmental Group of Experts (UN GGE) provide a general framework for EU-US cooperation, the fiasco of the most recent meeting of the UN GGE, which was expected to present its report in June 2017, clearly point to the limits of the political process within the UN system. Nonetheless, the conclusions of the UN GGE report published in June 2015, to which both EU Member States and the US have actively contributed, set the stage for possibly advancing the conversation about the application of existing international law to cyberspace and norms of responsible state behaviour.⁶ These, for instance, forbid states from knowingly allowing their territory to be used for cyber-attacks; to conduct or knowingly support attacks that damage critical infrastructure; to conduct or knowingly support activity intended to harm the information systems of another state's emergency response teams (CERT/CSIRTS), and to use their own teams for malicious international activity. The efforts aimed at promoting the implementation of these norms globally and through regional organisations (including the OSCE, ASEAN Regional Forum, and the Organization of American States) offer a possibility to streamline EU-US cooperation in this respect. The EU and US are also at the forefront of discussions on confidence-building measures that may minimise the risk of misunderstanding and help avoid escalation and conflict in cyberspace. To that effect, both sides work closely in the framework of the

⁶ United Nations (2015), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=E.

Organization for Security and Co-operation in Europe (OSCE). The agreement between the EU Computer Emergency Response Team (CERT-EU) and the NATO Cyber Incident Response Centre (NCIRC), signed in February 2016, and the EU-NATO Joint Statement issued at the NATO Warsaw Summit in July 2016, provide an additional opportunity to strengthen cooperation between the EU and the US.

Cautionary tale for policy- and law-makers

Several studies demonstrate that vulnerability to digital risks and the total costs it implies may be reduced, provided certain features are in place, including a national cybersecurity strategy and an adequate institutional framework.⁷ Both EU and US cybersecurity strategies list stronger relations with international partners as one of the mechanisms towards preserving open, free and secure cyberspace. They also recognise engagement with key like-minded partners as a possible way towards promoting their respective political, economic and strategic interests. Given the scope of their bilateral relationship, shared values and the exposure to similar threats, the EU and US may be natural partners in cooperating to counter online criminal networks, improve resilience of their societies, and counter the threat posed by third parties. However, despite these concurrent objectives, policy and law-making in relation to various cyber-related aspects suffer from several weaknesses.

First, awareness and understanding of cyber issues in broader policy cycles is often limited. This is partly due to the perception of cybersecurity as an exclusively technical matter. However as the scale of malicious incidents throughout 2016 and 2017 has proven, the cyber-domain is increasingly becoming another dimension in which political, economic and ideological interests collide. In order to better grasp the complexity of cyberspace as yet another domain of political activity – beyond the current understanding of it as a mere 'instrument' or 'tool' – there is a clear need to demystify cyber-related concepts and issues.

Second, policy-makers and legislators are often confronted with imperfect information and subject to a quasi-monopoly on cyber-related intelligence from the private sector and private-sector risk management companies with a clear interest in promoting a specific vision of the cyber-domain – one full of risks to the economy and national interests. While there is certainly a real danger, the evidence supporting such claims is often interest-driven in order to push for additional investment in cybersecurity or to achieve certain policy outcomes. For instance, Microsoft has used the havoc caused by the recent wave of 'WannaCry' ransomware attacks in Europe and the United States to promote its idea for a 'Digital Geneva Convention' – a concept in clear contradiction to the approach adopted by the European Union and like-minded countries, which maintain that existing international law also applies in the cyber-domain.⁸

In addition, evidence concerning the impact of specific policy choices is simply missing, or is ambiguous in the absence of reliable data concerning the scale of potential benefits from cooperation or the costs of the absence thereof. For instance, some studies suggest that, by 2025, internet-related technologies such as mobile internet, the Internet of Things and cloud computing will generate potential economic benefits

⁷ See, for instance, security guidelines and recommendations published by the European Union Agency for Network and Information Security. Available at: <http://www.enisa.europa.eu>.

⁸ Council of the European Union (2017), Council Conclusions on Framework for a joint EU diplomatic response to malicious cyber activities ('cyber diplomacy toolbox'), 19 June 2017.

of between US\$8.1 trillion and US\$23.2 trillion annually.⁹ However, there is no reliable information on how many internet-connected devices are in use, even today. At the same time, 'guesstimates' of the cost of cybercrime and cyber-insecurity also vary significantly in their scope. Some studies show that up to 20 % of the US\$3 trillion that the internet economy contributes to the global economy is lost due to cybercrime (US\$400 billion).¹⁰ A different study conducted regularly by the Ponemon Institute estimates the average total cost of a data breach at US\$3.79 million. Simulations of the potential impact of a large-scale cyber-crisis in critical infrastructure are also common. One such model, focused on a cyber-attack on the power grid in the north-eastern United States, estimates that, in addition to severe impact on the population (e.g. a rise in mortality rates as health and safety systems fail, and disruption to water supplies as electric pumps break down), such an attack could potentially cost the US economy between US\$243 billion and US\$1 trillion.¹¹ While such numbers can help policy-makers when thinking about and designing policy solutions, they need to be read and used with a high degree of caution. This is further complicated by the fast pace of technological progress, which often leaves policy-makers 'behind the curve'.

About this study and its findings

Recognising the complexity of potential EU-US cooperation in building cyber-resilient states and societies, this report examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues on which policy-makers on both sides of the Atlantic could work together, and explains where cooperation is impeded. Looking critically at the publicly available data, the main findings of this report suggest that:

- In spite of their high visibility, the direct economic costs of genuine cybercrimes are relatively low in both the EU and US. For instance, the reported criminal revenues from frauds and scams worldwide, including ransomware, were below US\$1 billion in 2015. This equates to a per capita cost of less than US\$1.50 per person in the US and EU. The costs of traditional categories of crime that have migrated online – such as tax evasion and welfare fraud – outstrip the direct costs from other categories many times over. Given their transnational nature, any cooperation between the EU and US could be important in reducing or containing these direct costs in the future.
- The indirect losses from cybercrimes are greater than the associated direct costs. While hard to estimate reliably, security concerns prevented around one-in-six EU consumers and enterprises from performing a task online in 2015. This suggests that building greater trust in digital technologies – by making them more secure – could bring large economic benefits through reducing the indirect losses resulting

⁹ McKinsey Global Institute (2013), *Disruptive technologies: Advances that will transform life, business, and the global economy*. Available at:

http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

¹⁰ Centre for Strategic and International Studies (2014), *Net losses: estimating the global cost of cybercrime*, June 2014. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

¹¹ Lloyd's (2015), *Business blackout. The insurance implications of a cyber attack on the US power grid*. Available at: http://www.lloyds.com/~media/files/news_and_insight/risk_insight/2015/business_blackout/business_blackout20150708.pdf.

from cybercrimes. The EU and US could work together to ensure that more secure technologies are made available – particularly given that the EU is a net importer of these technologies from the US.

Many of the available statistics cited are not the soundest methodologically – but are the only ones available. Unfortunately, some of the most reliable data on the frequency of cybersecurity incidents and their impact on enterprises, such as the US National Computer Security Survey, have not been conducted in over a decade. The Eurostat surveys on cybersecurity-related issues do not contain questions on the impact of incidents on firms or individuals. Major improvements are needed in the data and statistics available for cybercrime/cybersecurity incidents and impacts.

EXECUTIVE SUMMARY

Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has permitted costly new forms of crime ('cybercrime') to emerge and has created new, systemic risks to transatlantic and national critical infrastructures.

A great deal is at stake. The smooth functioning of our economies and societies is increasingly reliant on digital technologies. This reliance and dependency – in both the EU and US – is only likely to increase in the future. Alarming, the failure of these technologies can be precipitated by a complex array of state or non-state actors, with differing means and motives, or simply – and commonly – by the accidental actions of operators and technical malfunctions. Stakeholders in the EU and US face these same threats and vulnerabilities.

The transnational nature of these phenomena precludes effective and cost-effective policy solutions being implemented unilaterally by any one nation. The failure of critical information infrastructures – such as submarine cables, the Domain Name System and internet exchange points – have impacts that are inherently transnational. Likewise, many forms of cybercrimes can be perpetrated across borders – safely out of the reach of a single national jurisdiction and authority of police and law enforcement agencies.

Cooperation between stakeholders in both the EU and US is desirable to develop and implement policies to increase the security of these technologies. However, because a zero-risk scenario is neither realistic nor cost-effective, we also need to enhance societal resilience to the risks that these technologies create. Without effective cooperation, it will be difficult to develop and implement policies to address such a complex and global environment.

This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues upon which policy-makers on either side of the Atlantic could work together, and explains where effective cooperation may be impeded. Finally, this report provides a set of suggestions of areas in which the EU and US might cooperate in the development and implementation of policies with the goals of improving cybersecurity, reducing cybercrime and eventually improving cyber-resilience.

TABLE OF CONTENTS

1. FOREWORD.....	i
EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	3
2. Introduction.....	5
3. Methodology	8
3.1. Benefit-cost framework.....	8
3.2. Key definitions	12
4. Indirect benefits of digital technologies.....	16
4.1. Economic growth.....	16
4.2. Employment creation	18
4.3. Productivity increases.....	20
4.4. Consumer surplus	23
4.5. Indirect benefits to critical infrastructure operators	24
4.6. Conclusions.....	25
5. Cybercrime: Direct costs and indirect losses.....	26
5.1. Direct costs	26
5.2. Indirect losses	30
5.3. Conclusions.....	34
6. Cyber-resilience of critical infrastructure: Costs and risks.....	34
6.1. Transatlantic critical information infrastructure.....	36
6.2. Cybersecurity-related risks to critical infrastructure	38
6.3. Direct costs of investment in improving cyber-resilience.....	39
6.4. Indirect losses from past disruption and failures of critical infrastructure.....	41
6.5. Conclusions.....	47
7. Current and potential EU-US cooperation	48
7.1. Looking ahead: issues for EU-US cooperation.....	51
7.2. EU-US competition	56
7.3. Conclusions.....	59
8. Main references.....	61
9. Appendix 1: Direct costs of cybercrimes	73
10. Appendix 2: Sources for direct cybercrime cost figures.....	74
11. Appendix 3: Consumer surplus.....	76
12. Appendix 4: Comparing sector-specific regulatory focus of EU NIS Directive with US critical infrastructures	78
13. Appendix 5: Comparing the EU NIS Directive with equivalent US policy.....	79

List of main acronyms used

APEC:	Asia-Pacific Economic Cooperation
CDCs:	Centres for Disease Control and Prevention
CERT:	Computer Emergency Readiness (or Response) Team
CSIRT:	Computer Security Incident Response Team
ECB:	European Central Bank
EU:	European Union
€:	Euro
FBI:	Federal Bureau of Investigation
FISMA:	Federal Information Security Modernization (FISMA) Act
GAO:	Government Accountability Office
GDP:	Gross domestic product
IC3:	Internet Crime Complaint Center
ICTs:	Information and communication technologies
IoT:	Internet of Things
MLAT:	Mutual legal assistance treaty
NATO:	North Atlantic Treaty Organization
NIS:	Network and Information Systems
OECD:	Organisation for Economic Co-operation and Development
PPP:	Public-private partnership
R&D:	Research and development
SARS:	Severe acute respiratory syndrome
SEPA:	Single Euro Payment Area
UN:	United Nations
US\$:	United States dollar
WHO:	World Health Organization

2. Introduction

Over the past two decades, a relatively 'open internet'¹² and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the proliferation of relatively insecure digital technologies has permitted costly new forms of crime to emerge and has created new, systemic risks to transnational and national critical infrastructures. Faced with these new security – and ultimately economic – challenges, stakeholders in both the EU and US may see advantages to working together to improve the security of these technologies and strengthen collective responses to cybersecurity incidents.

The transnational nature of these phenomena in some way precludes effective policy solutions being implemented unilaterally by any one nation. The failure of critical information infrastructures – such as submarine cables, the Domain Name System and internet exchange points – have impacts that are inherently transnational. Likewise, many forms of cybercrime can be perpetrated across borders – safely out of the reach of a single national jurisdiction and authority of police and law enforcement agencies.

Cooperation between stakeholders in the EU and the US is therefore desirable to develop effective and ultimately successful policy in these areas. However, in spite of congruence in policy goals, the EU and US sometimes find it difficult to operationalise such cooperation. Policymakers in the EU and the US face a global environment where cooperative endeavours will be increasingly necessary given shifts in the composition of internet users. For instance, in 2000, internet users in the US and Europe comprised 26 % of all global users. By 2014, this proportion had fallen to 9 %. Over the same period, China's internet users rose from 6 % to 21 % of global internet users (Twomey, 2015). This continued shift in composition has and will have important consequences on cybersecurity and cybercrime and, in a diminished global position, the US and Europe will possibly find it increasingly difficult to protect their values and interests effectively.

On a more operational level, policy-makers in the EU and the US face five particularly difficult issues that hamper the development and implementation of policies to address cybercrime, improve cybersecurity and strengthen cyber-resilience. These issues subsequently impede effective cooperation because they impair clear and effective decision-making on both sides of the Atlantic.

Coping with a dynamic environment: Technological change is dynamic, non-linear and difficult to predict. New cybersecurity threats and vulnerabilities emerge with each new wave of digital technologies. This makes forecasts or predictions about the future impact of technological change, such as the Internet of Things or artificial intelligence, inherently speculative.

Making policy decisions with a deficient evidence base: Much of the data and information that serve as inputs to public policy debates about the effects of cybercrime, cybersecurity and cyber-resilience are developed by security vendors, software developers and other interested parties. These studies often lack the rigor

¹² Relatively 'open internet' being defined as a system characterised by people's ability to do more activities online, 'whether it is starting a business, creating new services or revolutionising existing ones, expressing opinions, raising capital, sharing knowledge and ideas, conducting research, interacting with government or using a map.' (OECD, 2015a)

and objectivity required to make sensible public policy choices. Policy-makers thus do not always base their decisions on the most reliable evidence. Moreover, it is not clear how much public funds are spent on cybersecurity and cybercrime policies and to what specific end. In the US, this has partly to do with the fact that intelligence agencies have been some of the largest recipients of said funds. In the EU, the spending figures were not included in the EU cybersecurity strategy itself¹³ and the spending of individual Member States is not monitored regularly. It is thus not clear if and how much individual Member States are investing in combatting cybercrime or improving cybersecurity.

Determining the optimal allocation of public funds: Cybersecurity policy decisions should lead to outcomes where the social and economic benefits of a policy intervention outweigh the related costs. In the event that the policy intervention does not deliver a net economic and social benefit at least equal to the long-term bond rate, then public resources are not being used in an optimal way (OECD 2011). The economics of security spending make it impossible to achieve 100 % security against all threats over time (OECD, 2015b). Governments and companies have finite limits on the amount of money that they can spend on security. Add to this that security spending is subject to diminishing marginal benefits.¹⁴ The volume of spending does not automatically and proportionately translate into more/less security. All of these elements make a risk management approach essential, so as to effectively deploy finite resources to policies that reduce the potentially most costly risks associated with cybersecurity and cybercrime (ibid).

Determining which security measures ‘work’: At present, there is a dearth of evidence as to the policies that ‘work’ and those that ‘don’t work’. Cybersecurity is an area where the outcomes are rarely measured (Herley et al. 2014). In spite of many countries having implemented national cybersecurity strategies, and having invested many billions of taxpayer funds, over the past decade, very few of these policies have been subjected to any form of evaluation. Very often measures are introduced to ‘improve security’, potentially impose substantial efficiency/productivity costs, that have no security benefits whatsoever, or make the problem worse¹⁵ e.g. example password policies.¹⁶ Identifying which measures work and under what conditions, is essential for the improvement of cybersecurity and cybercrime policies in the future.

¹³ Though some figures can be found in the impact assessment for the strategy.

¹⁴ At a certain point, the marginal benefits from each additional dollar or euro spent becomes so small that additional spending becomes uneconomic. Every dollar or euro of taxpayer funds spent on cybersecurity or cybercrime is a dollar taken away from some other public service.

¹⁵ Cybersecurity policies come with substantial costs of their own – which can potentially be higher than the costs of no intervention at all. The phenomenon, called *iatrogenics*, was common in the medical field prior to the early twentieth century. In simple terms, going to the doctor would increase one’s probability of dying (Taleb 2014). This situation began to change in the early 20th century with the advent of science-based medical practices, which require that the results of treatments be testable and [reproducible](#).

¹⁶ For years the security mantra has been that people change their passwords periodically (e.g. every three months) (Brand & Makey, 1985). When subjected to study though it has been found that such an intervention has little to no security benefits particularly in light of overall costs it imposes on organisations (e.g. increased IT support costs for personnel to revoke/reset forgotten passwords) and users (e.g. time taken to reset forgotten passwords) (Zhang et al, 2010; Chiasson & van Oorschot, 2015).

Avoiding government failure when attempting to remedy market failure: Government interventions to correct market failures may, in turn, create systemic failures of their own (so-called ‘government failures’). When attempting to address the many market failures that lead to poor cybersecurity (Dean, 2015), policy-makers require a way in which to monitor programme and policy performance. This would reduce the occurrence of government failure. Such a performance monitoring and evaluation mechanism does not yet exist.

Section three of this study presents **the methodology** used throughout the report. It provides an explanation of the benefit-cost framework used to provide a scale of the economic costs, losses and benefits associated with cybercrime, cybersecurity and cyber-resilience. It then defines some key economic concepts and terms that underpin the report.

Section four provides an **overview of the indirect economic benefits** that accrue from the adoption of digital technologies. Essential to this chapter is the understanding that more secure technologies would lead to greater adoption and use, which in turn may generate additional indirect economic benefits for the EU and US alike.

Section five examines the **direct costs and indirect losses due to cybercrime**. In a sense, the direct benefits of greater cybersecurity and less cybercrime are seen in cost-avoidance. That is, the cost and loss figures cited in this chapter represent a ceiling on the maximum benefits that could be achieved through efforts to improve cybersecurity or reduce cybercrime.

Section six explores the **cybersecurity risks of critical infrastructure**. In particular, transatlantic critical information infrastructure such as submarine fibre optic cables, the Domain Name System (DNS) and internet exchange points. The potential direct costs and indirect losses from disruption or failure of critical infrastructures, whether intentionally or accidentally, are examined with reference to past events and possible future scenarios.

Section seven provides an **overview of the global context** for the development of digital technologies. Particular focus is given to trends that have a direct bearing on EU and US cooperation in relation to the international environment.

Based on the discussion presented in this study, section eight offers **policy recommendations** on ways in which the EU, its Member States, and the US might possibly pursue cooperative initiatives that could increase cyber-resilience, increase cybersecurity and reduce cybercrime, thereby maximising the economic benefits that more secure digital technologies have to offer.

To explain, weaker passwords end up being the outcome of an intervention intended to strengthen passwords. Mandated, periodic password changes for someone with many accounts requires that person to remember many, changing passwords. It simply isn't humanly possible to remember more than 7-8 continuously changing passwords. To cope, the person reuses the same passwords across accounts. This creates a new risk with higher negative outcomes because if someone hacks one account/password, he/she can now access all of someone's accounts. The same conditions lead people to write down their passwords and stick the post-it to the monitor, which again creates new security risks. People also tend to make small changes to their passwords with each iteration, which then makes it easy to develop algorithms that can quickly guess what someone's new password is based on their old ones.

3. Methodology

This study focuses on cybercrime, cybersecurity and cyber-resilience. While much care has been put into maintaining this focus, due to the nature of the technologies involved and the overlap between concepts that are still in flux, reference will also occasionally be made to related topics or issues including: data protection, data privacy, internet governance, and digital trade, among others. The study does not focus on military aspects of cybersecurity.

3.1. Benefit-cost framework

A benefit-cost framework has been used in this report to help policy-makers understand the *scale* of the various economic costs and losses associated with cybercrime as well as benefits of cybersecurity and cyber-resilience. An economic-centric perspective is rarely taken in policy examinations of these issues. It is a useful perspective because, given that cybersecurity risks cannot be entirely eliminated, a risk management approach is required to allocate finite resources to areas where they can be most productively deployed. An economic perspective, combined with an understanding of probabilities, assists us in implementing a risk management approach. This in turn helps identify areas where EU and US cooperation might reap the greatest benefits, while minimizing costs, in the areas of cyber-resilience, cybersecurity and cybercrime. While the political, social and technical perspectives are important to any policy-making decision, the focus of this study is on the economic perspective. The study should be seen as an input to a policy-making process in which these additional perspectives are also included.

This study integrates two existing frameworks to deliver a benefit-cost framework for cyber-resilience, cybersecurity and cybercrime. For each side of the benefit-cost equation, there is a direct and an indirect component. The statistics presented in each part of the framework provide a partial view of the scale of the costs, losses or benefits in question. They are not intended to be aggregated. These figures present a necessarily incomplete picture. This owes to the dynamic phenomena under examination and the imperfect data available to measure them. The inability to aggregate statistics, however, does not hamper the goal of the framework.¹⁷ These disaggregated statistics allow policy-makers to identify where the possible costs, losses and benefits from EU and US cooperation are (potentially) highest and adjust policy to initiatives which could minimise costs/losses while maximising benefits (given the finite resources available).

¹⁷ Namely, to present a scale of the economic costs, losses and benefits associated with cybercrime and cyber-resilience.

Table 1 – Cost and benefit framework for cybercrimes and cyber-resilience

	Benefits	Costs/losses
Direct	Cost-avoidance	Cost of preventative measures Cost of post-incident recovery Reapportioned wealth from theft
Indirect	Economic growth Employment creation Increased productivity Higher consumer surplus	Foregone economic activity Opportunity costs Efficiency losses

With regard to the assessment of benefits, Gordon and Loeb (2006) define the **direct benefits** from investment in preventative measures as the cost savings (reduced costs and losses) associated with reduced cyber-incidents. This can also be termed ‘cost avoidance’. This applies for organisations and critical infrastructure alike. In a sense, the direct cost and indirect loss statistics in section five of this study are the flip-side of potential benefits. Were preventative measures not put in place, the costs and losses from incidents would be higher. Reductions in these potential costs and losses are the direct benefits of cybersecurity investments.

This paper adapts a framework developed by Hughes et al (2015) to estimate the scale of the **indirect benefits** of more secure digital technologies (‘cybersecurity’). Improvements in cybersecurity, and reductions in the risk of or incidence of cybercrime, lead individuals and enterprises to have greater trust in digital technologies. This increased trust translates into higher adoption of such technologies, and this increased use allows the individuals and enterprises to generate subsequent benefits. These benefits include:

- Increased economic growth;
- Increased employment;
- Increased productivity; and
- Increased consumer surplus.

With regard to **costs and losses**, this study adapts a framework for estimating the costs of cybercrime previously developed by Anderson et al (2012). It expands upon the original framework, which only contained figures on the United Kingdom, by including data on the aggregate for EU Member States and for the United States. With additional resources in the future, the framework could potentially be expanded to include specific estimates for individual EU Member States.

This framework divides the **direct costs of cybercrimes** into three categories: genuine, transitional and traditional cybercrimes.

- Genuine cybercrimes are new forms of crime perpetrated with digital technologies e.g. botnets.
- Transitional cybercrimes are crimes that were once perpetrated offline but are now increasingly, though not entirely, perpetrated online e.g. card fraud, ransomware.
- Traditional cybercrimes were once committed offline but are now largely or entirely committed online owing to adoption of digital technologies e.g. tax evasion.

The **indirect costs and losses from cybercrimes** or poor cybersecurity are those that cannot be linked by a reasonable degree of accuracy directly to a particular incident (Gordon and Loeb, 2006). Such categories typically comprise: loss of customer trust/reputational damage, reduced uptake of digital technologies due to lack of trust, and opportunity costs and foregone productivity associated with the need to invest in non-digital infrastructure (Anderson et al, 2012).

It is important to conceptually distinguish between costs, including opportunity cost, and economic losses. Unfortunately, economic and accounting concepts are commonly misapplied in the literature on cybercrime and cybersecurity (e.g. World Economic Forum, 2010; Symantec, 2013; McAfee and CSIS, 2014; Lloyd's Insurance, 2015). When a cybersecurity incident occurs, like a data breach, there are direct 'costs' incurred by the organisation that has been breached. These costs might include network repair, hiring of security consultants and purchase of credit monitoring services for those affected. These costs represent additional economic activity – people are being paid to do this work. Those people subsequently spend the money they have been paid on other goods and services, thereby contributing to the overall economy through a multiplier effect. This is similar to the way in which an oil spill is accounted for as a positive contribution to GDP. The costs that are not included (externalities), like loss of privacy, are not counted in the cost figures similar to the way that environmental damage isn't factored into an oil spill.

Direct costs are redistributive. Redistribution does not shrink the total capital stock of an economy ('shrink the economic pie'). For example, if a firm incurs a cybersecurity incident, and pays consultants to help repair the damage, then resources are redistributed from one party (the enterprise) to the other (the consultants). For another example, if someone commits fraud and manages to steal money from someone else's account, this represents a redistribution of money from the victim to the thief. **Economic losses** are conceptually different to costs. Economic losses occur when income generating economic activity does not occur or when the perceived value of a good or service is reduced. This is destroyed value – the 'economic pie' shrinks. Costs and losses may occur at the same time. For instance, if wiper malware is used to destroy a network, in addition to the redistributive costs (like consultants) there may also be an economic loss. There are also **opportunity costs** associated with the direct costs of cybersecurity failures, investment in preventative security measures and measures to combat cybercrime.

- For private sector companies, rather than spending funds on security consultants and preventative measures, those same funds could have been invested in activities that contribute to the top-line revenue generating activities or measures to increase the productivity of the firm.
- For the public sector, taxpayer funds spent combatting cybercrime or on improving cybersecurity could otherwise have been invested in other areas where (greater) social benefits might accrue e.g. health or education.

That these funds have to be invested in protecting against incidents that might not eventuate, or against crimes that might be unpreventable, makes the investment decisions problematic. It is for this reason that adopting a risk management approach, grounded in probabilities of incidents and their potential economic impacts, is an essential step towards more effective cybersecurity and cybercrime policy.

When examining the 'costs' of cybersecurity and cybercrime, it is pertinent to ask: who incurs the cost and who receives a benefit? Particular concern should be placed on those outcomes where value is destroyed or not realised rather than instances where value is being redistributed from one party to another. Moreover, attempts to improve cybersecurity, improve cyber-resilience or reduce cybercrime should be weighed against the opportunity costs and efficiency losses that the risk-reduction measures would entail.

