Legislative Developments in Cybersecurity in the EU

Faye F. Wang

Brunel University London

Abstract

Cyber-attacks have become a very serious issue in Europe, targeting essential services such as national health systems, banks, electoral campaigns or mobile services. There is certainly no one single solution to the need to improve cybersecurity, but a wide range of collective and far-reaching technical and legal measures may make it as hard as is possible for those who want to attack the security of infrastructures, services and products. This article aims to aid our understanding of cybersecurity, cyber threats, cyber-attacks and cyber defence from both legal and technological perspectives. It discusses the most recent EU cybersecurity legislative movements and considers whether current legal and technical measures, including the newly adopted EU Cybersecurity Act 2019, have provided efficient solutions to respond to radically changed cyber threats and attacks, in particular in critical services in the EU. It offers insights into the scope and limitations of technical measures in achieving the highest possible level of cybersecurity due to the unpredictable nature of certain cyber-attacks.

Keywords: cybersecurity, cyber-attacks, cyber defence, cybercrime, cyber threat, Fintech, artificial intelligence

[A] INTRODUCTION: THE RISE OF CYBERSECURITY CONCERNS

'Cybersecurity' is a term which often refers to the confidentiality, integrity and availability (known as the CIA) of information in cyberspace (ENISA 2016a). Cybersecurity is considered to be a relatively new term (Kosseff 2018: 1010), and the US courts first used the term 'cybersecurity' in a court opinion in 2007 (*Pisciotta v Old National Bancorp* 2007: 638).

Cybersecurity also concerns how individuals and organizations reduce the risk of cyber-attacks, a point emphasized by the National Cyber Security Centre (n.d.) in the UK. Breaching or attacking cybersecurity is conduct that may constitute cybercrime. One of the most common forms of cyber-attack is cyber espionage. Cyber espionage (such as botnets, ransomware, spyware and backdoor) is considered the biggest motivator for cyber-attacks (McAfee 2018). Computer networks are used to gain unauthorized access to confidential information in public or private organizations, so as to enjoy an advantage over competitors, including state-sponsored actors. In order to deliver these cyber-attacks, phishing (tricking someone to click on a malicious link or download a malicious attachment via email) is often used as the first step (ENISA 2017).

Nowadays, cyber-attackers are able to deliver high-profile and sophisticated attacks to both public and private sectors, including sensitive public services, national infrastructures and businesses for consumers. They have primarily taken the forms of physical damage, psychological damage, financial damage or invisible damage, as pointed out in an earlier essay in *Amicus Curiae* by Chatterjee and Lefcovitch (2016: 2). Their hidden nature can make it difficult to identify the attacker. Many of these attackers use an advance persistent threat and may remain undetected for years. This poses a growing concern over our safety, health and security. In early 2018, it was reported that Europe continues to be a cybercrime hub—cyber-attacks in Europe in 2017 increased by 30% compared with the previous year, whilst 38% of these attacks were initiated from Europe (ThreatMetrix 2018). In 2019, more than half of British firms reported cyber-attacks (*BBC News* 23 April 2019). During the first quarter of 2019, nearly 50% of human-initiated cyber-attacks came from the EMEA (Europe, Middle East and Africa) region, with UK and Germany being the top two targets for cybercrime attackers by volume (LexisNexis Risk Solutions and ThreatMetrix 2019).

In the public sector, it is often the case that hackers try to break into telecommunication networks to steal sensitive or valuable data to sell on or use to blackmail the legitimate owner. For example, in the UK case of *R v Connor Douglas Allsopp*, there was a hacking attack to TalkTalk telecommunication network. Computer files of TalkTalk's customers were unlawfully accessed and the Chief Executive Officer of TalkTalk at the time was blackmailed to pay bitcoins to the hacker for the stolen data (*R v Connor Douglas Allsopp* 2019: 9).

Concern about cyber-attacks in the public sector continues to grow. It is estimated that 90% of critical national infrastructures in the US, UK,

Germany, Australia, Mexico and Japan have experienced at least one successful attack over the past two years (Ponemon Institute, 2019). In January 2019, German politicians were targeted in a mass data attack after which their personal data was unlawfully published online (*BBC News* 4 January 2019).

It has been suggested that the four most important ways to protect infrastructures are: to be prepared for attacks; to be aware of attacks being non-stop; to be guarded (i.e. against employees clicking on phishing emails); and to be willing to share intelligence with similar organizations (Simmons 2019). From a technical perspective, it is argued that the two most effective ways to reduce the chance of circumventions to security are: firstly, to change the names, locations and references of files and software applications in a computer's memory so that the system is not configured the same way each time the computer is turned on; and, secondly, to isolate computers from local networks and the internet—known as 'air gapping'—(Russon 2019). However, none of these measures can completely guarantee cybersecurity because it is possible for hackers to hack an air-gapped computer while the supply chain is being built or via attached storage during software and firmware updates. For example, a hacker could hack a nuclear power station in this way resulting in power cuts or a nuclear gas leak without the need for a physical presence of an attacker entering into a highly secure nuclear power station building.

In the private sector, hacking into email accounts is very common, in that data from email accounts may be extracted by obtaining users' credentials or by sniffing network traffic. Email is historically not considered as secure because many email providers do not encrypt messages while they are in transit. For example, in the UK case of *J Brazil Road Contractors v Belectric Solar Ltd*, a contractor's British Telecom email account was hacked, which caused his customer to send payment to the bank account of the hacker (*J Brazil Road Contractors v Belectric Solar Ltd* 2018: 294). In recent years, there is a growing trend for email providers to encrypt messages in transit, making it harder for others to hack into email accounts and extract data from them. For example, since 2014 Google has been applying a security protocol called transport-layer security (TLS) to make email messages more secure in transit (Google n.d.; Walder 2016).

More recently, there is increased alarm over cybersecurity concerns from the rise of the employment of artificial intelligence in products. For example, it may be possible to hijack an expensive car via the smartphone apps linked to smart car alarms (*BBC News* 8 March 2019). Breaches of

smart car systems could also lead to car crashes. This is a rather difficult issue to resolve. It is understood by professionals that there is no software system that is 100% safe and secure, though software engineers have been working to review and improve their codes and engineering practices, in order to enhance the safety and security of their products at all times. However, it is argued that, if the costs of circumventing a security system are higher than the profit hackers can make, it