Another concept that is frequently misapplied is cost and losses with relation to **intellectual property theft**. A substantial proportion of the estimated economic losses from cybercrime in reports such as McAfee and CSIS (2014) are attributed to intellectual property theft. However, the theft of data is not the same as, for instance, if someone were to rob a bank. When data are 'stolen' in a hack, a copy of the data is typically made. These data are then used subsequently for some purpose which may end up creating additional economic value beyond that which would have occurred had the data only been held by its originator. For instance, a large database of stolen email addresses could be sold on an online network then used to send out sales (or spam) emails. In this scenario, the stolen database has created value for the thief, or for the individual or entity that bought it from the thief, and for the people who subsequently sell products or services to these parties. When talking about the costs or losses from data breaches or theft of intellectual property, it is important not to conflate one form of theft, and its effects, with the other. If data are stolen and/or destroyed, on the other hand, this is a relatively more serious matter. Such a situation represents the destruction of data and the economic value that might have been generated from the data.

To estimate the scale of costs due to intellectual property theft/infringement, the framework for this study uses estimates of the revenues that the operators of intellectual property infringing platforms generate from their activities. Their revenues are, in a sense, the costs to intellectual property right owners in terms of reduced revenue. Again, this is redistributive. The intellectual property rights owners are still free and able to generate economic value from these intangible assets. It is just that another entity or person is appropriating part of those benefits. As with all technological change – there are winners and losers. Piracy and intellectual property theft are distributional issues – who captures the consumer or producer surplus and how much can they capture? This is conceptually different from destroyed economic value. While undoubtedly some music label, film studios and taxi drivers have lost revenue since the late 1990s, at an aggregate level this technological shift has generated large consumer surplus benefits (consumers can access music, films or taxi rides at a lower price than before – at least in the short-term). This unavoidable process, the Schumpeterian gales of creative destruction,¹⁸ is what ultimately drives technological change.

¹⁸ Joseph Schumpeter thought that the process that drives technological progress was one of 'creative destruction'. For technology – and society more generally – to advance, the old has to be replaced with the new. This necessitates modification or destruction of the old but, in its place, something new (and possibly – though not necessarily – 'better') is left in its place.

3.2. Key definitions

The terms '**cyber**', '**computer**', '**information**', '**information and communication**', '**network**' and '**digital**' are used interchangeably in the literature. Throughout this study, every effort has been made to ensure consistency in the use of the terms defined in this section. However, owing to the use of other related terms in various government reports, academic papers, official statistics and surveys, in some cases the term used in the original source material has been used and a footnote provided to help readers understand to what is being referred.

In this report, the term '**cybersecurity**' will be used to refer to the ability of digital technologies to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those digital technologies.

The European Commission defines '**cybercrime**' as: 'Criminal acts that are committed online by using electronic communications networks and information systems. Following this definition, cybercrime comprises three broad categories:

1. Crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
2. Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
3. Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia' (European Commission, 2007).

In the benefit-cost framework used in this study, the cost-side of the framework relating to cybercrime encompasses the EU definition. However, rather than differentiating categories by the type of cybercrime, as per the EU definition, it differentiates the categories by the degree to which a cybercrime is performed online.¹⁹ This decision has been made for two reasons.

First, the EU definition treats crimes/cybercrimes in a binary way. Crimes are either committed 'online' (a cybercrime) or not. Yet in reality, many crimes are and are not cybercrimes at the same time. In the literature, cybercrimes are typically categorised according to whether they are 'computer-assisted' or 'computer-focused' (Yar, 2005); that is, whether a crime is **enabled** by a computer, or simply **enhanced** by the use of a computer (Grabosky, 2007). Categorising cybercrimes according to the narrower EU definition potentially misses certain important or emergent categories of cybercrimes. The spread of digital technologies is gradual. These technologies evolve and new ways in which to use these technologies to commit crimes ebb and flow. This framework's advantage is that it allows for these dynamic elements to be taken into account through a categorisation that is based around wider and more dynamic criteria.

Second, the EU definition of cybercrime does not lend itself well to the identification of the economic impacts from cybercrimes. For instance, the actual committing of a data

¹⁹ In Appendix 1, readers are provided with an alternative presentation of the cybercrime figures in chapter 3, which accords more closely though not perfectly with the EU definition.

breach would fit under category 1 'Crimes specific to the internet' under the EU definition, as a data breach is an attack on an information system. However, the eventual monetisation of the stolen data would fit under category 2 'Online fraud and forgery' (though there is no guarantee that the fraud will be committed online, which in this event would exclude the related data breach from the definition of cybercrime altogether).

Finally, as digital technologies have evolved, it is not always clear what it means to 'commit a crime online' – the key condition for designating something a cybercrime under the EU definition. Such a definition may have made more sense twenty years ago when web browsers were almost the sole means by which people interacted with the internet (that is, were 'online'). Today, people might be online when using peer-to-peer networks or apps or even on the 'darknet' via the TOR ('The Onion Router') browser. This becomes important when examining phenomena, such as tax evasion, which are crimes that are facilitated by digital technologies. The people who commit these crimes are largely online when doing so – though they might not be using a web browser.²⁰ As people's physical lives have become more and more enmeshed with digital technologies, the term 'online' is gradually losing its meaning.

The definition of **critical infrastructure** is relatively similar in both the EU and the US. In the EU, critical infrastructure is defined in Council Directive 2008/114/EC as, 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.' In the US, critical infrastructure is defined in Presidential Policy Directive 21 (PPD-21) of 2013: 'Critical Infrastructure Security and Resilience' as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.' The EU has a subset of critical infrastructure, called **critical information infrastructure**, which is defined as, 'ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)' (European Union, 2008). In the United States, PPD-21 identifies 16 critical infrastructure sectors. Two such sectors, the communications sector and the information technology sector, comprise infrastructures that would partly fall under the EU definition of 'critical information infrastructures'.

This report uses the term '**cyber-resilience**' to refer to the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions to critical infrastructures and critical information infrastructures. Resilience includes the ability to withstand and recover from deliberate cyber-attacks, accidents, or naturally induced cybersecurity incidents. This definition draws on and slightly modifies the definition of 'resilience' from Presidential Policy Directive 21. **Cyber-resilience is different to cybersecurity.** The former focuses on recovering following an incident. The latter focuses on measures to prevent an incident occurring in the first place.

²⁰ Moreover, many phone calls are now done over voice over internet protocol (VoIP), text messaging done by short message service (SMS) but over apps, file management done using the Cloud.

Table 2 – Key concepts and definitions employed in the study

Term	Definition
Costs and losses of precautionary measures	The monetary equivalent of efforts made to prepare for and prevent cybercrime or bolster cybersecurity (Anderson et al, 2012). Costs are seen both in direct terms and in terms of opportunity cost. Losses are seen in terms of lower efficiency/productivity.
Critical infrastructure	An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions. Based on the definition in the EU NIS Directive, which is broadly similar to the definition used in the US.
Cyber-resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions to critical infrastructures and critical information infrastructures. Resilience includes the ability to withstand and recover from deliberate cyber-attacks, accidents, or cybersecurity threats or incidents. Modified definition of 'resilience' from US Presidential Policy Directive 21.
Cybercrime	Criminal acts that are committed online by using electronic communications networks and information systems ('digital technologies'). Cybercrime comprises three broad categories: <ol style="list-style-type: none"> 1. Crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts). 2. Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code. 3. Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia. <p>Based on European Commission (2007).</p>
Cybersecurity	The ability of digital technologies to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those digital technologies. Modified definition of 'security of network and information systems' in the EU NIS Directive.
Digital technologies	<ol style="list-style-type: none"> a) Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed; b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or c) digital data stored, processed, retrieved or transmitted by

	<p>elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.</p> <p>Based on the definition for 'network and information system' in the EU NIS Directive.</p>
Direct benefits from investment in precautionary measures	Cost savings associated with avoiding or mitigating cybersecurity incidents or cybercrime (also termed 'cost avoidance') (Gordon and Loeb, 2006).
Direct costs from cybercrime	'Losses, damage, or other suffering felt by the victim as a consequence of a cybercrime' (Anderson et al, 2012). This might include the amount of money stolen from one's bank account through fraud or money spent hiring cybersecurity consultants following (but not prior to) a data breach.
Cybersecurity risks	<p>A category of risk related to the use, development and management of the digital environment in the course of any activity.</p> <p>Modified definition of 'digital security risks' taken from (OECD, 2015b).</p>
Genuine cybercrimes	New forms of crime perpetrated with digital technologies e.g. botnets (Anderson et al, 2012).
Indirect benefits from investment in precautionary measures	The knock-on effects from greater adoption and use of digital technologies due to allayed security concerns. Seen in higher economic growth, employment, productivity, and consumer surplus (Hughes et al, 2015).
Indirect economic losses from cybercrime	Those activities that are not carried out due to cybercrime, or the prospect of such crimes being perpetrated. This might include lost business (revenues) due to consumers not purchasing a device out of fear that it is not secure or reputational damage leading to lost revenue (Anderson et al, 2012).
Traditional cybercrimes	Crimes once committed offline but now largely or entirely committed online owing to adoption of digital technologies e.g. tax evasion (Anderson et al, 2012).
Transitional cybercrimes	Crimes that were once perpetrated offline but are now increasingly, though not entirely, perpetrated online e.g. card fraud, ransomware (Anderson et al, 2012).

4. Indirect benefits of digital technologies

The past two decades have been a time of a relatively 'open' internet, and freer exchange of digital technologies as well as the goods and services generated and exchanged with their help. Relatively early adoption of digital technologies in the EU and the US has benefited their economies and societies. One of the drivers of the adoption of these technologies is their security (OECD, 2004; OECD, 2015c). If the technologies are perceived to be insecure, a threshold that will differ across individuals and enterprises, they are not adopted and no indirect benefits are realised.

This chapter examines the four primary areas where the adoption of digital technologies has generated **indirect** economic benefits over the past two decades in the EU and US. These four areas are: higher economic growth, particularly through increased cross-border trade; greater employment generation, though mostly in high and low-skilled professions; possible increases in productivity; and short-run consumer surplus gains. Where possible, the following sections offer a forward-looking perspective as to what scale of benefits might be expected in the future were the EU and US to continue and/or possibly deepen cooperation. It should be noted that the **direct** benefits from more secure digital technologies are seen in cost-avoidance (Gordon and Loeb, 2004). Given that these benefits are simply avoided costs or losses, this issue will be covered in the next chapter on costs and losses.

4.1. Economic growth

Across numerous studies, the information and communication technology (ICT)²¹ share of total economic growth is thought to be around 6 % of annual GDP (Hughes et al 2015). This rate of contribution has been stable for many years. It is thought that 20 % of GDP growth has been derived from ICTs over the past decade (ibid). If this is indeed the case, then between 2005-2015 these technologies provided the equivalent of US\$115 billion and US\$50.5 billion in GDP growth on average per year in the US and EU respectively (author's calculations based on World Bank data). However, these figures mask some important underlying dynamics.

First, were these technologies more secure, they may have been adopted by more individuals and enterprises, which would have in turn contributed to higher GDP growth (OECD, 2004; OECD, 2015c). In the EU-28 for 2015, security concerns prevented 15 % of consumers downloading software, music, video files, games or other data files; carrying out banking activities online; or ordering or buying goods or services online. Moreover, 14 % of enterprises in the EU-28 did not partake in online sales in 2015 due to perceived problems related to ICT security or data protection (Eurostat, 2015). This implies that up to one in six individuals and enterprises may have used these technologies for these purposes, which would have contributed to higher GDP growth, but did not specifically due to security concerns.

Second, what has traditionally been classified as the ICT sector has been gradually expanding into what are considered 'traditional' industries or sectors (i.e. energy, transportation, health and education). Therefore, a stable proportion of 6 % of GDP likely understates the current and future contribution of digital technologies to the larger economy. As a new wave of 'Internet of Things' devices are adopted in the consumer and commercial markets, the overall contribution to GDP of digital

²¹ A sub-set of digital technologies, this term has traditionally been used in the economic literature.

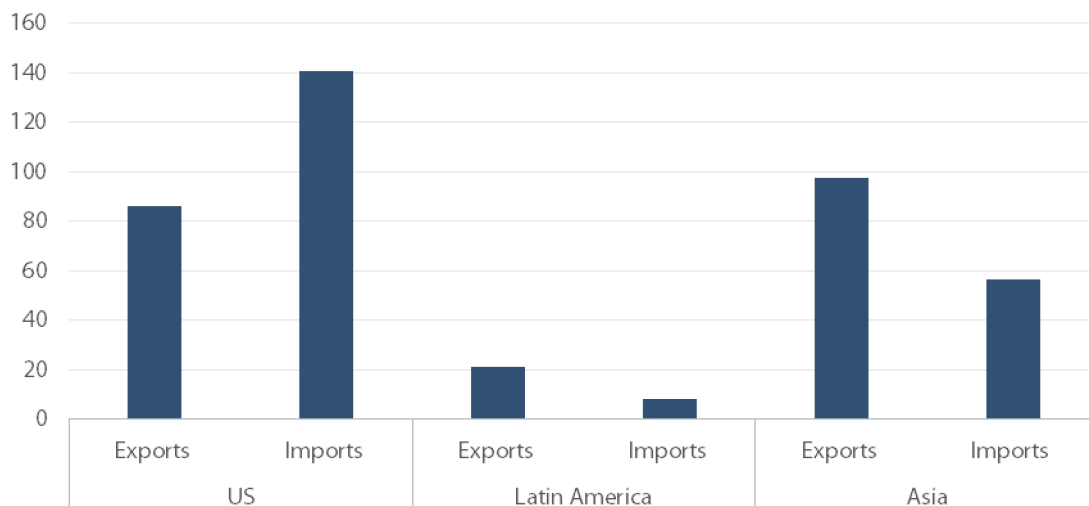
technologies could increase further. If these technologies are more secure, greater adoption will occur, and thus GDP benefits would be greater.

Third, these GDP figures comprise tens of billions of dollars/euros of security spending.²² Security spending, much like cleaning up an oil spill, contributes positively to GDP. While this spending might represent a positive contribution, it possibly represents a net social loss and certainly represents opportunity costs.

A major source of value creation from the internet and digital technologies – particularly for the EU and US – has historically been cross-border trade in products and services. The EU and US are one another's largest trading partners in terms of digitally deliverable services. In 2012, the EU exported US\$86.3 billion and imported US\$140.6 billion worth of such services from the US (Meltzer, 2014). With the emergence of global value chains, made possible at such scale partly by digital technologies, many final goods or services are the result of imports/exports of intermediate components. In 2009, the only year for which this study was conducted, approximately 16 % of EU goods exported included value from imports. This equated to US\$234 billion (ibid).

Figure 1 – EU digitally deliverable services trade, 2012

US dollars, billions



Data source: Meltzer (2013) based on data from the US Bureau of Economic Analysis and Eurostat.

These technologies also provide lower-cost access to global markets for companies that might otherwise not be able to afford such access. Small and medium enterprises (SMEs), in particular, benefit from digital technologies in two primary ways. First, access to larger markets permit them to sell greater quantities of products, thereby increasing revenues. Second, through 'increased access to business services that increase their productivity and global competitiveness' (ibid). However, in light of the current policy initiatives towards 'data localisation', their contribution may potentially be lower in the future.²³ Such requirements are thought to make it 'practically impossible for small businesses that cannot afford to implement separate systems and standards in every country in which they do business' (Nicholson and Noonan, 2014).

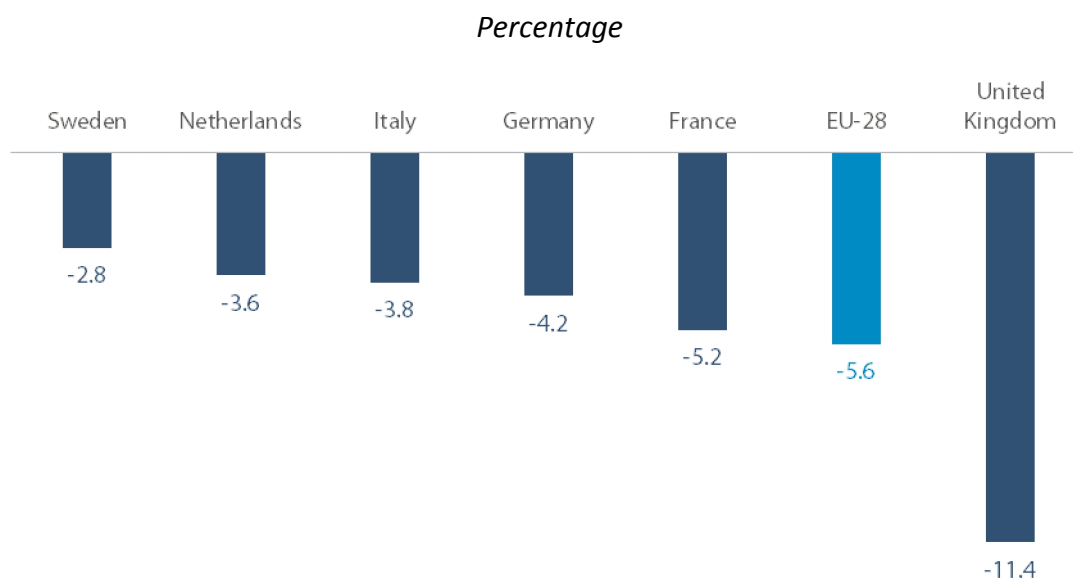
²² Section 3.4.4 goes into detail as to how much this spending/investment has been historically.

²³ See Chapter 6 for an explanation of the trend towards data localisation.

SMEs make an outsized contribution to GDP, employment, and value-added, in both the EU and the US (OECD, 2014a). For this contribution to grow in the future, it is important to ensure that SMEs are able to continue to take advantage of the potential benefits that more secure digital technologies provide.

The EU is a net importer of digital services from the US with a trade deficit of 5.6 % in 2012²⁴. On the one hand, this indicates that the EU is reliant on US companies for access to relatively more secure digital technologies. On the other hand, it also indicates that US technology companies are reliant on EU consumers and enterprises for revenue, which may provide some leverage in policy efforts to improve the security of these technologies.

Figure 2 – Digital services trade balance between US and EU-28 and selected Member States, 2012

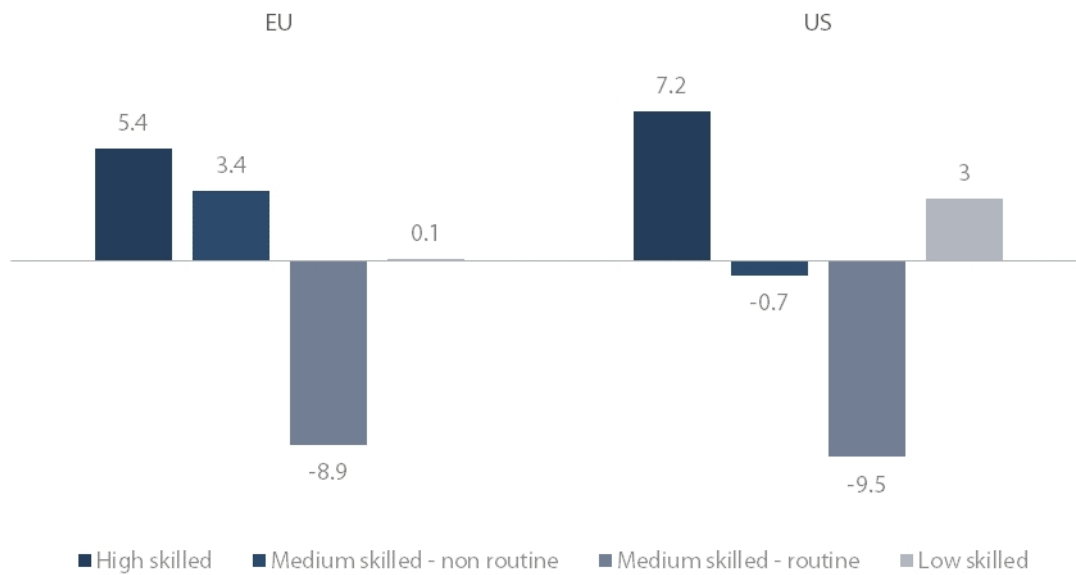


Data source: McKinsey Global Institute based on data from the US Bureau of Economic Analysis and Eurostat.

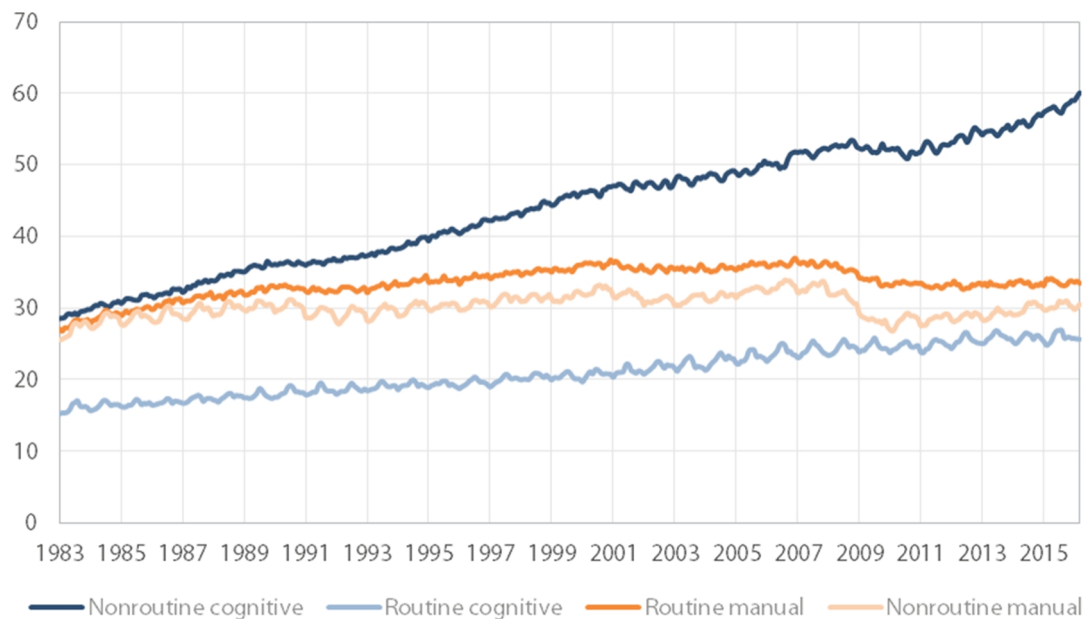
4.2. Employment creation

Digital technologies have had a complicated impact on the composition of jobs and employment in the EU and US. In terms of net job creation/loss, the total stock of jobs has not substantially declined in the OECD region over the past decade (OECD, 2016a). However, occupations that involve routine tasks have experienced declines in both the EU and United States. Over the same period, non-routine (particularly high-skilled) occupations have experienced the highest growth. Low-skilled occupations have also experienced growth in the US, but not the EU (see figures below). This phenomenon has been termed 'job polarisation'. While the OECD cautions that these effects may be attributable to off-shoring or international trade, these processes have also been driven and facilitated by digital technologies.

²⁴ Unfortunately more recent statistics are not available. These statistics do not include the value from intermediate service imports and exports.

Figure 3 – Job polarisation in EU and US, 2002-14*Percentage point changes in employment shares by occupation*

Data source: OECD estimates based on EU-LFS and BLS Current Population Survey

Figure 4 – Employment in the US by relative cognitive requirement and relative routineness, 1983-2013*Persons, millions*

Data source: FRED Graph Observations, Federal Reserve Economic Data, Economic Research Division, Federal Reserve Bank of St Louis.

Looking to the future, two questions are particularly pertinent:

- How digital technologies might contribute to more broad-based employment creation – rather than the ‘job polarisation’ that has occurred over the past two decades; or
- How individuals might be better trained to take advantages of the employment opportunities offered by a drive towards more secure digital technologies.

Regarding the first question, SMEs contribute between 60-70 % of job creation across OECD countries (OECD, 2014a). In particular, a sub-set of small, high-growth businesses (so-called gazelles, which do not stay small for long as they grow in excess of 20 % per annum) make up the lion's share of this contribution (ibid). Digital technologies permit SMEs access global markets at a cost that was previously prohibitive. Yet these same small enterprises unfortunately have less internal capabilities for ensuring their cybersecurity. For instance, in 2015, 27 % of small enterprises and 51 % of medium enterprises had a formally defined ICT security²⁵ strategy in the EU-28. This compares to 72 % of large enterprises that same year (Eurostat, 2015). In the future, ensuring SMEs continue to have access to a global market via the internet, and the cybersecurity knowledge and technical capabilities to take advantage of this access, will be important, if this class of enterprises is to continue to make an outsized contribution to job creation (among other indirect economic benefits).

Concerning the question of digital skills, it is expected that demand for employees with skills relevant to enterprises with cybersecurity needs will increase in both the EU and US over the coming years.

- In the EU, the employment growth rate for ICT specialists²⁶ has averaged a 3 % growth per annum since 2006 (Eurostat, 2016a). This was more than eight times higher than the average growth rate of total employment over the same period. Some 41 % of EU enterprises which recruited or tried to recruit ICT specialists in 2015 reported difficulties in filling vacancies, indicating some tightness in the labour market (Eurostat, 2016b).
- Some EU Member States have announced public sector hiring for cybersecurity specialists. For instance, in France, the government plans to hire 2 600 cybersecurity experts in 2017-2019 for its new Army Cybersecurity Command (Reeve, 2016). Aggregate figures on public sector hiring for cybersecurity across all EU Member States are not yet available.
- The US Bureau of Labor Statistics (2014) forecasts projected growth of 14 800 new information security analyst positions in 2014-2024. The rate of growth for information security analysts is expected to be 18 %, which is faster than the rate for 'computer occupations' (12 %) and 'all occupations' (7 %).
- The US Department of Defense has hired 6 000 cybersecurity experts in recent years (Nakashima, 2014). Other Federal agencies have hired 6 500 more information technology and security specialists over the course of 2016 (White House, 2016a). The US Commission on Enhancing Cybersecurity (2016) has recommended training 100 000 new cybersecurity practitioners and an apprenticeship programme for 50 000 more by 2020.

Policymakers should focus on ensuring that education and training programmes provide skills relevant to these growing occupation categories.

4.3. Productivity increases

Debate continues regarding the contribution of digital technologies to productivity growth. Studies such as Jorgenson (2005) claimed that information technologies²⁷

²⁵ The term 'ICT security' is used in the survey instead of 'cybersecurity'.

²⁶ Not 'cybersecurity specialists', a category which Eurostat does not use.

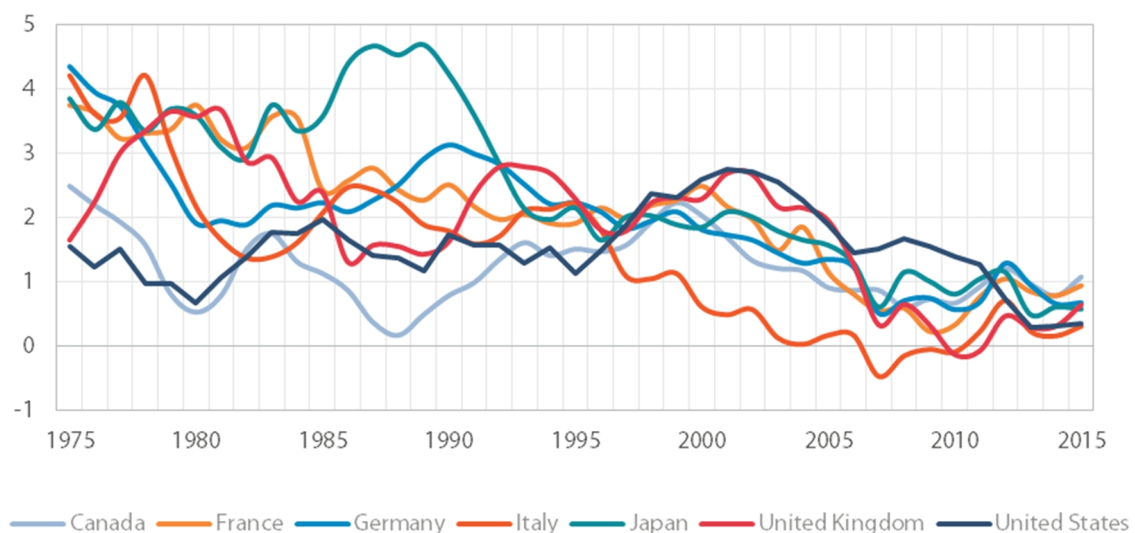
²⁷ Term originally used in the paper.

accounted for 48 % of labour productivity growth in 1995-2004 in the US. A number of other studies claim that productivity gains from these technologies were most noticeable in industries where these technologies were being developed rather than those where they were being adopted (Oliner & Sitchel 2000, Jorgenson 2001, Stiroh 2002).

Yet, as Robert Solow once stated, 'You can see the computer age everywhere but in the productivity statistics'. Termed the 'productivity paradox' or 'secular stagnation', for some time economists have attempted to explain falling productivity rates. The adoption of digital technologies from 1990-2000 saw what was to be a temporary productivity boost. It is thought that, 'the surge in productivity in the US economy for nine years starting after 1995 was linked to the rapid drop in semiconductor prices' (Baily et al, 2016). These gains were short-lived. Productivity rates then fell far below their historical average over the subsequent decade in both the EU and the US (see figure below). While annual productivity growth rates on both sides of the Atlantic were between 2-3 % in the late 1970s, these rates have fallen below 1 % over the past decade.

Figure 5 – Slowing labour productivity in G7 countries, 1972-2014

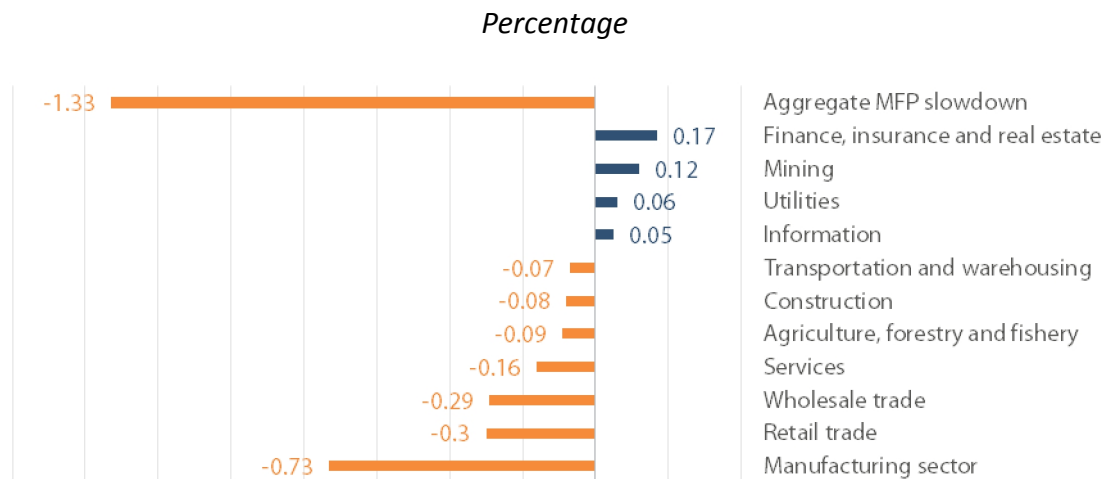
Annual growth, five-year moving average, %



Data source: OECD.

More up to date figures on the sectoral contributions to multi-factor productivity growth in the US show net declines in most sectors (see figure below). The earlier period (1995-2004) was the initial phase in which digital technologies were adopted in the US. Productivity growth during the earlier period was not repeated in the later period (2004-2014) across many sectors in the economy.

Figure 6 – Contributions to multi-factor productivity (MFP) growth 2004-2014 minus contributions 1995-2004, United States, by sector



Data source: Baily et al 2016.

No conclusive answer has yet been reached as to why this has occurred. One explanation is that a cohort of high-performing enterprises ('frontier firms') have pulled ahead of their less productive competitors ('laggards'). The best practices developed by the frontier firms have not diffused to the laggards – thereby explaining lower overall productivity growth (Baily et al, 2016; Andrews, Criscuolo, and Gal, 2016; Decker, Haltiwanger, Jarmin, and Miranda, 2016). Possible reasons for this lack of diffusion include: lack of competition, lack of managerial capability to adopt best practices, lack of worker skills, continued cyclical weakness, and regulation (Baily et al, 2016). If this is indeed the case, policy-makers might consider ways to remove the barriers to knowledge diffusion. Digital technologies play an important role in the diffusion of knowledge and facilitation of collaboration throughout economies (OECD, 2017a). Ensuring that these technologies are more secure might be one way in which to encourage their adoption and use, which might in turn stimulate greater knowledge diffusion and thus productivity growth.

However, it may also be the case that more secure technologies result in measures that impede use, which could in turn reduce efficiency/productivity. For instance, a password policy that requires changes every three months means that a percentage of people will forget their new password and thus have to go through the reset process. The security measure, in this instance, has reduced the productivity of the person, who loses time not just having to reset the password every three months, but once again if forgotten. The way in which the security of technologies is increased is therefore an important element and will differ depending on the technology in question. One example of a measure to make a technology more secure without reducing 'usability' (and thus reducing productivity) is the 'baked-in' encryption now available with widely-used instant messaging applications (e.g. Whatsapp). While just one example, the principles of which do not apply across all cases, this points to one way in which security may be increased without sacrificing potential productivity gains.

4.4. Consumer surplus

The consumer surplus is the difference between the maximum that a person would be willing to pay for a good or service and the actual price of that good or service. When prices fall below that which users are willing to pay for a product or service, the consumer surplus increases.²⁸ The underlying intuition is that a consumer is getting more benefits (i.e. greater utility) from a good or service than that which they have paid for. Measures of gross domestic product do not include the economic surplus, of which the consumer surplus is one part (Katz, 2012).

One of the major benefits that digital technologies deliver to consumers is lower prices of certain products and services. These reductions in prices may be driven by declining unit prices, which are, in turn, driven by productivity gains in the presence of competition (Katz, 2012; Hughes et al, 2014). The consumer surplus may also increase due to a shift left in the demand curve, which is the consequence of more consumers using the digital technology in question. This latter point is important as one driver of increased technology adoption and use is its perceived level of security.²⁹

Precise estimates of the consumer surplus are difficult to model because they require comprehensive data on consumers' maximum willingness to pay. In practice, this is extremely costly and generally infeasible, particularly when attempting to model all products/services available in an entire country at any point in time. Greenstein and McDevitt have undertaken many studies that estimate the consumer surplus related to broadband internet (Greenstein and McDevitt, 2009; 2012). In the 2012 study, it was estimated that the annual quality-adjusted consumer surplus for the 30 OECD countries was US\$436.9 billion in 2010 or about 0.89 % of GDP. In a 2009 study, focused on the US between 1999 and 2006, the authors determined that in 2006 the consumer surplus generated by broadband represented US\$7.5 billion. However, broadband prices are but one of many products and services related to digital technologies, albeit an integral one. This suggests that the total consumer surplus gains from these technologies are far higher. By examining the findings of a number of other studies, an idea of the scale of these consumer surplus gains can be acquired.

A study by Cohen et al (2016) looked at the consumer surplus effects that Uber had in four US cities in 2015. The authors estimated such benefits to have amounted to US\$2.9 billion. A different study, by Brynjolfsson and Oh (2012), examined the value of free services available via the internet.³⁰ They estimated an increase in consumer surplus from these services to be over US\$100 billion per year in the US alone. Chen, Jeon and Kim (2013), of the University of Michigan, examined consumer surplus gains based on how much time people save by using search engines for their information needs relative to undertaking an equivalent offline search. On average, it took participants seven minutes to answer the questions using a search engine, and 22 minutes using the University of Michigan's library (The Economist, 2013). Hal Varian, Google's chief economist, used these findings to estimate US\$500 in consumer surplus

²⁸ For a more in-depth explanation of this concept, see Appendix 3.

²⁹ Greater security results in greater adoption/use and subsequently larger consumer gains in the short-run.

³⁰ Many online services, such as search engines or social networks, are 'free' in monetary terms to the end user. However, users end up paying with their time ('attention') and with personal or behavioural data – which are extremely valuable – that are collected by the online service provider.

gains per Google user annually then extrapolated this out to US\$65 billion-US\$150 billion in the US annually (Varian, n.d.).

All these estimates point to very large consumer gains in the short-run relative to the other indirect benefits from digital technologies. However, there is no guarantee that such gains will continue to accrue in the long-run. This is because increasingly pervasive data collection is permitting companies to exercise greater price discrimination (sometimes termed 'price personalisation'). The airline industry has performed such pricing practices for many decades. Now companies like Uber, with its surge pricing, and Amazon, through cookie-based price targeting, are adjusting prices more closely to consumers' maximum willingness to pay. When such pricing occurs, the consumer surplus is appropriated by the company thereby becoming a producer surplus. This means that an increasing proportion of the total economic gains are captured by producers rather than consumers.

4.5. Indirect benefits to critical infrastructure operators

It is thought that the installation of (potentially internet-connected) sensors to infrastructure in various sectors, sometimes referred to as the 'Internet of Things' or 'Smart Cities', 'Internet of Everything' or the 'Industrial Internet', will generate various and substantial economic benefits over the coming decade. For example, one account by Thierer and O'Sullivan (2015) claims that, 'Improved industrial monitoring and automation techniques will help manufacturers and distributors to quickly pinpoint inefficiencies, minimise waste, and streamline processes.... 'Smart' city technologies can help municipalities to improve service delivery and save resources through infrastructure monitoring and automatic optimisation'. One would expect to see indirect benefits to infrastructure operators in terms of higher productivity and cost-reductions. In turn, these two elements might translate into lower prices for consumers, and thus higher consumer surplus, if robust competition ensures that cost savings are passed on to consumers.³¹

As of yet, there have been few systematic examinations of the real economic impact of these technologies on critical infrastructure. One of the few was undertaken in Chatanooga, in the US, focused on the benefits of a 'smart' electrical grid network. Such a network involves the automation of electricity distribution through the installation of automated circuit switches and sensors in the network. The authors attributed the primary benefit of distribution automation to, 'increased reliability or reduced power outage duration and frequency.' A 43.5 % reduction in annual outage minutes was estimated as having occurred since 2012. This in turn led to an estimated total savings of US\$26.8 million per year (Glass et al, 2016).

Additionally, a number of industry-sponsored studies provide predictions of the eventual economic impacts of these technological changes. A Cisco white paper from 2013 estimated, '\$4.6 trillion in public sector Value at Stake will result from IoE's [Internet of Everything's] ability to help public-sector organisations manage assets, optimise performance, and create new business models' (Bradley et al, 2013). The McKinsey Global Institute estimated that the potential economic impact of Internet of Things technologies would be US\$2.7 trillion to US\$6.2 trillion per year by 2025

³¹ Though in some countries, many critical infrastructure sectors have regulated price caps (e.g. power, water). In these instances, the cost savings would not be passed on to consumers in terms of lower prices. Infrastructure operators would capture all of these economic benefits.

(Manyika et al, 2013). A General Electric report estimated that industrial Internet of Things technologies could add US\$15 trillion to global GDP by 2030 (in constant 2005 dollars) if they raise global annual productivity growth by 0.5 to 1 percentage points (Evans and Annunziata, 2012).

Studies such as these, while popular, are typically built on extrapolations from unproven implementations of technologies. They do not adequately separate concepts such as GDP gains/losses (and to whom) and cost savings (and whether these are passed on to consumers or not). They typically do not include up-front capital investment or maintenance costs, costs and losses due to security incidents and changes in the distribution of economic surplus (consumer/producer effects). For these reasons, policy-makers should approach estimates such as these with caution when considering policy responses.

4.6. Conclusions

- More secure digital technologies result in greater adoption – this in turn results in greater indirect benefits across many areas (economic growth, employment, productivity and consumer surplus).
- Digital trade is a major source of GDP and future growth. The EU and US are one another's largest digital trade partners. SMEs stand to benefit a great deal from the increased access to international markets that a relatively 'open' internet provides. The trend towards data localisation has the potential to impede this access due to increased cross-border regulations and potentially higher costs of digital technologies.
- The EU is a net importer of US digital technology. Cooperation is important if individuals and enterprises in the EU are to have access to more secure technologies by design, rather than retro-fitting security measures to technologies after purchase.
- Demand for employees with skills relevant to government agencies and enterprises with cybersecurity needs will increase in both the EU and US over the coming years.
- Historically low productivity rates have been seen in EU Member States and the US over the past decade. One explanation for this trend is that frontier firms are pulling ahead on productivity and their best practices are not being transferred to laggard firms, which continue to fall behind in terms of productivity (Andrews, Criscuolo, and Gal, 2016). If this is indeed the case, policy-makers might consider ways to remove these barriers to or provide incentives for information/knowledge diffusion.
- Digital technologies play an important role in the diffusion of knowledge and facilitation of collaboration throughout economies (OECD, 2017a). Ensuring that these technologies are more secure is one way in which to encourage their adoption and use.
- Consumer surplus gains are the largest of all indirect benefits from adoption of digital technologies, in monetary terms, in the short-term. Ensuring these gains continue requires greater development and adoption of secure digital technologies (to shift the demand curve) coupled with robust competition policy (to drive down prices).
- Few robust studies have been undertaken on either side of the Atlantic to assess the net impact, and the cybersecurity consequences, of the impending wave of (potentially internet connected) embedded devices in critical

infrastructure. Such studies are important, because they would allow policy-makers to allocate scarce resources, following a risk management approach, to the minimisation of the potentially large costs/losses that cybersecurity incidents, related to these technologies, might impose on society.

5. Cybercrime: Direct costs and indirect losses

Digital technologies and the internet have facilitated the proliferation of new and existing forms of crime. This is a fast-moving space with new methods emerging and retreating each year. This chapter examines the direct costs and indirect losses associated with various forms of cybercrime. With regard to costs and losses, this paper adapts a framework for estimating the costs of cybercrime previously developed by Anderson et al (2012). The original framework, which only contained figures on the United Kingdom, has been expanded by including data on the aggregate for EU Member States and for the United States.

5.1. Direct costs

With a rapidly evolving threat environment, the line between crime committed in cyberspace and in the real world is becoming increasingly blurred. Consequently, the model proposed by Anderson et al (2012) divides direct costs of cybercrime into three main categories:

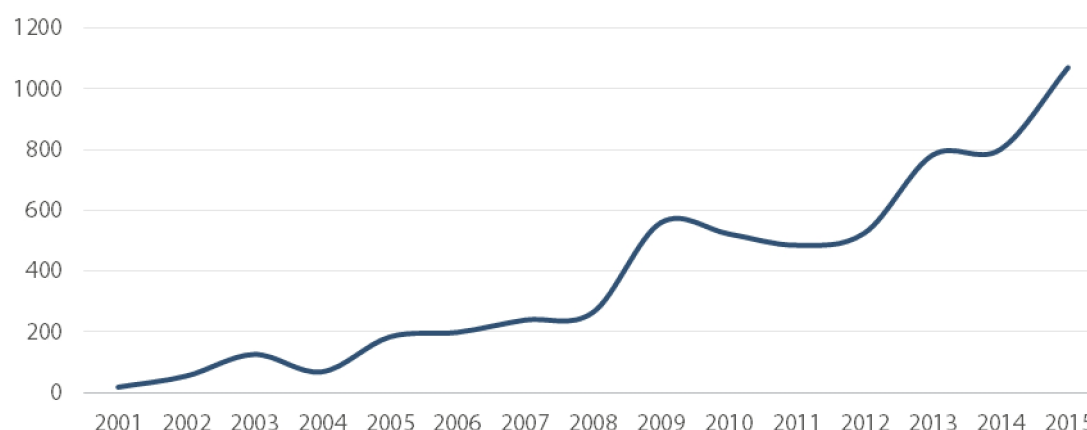
- Genuine cybercrimes are new forms of crime perpetrated with digital technologies e.g. botnets.
- Transitional cybercrimes are crimes that were once perpetrated offline but are now increasingly, though not entirely, perpetrated online e.g. card fraud, ransomware.
- Traditional cybercrimes were once committed offline but are now largely or entirely committed online owing to adoption of digital technologies e.g. tax evasion.

5.1.1. *Genuine cybercrimes*

Genuine cybercrimes are new forms of crime that are perpetrated over and using the internet. Since the late 1990s, **copyright infringement and piracy** over peer-to-peer networks were thought to be the major cybercrimes perpetrated on the internet.³² The revenues earned by pirates and services that sell pirated music, videos, software and games or patent-infringing pharmaceuticals are relatively low per capita – less than US\$0.20 per person per year.³³

³² While the official EU definition of cybercrime does not include intellectual property right infringement, the Budapest Convention on Cybercrime does have passages relating to these crimes. The revenues to those who commit such crimes have thus been included in this framework.

³³ This is just the revenue earned and does not include the costs that those who operate these services incur, which suggests that the profits from these crimes are relatively low.

Figure 7 – Reported costs to victims of internet-enabled scams worldwide, 2001-2015*US dollars, millions*

Data source: IC3 2015 Internet Crime Reports 2001-2015

Notes: A total for 2010 was not provided in the relevant annual report. As a result, half of the difference between 2009 and 2011 was subtracted from the 2009 figure to smooth out the decrease over the three years 2009, 2010 and 2011.

Table 3 – Losses to victims of internet-enabled scams worldwide, 2015*US dollars, percentage*

	Total (US\$)	% of total
Total worldwide	1 070 711 522	100
Business email compromise	246 226 016	23
Confidence/romance fraud	203 390 531	19
Non-payment/non-delivery	121 329 122	11
Investment	119 177 899	11
Identity theft	57 294 589	5
Advance fee	50 721 226	5
Other	56 153 977	5

Source: IC3 2015 Internet Crime Report

Note: % of total does not add up to 100 % as only those categories of scams that contribute most to the total have been included in this table.

By contrast, a constantly changing variety of **scams and frauds** have resulted in steadily increasing reported costs to internet users.³⁴ According to the FBI's International Crime Complaint Center, in 2015, worldwide just over US\$1 billion was stolen from victims of these scams. This is an increase from US\$183 million in 2006 (see figure below).³⁵

³⁴ This churn owes to the 'predator-prey' dynamics that characterise fraudsters and their targets. As in nature, when a predatory successfully claims its prey, the prey in turn adapts to evade predators in the future, which again the predator must subsequently adapt to. As a result, it is impossible to eradicate all fraud and scams. It also renders spending on combatting such frauds and scams uneconomic at a certain point, given that the benefits of reduced incidents are outweighed by the costs of law enforcement.

³⁵ This increase over the past decade may be attributable to greater numbers of people reporting these crimes having taken place rather than an absolute increase in incidences. Increases in reported cybercrime costs might also just be a consequence of more people using digital technologies (Jardine, 2015). If this is the case, the costs have to be normalised by weighting them with some proxy for the

Figures from 2014 suggest that the annual per capita losses were US\$2.11 per capita in the US and US\$0.51 in the EU. Statistics on costs to victims of internet-enabled scams are provided for 2015, broken down by the type of scam, in the table below. These are worldwide figures though the IC3 data primarily cover the US.³⁶ The most noticeable change in recent years has been the emergence of business email scams. These scams involve criminals compromising the accounts of company executives, then wiring-out funds under the guise of being payments to suppliers or clients. These made up the largest proportion of reported cybercrimes to the IC3 in 2015 (23 %). A great deal of attention is currently being paid to **ransomware**, which involves encrypting the victim's hard-drive and demanding a ransom. The ransom is typically paid using the pseudonymous digital currency Bitcoin (Europol, 2016). In 2015, the reported payments by 2 453 victims amounted to US\$1.6 million, which was a fraction of 1 % of all reported scam costs for that year. By contrast, in 2016, the IC3 received 2 673 complaints identified as ransomware with losses of over \$2.4 million³⁷ (IC3, 2015; 2016).

Table 4 – Costs of genuine cybercrime, various years

	United States		European Union	
	Total \$US	Per capita	Total \$US	Per capita
Copyright-infringing software	23 042 782	0.07	1 728 209	0.003
Subscription revenue from cyberlockers	21 120 000	0.07	21 120 000	0.04
Ad revenue from cyberlockers	54 408 000	0.17	49 874 000	0.10
Patent-infringing pharmaceuticals	71 926 572	0.23	5 394 493	0.01

Sources: see appendix 1 for sources and years of each indicator.

5.1.2. Transitional cybercrimes

Transitional cybercrimes are those crimes that were once primarily perpetrated offline and are now in the process of transitioning online as well. One of the most visible of these cybercrimes is **payment card fraud** – either with debit or credit cards. According to the 2016 US Federal Reserve's Payments Study, the majority of payment card fraud occurred offline in the US in 2015 (54 %). This is a slightly lower proportion than that in the previous study (59 %) with figures from 2012. By contrast, the European Central Bank found that the majority of card fraud in the Single Euro Payments Area (SEPA)³⁸

number of people using the digital technologies. In other words, the reported costs might be increasing but they might be increasing at a slower rate than the increase in the number of users.

The vast majority of these reports originated in the United States and, given that these statistics are self-reported, they may understate the true extent of the costs of these crimes. At the same time, reported costs may be overstated as they may have been subsequently recouped or reimbursed through insurance.

³⁶ Similar statistics are not collected and aggregated by an authority in the EU

³⁷ It may be that these crimes are not reported, thus the figures underestimate the true extent of the problem, or that the use of ransomware has grown rapidly over the course of 2016 and is not included in these statistics.

³⁸ The Single Euro Payment Area is a payment-integration initiative of the EU for simplification of bank transfers denominated in euros. As of July 2015, SEPA consisted of the 28 Member States of the European Union, the four member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco and San Marino (European Payments Council, 2016).

occurred online in 2013 (66 %). When converted to per capita figures, the online card fraud amounted to US\$5 per person in the US in 2012 and US\$2.47 (€1.87) in SEPA in 2013. The costs of payment card fraud are typically paid by either the payment provider, the bank that issued the card, or the merchant – not the card-user. Moreover, an interchange fee – which is nominally imposed to offset fraud – of between 1-4 %³⁹ is levied on each card transaction, which more than offsets the annual level of fraud.⁴⁰

Another emerging area of transitional cybercrime is conducted through **darknet (or crypto) markets**. These are pseudonymous, eBay-like markets where users can typically purchase drugs, but some markets also offer weapons and other illicit goods. These markets can only be accessed on the ‘darknet’ using the TOR (‘The Onion Router’) browser. The first and biggest of these markets was Silk Road. At one point, Silk Road was processing somewhere in the order of US\$1.2 million in orders per month (Christin, 2013). When the FBI closed down Silk Road it splintered the market and several dozen more emerged to take Silk Road’s previously dominant place. A report by Kruithof et al (2016) examined the revenues of eight of the largest cryptomarkets in January 2016. If the revenues to sellers on these markets are annualised, the total would be approximately US\$61 million both in the US and the EU (France, Germany, Netherlands, Spain and UK), which equated to US\$0.19 per capita in the US and US\$0.12 in the EU per capita. Around one-third of this cryptomarket trade (whether measured by transactions or revenues) occurs within and between the US and EU. To put the total trade in further context, it is estimated that the annual, global drugs trade is somewhere in the order of US\$435 billion a year (UN 2013). This implies that trade on cryptomarkets still only accounts for a fraction of 1 % of all drug trade worldwide.

Table 5 – Costs of transitional cybercrime, various years

	United States		European Union	
	Total \$US	Per capita	Total US\$	Per capita
Online payment card fraud	1 561 520 000	4.97	1 256 850 000	2.47
Offline payment card fraud	2 277 700 000	7.25	648 270 000	1.28
Darknet markets (revenues to sellers)	61 189 836	0.19	59 435 424	0.12
Darknet markets (products to buyers)	51 515 700	0.16	9 268 668	0.02

Sources: see appendix 1 for sources and years of each indicator.

³⁹ In 2011, interchange fees on debit card transactions were capped at 0.05 % plus US\$0.21 in the US through the Durbin Amendment to the Dodd-Frank Act. The interchange fee for credit card transactions is not capped. In 2015, as a result of the Interchange Fee Regulation 2015/751, interchange fees were capped in the EU at no more than 0.2 % of the transaction value for debit cards and 0.3 % for credit cards.

⁴⁰ To give some scale to the differential, US\$25 trillion in card transactions occurred in the US in 2013. Of this, 1-4 % equates to between US\$24-100 billion against total fraud of US\$3.7 billion. In the EU, it was estimated that €9 billion was paid in interchange fees in 2011 (European Commission, 2015). This compares to total card fraud that same year of €1.16 billion (European Central Bank, 2013). The differential between fraud and interchange fees could be interpreted as the amount of consumer surplus that banks and payment providers appropriate (reduce) from consumers, who benefit from the convenience that payment cards offer.

5.1.3. Traditional cybercrimes

Traditional cybercrimes are those crimes that have migrated almost entirely online as digital technologies have been adopted and governmental services have become available online. For instance, it is now possible to file for **government welfare, healthcare** and **unemployment claims** online. In 2013, the US Department of Labor estimated that US\$4 billion of taxpayer funds were paid out fraudulently to people who did not qualify for unemployment benefits. This equated to US\$12.89 per capita per annum. Medicare fraud, which is perpetrated using electronic filing systems, resulted in almost US\$50 billion – ten times more than payment card fraud – in losses to taxpayers in 2013 alone (GAO, 2014; Sparrow, 2011). In the EU, **value-added tax fraud** amounted to US\$186 billion (€168 billion) in 2015, which equated to US\$365.88 (€330.68) per capita per annum.⁴¹ Tax evasion (including online and off-line) has been facilitated internationally with the advent of the internet and digital technologies. For an indication of how offshore holdings, which are linked to tax evasion, have evolved over the past fifty years, at the end of 1959, about US\$200 million was on deposit in tax havens.⁴² By 1961 the total had hit US\$3 billion. At present, it is estimated that US\$7.6 trillion is held in tax havens globally – around 8 % of the world's wealth (Rusbridger, 2016).⁴³ Losses to government coffers were estimated to be US\$337.3 billion in 2011 and US\$841.6 billion in Italy, Germany, France, Spain and the UK in that same year.⁴⁴ In these countries, the per capita loss to authorities from **tax evasion** exceeds US\$1 000 per person each year.

Table 6 – Costs of traditional cybercrime, various years

	United States		European Union	
	Total \$US	Per capita	Total US\$	Per capita
Welfare fraud	4 079 807 841	12.89	-	-
Tax evasion (tax gap)	337 300 000 000	1 082.06	841 600 000 000	1 664.80
Tax filing fraud	3 100 000 000	9.72		
VAT fraud/gap	-	-	186 480 000 000	365.88

Sources: see appendix 1 for sources and years of each indicator.

5.2. Indirect losses

The indirect losses from cybercrimes or poor cybersecurity are those that cannot be linked by a reasonable degree of accuracy directly to a particular incident (Gordon and Loeb, 2006). Such categories typically comprise: loss of customer trust/reputational damage, reduced uptake of digital technologies due to lack of trust, and opportunity costs and foregone productivity associated with the need to invest in non-digital infrastructure (Anderson et al, 2012).

⁴¹ While not all of this fraud is committed online, welfare and tax payments are increasingly conducted online. This trend will continue. The point is that these (cyber)crimes impose costs on society many times greater – every year – than the categories of cybercrimes that are typically given most attention (e.g. ransomware, card fraud, copyright infringement, etc.).

⁴² It is not clear if this estimate has been adjusted for inflation. If not, it equates to US\$1.65 trillion in 2017 dollars.

⁴³ See OECD (2017b) for more information on the role of digital technologies in facilitating tax evasion. See Zucman (2013) for more information on trends relating to tax havens and tax evasion.

⁴⁴ While not all tax evasion is committed using digital technologies, even a small percentage of these figures fitting the definition of 'cybercrimes' would dwarf the direct costs of all other categories.

Estimating the indirect losses of cybercrimes is difficult. Part of the difficulty lies in the variance of the possible values for categories of losses across a heterogeneous population e.g. lost time will have a different value for each person depending on how much he/she is paid per hour. Moreover, many of the indirect negative effects of cybercrimes are not easily converted into monetary terms. For instance, emotional reactions like distress and changes in behaviour due to fear of being a victim of a crime. Considering that each person and their circumstances are different, when aggregated across a country or worldwide, these aggregate figures hide substantial variance between the indirect losses that afflict an individual or organisation in one case compared to those losses of a similar case.

Nevertheless, some attempts have been made to estimate some of these categories of indirect losses. Anderson et al (2012) found that the indirect losses associated with transitional and genuine cybercrimes were much higher than their related direct costs. For instance, while the direct costs associated with online and off-line payment card fraud were estimated to be US\$306 million in the UK in 2010, the equivalent indirect losses due to consumer loss of confidence in such payment methods were estimated at US\$700 million in 2010. Lost sales of US\$1.6 billion were estimated to have been incurred due to merchants turning down orders out of fear of fraud in 2009.⁴⁵

Much of the indirect losses from the risk of cybercrime or poor cybersecurity are due to non-adoption of digital technologies out of security concerns. According to Eurostat (see figure below), security concerns prevented 15 % of consumers downloading software, music, video files, games or other data files; carrying out banking activities online; or ordering or buying goods or services online across the EU-28 in 2015. These figures are stable when compared with 2010. Some 14 % of enterprises in the EU-28 did not partake in online sales in 2015 due to perceived problems related to ICT security or data protection. While these statistics hide country-level differences, one can broadly conclude that approximately one in six consumers and enterprises across the EU do not partake in the opportunities afforded by digital technologies due to security fears. This would equate to a large amount of foregone economic activity.⁴⁶ It is unlikely that this proportion would ever be brought to zero, not least because 100 % secure technologies are impossible (OECD, 2015c), but reductions in this proportion may be possible if technologies are made relatively more secure than they are at present.

Estimates of the impact of information security failures on corporate earnings, a proxy for reputational damage and perceived loss of productivity or competitiveness, present a mixed picture. Campbell et al. (2003) found a statistically significant adverse effect among breaches involving unauthorised, confidential data, but no effect when the data was not confidential. Cavusoglu et al. (2004) found that announcing an internet security

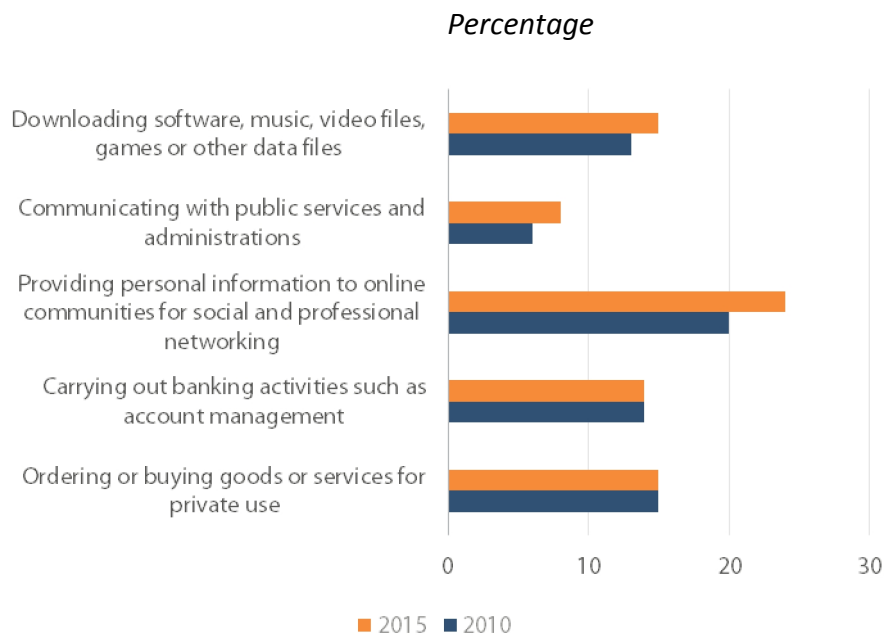
⁴⁵ The consumer loss of confidence statistics were estimated by taking the percentage of consumers who refrained from buying goods or services online because of security concerns then scaling it to total retail sales. However, the total was revised down because those who do not purchase online may simply have made the same purchase off-line instead, which would have no net effect on overall sales in the economy.

The merchant loss of confidence statistics were estimated using the percentage of revenues lost due to merchants refusing orders out of fear of fraud multiplied by the total revenues of the 'digital economy'.

⁴⁶ Though some people may simply perform the same activities off-line, the need to provide such off-line facilities requires additional expenditure, which comes with opportunity costs.

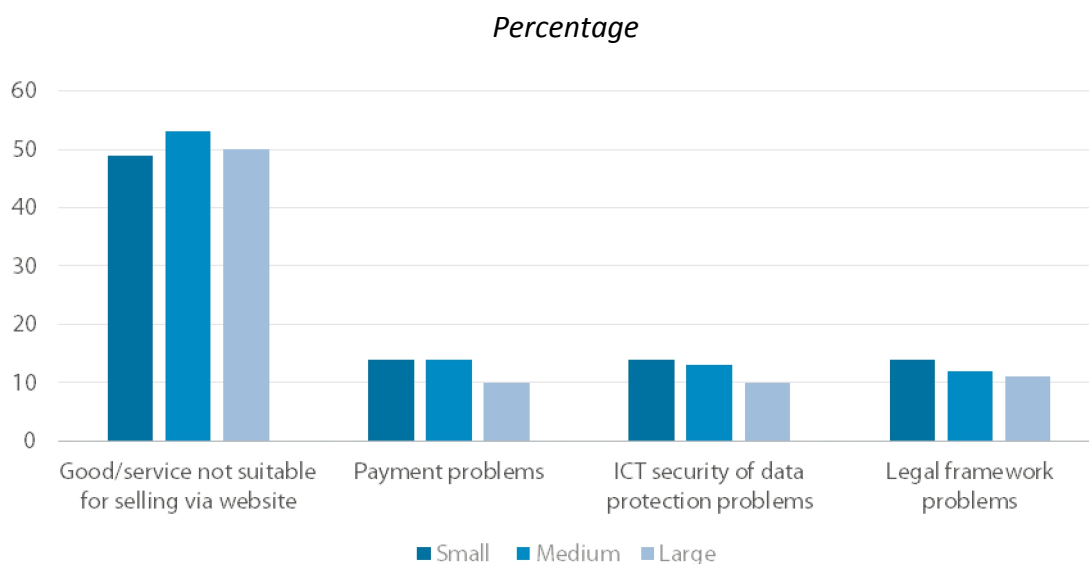
breach is negatively associated with the market value of the announcing firm, though the bulk of the decline is regained after two days. Kannan et al. (2007) later found that firms do not earn significantly negative abnormal returns in the long-term due to information security incidents. These studies focus on data breaches, a narrow category of overall security incidents, but the mixed results point to how little is known about whether cybersecurity failures actually impose indirect losses in terms of reputational damage and, if so, the scale of these losses.

Figure 8 – Security concerns kept individuals from doing... EU-28, 2010 & 2015



Data source: Eurostat.

Figure 9 – Obstacles to enterprise web sales, EU-28, by size of firm, 2013



Data source: Eurostat.

Box 1 – Estimating the cost of data breaches

One of the most visible consequences of poor cybersecurity and escalating attacks has been a series of high-scale data breaches in recent years. High-profile incidents have occurred on both sides of the Atlantic affecting public and private organisations alike. While the negative effects of these breaches exist, the true scale of their direct financial costs across cases is debatable.

The most common approach to estimating such direct costs is to determine an average cost per record then multiply by the number of records stolen to reach a total. One method, developed by Ponemon Institute, uses an average loss per record figure of US\$154. Another, put forward by Verizon, estimates this same number at US\$0.58. When data breaches involve hundreds of millions of records, the difference in estimated impact between these two methods become readily apparent. To illustrate, consider the case of Target, which saw 40 million credit and debit card records and 70 million other records stolen. Using the average cost per record approach, the Ponemon method suggests costs of US\$16.9 billion while the Verizon method suggests US\$6.275 billion. However, Target disclosed the costs attributable to this breach in its SEC reports. In the first quarter of 2015, Target estimated the gross expenses from the data breach as US\$252 million. When the insurance reimbursement is factored in however, the losses fall to US\$162 million. If tax deductions are also factored in, the net losses tally US\$105 million. This is a fraction of the total Verizon and Ponemon estimates. While Target sustained additional indirect costs, such as reputational damage, these losses are difficult to model and are not likely to remain constant over time (see section above). Using these totals, one can calculate the average direct cost per record from the Target breach. If the gross expenses of US\$252 million are divided by 110 million records lost, the average cost per record is US\$2.29. Using the net expense figure of US\$105 million, the average cost per record is US\$0.95. These costs equate to less than 1 % of the annual revenue of Target in 2015.

These results are consistent with a recent large-scale study on 20 000 cybersecurity incidents (including include data breaches, security incidents, privacy violations, and phishing crimes). It was found that, 'the cost of a typical cyber incident... is less than US\$200 000 (about the same as the firm's annual IT security budget), and that this represents only 0.4 % of their estimated annual revenues' (Romanosky, 2016).

Table. Comparison of estimates using Ponemon and Verizon cost-per-record figures

U.S. dollars

Method	40 million card records	70 million other records	Total estimated cost
Ponemon method			
(\$154 per record)	6 160 000 000	10 780 000 000	16 940 000 000
Verizon method			
(\$0.58 per record)	23 200 000	6 252 400 000	6 275 600 000

Table. Costs to Target due to data breach as disclosed in SEC filings

U.S. dollars

	Gross expenses	Insurance reimbursement	Pre-tax net expenses	Net of tax expenses
2013	191	46	145	94
2014	61	44	17	11
Total	252	90	162	105

The shortcomings of the cost per record approach are apparent. Part of the problem is that there is no such thing as an 'average data breach'. The outcomes will be probabilistically determined depending on many factors, such as, but not limited to, the preparedness of the organisation, the type of data stolen and how interconnected the entity is with other entities. Moreover, averages hide a great deal of variance, particularly for phenomena that where the losses are not normally distributed such as data breaches (Edwards et al, 2014).

The main takeaway for policy-makers is that the impacts of data breaches are unpredictable and difficult to model. While even large-scale data breaches have not been sufficient to render companies like Target insolvent, this does not mean that such an event could not happen in the future.

5.3. Conclusions

- In spite of their high visibility, the direct costs of genuine cybercrimes are relatively low in both the EU and US. For instance, the reported criminal revenues from frauds and scams worldwide, including ransomware, were below US\$1 billion in 2015. This equates to a per capita cost of less than US\$1.50 per person in the US and EU. Costs of traditional categories of crime that have migrated online – such as tax evasion and welfare fraud – outstrip the direct costs from other categories many times over. Given their transnational nature, cooperation between the EU and US could be important to reduce or contain these direct costs in the future.
- Indirect losses from cybercrimes are greater than the associated direct costs. While hard to estimate reliably, security concerns prevented around one in six EU consumers and enterprises from performing a task online in 2015. This suggests that building greater trust in the digital technologies – by making them more secure – would bring large economic benefits by reducing the indirect losses in which cybercrimes result. The EU and US can work together to ensure that more secure technologies are made available – particularly given that the EU is a net importer of these technologies from the US.
- Many of the available statistics cited are not the soundest statistics methodologically – but are the only ones available. Unfortunately, some of the most reliable data on the frequency of cybersecurity incidents and their impact on enterprises, such as the US National Small Business Cybersecurity Study, have not been conducted in over a decade. The Eurostat surveys on cybersecurity-related issues do not contain questions on the impact of incidents on firms or individuals. Major improvements are needed in the data and statistics available for cybercrime/cybersecurity incidents and impacts.

6. Cyber-resilience of critical infrastructure: Costs and risks

Critical infrastructures form the backbone of complex and interconnected systems that provide for essential societal needs e.g. food, energy, water, etc. Critical information infrastructure, a sub-set of critical infrastructures, provide the communication capabilities on which our increasingly digitised societies rely upon to function. Being a part of a complex, interdependent system means that the potential economic losses due to critical (information) infrastructure failure or disruption can be enormous. That the EU and the US seek to develop cooperative mechanisms for threat identification, risk management and crisis response is therefore important.

The EU and US have different, though broadly similar, definitions of critical infrastructure.

- The EU NIS Directive defines 'critical infrastructure' as, 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.
- The US defines 'critical infrastructure' in Executive Order 13636 (from 2013) as, 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'.

Consensus has not been reached amongst countries globally as to what constitutes 'critical information infrastructure' (OECD, 2007). The UN Resolution 64/211 on the 'creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures' recognises each country will determine its own critical information infrastructures.

- The EU Council Directive 2008/114/EC on the 'identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection' provides a definition of 'critical information infrastructures' as, 'ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)'. In practice, this definition is unevenly applied across Member States, although this is likely to change with the implementation of the NIS Directive (ENISA, 2014a).
- The US does not have a specific definition for 'critical information infrastructure'. However, the concept is captured Homeland Security Presidential Directive 7 (HSPD-7), which includes protection of the IT sector communications sector (OECD, 2007).

The NIS Directive makes provisions for 'digital service providers', which are defined as a(n): 1. Online marketplace. 2. Online search engine. 3. Cloud computing service. No equivalent for this concept exists in US policy documents. While not critical information infrastructure, entities that fall under the relevant definition in the NIS Directive will have to report less stringent obligations than what are termed 'operators of essential services'.

Box 2 - The NIS Directive and NIST Framework

On 6 July 2016, the European Parliament adopted the Directive on security of network and information systems directive (NIS Directive). This directive aims to bring cybersecurity capabilities to the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

On 10 February 2013, Executive Order 13636 'Improving Critical Infrastructure Cybersecurity' (EO 13636) was released by US President, Barack Obama. This Executive Order covered a number of different measures to bolster the cybersecurity of critical infrastructure in the US under section 7: 'Baseline Framework to Reduce Cyber Risks to Critical Infrastructure', a request was made for the National Institute of Standards and Technology (NIST), under the Department of Commerce, to develop what would later become known as the NIST Cybersecurity Framework. An Executive Order on 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', released on 11 May 2017, required all federal agencies to implement the NIST Framework and report on implementation within 90 days (White House, 2017).

The goals of the NIS Directive and the NIST Framework are very different. The NIST Framework is much more operational than the NIS Directive. The NIST framework was originally designed for critical infrastructure operators. It has subsequently been adopted by other private sector organisations to assess and improve their ability to prevent, detect, and respond to cyber-attacks. The NIS Directive is rather a high-level policy around information sharing and coordination for critical infrastructure in the EU. Therefore, for a more useful comparison, it is helpful to compare the NIS Directive with provisions in EO 13636 as well as other legislation, Presidential Policy Directives (PPD) and other cybersecurity or critical infrastructure policies in the US. Such a comparison can be found in Appendix 4.

Broadly speaking, the NIS Directive contains three key sets of measures: 1. Specific measures to upgrade national cybersecurity preparedness (e.g. creation of CSIRTs in all Member States); 2. Measures to foster cooperation amongst Member States; and 3. Measures to instil a 'culture of security' amongst critical infrastructure sectors that are reliant on ICTs as well as 'key digital service providers'. In the US, on the other hand, measures to ensure national cybersecurity preparedness date back to 2000, with the creation of the Federal Computer Incident Response Center (FedCIRC), which would later be renamed US-CERT (with its partner in critical infrastructure protection, ICS-CERT). However, many US states do not have a CERT. Cooperation between government agencies is laid out in PPD-21, EO 13636 Sec 3 and PPD-21. International cooperation in the protection of critical infrastructure is specifically called for in PPD-21. Finally, measures relating to critical infrastructure protection are listed in PPD-21 (which names all 16 critical infrastructure sectors as well as sector-specific agencies with responsibility for each sector). The equivalent of some 'digital service providers' would be found in the communication, information technology or defence industrial base sectors.

A key difference between the approaches is the application of extra-territoriality of the NIS Directive as it requires digital service providers to name a representative in the EU if their head office is not within an EU country. Similar provisions do not exist in the US.

6.1. Transatlantic critical information infrastructure

While critical infrastructures, broadly speaking, face many cybersecurity risks, three specific transatlantic critical information infrastructures bear specific examination: submarine fibre optic cables, the Domain Name System (DNS) and internet exchange points.

Submarine communication cables have crisscrossed the Atlantic for well over a century. First with telegraph lines, then telephone lines, and now with fibre optic cables. Fibre optic cables now carry an enormous and continually growing amount of data. In fact, the traffic exchanged between the EU and the US is the highest of any inter-regional exchange globally (Meltzer 2012). This traffic will continue to increase as companies exchange data between their affiliates/subsidiaries, as individuals and organisations continue to migrate towards Cloud services, and with the arrival of a new generation of internet-connected devices (the 'Internet of Things').

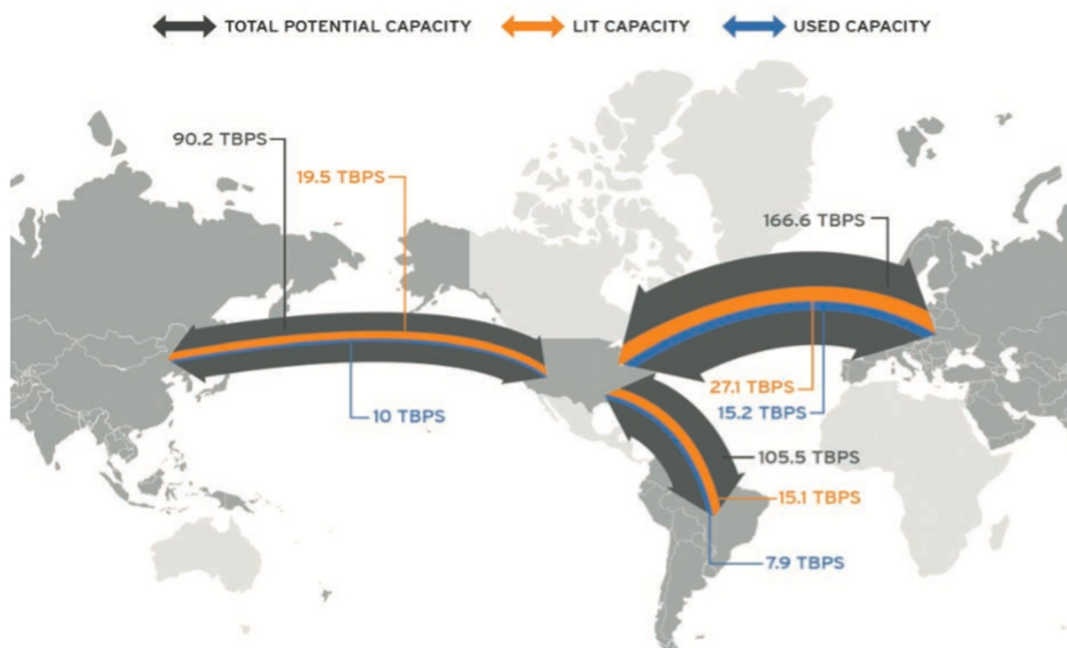
Greater transatlantic data exchange increases the potential impact of any incident that might disrupt the functioning of submarine fibre optic cables. Possible incidents might range from unexpected shifts in the ocean floor to anchors being dropped on cables and severing them (Lacroix et al 2001). As a result, redundancy has been planned into the network of many cables. Were one cable to fail, internet traffic could be rerouted through other cables. The issue is that a lack of suitable sites for cables to come ashore has led to many cable termination points being located on the same shore. Concentration of these termination points means that, theoretically, 'an attack on two or three of these sites—at the point where the cables come together in the undersea trench before coming ashore—could cause enormous damage to the entire system' (ibid).

The internet infrastructure contains a number of components and systems. One such system, **the Domain Name System (DNS)**, is in essence a directory for all the devices, services and resources connected to the internet. One important task it performs is the conversion of relatively difficult-to-remember strings of numbers (the IP address) into easier-to-remember domain names for internet browsing. For example, the DNS reconciles the IP address 136.173.60.59 with the domain name <http://www.europarl.europa.eu/>. While the end-users of the internet are relatively highly distributed, the DNS is not as distributed. Its systemic importance makes the DNS a potential source of systemic risks and cascading effects in the event of disruption or failure.

Another part of the internet infrastructure is **internet exchange points**. These points exchange traffic between countries. The United States has 41 exchange points (in at least 70 locations) while Egypt has 1 (Data Center Research, 2016). The failure of an exchange point in the US is likely to be less costly than a failure of the only point in Egypt. Some countries are more deeply enmeshed in the global network than others. For instance, the majority of global internet traffic flows through just three countries: the US, the United Kingdom, and Germany (Karlin et al, 2009). This concentration of internet traffic creates choke-points in the network, which creates the potential for large-scale network interference/disruption and surveillance.

The interconnected nature of these critical information infrastructures, and the reliance thereon of business operating across the Atlantic (e.g. shipping and transport), mean that an incident on one side of the Atlantic can have impacts on the other side. Similarly, poorly managed risk on one side of the Atlantic exposes entities or societies on the other side to additional risk. There is thus a need to ensure that risk is adequately managed on both sides, so as to reduce the probability of critical information infrastructure failure, and that crisis response plans are developed and implementable should an incident occur.

Figure 10 – Submarine cable bandwidth, Terabits per second, 2014



Source: Meltzer (2012); based on data from Teleographic (2014).

6.2. Cybersecurity-related risks to critical infrastructure

Cybersecurity risks to critical infrastructure operators are similar on both sides of the Atlantic (e.g. malicious insider, malware, ransomware, etc.). For many years, concerns have been expressed about the potential for cyber-threats to disrupt the operation of critical infrastructures (Lewis, 2006). This is primarily due to vulnerability of the industrial control systems (ICS) – that can be found in electrical, water, oil, gas and data infrastructures – to access and manipulation by external actors, or internal error/accident, potentially leading to disruption or failure.

Miller and Rowe (2012) provided a survey of numerous cyber-related incidents involving supervisory control and data acquisition (SCADA) systems and critical infrastructure dating back to 1982. Incidents span aviation, energy and water infrastructures. The major issue here is that complex and interdependent systems are involved. There is a risk of cascading effects from the disruption or failure of one part of such systems, which then affects other parts of the system (Geer, 2016). A relatively small, isolated incident for one organisation can escalate to a sector-wide emergency then subsequently result in a system-wide crisis.⁴⁷ This can have a significant negative effect on capital stocks, productivity and economic output (Kelly, 2015).

A continuing concern is that the risk factors to critical infrastructure are changing rapidly – too rapidly for operators to manage adequately. For instance, in its most recent Quadrennial Energy Review, the US Energy Department warned that the electrical grid, 'faces imminent danger' from cyber-threats which are, 'increasing in sophistication, magnitude, and frequency'. Compounding the problem is that these, 'rapidly evolving threats and vulnerabilities', have to be managed through, 'slower-moving deployment of defense measures.' These concerns are increasingly borne out in real incidents. In 2015, an unprecedented and sophisticated cyber-attack on the energy grid in Ivano-Frankivsk, a town in Ukraine, was reported (Tuptuk, 2016). A combination of malware, denial of service attacks and other techniques were used to bring down thirty substations. The result was a blackout that affected 230 000 people (Zetter, 2016). The Ukrainian energy ministry subsequently accused the Russian Federation of launching the attack (Tuptuk, 2016).

Compounding the already difficult situation, the trend in the critical infrastructure sector is towards greater use of digital technologies. A transition across societies is occurring towards an 'Internet of Things', the embedding of (potentially internet-connected) sensors into objects such as cars, household appliances, buildings, etc. This transition is also occurring in critical infrastructure. Sometimes termed the 'Industrial Internet' (Evans and Annunziata, 2012), the goal is to install sensors within critical infrastructure. This could create greater reliance on the reliable functioning of critical information infrastructures, which technologies associated with the 'Industrial Internet' require in order to function.

On the other hand, although malicious 'cyber-attacks' receive a great deal of press attention, the majority of cybersecurity incidents are caused by human error or other hazards. In the European power industry, in 2015, human error was the most common root cause category for network outages with the most users affected. Malicious

⁴⁷ This is already occurring with the Domain Name System. See Section 5.5.2 below for more information.

actions, by contrast, only contributed to 2.5 % of outages (ENISA, 2016b). In the aviation industry, airlines frequently experience outages, and extensive delays for passengers, due to IT system failure caused partly by legacy systems (e.g. Delta airlines in September 2016 and again in January 2017) (Isidore, 2016; McLean et al, 2017). Moreover, critical infrastructures are disrupted or fail frequently. Power grids in the US are regularly disrupted – by small animals – which cause failures in power grids dozens of times a year (Peterson, 2016). The issue is that parameters and effects of ‘cyber-attacks’, unlike human errors or small animals, are difficult to predict. Preparing critical infrastructure operators to recover following such rare but potentially costly incidents is necessary. Regular threat or incident-sharing among critical infrastructure operators would help them to be adequately prepared to recover from the outcomes of incidents related to these dynamic, unpredictable threats.

For critical infrastructure operators to adequately manage the potential for and recover from the impacts of cybersecurity incidents – whether caused by malicious or accidental actions – in this dynamic and fast-moving environment is, and will continue to become, more difficult. Efforts to build this responsive capability, often termed ‘building cyber-resilience’, is likely to require collaboration between private and public sectors, particularly around sharing of best practices, development of safety standards and the exchange of threat information.

6.3. Direct costs of investment in improving cyber-resilience

Both the public and private sectors in the EU and the US have been increasing investment in measures to improve cybersecurity and cyber-resilience. Unfortunately, data on the proportion of this spent on specific critical infrastructure initiatives are not widely available. Data on private sector spending broadly on cybersecurity are available, however they are based on speculative forecasts or extrapolated totals. The data on public sector spending in the US are more complete than the equivalent for the EU. It is difficult to know whether this spending has been optimal at a national level or across both the EU and the US, given that cost-avoidance estimates have not been developed. In the EU, Micro Market Monitor, a private consulting firm, forecasts that private sector cybersecurity spending will rise to US\$37.38 billion by 2020.⁴⁸ This estimate does not include public sector spending. It is not clear whether the number was derived from a top-down, bottom-up, or a demand-side estimate, which makes comparison with other countries or regions difficult.⁴⁹

Unfortunately, the total public spending on cyber-resilience measures across EU Member States are not available, nor are data available at the EU level. However, some data points are available for some specific initiatives and some individual countries. In

⁴⁸ In further correspondence with the team that compiled these figures, a revised set of figures were provided for the market size of Europe of US\$24.75 billion, which will grow by 7.9 % during 2016 to 2021. The reason for this revision was because, ‘the values are generated by RT (software) The numbers published on [the] MMMs site are not accurate as this are software and system generated number’ [sic].

⁴⁹ Top-down involves estimating the global market size then, to find the country or regional figure, dividing by the percentage contribution that each country or region makes. Bottom-up involves estimating the sales of major companies in the market and their market share to determine a country or regional amount. Demand-side involves determining the key customers for a product or service then, based on their average annual expenditures on the product or service, estimating the total sales in a country or region.

the Impact Assessment for the EU Cybersecurity Strategy (European Commission, 2013), some of the major costs associated with the strategy were estimated to be:

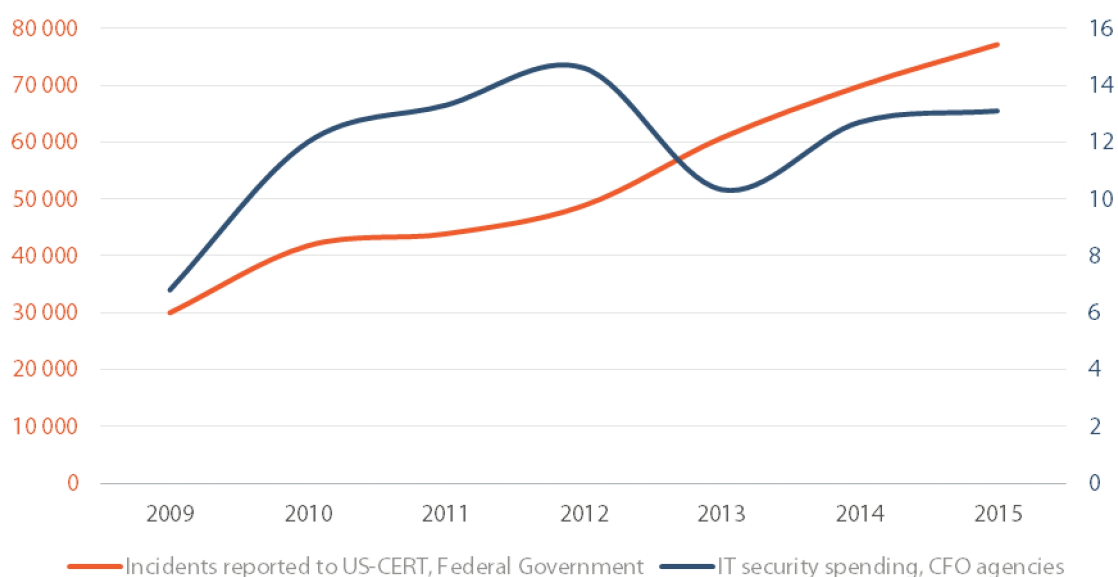
- €7.5 million to establish 3 computer emergency readiness teams in Cyprus, Ireland and Poland.
- A theoretical maximum of €9.72 million to develop and implement a cyber-incident contingency/cooperation plan and a national cybersecurity strategy.
- €55 555 per Member State to conduct and take part in pan-European cyber-incident exercises.
- A maximum of €10 million or a minimum of €1 million to establish the physical infrastructure necessary for the sharing of information between authorities (depending on whether the infrastructure is newly built or adapted from existing infrastructure).
- €1-2 billion in additional compliance costs for the Directive on Security of Network and Information Systems (NIS Directive).
- €4.25-8.5 million for administration related to the incident response requirements of the NIS Directive.

Additional data points can be seen in the following publicly released information:

- The European Union plans to spend an additional €450 million on a public-private partnership for cybersecurity under its research and innovation programme Horizon 2020 (which equates to an average of €112 million annually) (EC 2016). It is hoped that this will be augmented with investment from the private sector totalling €1.8 billion. Provisions exclude US companies from investing.
- The UK spent GBP860 million over five years, 2011-2016 (or an average of GBP172 million per year (UK Cabinet Office, 2014). Spending of GBP1.9 billion is also planned over the coming years (Osborne, 2015).

Figure 11 – US Federal cyber incidents and defensive cyber spending by CFO Act Federal agencies, 2009-2015

Number of incidents and billions of US dollars



Data source: Office of Management and Budget (OMB), Annual Reports to Congress on implementation of The Federal Information Security Management Act (FISMA) of 2002.

Government spending on cybersecurity at a federal level in the US has increased with each passing year. President Obama's White House Budget request for 2017 included US\$19 billion in government spending on cybersecurity, which equated to approximately US\$60 per capita for that year. This was close to four times the level of the previous decade (Zatko, 2013). Reported spending by Chief Financial Officer (CFO) Act agencies increased from approximately US\$8 billion in 2009 to approximately US\$12.5 billion in 2015 (see figure above). These figures on actual funds spent are required by the Federal Information Security Modernization (FISMA) Act. They are superior figures in that they report the actual amounts spent, rather than the amount budgeted or a speculative forecast or an estimate of future spending. Aggregate figures on public spending on cyber-resilience measures are not available in the EU. Fortunately, incident data are collected and released by ENISA each year. If combined with accurate cybersecurity spending data, it might be possible to derive statistics based on detected incidents given a certain level of spending.

The direct benefits from spending on measures to improve cyber-resilience are realised in terms of cost-avoidance, that is, economic losses that do not occur due to the mitigation of risks that would have led to critical infrastructure failure or disruption. This is difficult to measure. Where aggregate figures are available, such as is done in the US for federal spending for FISMA, there is rarely accompanying data or analysis of the outcomes of the security spending and incidents. FISMA reporting includes data on the number of incidents detected across federal agencies for the year in question (see figure above).⁵⁰ Yet the associated costs/losses to federal agencies as a result of these incidents is not estimated. Such data are required before any analysis can be done to determine cost-effectiveness or benefits from cost-avoidance due to investment in measures to increase cyber-resilience.

6.4. Indirect losses from past disruption and failures of critical infrastructure

In the event that the operation of critical infrastructure is disrupted or fails, indirect losses are borne by those who are reliant on the infrastructure to conduct their business activity or to meet their basic needs. When millions of people are reliant on critical infrastructures, these indirect losses can be enormous. Unfortunately, there are few robust, rigorous and standardised estimates of the indirect losses due to failure of critical information infrastructure. Indeed, there is still no consensus on the correct approach for estimating economic loss from such failures (Kelly, 2015).

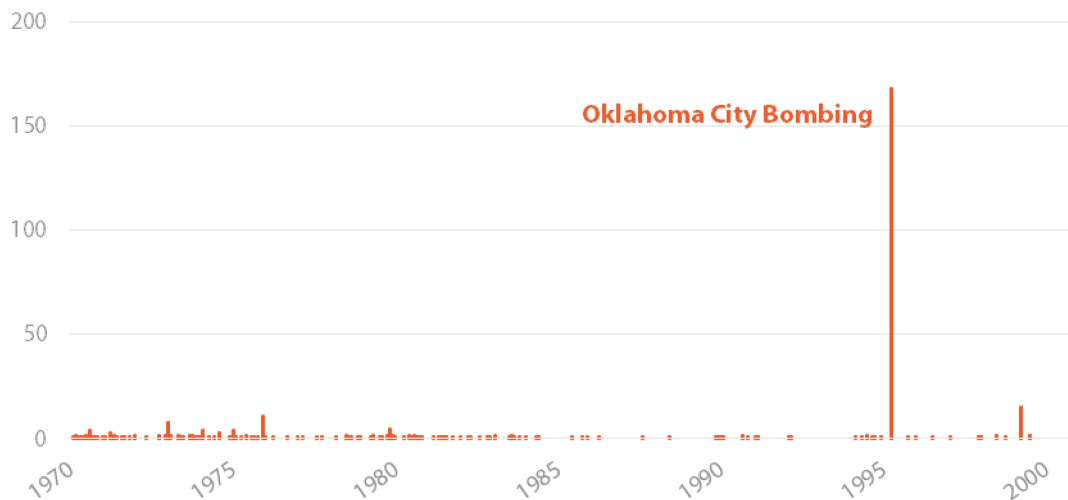
Critical infrastructure and critical information infrastructure exist within complex, interdependent systems. A key concept to understand when attempting to model such systems is that, when modelling the outcomes of certain 'fat-tailed' phenomena, past events are not necessarily a reliable indicator of the outcomes of future events. In such an environment, 'Black Swan' events may occur.⁵¹ A similar situation is found in the

⁵⁰ Although the number of detected incidents are increasing with each year, an unknown percentage are not detected and thus are not recorded. Moreover, an analysis of whether the situation is getting 'better' or 'worse' would have to normalise these figures by weighting them to the size of the network over time (Jardine, 2015). In other words, detected incident numbers might be increasing but this might just be a consequence of a larger network with more users.

⁵¹ Unforeseeable events [for some] with low-probability with high-impact. See: Taleb, 2007, *The Black Swan: The Impact of the Highly Improbable*, Random House: New York.

study of terrorism. Observing the two figures below, consider that in the US, between the years 1970-1995, the highest number of casualties from terrorist attacks was 168, due to the Oklahoma City bombing. Up until this incident, observation of historical events would suggest this as a maximum number of casualties. However, in 2001 the September 11 attacks resulted in casualties amounting to 1 382 – an order of magnitude (and twenty times more) casualties than the previous maximum five years before (pay particular attention to the scale on the y-axis).

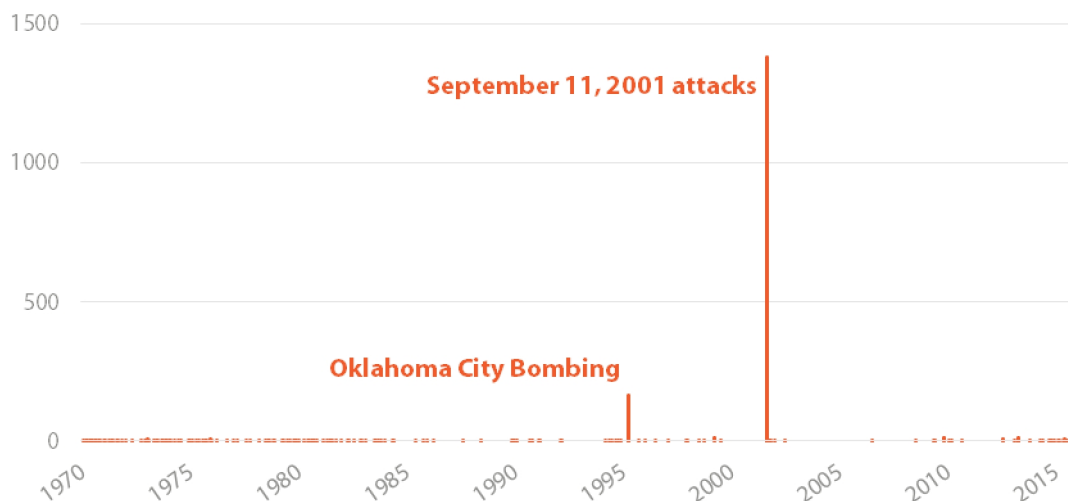
Figure 14 – Casualties from terrorist attacks in the US, 1970-2000



Data source: National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database.

Note: Based on the work of Prof. Pasquale Cirillo.

Figure 15 – Casualties from terrorist attacks in the US, 1970-2015



Data source: National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database.

Note: Based on the work of Prof. Pasquale Cirillo.

The key question for policy-makers to consider now is whether, in the cybersecurity and cybercrime domain post-Ivano-Frankivsk/Ukraine, we are at the equivalent point in the chart above just following the Oklahoma City bombing? If so, what might be the outcome in the future? There are unfortunately no clear answers. However, there is reason to be concerned, given the rate at which offensive cyber capabilities are

proliferating and the rate at which critical infrastructure operators plan on adopting digital technologies as a part of the 'Industrial Internet'.

In its survey of prior studies that estimated losses from failure in critical information infrastructures,⁵² ENISA (2016a) identified one notable conclusion, 'measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task.' Part of the issue is that the organisations producing such reports used different methodologies (surveys and questionnaires, log analysis, public information collection), data sources (experts, internal data, public information, partners), and cost frameworks (cost by threat, cost by country, cost by sector, cost by region). ENISA concluded that these decisions appear to be, 'often driven by business factors rather than actual interest of stakeholders or realistic needs' (ibid). With the caveats on past events being indicative of future outcomes in mind, a survey of the field can be used to gain at least a sense of the scale of possible indirect losses linked to critical infrastructure and critical information infrastructure failure.

With regard to failure of **submarine cables**, a study commissioned by APEC (2013) sought to estimate the losses that could occur due to cable failure given several choke points in the region where cables come ashore. The study was based on a model that combines internet traffic with direct and indirect cost estimates. The report mentions that the direct costs, such as repairing the cable, are relatively low. The indirect costs vary depending on the country in question and the relative connectivity (the number of submarine cables or alternative overland internet exchange points) of the country in question. To illustrate these consequences, the findings state:

'A fault in all landing points in Australia would entail direct costs (for cable repair) of US\$2.2 million and indirect economics [sic] cost of US\$3 169 million mostly due to the loss of 100 % of international internet traffic. It should be noted that the loss of internet connection in Australia would also cut off the internet connection in Papua New Guinea. For a similar case in Korea, the indirect economic costs would be around US\$1 230 million. But for a similar case in Canada, the economic costs would be zero, as there is alternative overland connectivity available to the US.'

In spite of some stated limitations, such a model might provide a basis on which to arrive at a rough estimate of the potential economic losses due to failure of transatlantic submarine cables under a variety of scenarios. Such a study has not to date been conducted.

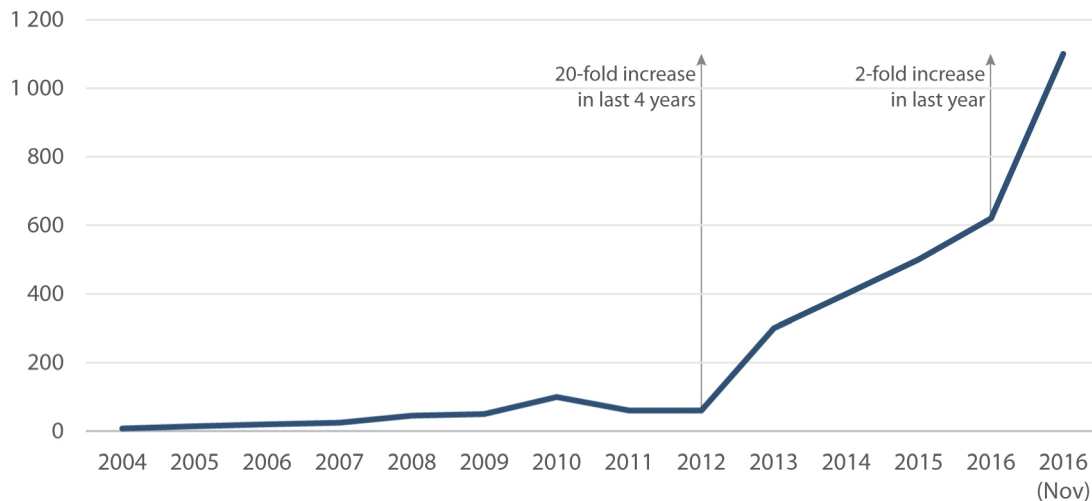
Regarding the **Domain Name System** (DNS), a large portion of DNS traffic is managed by one company, Dyn, which is located on the east coast of the US. On 21 October 2016, Dyn was subject to two unprecedentedly high-powered distributed denial of service (DDos) attacks. The attacks flooded the Dyn servers with over one terabyte of traffic per second until the system could no longer handle the high level of traffic. Once down, an estimated 1 200 websites could no longer be accessed by end users. Some notable sites included PayPal, Twitter, Amazon, Netflix and Spotify (Gallagher, 2016). The attack was linked to the Mirai botnet, which hijacks insecure 'Internet of Things' devices (e.g. DVR players, surveillance cameras). These 'Internet of Things' devices do not have sufficient security measures built into them at the time of design and

⁵² In actual fact, much of the content of this ENISA report relates to cybercrime and cybersecurity failures more broadly, rather than critical (information) infrastructure in a narrow sense as the title of the report would suggest.

manufacture, partly because the producers are not held liable for the harms caused by technology failure, and are therefore vulnerable to bot-net hijacking.

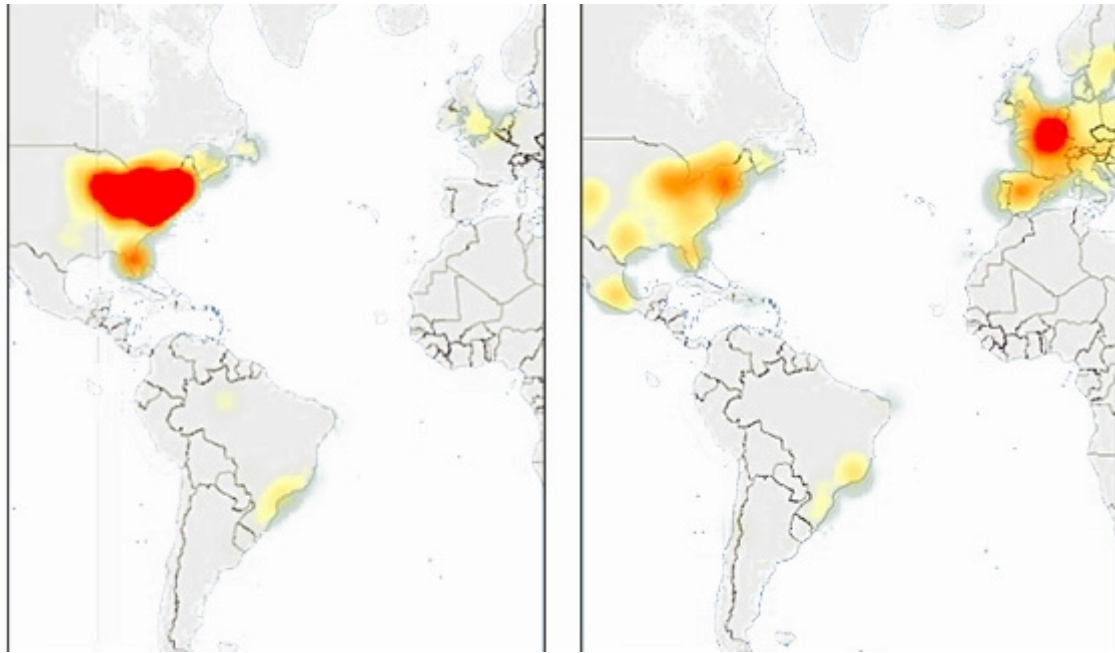
Figure 12 – Evolution of DDoS attack strength

Gigabits per second, 2004-2016 (Nov)



Data source: Arbor Networks Inc. (for 2004-2015) & Gallagher (for 2016).

These incidents demonstrate two important dynamics. First, the power of some cyber-threats, such as botnets, is rapidly increasing. These rapid increases coincide with the first wave of adoption of 'Internet of Things' technologies. The Mirai botnet attack on Dyn was two times more powerful than the most powerful attack seen one year before. It was twenty times more powerful than the most powerful seen just four years previously. This growth rate is likely to continue to accelerate as relatively insecure 'Internet of Things' technologies proliferate. Second, internet users in Europe are somewhat reliant on the functioning of critical information infrastructures in the US, and vice-versa. The map below, on the left, shows regions affected due to the first attack, on Dyn in the US, and its effects in Europe. On the right, the effects of a second attack, this time in London, is shown. In both cases, failure of critical infrastructure on one side of the Atlantic had effects on the other side of the Atlantic. It is still too early to assess the economic losses from this incident. Such a study could be performed however with sufficient resources.

Figure 13 – Internet outages caused by DDoS attack on Dyn, 21 October 2016

Source: Down Detector.

Regarding **internet exchange points**, in the wake of the 2011 revolution in Egypt, the government at the time shut off the sole internet exchange point out of the country. In a hastily put-together exercise, the OECD (2011) estimated that the direct costs of this action led to a minimum of US\$90 million in total. However, this figure does not incorporate the indirect economic losses resulting, 'from a loss of business in other sectors affected by the shutdown of communication services e.g., e-commerce, tourism and call centres.' Such disruption would not be as pronounced in countries with greater numbers of internet exchange points as traffic could be re-routed out of the country via other points.

New concerns have also arisen about the stability of **power grids** when faced with cyber-threats (e.g. incident in Ivano-Frankivsk, Ukraine; and the US Energy Department's Quadrennial Energy Review). There are many studies on the losses associated with power grid failure though not linked particularly to a cyber-related incident. An examination of the results of these studies points to the difficulty in modelling such phenomena however. A commonly cited study, conducted by Lloyds Insurers and the Cambridge Centre for Risk Studies, provides an estimate of the potential losses due to a cyber-attack on the US power grid. The study finds potential losses could amount to between US\$243 billion and US\$1.34 trillion. The range of this estimate – around US\$1 trillion – points to the inexact nature of such modelling exercises. In 2003, a blackout occurred across the north-eastern US and Canada. In a subsequent report, the US-Canada Power System Outage Task Force cited figures suggesting, 'total costs in the United States range between \$4 billion and \$10 billion (US dollars).'⁵³ In a study estimating the direct and indirect economic losses as a result of a

⁵³ However, the original report from which these statistics are derived, from ICF Consulting, calculated total losses based on a survey of consumer's willingness-to-pay (WTP) to avoid such outages. Survey methodologies such as these do not tend to deliver reliable figures at scale as they exclude the complex interrelationships that characterise critical infrastructures and lead to knock-on losses. This is something acknowledged in the original report that, 'the data for the August 2003 outage is preliminary and further refinements will be necessary.'

less than two-day electricity infrastructure outage in Italy in 2003, a rough estimate suggested losses of € 81.79 million for the 11 critical infrastructure industries and €123.17 million for all industries together (Jonkeren et al, 2012).⁵⁴ This study used an input-output model, now a popular method for modelling infrastructure collapse given its ability to model complex inter-relations. These results are a fraction of those found by both the Lloyds/Cambridge and the ICF Consulting studies.

The **aviation sector** also faces certain risks due to digital technologies. These risks might affect the computer systems of airlines, air traffic control systems and the cybersecurity of planes themselves. The example of extensive delays for passengers due to failure of Delta's legacy IT systems has already been mentioned in this chapter (Isidore, 2016; McLean et al, 2017). For a different example, in November 2015, air traffic control systems across much of Sweden were unavailable, resulting in the cancellation of multiple domestic and international flights at the airports of Arlanda, Landvetter and Bromma. Sweden reportedly suspected that a hacker group linked to Russian military intelligence service (GRU) was responsible for an attack (Leyden, 2016). Finally, software vulnerabilities in planes themselves have previously been linked to incidents. In 2008, a Qantas Airbus 330 nose-dived suddenly, twice, while flying off the coast of Western Australia. A number of passengers who were not wearing seat belts, as well as crew members, were seriously injured. According to a government investigation following the incident, it was due to the malfunction of the software on one of the air data inertial reference units, which are used in the on-board autopilot system (Australian Transport Safety Bureau, 2008).

In sum, there are a number of threats and vulnerabilities in the aviation industry that could lead to cyber incidents. It is difficult to estimate the potential losses from these incidents given their low probability and potentially high impact. While an extreme case, an idea of the economic losses due disruption to transatlantic aviation can be ascertained from the eruption in mid-April 2010 of Iceland's Eyjafjallajökull volcano. The ash cloud projected into the atmosphere spread across Europe over the subsequent week. The effects of the eruption on critical transport infrastructure, aviation, was unprecedented and led to the cancellation of over 100 000 flights over one week. The eruption was particularly damaging to transatlantic transport. This is because inter-European travellers could resort to other modes of transport (e.g. train, bus). Such alternatives were not open to transatlantic travellers. The International Air Transport Association (IATA) (2010) estimated that the economic losses to airlines servicing some major transatlantic routes totalled US\$49.9 million for Monday 19 April 2010 (see table below). The total losses to airlines across all flights and routes over the week was estimated to be US\$1.7 billion. While such a system-wide shutdown of aviation due to a cyber-incident is of low probability, these aggregate figures provide at least some idea of the scale of economic losses that might accrue in the event of isolated incidents resulting in delays.

⁵⁴ The study notes that this is likely a slight overestimate owing to the use of an inoperability input-output model.

Table 7 – Economic losses to airlines due to cancelled transatlantic flights**Monday 19 April 2010***Various*

Route	Passengers	% total	Revenue \$US millions	% total
UK-US	37 018	3.0	24.9	8.0
Germany-US	20 681	1.7	7.7	2.5
France-US	13 474	1.1	7.4	2.4
Switzerland-US	4 652	0.4	3.6	1.2
Netherlands-US	7 000	0.6	3.4	1.1
Ireland-US	5 501	0.4	2.9	0.9
Total	88 326		49.9	

Data source: IATA.

6.5. Conclusions

- Failure of critical information infrastructure on one side of the Atlantic impacts those on the other. There is therefore a need coordinated risk management and response (improved cyber-resilience). This in turn is facilitated by governance mechanisms that bring public and private stakeholders, on both sides of the Atlantic, together. Such mechanisms are not as yet in place.
- Dynamic, fast-moving and intensifying threats are emerging for critical infrastructure operators on both sides of the Atlantic. There is a need to facilitate information sharing and best practice development and exchange for critical infrastructure operators so that the most effective measures are implemented widely.
- Technologies associated with the Internet of Things/Industrial Internet do not have sufficient cybersecurity measures built-in at the design and manufacturing stages. As they are adopted, including by operators of critical infrastructure, the number of threat vectors are increasing and new vulnerabilities are being created. These in turn increase the risk of cascading disruptions or failures of critical infrastructures, which could result in high indirect losses.
- The EU and US are spending increasing amounts of public funds on cybersecurity and cyber-resilience measures to mitigate risks. Yet the direct investments are not aggregated in a reliable way for the EU and the US. Moreover, the potential economic losses of disruption or failure to critical (information) infrastructures are difficult, though not impossible, to model *ex ante*. This makes it difficult to implement a risk management approach so as to allocate limited public funds in the most cost-effective way.

7. Current and potential EU-US cooperation

There is a great deal of congruence between the stated policy goals in both the EU and US relating to cybersecurity, cyber-resilience and cybercrime. Cooperation in several areas is already under way. In practice, however, cooperation on some issues has advanced at a faster pace. This is most often a function of the political urgency, congruent or conflicting interests, and the pre-existing tradition of working together. The discussions about cyber-related issues are pursued in several venues, which were established to accommodate the growing preference for closer policy coordination and exchange of information across the Atlantic. This was driven by the increasing complexity of the institutional and regulatory issues; new cybersecurity threats going beyond cybercrime and espionage; and evolving efforts to undermine democratic institutions and values.

Table 8 – Current fora for EU-US cooperation in cyber policy

Name	Description and typical issues addressed
EU-US Cyber Dialogue	Annual forum for discussion of international cyberspace developments, promotion of human rights online, politico-military and international security issues (e.g. establishment of norms of behaviour online) and cybersecurity capacity building in third countries.
EU-US Working Group on Cybersecurity and Cybercrime	Established in 2010 following the EU-US summit in Lisbon. Focus on cyber incident management, public-private partnership on critical infrastructure cybersecurity, cybersecurity awareness raising and cybercrime (White House 2014).
EU-US Information Society Dialogue	Discussion on issues related to ICTs and the digital economy. The fourteenth such dialogue was held in June 2016 and involved discussions on, 'the role of digital platforms, ICT standards, connectivity, copyright, data flows, ICT-enabled research, and international cooperation' (State Department 2016).
EU-US Innovation and Investment in the Digital Economy Dialogue	The first forum was held in March 2016 and brought US Secretary of Commerce Penny Pritzker and Vice President of the European Commission, Andrus Ansip, together for a bilateral meeting. The discussion focused on personal data protection, internet governance, the Internet of Things and policies to create an ecosystem in which innovation and investment in digital technologies may thrive (Commerce Department 2016).
EU-US ICT standardisation roundtable	Addresses broad issues linked to technology standardisation. The most recent edition was held in September 2016 with the participation of US Secretary of Commerce, Penny Pritzker, and EU Commissioner Oettinger. The topics on the agenda include standard-setting for technologies that constitute the Internet of Things, 5G and cybersecurity in a technology-neutral fashion (State Department 2016).
Transatlantic Economic Council	Established in 2009. The cyber-related issues on the agenda include international standards to support the interoperability of patient health records, and of EU-US cooperation on training and workforce development in e-Health/Health IT sector.

In recognition of the growing importance of cyber-related issues for the transatlantic partnership, at the EU-US Summit of 2014, leaders agreed to establish the EU-US Cyber Dialogue, which serves as an umbrella venue for discussing a wide spectrum of cyber-related issues. Areas of broad focus for the dialogue include: international cyberspace developments, promotion of human rights online, politico-military and international security issues (e.g. establishment of norms of behaviour online) and cybersecurity

capacity building in third countries (EU, 2014). A more focused transatlantic conversation also takes place within dedicated venues, such as the EU-US Information Society Dialogue and the EU-US Working Group on Cybersecurity and Cybercrime. The most recent EU-US Cyber Dialogue in December 2016 focused on the following issues:

- **Internet governance:** The Internet Assigned Numbers Authority (IANA) transition that took place in 2016 (see Box 3) was an important step in re-affirming the multi-stakeholder model of internet governance and helped to move away from the state-controlled model proposed by Russia and China under the auspices of the UN. However, both the EU and the US are concerned that the planned International Telecommunications Union (ITU) Plenipotentiary conference in 2018 might be used to challenge the current model of internet governance. This drives a preference for closer EU-US cooperation.
- **International cyberspace issues:** Given the increasing importance of cybersecurity issues in international debates, the EU and the US are working closely on coordinating their positions. This is particularly relevant given that a group of countries, led by China and Russia, is increasingly focused on proposing new conventions or codes which would undermine the open and free nature of the internet. To that aim, the EU and the US work closely to support work on an 'International Cyber Stability Framework' within the UN Group of Governmental experts, and remain committed to promoting global confidence-building in the Organisation for Security and Co-operation in Europe (OSCE). Both are also interested in a possible closer coordination of positions in the framework of the Ise-Shima Cyber Group under the G7 umbrella.
- **International security issues and norms:** The EU and US are each other's closest allies with regard to their positions on the application of international law in cyberspace and norms of responsible state behaviour. 'Attribution' is an issue that requires further discussion. In the absence of a mechanism that would allow for an absolute certainty of the origin of incidents, assigning responsibility for an incident remains a subjective issue based on evidence from various sources.
- **Capacity building in third countries:** There is a general agreement on both sides that strengthening the capacity of partner countries to deal with cybersecurity threats may help effectively combat cybercrime. While some coordination in the capacity building efforts of the EU and the US is already taking place, both sides face similar challenges in the lack of available expertise and in ensuring effective coordination between different stakeholders.
- **Cybercrime:** In order to ensure an effective law enforcement response so as to successfully mitigate incidents, the EU and the US established a robust dialogue on cybercrime. Both the EU-US Working Group on Cybersecurity and Cybercrime and the Justice and Home Affairs Ministerial serve as venues where key cybercrime issues are discussed. The EU and the US are spearheading international efforts to promote legal and institutional solutions proposed in the framework of the Council of Europe Convention on Cybercrime ('Budapest Convention'). This treaty was the first international treaty seeking to address cybercrime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. By 2017, fifty-five states had ratified and four have signed but not yet ratified the convention, including many EU Member States and the US (which ratified the convention in 2006). However, there is the strong effort by a group of countries – including Brazil, China, Russia

and South Africa – to push for a new legal instrument. These conflicting positions have politicised some of the discussions – for instance within the United Nations Office on Drugs and Crime (UNODC). An additional issue that requires further debate is ‘internet jurisdiction’ and the question of access to evidence stored abroad or held by companies established outside of the national jurisdiction of any law enforcement agency.

- **Cyber-resilience:** In light of the accelerating efforts to strengthen cyber-resilience, the EU and the US may aim to coordinate the exchange of information relating to the ongoing or planned activities more closely. In the EU, progress on the implementation of the NIS Directive and communication on strengthening Europe’s cyber-resilience systems may be of particular interest to the US. The EU, on the other hand, may be interested in gaining a better understanding of the functioning of the sector-based Information Sharing and Analysis Centers (ISACs). The EU and the US are also working towards exploring similarities and divergences between the NIS Directive and the Framework for Improving Critical Infrastructure Cybersecurity released by the National Institute of Standards and Technology (the ‘NIST Cybersecurity Framework’).

Box 3 – The significance of the IANA transition for global internet governance

The past decade has seen two particularly important and interrelated developments in internet governance that are relevant to EU and US cooperation. For many years, the US government has been gradually reducing its role in the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA) function that it performs. The IANA function relates to the Domain Name System. It is the high-level system whereby IP addresses are coordinated (ICANN, 2014). Historically, the US Department of Commerce has owned and operated the IANA functions through the National Telecommunications and Information Administration (NTIA). The functions were contracted out to ICANN in 1998.

As the internet was adopted worldwide, the US Department of Commerce sought to step away from its contract with ICANN and to transfer the IANA functions to the international community. Critical to this transfer was the maintenance of the same ‘multi-stakeholder’ model that had been used to govern ICANN decisions throughout its history. The multi-stakeholder model is built around participation, partnership and cooperation of governments, the private sector, civil society, international organisations, the technical and academic communities and all other relevant stakeholders (DeNardis, 2015). The EU and US (among many other countries) have supported this model for over two decades.

At the 2012 World Conference on International Telecommunications in Dubai, several countries supported a new form of internet governance that would give greater control over managing critical internet functions to their own governments via an increased role of the United Nations in such matters. This proposed ‘multilateral’ model would have given sovereign nations more of a role in internet governance matters, in a marked departure from the ‘multi-stakeholder’ model (ibid). After long negotiation, this matter was resolved, for the time being, at a meeting of the World Summit on the Information Society’s ten-year review on 15-16 December 2015. At this meeting, the nations present reaffirmed their support of a multi-stakeholder model (UN General Assembly, 2016). Moreover, on 1 October 2016, the NTIA contract with ICANN expired and the IANA functions were finally transferred to an ICANN that is entirely free from US government oversight (IANA SCG, 2016).

7.1. Looking ahead: issues for EU-US cooperation

The analysis of relevant EU and US strategies allows identification of six areas of congruence related to cybersecurity, cyber-resilience and cybercrime (see Table 9). These are potential areas of cooperation. In practice, some have been taken forward on a cooperative basis and others have not for a variety of reasons.

The resilience of critical infrastructure is paramount for the EU and US. Recognition of this importance is reflected in the EU with the NIS Directive and in the US with both EO 13636 and the 2017 EO on 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure'. Measures to ensure the continued and reliable functioning of portions of the internet infrastructure/architecture, such as transatlantic submarine cables and the DNS system, are vital to avoid the costs and losses – on both sides of the Atlantic – that would be incurred were these infrastructures to be disrupted or fail. The potential for low-probability but high impact events with critical (information) infrastructure cannot be understated. Most of the critical information infrastructure is owned and operated by private companies which operate on both sides of the Atlantic. This ensures some measure of cooperation. Yet there do not appear to be many formal mechanisms through which critical infrastructure operators might cooperate in the development of risk management/crisis response on a sector-by-sector basis with their public and private sector transatlantic counterparts. Such mechanisms may be useful to investigate and implement in the future especially when the NIS Directive and PPD-21 both call explicitly for international cooperation.

Both the EU and US have called for **direction of research and development efforts towards technologies that would increase cybersecurity**. Substantial public funds have already been allocated towards such efforts. In July 2016, the EU announced the creation of a public-private partnership on cybersecurity. The EU will invest € 450 million in public funds in this partnership under its research and innovation programme Horizon 2020 (European Commission, 2016b). It is hoped that the initiative will result in € 1.8 billion in total public and private investment. In the US, the 2016 Cybersecurity National Action Plan called for creation of a US\$3.1 billion Information Technology Innovation Fund.⁵⁵ The draft budget for FY 2018 includes US\$1.5 billion for the Department of Homeland Security for activities related to protecting federal networks and critical infrastructure from attacks (DHS, 2017). The US also has a 2016 Federal Cybersecurity Research and Development Strategic Plan⁵⁶. Rather than separately investing in technologies with the same goal or purpose, thereby duplicating the research effort, it may be more prudent to investigate in what ways research might be coordinated so as to deliver the greatest or most useful research output.

⁵⁵ The legislation that would have created this initiative, the Information Technology Modernization Act 2016, was not subsequently enacted by Congress. That the initiative was proposed however indicates a desire on the part of the Federal government to invest substantial funds in improving the security of Federal IT systems.

⁵⁶ On a related note, on 23 January 2017, the Chinese government announced the equivalent of a US\$14.5 billion public fund to invest in internet-related technologies (Ge, 2017).

Table 9. Comparison of the EU and US Cybersecurity Strategies

Potential area of cooperation	EU	US
Develop cyber-resilience	<p>EU Cybersecurity Strategy</p> <ul style="list-style-type: none"> Achieving cyber-resilience <p>Digital Agenda for Europe</p> <ul style="list-style-type: none"> Action 28: Reinforced NIS policy Action 33: Support EU-wide cybersecurity preparedness Action 38: Member States to establish pan-European CERTs Action 41: Member States to set up national alert platforms Action 123: Proposal for NIS Directive. 	<p>Cybersecurity National Action Plan, 2016</p> <ul style="list-style-type: none"> Enhance critical infrastructure security and resilience Establish National Center for Cybersecurity Resilience
Combatting cybercrime	<p>Digital Agenda for Europe</p> <ul style="list-style-type: none"> Action 30: Establish a European cybercrime platform. Action 31: Analyse the usefulness of creating a European cybercrime centre. Action 32: Strengthen the fight against cybercrime and cyber-attacks at international level. 	<p>Cybersecurity National Action Plan, 2016</p> <ul style="list-style-type: none"> Deter, Discourage, and Disrupt Malicious Activity in Cyberspace
Fortifying cyber defence	<p>EU Cybersecurity Strategy</p> <ul style="list-style-type: none"> Improve cyber-defence training and exercise opportunities for military in European and multinational context Cooperation between EU and NATO <p>Common Security and Defence Policy Cyber Defence Policy Framework</p>	<p>Department of Defense Cyber Strategy</p> <ul style="list-style-type: none"> Defend DoD networks, systems, and information. Defend the US homeland and US national interests against cyber-attacks of significant consequence. Provide cyber support to military operational and contingency plans.
Information sharing and response	<p>EU Cybersecurity Strategy</p> <ul style="list-style-type: none"> Achieving cyber-resilience: Information sharing and mutual assistance 	<p>Comprehensive National Cybersecurity Initiative, 2009</p> <ul style="list-style-type: none"> Information sharing between government information security centers and strategic operations centers
Establishing norms	<p>EU Cybersecurity Strategy</p> <ul style="list-style-type: none"> Establish a coherent international cyberspace policy for EU and 'promote core EU values' 	<p>Cybersecurity National Action Plan, 2016</p> <ul style="list-style-type: none"> Norms e.g. states should not conduct the cyber-enabled theft of intellectual property for commercial gain
Coordination of R&D	<p>EU Cybersecurity Strategy</p> <ul style="list-style-type: none"> R&D investment and innovation Coordinate funding through Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation Coordinate research agendas across EU institutions and member states 	<p>Comprehensive National Cybersecurity Initiative, 2009</p> <ul style="list-style-type: none"> Coordinate R&D efforts Reorient R&D spending to 'develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years'

Potential area of cooperation	EU	US
		Cybersecurity National Action Plan, 2016 <ul style="list-style-type: none"> • \$3.1 billion Information Technology Innovation Fund • 2016 Federal Cybersecurity Research and Development Strategic Plan

International cooperation is desirable to **effectively combat cybercrime**, which can be conducted trans-nationally. There are many formal and informal mechanisms in place to facilitate cooperation in this area. For instance, the Budapest Convention, Global Alliance against Child Sexual Abuse Online and mutual legal assistance treaties (MLATs). Access to evidence for the purpose of criminal proceedings is officially conducted through MLATs between the US, the EU, and EU Member States. However, the increasing reliance of law enforcement on alternative methods for accessing evidence suggests a need to rethink the MLAT processes. For instance, governments and law enforcement agencies are making more formal requests for access to metadata held by major technology companies outside of the MLAT process (see figure 16 below). This, coupled with the recent Microsoft vs FBI case in Ireland, in which the FBI sought to access emails of a Microsoft customer held in an Irish data centre (Brown et al, 2016), indicate that needs related to access to evidence are not being met through the traditional MLAT process. One reason for this circumvention of the MLAT process is that the process has not kept pace with technological change. Requests made within the MLAT process tend not to be fast enough to meet the needs and requirements of law enforcement entities. Requests made outside the MLAT process lack adequate oversight and transparency (Fidler, 2015). Governments have been attempting to circumvent/avoid the MLAT process in a number of ways, which have had associated negative effects. For instance, governments are:

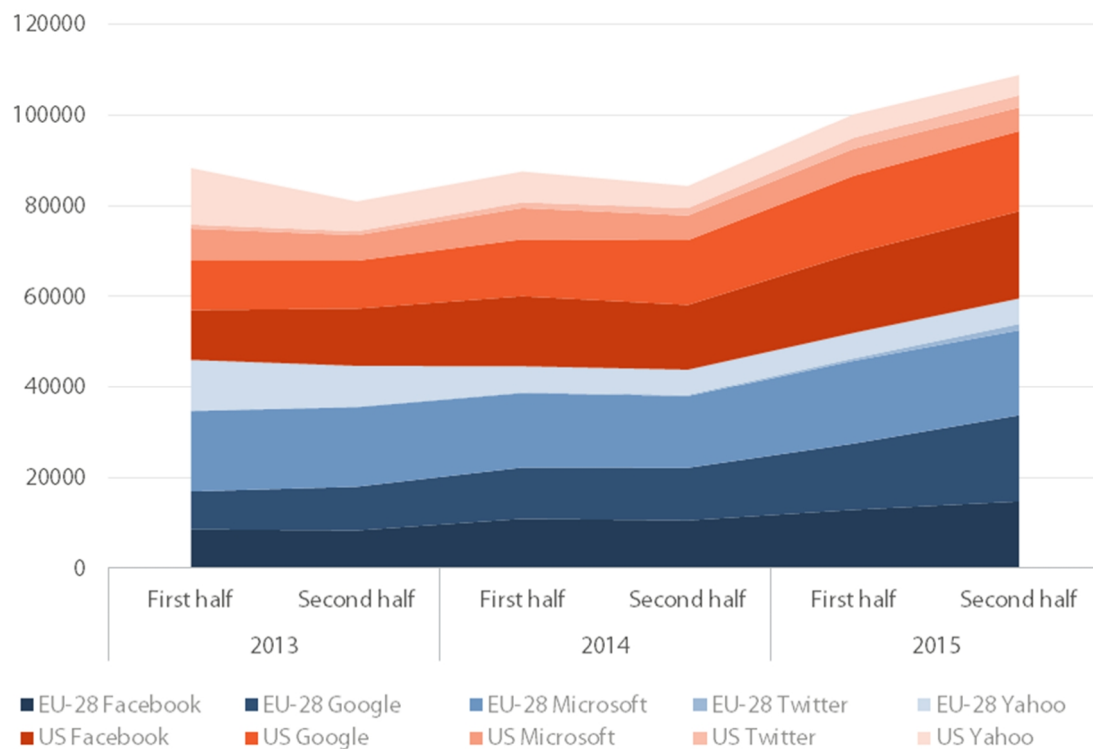
'requiring companies to store content locally so as to ensure access; demanding mandatory anti-encryption regimes as an end-run on the restrictions on access; asserting broad authority to access the data extraterritorially, thereby bypassing more stringent privacy protections that apply under the domestic law where the data is held; and subsequently harassing, indicting, and threatening with arrest employees or officers of local subsidiaries for refusing to turn over the requested data' (Daskal and Woods, 2016).

Without reform of the MLAT process, these negative side-effects are likely to persist. National law enforcement authorities in the EU and US are likely to remain hamstrung in acquiring information to assist with the investigation of cybercrime cases investigations and cases relating to other criminal activities.

In addition, EU and US efforts to promote the solutions proposed in the Budapest Convention face criticism. A number of nations with large and fast-growing populations of internet users are not signatories to the Budapest Convention. These countries include Brazil, China, India and Russia (among many others). Opposition to signing the Budapest Convention commonly includes the position that negotiations for the original convention did not have the input of the countries that have not yet signed the convention (UNODC, 2015). As a result, the convention does not adequately reflect their values or views. Some also contend that provisions in the convention violate principles of state sovereignty (Grigsby, 2014). Rather than sign and ratify the Budapest Convention, some of these countries would prefer the development of a new convention potentially under the aegis of the United Nations (UNODC, 2015).

Figure 16 – Account requests by EU and US governmental agencies and law-enforcement agencies, 2013-15

Thousands



Data source: Quarterly transparency reports from relevant companies.

Information sharing can assist organisations in preparing for, responding to and recovering from cybersecurity incidents. There are many forums through which transatlantic discussions are held on issues related to digital technologies and their consequences. The EU-US Cyber Dialogue in particular provides a regular forum in which new issues can be raised and subsequent cooperative arrangements pursued. However, there are less formal mechanisms by which information sharing on cyber threats and incidents – particularly pertaining to critical infrastructure – can occur between public and private sector stakeholders in the EU and US.

The NIS Directive calls for closer international cooperation between a CSIRT network, a Collaboration Group, and agencies in other countries to improve security standards and information exchange, and to promote a common global approach to security issues. The European Public-Private Partnership for Resilience established following the European Commission policy initiative on Critical Information Infrastructure Protection is another suitable venue on the EU side where such discussions could take place.

In the US, the Department of Homeland Security (DHS) is the lead organisation for threat and incident information collection and dissemination. US-CERT and ICS-CERT are both housed within DHS. Moreover, a number of sectoral information sharing and analysis centres (ISACs) have been set-up in the US. These centres have a long track record in bringing together public and private entities around information sharing and critical infrastructure. A National Council of ISACs permits information sharing across different sectoral ISACs.

Transatlantic cooperation around threat and incident intelligence sharing – particularly around critical infrastructure – could thus be pursued through a forum or vehicle that

brings together representatives from the NIS platforms, the EP3R (through ENISA), the US-CERT, ICS-CERT (through the Department of Homeland Security) and the National Council of ISACs.

The EU and the US have made concerted efforts to **work towards norms of behaviour in cyberspace** through bilateral efforts with third countries and international organisations and bodies within the UN system (e.g. the United Nations Group of Governmental Experts), the Organisation for Security and Cooperation in Europe and the ASEAN Regional Forum (State Department, 2015). While establishment of such norms is difficult, owing to obstacles in reaching consensus and to difficulties in enforcement, the relatively low cost that such efforts entail, combined with even a small probability of success, imply that continuation of such efforts may be warranted.

One area that has not been covered in such discussions is the how multiple countries might coordinate the imposition of 'non-cyber' sanctions in response to a state-sponsored cyber-incident. To date, some instances of unilateral sanctions and other measures have occurred due to cyber-incidents, e.g. President Obama imposed sanctions on the Russian Federation via Executive Order following the US Presidential elections in 2016 (White House, 2016d). It is worth noting that, while the initial impetus for such measures was a 'cyber-incident', the response was a 'non-cyber' measure (economic sanctions and expulsion of diplomats).

With such a wide range of possible responses to a cyber-incident, it becomes difficult to determine under what conditions a response is warranted and, in instances where the conditions are met. It is not clear, for instance, what is considered a 'proportional response'. Joint-imposition of economic sanctions is a common response to incidents in other fields (e.g. military aggression). It is not known if economic sanctions, or any other restrictive measures, would be deemed appropriate and, if so, under what conditions.

Evaluation of policies can lead to improvements in future policy outcomes. There is a long history of evaluation of technology and innovation-related policies on both sides of the Atlantic. In their review of policy evaluation in innovation and technology, Papaconstantinou and Polt (1997) define evaluation as, 'a process that seeks to determine as systematically and objectively as possible the relevance, efficiency and effect of an activity in terms of its objectives, including the analysis of the implementation and administrative management of such activities'. Indeed, the EU cybersecurity strategy specifically calls for monitoring and evaluation of the policies contained within the strategy. Unfortunately, cybersecurity is an area where the outcomes are rarely measured (Herley et al. 2014). In spite of many countries having implemented national cybersecurity strategies, and having invested many billions of taxpayer funds, over the past decade, very few of these policies have been subjected to any form of evaluation. The gold standard for research design to evaluate policies is the randomised controlled trial (Sanson-Fisher et al, 2007; Lee & Lemieux, 2013). However, such methods are often too costly, impractical, or raise ethics concerns (Sanson-Fisher et al, 2007).

Quasi-natural experiments overcome some of these issues. They involve application of an exogenous treatment due to social or political interventions, such as a change in laws or implementation of a new government programme. By virtue of the fact that policy interventions themselves are exogenous events, quasi-natural experiments are a promising direction for the evaluation of cybersecurity policies. Indeed, quasi-natural experiments can be conducted using a wide-ranging and methodologies (Remler & Van Ryzin, 2015). This flexibility further increases the applicability of quasi-natural

experiments to cybersecurity policies (Dean, 2017). The conduct of evaluations, and sharing of best practices, might possibly be an area for future EU and US cooperation in cyber-resilience and cybercrime policy.

Box 5 – Evaluations of online music piracy laws using quasi-natural experiments

Quasi-natural experiments have been successfully conducted to assess the effectiveness of legislation on reducing online music piracy. As a result of these evaluations, it is now known that music piracy laws result in a lower incidence of piracy, though only if the law is enforced over time (though this may be at a cost that may not in turn generate sufficient benefits).

Adermon and Liang (2014) took advantage of the quasi-natural experimental conditions created by the change in Sweden's laws concerning online music piracy in 2009. The changes involved allowing intellectual property rights holders to request the identity of infringers from internet service providers. Using a difference-in-difference method, the researchers compared Sweden (the treatment group) with Norway (the comparison group). It was found that, 'the reform decreased internet traffic by 16 % and increased music sales by 36 % during the first six months' though the impact disappeared after six months, 'likely because of the weak enforcement of the law'.

So too, Danaher et al. (2013) examined the impact of France's HADOPI laws on online music sales. Using five other European countries without such laws as the comparison group, it was found that, following the law's implementation, iTunes sales in France increased by around 25 %. The implication of these studies is that anti-piracy laws have some beneficial impact (in terms of reducing piracy and increasing sales for rights holders).

7.2. EU-US competition

The US and EU have experienced a number of incidents in recent years relating to the data privacy requirements for 'over the top' messaging apps and protections for the personal data of EU citizens. These incidents have been precipitated by diverging policies, laws and regulations between the EU and US. In some cases, however, the disagreements over the security of these technologies may in fact lead to better cybersecurity outcomes than maintenance of the status quo. This suggests that transatlantic cooperation in all aspects of policy relating to digital technologies may not be desirable, at least if the goal of policy is to improve cybersecurity outcomes.

One area of divergence between the EU and US in recent years has been the **privacy requirements placed on app-based communication platforms**, including those of US companies, in the EU. Proposed changes to the European Electronic Communication Code would include 'over-the-top' online communications platforms (e.g. Whatsapp) under telecommunication rules. This would require servers and networks to be more secure, that disabled users have equivalent access to services, and that users be able to reach emergency numbers if technically possible. It would also require compliance with certain ePrivacy rules (Baker, 2016). US regulations in this area are different to the proposed EU rules. Some similarities in the application of privacy rules can be seen in the Federal Communication Commission's recent decision to restrict broadband providers' ability to collect and use customer data (FCC, 2016). To date though, online communications platforms are regulated differently to the way that the US regulates telecoms. Privacy is in some ways the flip-side of data security. If data (and the servers on which they are stored) are secure, in the sense that they remain confidential, then

privacy is maintained.⁵⁷ Given the new provisions that would, in theory, improve the security of these platforms, this is one area where difference may in fact result in greater security than the status quo.

Another area of divergence relates to the implementation of **the EU General Data Protection Regulation and Directive**. These policy changes impose tighter regulatory requirements around commercial and governmental handling of personal data. They include a more punitive system, relative to the present system in place in the US, of fines for non-compliance. The rules will apply to all foreign companies processing the personal data of EU citizens – including US companies. Given that many US technology companies (particularly social networks and Cloud providers) handle large amounts of data in the EU, they will have to comply with these new rules and regulations. Again, imposition of penalties for non-compliance with data protection rules is likely to lead to improved security of the personal data in question. This is another area where policy differences may result in greater security than the status quo.

One area of continued negotiations and contention relates to the protections afforded to EU citizens' data held in the US (by US companies). In October 2015, the European Court of Justice struck down the **EU-US 'safe harbour' provisions for transatlantic exchange of personal data** (Jourova, 2015). Since then, negotiations have been underway between the EU and US to seek to secure a new legal framework for the exchange of such data. In July 2016, the EU-US 'privacy shield', the outcome of these negotiations, was approved by representatives of EU Member States then adopted by the European Commission (2016a). However, legal challenges to the 'privacy shield' were made, most notably by Digital Rights Ireland (Fioretti and Volz, 2016). This issue has not yet been resolved. The framework will be reviewed in September 2017 (Ibraimova and LaFrance, 2017). If the EU and US are able to reach a cooperative agreement that is acceptable to all parties, as is hoped, it may provide significant policy initiatives to ensure the protection of the data of EU citizens.

That there will be differences between the EU and the US in terms of policy goals and the means used to achieve these goals, is likely. Competition or conflict are possibly unavoidable and may, in some cases, be desirable if they permit policy experimentation that, in turn, leads to the identification of best practices and subsequent adoption of those practices by other countries in the future. Overcoming the obstacles to cooperation in areas of deep disagreement – such as those areas covered in this section – requires, in some cases, changes to fundamental values or constitutional limits. Rather than focusing efforts on seeking to resolve these areas of deep disagreement, in the short-term, it may be more fruitful to examine areas where cooperation might be built on common ground.

⁵⁷ Data or cyber 'security' is often conceived as involving accessibility, authenticity, integrity and confidentiality. While security and privacy are sometimes pitted against one another in policy debates, with the framing involving a trade-off of one for the other, there are instances where the two are not mutually exclusive – indeed they can be mutually reinforcing.

Box 6 – Previous European and US cooperation to address global challenges

The EU and US have a long history of successful international cooperation in addressing global challenges. This can be seen in information sharing to manage infectious diseases, common defence, establishing global safety standards and managing complex issues around trade and ownership. In each case, there is some similarity or applicability to cybersecurity and reducing cybercrime, which might hold hints as to how EU-US cooperation might be successfully pursued in these areas in the future.

Managing infectious diseases

Similar to cybercrime, infectious diseases span across borders. The Centers for Disease Control were developed in the US in the 1940s to address malaria. Subsequently, Centers for Disease Control and Prevention (CDCs), modelled on the US example, were created in other countries. As a next step, the World Health Organization (WHO) was set up under the auspices of the United Nations to coordinate national responses to infectious disease outbreaks, share information and pool research efforts. To date, no equivalent of the CDCs or WHO has emerged for cybersecurity or cybercrime related issues.

Information-sharing is important to prepare for and respond to cyber-incidents. There are strong incentives to conceal the occurrence of security failures such as data breaches. An elaborate international apparatus emerged over the past century to allow for cooperation in information sharing related to the control and management of infectious diseases. The WHO provides a means by which Member States can report the emergence of infectious diseases. This information is then disseminated to other Member States through disease outbreak bulletins and annual statistics (e.g. The World Health Report). Very often though, public entities will not report to the WHO and its members when/if cases of an infectious disease have been found in their country. The cases are concealed because the negative effects that disclosure of such cases would have on trade and tourism are potentially large. This was seen in the emergence of SARS in China (FlorCruz, 2003). Similar information asymmetries and incentives are at play with cybersecurity and cybercrime. As of yet, no equivalent information sharing institutional structure has been set up to deal with these phenomena.

Safety standards and product liability

In the past, the global spread of new, transnational technologies – like aviation and automobiles – created a need for global safety standards and regulations. This need led to the emergence of several international institutional structures. The sharing of best practices, through forums such as the International Civil Aviation Organization, ensured that safety standards spread rapidly to the benefit of those consumers who otherwise would have been put at risk. So too, 50 years after the beginning of the mass production of the automobile, rigorous safety standards and product liability were imposed, first in the US, then in other countries. There is a need to develop cybersecurity standards worldwide and possibly a need to develop product liability laws (even more so with the impending wave of ‘Internet of Things’ devices). For the moment, some technology standards are managed through organisations such as the International Organization for Standardization (ISO) and EU-US technology standards are discussed through the EU-US ICT standardisation roundtable.

Trade access rights and ownership

The EU and US are one another's largest digital trade partners (Meltzer, 2014). The internet forms the infrastructural backbone for a growing proportion of world trade. Throughout much of human history, international maritime trade has been a source of wealth. Over many hundreds of years, a complex system of laws and institutions were formed to govern the activities associated with global trade like ports, land ownership, etc. For instance, the United Nations Convention on the Law of the Sea ('the Law of the Sea') defines the rights and responsibilities of nations with respect to their use of the world's oceans. The US has not yet ratified this convention. No equivalent multilateral instrument has emerged for communications networks such as the internet. To the extent that connected communications networks might be considered as a separate domain ('cyberspace'), similar to the way that the US Department of Defense considers cyber as an operational domain, so too might a need arise for development of a multilateral instrument to define the rights and responsibilities of nations with respect to their use of 'cyberspace'. The International Telecommunications Union (ITU) is active in the area of cybersecurity though the partnerships and collaborations do not involve legally binding instruments.⁵⁸ The 'Tallinn Manual on the International Law Applicable to Cyber Warfare' is an academic study on how international law connects to military-related issues such as cyber-conflict and cyber-war. It does not examine broader issues related to digital trade or stakeholders' responsibilities for issues related to cybersecurity, cyber-resilience or cybercrime.

7.3. Conclusions

- There are many possible areas of congruence in terms of policy goals between the EU and US. These are potentially promising areas where greater cooperation might be realised between the US and the EU in the future. These areas include: Developing cyber-resilience; coordination of research and development; combatting international cybercrime; information sharing and response; establishment of norms of behaviour in cyberspace. Nevertheless, there is sometimes disagreement between the EU and the US in terms of policy goals and the means used to achieve these goals. While the long-term focus should be on resolving such areas of disagreement, in the short-term, it may potentially be more fruitful to examine areas where cooperation might be built on common ground.
- Competition or conflict are possibly unavoidable and may, in some cases, be desirable if they permit policy experimentation that, in turn, leads to the identification of best practices and subsequent adoption of those practices by other countries in the future. Overcoming the obstacles to cooperation in areas of disagreement – such as those areas covered in this section – may require, in some cases, changes to fundamental values or constitutional limits. Rather than focus efforts on resolving disagreement, in the short-term, it may be more fruitful to examine areas where cooperation might be built on common ground.
- The EU and US have a long history of successful international cooperation in addressing global challenges. This can be seen in though information sharing to manage infectious diseases, common defence, establishing global safety standards and managing complex issues around trade and ownership. In each case, there is some similarity or applicability to cybersecurity and reducing cybercrime, which might hold hints as to how EU-US cooperation might be successfully pursued in the future.

⁵⁸ For more information see: ITU, 2017, Global partnerships, available from: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx>.

- Cybersecurity and cybercrime policy evaluation could potentially form a promising area for cooperation between the EU and US. Policy evaluation may lead to more effective outcomes (reduced incidents and associated impacts leading to higher benefits and lower costs/losses) due to cybersecurity failures and cybercrime. Quasi-natural experiments are a promising direction for the evaluation of cybersecurity policies.

8. Main references

- Adermon A. & Liang C. (2014), 'Piracy and music sales: the effects of an anti-piracy law', *Journal of Economic Behavior and Organization*, 105, 90-106.
- Anderson R., Barton C., Böhme R., Clayton R., van Eeten M. J. G., Levi M., Moore T. and Savage S. (2012), 'Measuring the cost of cybercrime', *Workshop on the Economics of Information Security*, available from: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf (accessed 19 November 2016).
- Andrews D., Criscuolo C. and Gal P. (2016), 'The Best versus the Rest: The Global Productivity Slowdown, Divergence Across Firms And the Role of Public Policy', *OECD Productivity Working Papers No. 5*, 2016.
- APEC (2012), 'Economic impact of submarine cable disruptions', APEC Policy Support Unit, December 2012.
- Arbor Networks Inc. (2016), 'Worldwide Infrastructure Security Report', Volume XI, available from: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf (accessed 25 January 2017).
- Australian Transport Safety Bureau (2008), 'In-flight upset - Airbus A330-303, VH-QPA, 154 km west of Learmonth, WA, 7 October 2008', Investigation number: AO-2008-070, available from: http://www.atsb.gov.au/publications/investigation_reports/2008/AAIR/pdf/AO2008070_interim.pdf (accessed 18 September 2017).
- Baily M. & Montalbano N. (2016), 'Why is US productivity so slow? Possible explanations and policy responses', *Brookings Institute*, Hutchins Center Working Paper 22.
- Baker J. (2016), 'New EU telco rules will 'fragment' market says Skype, WhatsApp, YouTube', *Ars Technica*, <http://arstechnica.co.uk/tech-policy/2016/09/skype-whatsapp-youtube-claim-eu-telco-rules-will-fragment-market/> (accessed 19 November 2016).
- Bradley J., Reberger C., Dixit A. and Gupta V. (2013), 'Internet of Everything: A \$4.6 Trillion Public-Sector Opportunity', available from: http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf (accessed 17 January 2017).
- Brand S. L. and Makey J. (1985), 'Department of Defense password management guideline', CSC-STD-002-85, Department of Defense Computer Security Center, April 1985.
- Brown I., Krishnamurthy V. and Swire P. (2015), 'Reforming Mutual Legal Assistance Needs Engagement Beyond the US', *Lawfare Blog*, available from: <https://www.lawfareblog.com/reforming-mutual-legal-assistance-needs-engagement-beyond-us> (accessed 26 January 2017).
- Brown T., Beyeler W. and Barton D. (2004), 'Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems', *Int J Crit Infrastruct*, 1:108–117.
- Brynjolfsson E. and Oh J. H. (2012), 'The Attention Economy: Measuring the Value of Free Digital Services on the Internet', *Thirty Third International Conference on Information Systems*, Orlando 2012.
- Bureau of Labor Statistics (2014), 'Information security analysts: Job outlook', available from: <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6> (accessed 19 January 2017).
- BYU Idaho (2012), 'Section 01: Monopolies', available from: https://courses.byui.edu/ECON_150/ECON_150_Old_Site/Lesson_08.htm (accessed 23 October 2016).

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou (2003): 'The economic cost of publicly announced information security breaches: Empirical evidence from the stock market,' *Journal of Computer Security*, 1, 431–448.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004), 'The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers,' *International Journal of Electronic Commerce*, 9, 69–104.

Chen Y., Young G., Jeon J. and Kim Y. (2012), 'A Day without a Search Engine: An Experimental Study of Online and Offline Searches', University of Michigan, available from: http://yanchen.people.si.umich.edu/papers/VOS_2013_03.pdf (accessed 17 January 2019).

Chiasson S. & van Oorschot P. C. (2015), 'Quantifying the security benefits of password expiration policies', *Designs, Codes and Cryptography*, December 2015, Volume 77, Issue 2, 401–408.

Christin N. (2013), 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace', *International World Wide Web Conference 13*, available from: <https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf> (accessed 21 November 2016).

Cohen P., Hahn R., Hall J., Levitt S. and Metcalfe R. (2016), 'Using big data to estimate consumer surplus: the case of Uber', *NBER Working Paper* 22627.

Colman S. and Joyce T. (2008), 'Minors' Behavioral Responses to Parental Involvement Laws: Delaying Abortion Until Age 18', *Perspectives on Sexual and Reproductive Health*, Vol 41(2), pp199-126.

Commerce Department (2016), 'Press release: First EU-US Innovation and Investment in the Digital Economy Dialogue', available from: <https://www.commerce.gov/news/press-releases/2016/03/first-eu-us-innovation-and-investment-digital-economy-dialogue> (accessed 16 September 2016).

Commission on Enhancing Cybersecurity (2016), 'Report on securing and growing the digital economy', National Institute of Standards and Technology, available from: <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf> (accessed 25 January 2017).

Danaher, B., Smith, M. D., Telang, R., & Chen, S. (2014), 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France', *The Journal of Industrial Economics*, 62(3), 541-553.

Daskal J. (2016), 'A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right', Just Security, available from: <https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/> (accessed 25 January 2017).

Data Center Research (2016), 'Internet exchange points map', available from: <http://www.datacentermap.com/ixps.html> (accessed 17 September 2016).

Dean B. C. (2015), 'Why companies have little incentive to invest in cybersecurity', The Conversation, available from: <https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570> (accessed 20 November 2016).

Dean B. C. (2017), Using natural and quasi-natural experiments to evaluate cybersecurity policies, *The Cyber Issue*, Winter/Fall 2017.

Decker R. A., Haltiwanger J., Jarmin R. S. and Miranda J. (2016), 'Declining Business Dynamism: What We Know and the Way Forward', *American Economic Review: Papers and Proceedings*, vol. 106, no. 5, pp. 203-07.

DeNardis L. (2015), 'Discussion on 'The Future of Multi-stakeholder Internet Governance'', *Proceedings of the Conference on Internet Governance and Cybersecurity 2015*, School of International and Public Affairs, Columbia University.

Department of Homeland Security (2017), 'Administration's Fiscal Years 2017 Budget Amendment and 2018 Budget Requests Advance DHS Operations', available from: <https://www.dhs.gov/news/2017/03/16/administrations-fiscal-years-2017-budget-amendment-and-2018-budget-requests-advance> (accessed 7 July 2017).

Department of Justice (2015), 'US Department of Justice FY 2015 budget request: Mutual legal assistance treaty process reform', available from: <https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf> (accessed 26 January 2017).

Detica and Office of Cyber Security and Information Assurance (2011), 'The cost of cybercrime', February 2011, available from: <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cybercrime> (accessed 20 November 2016).

Dvorkin M. (2016), 'Jobs Involving Routine Tasks Aren't Growing', St. Louis Federal Reserve, <https://www.stlouisfed.org/on-the-economy/2016/january/jobs-involving-routine-tasks-arent-growing> (accessed 19 November 2016).

The Economist (2013), 'Net Benefits: How to quantify the gains that the internet has brought to consumers', available from: <http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gains-internet-has-brought-consumers-net-benefits> (accessed 19 January 2017).

Edwards B., Hofmeyr S. and Forrest S. (2014), 'Hype and Heavy Tails: A Closer Look at Data Breaches', Workshop on the Economics of Information Security.

ENISA (2014a), 'Methodologies for the identification of Critical Information Infrastructure assets and services', Guidelines for charting electronic data communication networks, December 2014.

ENISA (2014b), An evaluation framework for national cyber security strategies, ISBN: 978-92-9204-109-0, DOI: 10.2824/3903.

ENISA (2016a), 'The cost of incidents affecting CII: Systematic review of studies concerning the economic impact of cybersecurity incidents on critical information infrastructures (CII)', August 2016.

ENISA (2016b), 'Annual incident report 2015', available from: <https://www.enisa.europa.eu/publications/annual-incident-reports-2015> (accessed 27 January 2017).

European Central Bank (ECB) (2013), 'Second Report on Card Fraud', ISBN 978-92-899-1013-2.

European Commission (2007), 'Towards a general policy on the fight against cybercrime', May 2007, COM(2007) 267 final, available from: http://europa.eu/rapid/press-release_MEMO-07-199_en.htm (accessed 18 November 2016).

European Commission (2011), 'Press release: Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cybersecurity and cybercrime threats', available from: http://europa.eu/rapid/press-release_MEMO-11-246_en.htm (accessed 16 September 2016).

European Commission (2013), 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union', SWD(2013) 32 final.

European Commission (2015), 'Competition policy brief: The interchange fee regulation', Issue 2015-3, June 2015, ISBN 978-92-79-38783-8, ISSN: 2315-3113.

European Commission (2016a), 'Press release: European Commission launches EU-US Privacy Shield: stronger protection for transatlantic data flows', available from: http://europa.eu/rapid/press-release_IP-16-2461_en.htm (accessed 21 January 2017).

European Commission (2016b), 'Press release: Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats', available from: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (accessed December 2017).

European Commission (2017), 'Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product', available from: <http://ec.europa.eu/docsroom/documents/23471> (accessed 7 July 2017).

European Payments Council (2016), 'EPC list of SEPA scheme countries', available from: <http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-list-of-sepa-scheme-countries/> (accessed 25 January 2017).

European Union (2008), 'Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection', available from: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0013> (accessed 18 November 2016).

European Union (2014), 'Fact sheet: EU-US cooperation on cybersecurity and cyberspace', available from: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf (accessed 17 September 2016).

European Union (2016), 'The Directive on security of network and information systems', Directive (EU) 2016/1148, available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (accessed 21 November 2016).

Europol (2016), 'Internet Organised Crime Threat Assessment', available from: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> (accessed 20 January 2017).

Eurostat (2015), 'ICT security in enterprises', available from: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises (accessed 25 January 2017).

Eurostat (2016a), 'ICT specialists in employment', available from: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment (accessed 19 January 2017).

Eurostat (2016b), 'ICT specialists - statistics on hard-to-fill vacancies in enterprises', available from: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises (accessed 19 January 2017).

Evans P. C. and Annunziata M. (2012), 'Industrial Internet: Pushing the bounds of mind and machine', available from: http://www.ge.com/docs/chapters/Industrial_Internet.pdf (accessed 19 January 2017).

FCC (2016), 'FCC Adopts Broadband Consumer Privacy Rules', available from: <https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules> (accessed 21 November 2016).

Federal Reserve System (2012), 'Federal Reserve Payments Study 2012', available from: <http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-August-Prepaid.pdf> (accessed 20 January 2017).

Federal Reserve System (2016), 'Federal Reserve Payments Study 2016', available from: <https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf> (accessed 20 January 2017).

Finkle J. (2016), 'Ransomware: Extortionist hackers borrow customer-service tactics', Reuters, available from: <http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X> (accessed 27 February 2017).

- Fioretti J. and Volz D. (2016), 'Privacy group launches legal challenge against EU-US data pact', Reuters, available from: <http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK> (accessed 21 January 2017).
- Flater D., Black P. E., Fong E., Kacker R., Okun V., Wood S. & Kuhn D. R. (2016), 'A rational foundation for software metrology', National Institute of Standards and Technology, <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8101.pdf>.
- Florczuk J. (2003), 'China censors SARS report', CNN, 14 May 2003, available from: <http://edition.cnn.com/2003/WORLD/asiapcf/east/05/14/sars.censor/> (accessed 17 September 2016).
- Florêncio D. and Herley C. (2011), 'Sex, Lies and Cybercrime Surveys', In Proceedings (online) of the Workshop on Economics of Information Security, June 2011, available from: <http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf> (accessed 20 November 2016).
- FTC (2016), 'Consumer Sentinel Network Databook for January – December 2015', February 2016, available from: <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2015> (accessed 10 January 2017).
- Galbraith J. K. (1982), Economics of the arms race, Boston Review, available from: <http://bostonreview.net/archives/BR07.4/galbraith.html> (accessed December 2017).
- Gallagher S. (2016), 'How one rent-a-botnet army of cameras, DVRs caused Internet chaos', Ars Technica, available from: <https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/> (accessed 25 January 2017).
- Geer D. (2016), 'State Power and Cyber Power', Chapter 5 in '2018 Security Outlook', Canada Security Intelligence Service, June 2016.
- Gidari A. (2016), 'MLAT reform and the 80 % solution – what's good for users?', The Center for Internet and Society, available from: <https://cyberlaw.stanford.edu/blog/2016/02/mlat-reform-and-80-solution-whats-good-users> (accessed 25 January 2017).
- Glass J., Melin A., Ollis B. and Starke M. (2016), Chattanooga Electric Power Board Case Study—Distribution Automation, ORNL Report Number: ORNL/LTR-2015/444.
- Gordon L. A. and Loeb M. P. (2006), 'Managing cybersecurity resources: a cost-benefit analysis', McGraw-Hill: New York.
- Government Accountability Office (GAO) (2013), 'National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented', GAO-13-187.
- Government Accountability Office (GAO) (2014), 'Medicare fraud: Progress Made, but More Action Needed to Address Medicare Fraud, Waste, and Abuse', GAO-14-560T.
- Grabosky P. (2007), 'Requirements of prosecution services to deal with cybercrime', *Crime, law and social change* 47(4/5): 201–223.
- Greenstein S. and McDevitt R. (2009), 'The Broadband Bonus: Accounting for Broadband Internet's Impact on US GDP', *NBER Working Paper No. 14758*.
- Greenstein S. and McDevitt R. (2012), 'Measuring the Broadband Bonus in Thirty OECD Countries.' OECD Digital Economy Papers no. 197. *OECD Publishing*, Paris.
- Grigsby A. (2014), 'Another country ratifies the Budapest Convention, Council on Foreign Relations', available from: <http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/> (accessed 25 January 2017).
- Hanclova J., Doucek P., Fisher J. and Vltavska K. (2015), 'Does ICT Capital Affect Economic growth in the EU-15 and EU-12 countries?' *Journal of Business Economics and Management* 16(2): 387–406. doi: 10.3846/16111699.2012.754375.

Horizon2020 (2017), 'Non-EU Partners: International Cooperation in Horizon 2020', available from: <http://www.horizon2020.lu/Toolbox/FAQ/Non-EU-Partners> (accessed 25 January 2017).

Hughes B., Bohl D. Irfan M., Margolese-Malin E., Solórzano J. (2015), 'Cyber benefits and risks: Quantitatively understanding and forecasting the balance', Extended Project Report from the Frederick S. Pardee Center for International Futures, Josef Korbel School of International Studies, University of Denver.

IANA Stewardship Transition Coordination Group (IANA SCG) (2016), 'ICG applauds transfer of IANA stewardship', available from: <https://www.ianacg.org/icg-applauds-transfer-of-iana-stewardship/> (accessed 21 January 2017).

IATA (2010), 'IATA Economic Briefing: The impact of Eyjafjallajökull's volcanic ash plume', available from: <http://www.iata.org/whatwedo/Documents/economics/Volcanic-Ash-Plume-May2010.pdf> (accessed 18 November 2016).

Ibraimova A. and LaFrance A. (2017), 'EU Parliament Adopts Resolution on Adequacy Afforded by EU-US Privacy Shield', The National Law Review, available from: <https://www.natlawreview.com/article/eu-parliament-adopts-resolution-adequacy-afforded-eu-us-privacy-shield> (accessed 7 July 2017).

IC3 (2015), '2015 Internet Crime Report', available from: https://pdf.ic3.gov/2015_IC3Report.pdf (accessed 7 July 2017).

IC3 (2016), '2016 Internet Crime Report', available from: https://pdf.ic3.gov/2016_IC3Report.pdf (accessed 7 July 2017).

ICANN (2014), 'IANA functions: the basics', available from: <https://www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf> (accessed 21 January 2017).

ICF Consulting (2003), 'The Economic Cost of the Blackout: An issue paper on the Northeastern Blackout', August 14, 2003, available from: <http://www.solarstorms.org/ICFBlackout2003.pdf> (accessed 18 November 2016).

Isidore C. (2016), 'Delta: 5-hour computer outage cost us \$150 million', CNN Money, available from: <http://money.cnn.com/2016/09/07/technology/delta-computer-outage-cost/index.html> (accessed 25 January 2017).

Jardine E. (2015), Global cyberspace is safer than you think: trends in cybercrime, Global Commission on Internet Governance paper no. 16, available from: https://www.cigionline.org/sites/default/files/no16_web_3.pdf (accessed 17 September 2016).

Jonkeren O. E., Ward D., Dorneanu B. and Giannopoulos G. (2012), 'Economic impact assessment of Critical Infrastructure failure in the EU: A combined Systems Engineering – Inoperability Input-Output Model', 20th International Input-Output Conference, available from: https://www.iioa.org/conferences/20th/papers/files/903_20120516091_JonkerenIIOA2012SE-IIMmodel.pdf (accessed 18 November 2016).

Jorgenson, D.T. (2001), 'Information technology and the US economy', *American Economic Review*, 91(1), pp. 1-32.

Jorgenson D.W. (2005), 'Accounting for growth in the information age'. In: Aghion, P., Durlauf S.N. (Eds.), *Handbook of Economic Growth*, vol. 1A. Elsevier B.V, Amsterdam, pp. 743–815.

Jourova V. (2015), 'Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (LIBE)', 26 October 2015.

Kanich C., Weaver N., McCoy D., Halvorson T., Krebich C., Levchenko K., Paxson V., Voilker G. M. and Savage S. (201), 'Show me the money: Characterizing spam-advertised revenue', available from: <http://cseweb.ucsd.edu/~savage/papers/UsenixSec11-SMTM.pdf> (accessed 16 September 2016).

Kannan, K., J. Rees, and S. Sridhar (2007): 'Market reactions to information security breach announcements: An empirical analysis,' *International Journal of Electronic Commerce*, 12, 69–91.

Karlin J., Forrest S. & Rexford J. (2009), 'Nation-state routing: censorship, wiretapping and BGP', available from: <http://arxiv.org/pdf/0903.3218v1.pdf> (accessed 17 September 2016).

Katz R. (2012), 'The impact of broadband on the economy: Research to date and policy issues', Broadband series, ITU, April 2012, available from: http://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf (accessed 19 January 2017).

Kelly S. (2015), 'Estimating economic loss from cascading infrastructure failure: a perspective on modelling interdependency', *Infrastructure Complexity*, 2:7, DOI 10.1186/s40551-015-0010-y.

Koppel T. (2013), 'Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath', Crown: New York.

Kruithof K., Aldridge J., Decary-Hetu D., Sim M., Dujso E. and Hoorens S. (2016), 'Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands', RAND Europe.

Lacroix F. W., Button R. W., Wise J. R., Johnson S. E. (2001), 'A Concept of Operations for a New Deep-Diving Submarine', RAND Corporation.

Lewis J. (2006), 'Cybersecurity and critical infrastructure protection', Center for Strategic and International Studies, available from: [http://cip.management.dal.ca/publications/Cybersecurity %20and %20Critical %20Infrastructure %20Protection.pdf](http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf) (accessed 16 September 2016).

Leyden J. (2016), 'Sweden 'secretly blames' hackers – not solar flares – for taking out air traffic control', The Register, 12 April 2016, available from: http://www.theregister.co.uk/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/ (accessed 25 January 2017).

Lloyds Insurance (2015), 'Business blackout: The insurance implications of a cyber attack on the US power grid', available from: [http://www.lloyds.com/~media/files/news %20and %20insight/risk %20insight/2015/business %20blackout/business %20blackout20150708.pdf](http://www.lloyds.com/~media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf) (accessed 18 November 2016).

Maass P. and Rajagopalan M. (2012), 'Does cybercrime really cost \$1 trillion?', ProPublica, available from: <https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion> (accessed 19 November 2016).

Manjoo F. (2015), 'Right to Be Forgotten' Online Could Spread', New York Times, <http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html> (accessed 19 November 2016).

Manyika J., Chui M., Bughin J., Dobbs R., Bisson P., and Marrs A. (2013), 'Disruptive technologies: Advances that will transform life, business, and the global economy', available from: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies> (accessed 19 January 2017).

Martin N. (2015), 'Google, the Wassenaar Arrangement, and vulnerability research', Google Security Blog, available from: <https://security.googleblog.com/2015/07/google-wassenaar-arrangement-and.html> (accessed 22 January 2017).

McAfee and Center for Strategic and International Studies (2014), 'Net losses: estimating the global cost of cybercrime', available from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf (accessed December 2017).

McKinsey Global Institute (2016), 'Digital Europe: Pushing the frontier, capturing the benefits', report in collaboration with Digital McKinsey.

McLean R. and Mullen J. (2017), 'Computer outage grounds Delta flights in US', CNN Money, available from: <http://money.cnn.com/2017/01/29/news/delta-system-outage/index.html> (accessed 29 January 2017).

Meltzer J. P. (2014), 'The importance of the internet and trans-Atlantic data flows for US and EU trade and investment', Brookings Institute, Working Paper 79, October 2014.

Micro Market Monitor (n.d.), 'Europe Cyber Security Market Research Report', available from: <http://www.micromarketmonitor.com/market/europe-cybersecurity-4129808188.html> (accessed 19 November 2016).

Miller B. and Rowe D. C. (2012), 'A Survey of SCADA and Critical Infrastructure Incidents', ACM Special Interest Group on Information Technology Education (SIGITE), available from: <http://sigite2012.sigite.org/wp-content/uploads/2012/08/session17-paper01.pdf> (accessed 18 November 2016).

Mozur P. (2016), 'China's Internet Controls Will Get Stricter, to Dismay of Foreign Business', available from: <http://www.nytimes.com/2016/11/08/business/international/china-cybersecurity-regulations.html> (accessed 19 November 2016).

Nakashima E. (2014), 'US cyberwarfare force to grow significantly, defense secretary says', Washington Post, available from: https://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html (accessed 19 January 2017).

National Institute of Standards and Technology (NIST) (2016), 'Draft NIST special publication 800-63B: Digital authentication guideline', available from: <https://pages.nist.gov/800-63-3/sp800-63b.html> (accessed 17 September 2016).

National Telecommunications and Information Administration (NTIA) (2017), 'Fostering the advancement of the internet of things', report by the Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, available from: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf (accessed 20 February 2017).

Nicholson, J. and Noonan R. (2014), 'Digital Economy and Cross-Border Trade: The value of digitally- deliverable services', *ESA Issue Brief* #01-14, US Department of Commerce: Economics and Statistics Administration.

Nojeim G. (2015), 'A strawman proposal for MLAT reform', Center for Democracy and Technology, available from: <https://cdt.org/insight/mlat-reform-a-straw-man-proposal/> (accessed 25 January 2017).

North Atlantic Treaty Organization (NATO) (2014), 'Largest ever NATO cyber defence exercise gets underway', available from: http://www.nato.int/cps/en/natohq/news_114902.htm (accessed 17 September 2016).

OECD (2004), 'ICT, e-business and SMEs', OECD Publishing: Paris.

OECD (2007), 'Development of policies for protection of critical information infrastructures', Ministerial background report: DSTI/ICCP/REG(2007)20/FINAL.

OECD (2003), 'A Proposed Classification of ICT Goods, OECD Working Party on Indicators for the Information Society', OECD: Paris.

OECD (2011), 'The economic impact of shutting down Internet and mobile phone services in Egypt', available from: <https://www.oecd.org/internet/broadband/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm> (accessed 21 November 2016).

OECD (2014a), 'Small businesses, job creation and growth: Facts, obstacles and best practices', Centre for Entrepreneurship, SMEs and Local Development, available from: <http://www.oecd.org/cfe/smes/2090740.pdf> (accessed 17 September 2016).

OECD (2014b), 'Reviews of SME and Entrepreneurship policies: Thailand', OECD Publishing: Paris.

OECD (2015a), 'Economic and Social Benefits of Internet Openness', Background for Ministerial Panel 1.1, DSTI/ICCP(2015)17/FINAL.

OECD (2015b), 'Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document', Directorate for Science, Technology and Innovation, OECD Publishing: Paris.

OECD (2015c), 'OECD Digital Economy Outlook 2015, Trust in the digital economy: Security and privacy', OECD Publishing: Paris.

OECD (2016a), 'New Markets and New Jobs', background report for the OECD Ministerial Meeting on the Digital Economy, 21-23 June 2016, Cancún, Mexico.

OECD (2017a), 'Key issues for digital transformation in the G20, Chapter 8: Digitalisation, SMEs, start-ups and dynamism', available from: <https://www.oecd.org/G20/key-issues-for-digital-transformation-in-the-G20.pdf> (accessed 17 January 2017).

OECD (2017b), 'Tax crimes: The fight goes digital', available from: <http://oecdinsights.org/2017/04/04/tax-crimes-the-fight-goes-digital/> (access 7 July 2017).

Oliner S. and Sichel D. (2000), 'The resurgence in growth in the late 1990s: Is information technology the story?', *Journal of Economic Perspectives*, 14(4), pp. 3-22.

Osborne G. (2015), 'Chancellor's speech to GCHQ on cybersecurity', speech delivered 17 November 2015, available from: <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cybersecurity> (accessed 28 February 2017).

Peterson A. (2016), 'Are squirrels a bigger threat to the power grid than hackers?', Washington Post, available from: <https://www.washingtonpost.com/news/the-switch/wp/2016/01/12/are-squirrels-a-bigger-threat-to-the-power-grid-than-hackers/> (accessed 17 September 2016).

Reeve T. (2016), 'France unveils cyber command in response to 'new era in warfare'', SC Media, available from: <https://www.scmagazine.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579677/> (accessed 19 January 2017).

Remler D. & Van Ryzin G. G. (2015), 'Research methods in practice: strategies for description and causation', 2nd edition, SAGE: Los Angeles.

Romanosky S. (2016), 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, Research paper, 1-15, DOI: 10.1093/cybsec/tyw001.

Rusbridger A. (2016), 'Panama: The hidden trillions', New York Review of Books, available from: <http://www.nybooks.com/articles/2016/10/27/panama-the-hidden-trillions/> (accessed 7 July 2017).

Sanson-Fisher R. W., Bonevski B., Green L. W. & D-Este C. (2007), 'Limitations of the randomized controlled trial in evaluating population-based health interventions', *American Journal of Preventative Medicine*, 33(2), pp155-162.

Shadish W. R., Cook T. D., and Campbell D. T. (2002), 'Experimental and quasi-experimental designs for generalized causal inference', Boston: Houghton Mifflin.

Smith B. (2014), 'Time for an International Convention on Government Access to Data', The Huffington Post, available from: http://www.huffingtonpost.com/brad-smith/time-for-an-international-convention-on-government-access-to-data_b_4644130.html Accessed 25 January 2017).

Sparrow M. (2011), 'Stop the Bleeding: An Interview With Medicare Fraud Expert Malcolm Sparrow', The Nation, available from: <https://www.thenation.com/article/stop-bleeding-interview-medicare-fraud-expert-malcolm-sparrow/> (accessed 28 February 2017).

State Department (2015), 'US – EU Cyber Dialogue: Media note', available from: <https://www.state.gov/r/pa/prs/ps/2015/12/250366.htm> (accessed 15 September 2016).

State Department (2015), 'International Security', available from: <https://2009-2017.state.gov/documents/organization/255014.pdf> (accessed 25 January 2017).

State Department (2016), 'Joint press statement for the 2016 US – European Union Information Society Dialogue', available from: <https://2009-2017.state.gov/r/pa/prs/ps/2016/06/259185.htm> (accessed December 2017).

Stiroh K. (2002), 'Information Technology and the US Productivity Revival: What do the Industry Data Say?', *American Economic Review*, 92(5), pp. 1559-1576.

Symantec Corporation (2013), '2013 Norton report', available from: <https://www.symantec.com/about/newsroom/press-kits/norton-report-2013> (accessed December 2017).

Taleb N. N. (2007), *The Black Swan: The impact of the highly improbable*, Random House: New York.

Taleb N. N. (2012), *Antifragile: things that gain from disorder*, Random House: London.

Taleb N. N. (2016), 'Where You Cannot Generalize from Knowledge of Parts (continuation of the Minority Rule)', Medium, available from: <https://medium.com/@nntaleb/where-you-cannot-generalize-from-knowledge-of-parts-continuation-to-the-minority-rule-ce96ca3c5739#6lqc15umj> (accessed 18 November 2016).

TeleGeography (2013), 'International Bandwidth Demand is Decentralizing', available from: <https://www.telegeography.com/products/commsupdate/articles/2013/04/17/international-bandwidth-demand-is-decentralising/> (accessed December 2017).

Thierer A. and O'Sullivan A. (2015), 'Projecting the Growth and Economic Impact of the Internet of Things', Technology Policy Briefing, available from: <https://www.mercatus.org/publication/projecting-growth-and-economic-impact-internet-things> (accessed 17 January 2017).

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).

Twomey P. (2015), 'Discussion on 'The Future of Multi-stakeholder Internet Governance'', *Proceedings of the Conference on Internet Governance and Cybersecurity 2015*, School of International and Public Affairs, Columbia University.

UK Cabinet Office (2014), 'The UK Cyber Security Strategy: Report on progress and forward plans', available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De_.pdf (accessed 15 September 2016).

United Nations (UN) (2010), 'Resolution 64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures', available from: <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf> (accessed 27 February 2017).

United Nations (UN) (2013), 'PMUNC 2013: UN Office on Drugs and Crime', available from: <http://irc.princeton.edu/pmunc/docs/UNODC%20BG%20formatted.pdf> (accessed 15 September 2016).

United Nations General Assembly (2016), 'Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society', available from: <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf> (accessed 22 January 2017).

UNODC (2015), 'Non-paper submitted by Brazil reflecting its views on the issue of cybercrime', Commission on Crime Prevention and Criminal Justice, available from:

https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf (accessed 21 January 2017).

US-Canada Power System Outage Task Force (2004), 'Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations', available from: <https://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf> (accessed 18 November 2016).

US-CERT (2016), 'Ransomware: what it is and what to do about it', available from: https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf (accessed 17 September 2016).

US District Court for the Northern District of New York (2015), Application for a search warrant for Case 5:15-mj-00154-ATB, available from: <https://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf> (accessed 28 February 2018).

US House of Representatives (2012), 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', available from: [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf) (accessed 21 January 2017).

Varian H., n.d., 'The value of Google', available from: <http://cdn.oreillystatic.com/en/assets/1/event/57/The%20Economic%20Impact%20of%20Google%20Presentation.pdf> (accessed 19 January 2017).

Verizon (2016), '2016 Data Breach Investigations Report', available from: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/> (accessed 17 September 2016).

Weissman C. G. (2015), 'Hacked company's documents show a laundry list of questionable clients', Business Insider, available from: <http://www.businessinsider.com/hacked-security-companys-document-2015-7> (accessed 22 January 2017).

White House (2014), 'Fact sheet: US – EU cyber cooperation', available from: <https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation> (accessed 17 September 2016).

White House (2016a), 'Federal Cybersecurity Workforce Strategy', available from: <https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce> (accessed 19 January 2017).

White House (2016b), 'The President's Budget for Fiscal Year 2017', available from: <https://www.whitehouse.gov/omb/budget/> (accessed 12 February, 2016).

White House (2016c), 'Fact Sheet: The Cybersecurity National Action Plan', Office of the Press Secretary, available from: <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> (accessed 5 August 2016).

White House (2016d), 'Executive Order: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', 29 December 2016, available from: <http://web.archive.org/web/20161230154856/https://www.whitehouse.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency> (accessed 24 January 2017).

White House (2017), 'Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', 17 May 2017, available from: <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal> (accessed 7 July 2017).

World Economic Forum (2010), 'Global risk report 2010—a global risk network report', available from: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2010.pdf (accessed 21 January 2017).

Xiaoxiao L., Min Q., Yuzhe Z., Hao N., Yunxu Q. and Peishan Z. (2014), 'China pulling the plug on IBM, Oracle, others', Caixin Online, available from: <https://secure.marketwatch.com/story/china-pulling-the-plug-on-ibm-oracle-others-2014-06-26> (accessed 21 January 2017).

Yang S., Zhai K. and Culpan T. (2014), 'China said to plan sweeping shift from foreign technology to own', Bloomberg News, available from: <https://www.bloomberg.com/news/articles/2014-12-17/china-said-to-plan-sweeping-shift-from-foreign-technology-to-own> (accessed 21 January 2017).

Yar M. (2005), 'The novelty of 'cybercrime': an assessment in light of routine activity theory', *European journal of criminology* 2(4): 407–427.

Zatko P. (aka: 'Mudge') (2013), 'Keynote presentation, CanSecWest Security Conference 2013', available from: <https://www.cansecwest.com/csw13archive.html> (accessed 17 September 2016).

Zetter K. (2016), 'Inside the cunning, unprecedented hack of Ukraine's power grid', 3 March 2016, Wired, available from: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> (accessed 18 November 2016).

Zucman G. (2013), 'The missing wealth of nations: Are Europe and the US net debtors or net creditors?', *The Quarterly Journal of Economics*, 1321–1364. doi:10.1093/qje/qjt012.

Zurich Insurance (2015), 'Risk nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures', report in conjunction with the Atlantic Council and the Pardee Center for International Futures at the University of Denver.

9. Appendix 1: Direct costs of cybercrimes

The table below provides a categorisation of the direct costs of cybercrimes which more closely mirrors the EU definition.

Crimes specific to the Internet	United States		European Union	
	Total \$US	Per capita	Total \$US	Per capita
Copyright-infringing software	23 042 782	0.07	1 728 209	0.003
Subscription revenue from cyberlockers	21 120 000	0.07	21 120 000	0.04
Ad revenue from cyberlockers	54 408 000	0.17	49 874 000	0.10
Patent-infringing pharmaceuticals	71 926 572	0.23	5 394 493	0.01
Darknet markets (revenues to sellers)	61 189 836	0.19	59 435 424	0.12
Darknet markets (products to buyers)	51 515 700	0.16	9 268 668	0.02

Online fraud and forgery	United States		European Union	
	Total \$US	Per capita	Total US\$	Per capita
Online payment card fraud	1 561 520 000	4.97	1 256 850 000	2.47
Offline payment card fraud	2 277 700 000	7.25	648 270 000	1.28
Welfare fraud	4 079 807 841	12.89	-	-
VAT fraud/gap	-	-	186 480 000 000	365.88
Tax evasion (tax gap)	337 300 000 000	1 082.06	841 600 000 000	1 664.80
Tax filing fraud	3 100 000 000	9.72		

10. Appendix 2: Sources for direct cybercrime cost figures

Genuine cybercrime	United States		European Union	
	Year	Source	Year	Source
Copyright-infringing software	2010	Kanich C. et al, Show me the money: Characterizing spam-advertised revenue	2010	Kanich C. et al, Show me the money: Characterizing spam-advertised revenue
Subscription revenue from cyberlockers	2014	Digital Citizens Alliance, Behind the cyberlocker door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions	2014	Digital Citizens Alliance, Behind the cyberlocker door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions
Ad revenue from cyberlockers	2013	Digital Citizens Alliance, Good money gone bad: Digital Thieves and the Hijacking of the Online Ad Business A Report on the Profitability of Ad-Supported Content Theft	2013	Digital Citizens Alliance, Good money gone bad: Digital Thieves and the Hijacking of the Online Ad Business A Report on the Profitability of Ad-Supported Content Theft
Patent-infringing pharmaceuticals	2010	Kanich C. et al, Show me the money: Characterizing spam-advertised revenue	2010	Kanich C. et al, Show me the money: Characterizing spam-advertised revenue

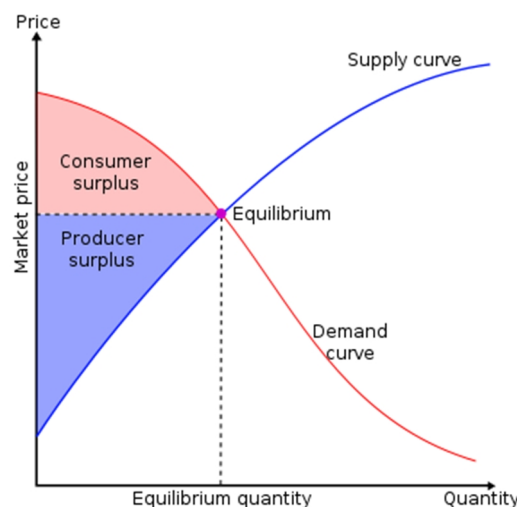
Transitional cybercrime	United States		European Union	
	Year	Source	Year	Source
Online payment card fraud	2012	2013 Federal Reserve Payments Study	2013	ECB, 4th Card Fraud Report. Converted from € to USD using average 2013 exchange rate of 1.1 euros to the dollar.
Offline payment card fraud	2012	2013 Federal Reserve Payments Study	2013	ECB, 4th Card Fraud Report. Converted from € to USD using average 2013 exchange rate of 1.32 euros to the dollar.
Darknet markets (revenues to sellers)	2016	Kruithof et al, Internet-facilitated drugs trade	2016	Kruithof et al, Internet-facilitated drugs trade
Darknet markets (products to buyers)	2016	Kruithof et al, Internet-facilitated drugs trade	2016	Kruithof et al, Internet-facilitated drugs trade

Traditional crime	United States		European Union	
	Year	Source	Year	Source
Welfare fraud	2013	United States Department of Labor		n/a
Tax evasion (tax gap)	2011	Tax Justice Network	2011	Tax Justice Network
Tax filing fraud	2014	Government Accountability Office	N/A	n/a
VAT fraud/gap	N/A	n/a	2015	Eurostat, Study to quantify and analyse the VAT Gap in the EU Member States. Converted from € to USD using average 2015 exchange rate of 1.11 euros to the dollar.

11. Appendix 3: Consumer surplus

New products or services create an economic surplus (sometimes termed as total welfare). The economic surplus is a combination of two portions: that which goes to the consumer (the consumer surplus) and that which goes to the producer of the good or service (the producer surplus). The consumer surplus is the difference between the maximum that a person would be willing to pay for a good or service and the actual price of that good or service (see figure below). The underlying intuition is that a consumer is getting more benefits (i.e. greater utility) from a good or service than that which they have paid for. Measures of gross domestic product do not include the economic surplus. The economic surplus can thus be estimated in dollar terms as an additional contribution to GDP.

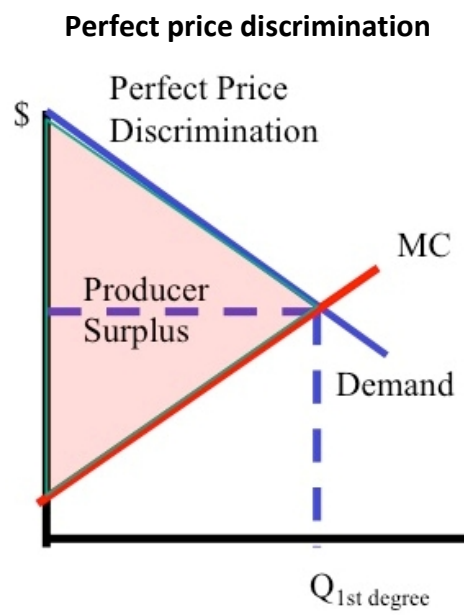
Economic surplus: the consumer and producer surplus



Source: User:SilverStar - Own work, CC BY 2.5, <https://commons.wikimedia.org/w/index.php?curid=1450405>

ICTs have contributed to the reconfiguration of the consumer and producer surplus across many products and services. There are many examples of products or services for which consumers presently pay no dollar price to use whereas in the past these products or services required payment for access (e.g. Wikipedia in place of an encyclopaedia set, international conference call services). In many of these cases, there has been little net value creation as the new product or service has appropriated market from prior market participants without creating additional value (e.g. Google's online advertising appropriating advertising revenues from television and print media) though there may have been consumer surplus gains.

Consumer surplus gains do not remain constant over time. Previously heavily used in the airline business, many companies are now developing the capability for individual (or perfect) price discrimination. This involves the collection of data that suggests how much individuals would be willing to pay given certain conditions. Such 'dynamic' pricing is increasingly found in online stores (e.g. Amazon and Apple pricing based on location of user) and in transport (e.g. Uber surge-pricing). Should this trend continue, with pricing increasingly set closer to or along the demand curve, the consumer surplus will be gradually appropriated by the producer (i.e. producers will receive the entire economic surplus from production).



Source: BYU Idaho (2012).

12. Appendix 4: Comparing sector-specific regulatory focus of EU NIS Directive with US critical infrastructures

EU NIS Directive sector-specific focuses	US critical infrastructures (from PPD-21)
	Chemical sector
	Commercial facilities sector
Digital infrastructures (IXPs, DNS, TLD)	Communications sector
	Critical manufacturing sector
	Dams sector
	Defense industrial base sector
	Emergency services sector
Energy (electricity, oil, gas)	Energy sector
Banking, Financial market infrastructures	Financial services sector
	Food and agriculture sector
	Government facilities sector
Healthcare	Healthcare and public health sector
Digital infrastructures (IXPs, DNS, TLD)	Information technology sector
	Nuclear reactors, materials and waste sector
Transport (air, rail, road, water)	Transportation systems sector
Drinking water supply and distribution	Water and wastewater systems sector

13. Appendix 5: Comparing the EU NIS Directive with equivalent US policy

NIS Directive articles	US equivalent policy (where relevant)
CHAPTER I: GENERAL PROVISIONS	
Article 5: Identification of operators of essential services	EO 13636 Sec 9: Identification of critical infrastructure at greatest risk
Article 6: Significant disruptive effect	PPD-41 Section I a, definition of a cyber incident (not limited to critical infrastructure)
CHAPTER II: NATIONAL FRAMEWORKS ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS	
Article 7: National strategy on the security of network and information systems	n/a The US does not have a national cybersecurity strategy. PPD-21 provides guidance on how federal agencies should cooperate and interact with regard to critical infrastructure protection.
Article 8: National competent authorities and single point of contact	PPD-21 names the Secretary of Homeland Security as main contact at a federal level. Sector-specific agencies also mentioned. Department of Homeland Security houses US-CERT, which is a branch of the Office of Cybersecurity and Communications' (CS&C) National Cybersecurity and Communications Integration Center (NCCIC).
Article 9: Computer security incident response teams (CSIRTs)	2000: Congress created the Federal Computer Incident Response Center (FedCIRC) at the General Services Administration 2000: creation of the Department of Homeland Security. 2003: FedCIRC was renamed 'US-CERT,' and its mission was expanded to include providing boundary protection for the federal civilian executive domain and cybersecurity leadership. US-CERT operates side-by-side with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Not all US states have a CERT.
Article 10: Cooperation at national level	EO 13636 Sec 3 explains that inter-agency cooperation is set down in Presidential Policy Directive-1 of 13 February 2009 (Organization of the National Security Council System).
CHAPTER III: COOPERATION	
Article 11: Cooperation Group	EO 13636 Sec 3 explains that inter-agency cooperation is set down in Presidential Policy Directive-1 of 13 February 2009 (Organization of the National Security Council System).
Article 12: CSIRTs network	Not all US states have CERTs.
Article 13: International cooperation	PPD - 21 has provisions for international cooperation around critical infrastructure protection.
CHAPTER IV: SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES	
Article 14: Security requirements and incident notification	EO 13636 Sec 4 has provisions for cybersecurity information sharing and dissemination. Data breach notification requirements differ across sectors and states in the US.
Article 15: Implementation and enforcement	n/a
CHAPTER V: SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS	
Article 16: Security requirements and incident notification	EO 13636 Sec 4 has provisions for cybersecurity information sharing and dissemination. Data breach notification requirements differ across sectors and states in the US.

Article 17: Implementation and enforcement	n/a
Article 18: Jurisdiction and territoriality	n/a
CHAPTER VI: STANDARDISATION AND VOLUNTARY NOTIFICATION	
Article 19: Standardisation	n/a
Article 20: Voluntary notification	n/a
CHAPTER VII: FINAL PROVISIONS	
Article 21: Penalties	n/a

Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has also enabled costly new forms of crime, and created systemic risks to transatlantic and national critical infrastructure, threatening economic growth and development.

The transnational nature of these phenomena make it very difficult for effective policy solutions to be implemented unilaterally by any one jurisdiction. Cooperation between stakeholders in both the EU and US is required in the development and implementation of policies to increase the security of digital technologies and increase societal resilience to the cybersecurity risks associated with critical infrastructure. Although there is a great deal of congruence between the stated policy goals in both the EU and US, obstacles to effective cooperation impede effective transatlantic policy development and implementation in some areas.

This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues that policy-makers on either side of the Atlantic could work together on, and explains where effective cooperation is sometimes impeded.

This is a publication of the
Members' Research Service

EPRS | European Parliamentary Research Service, European Parliament



PE 603.948
ISBN 978-92-846-1087-7
doi:10.2861/023034

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.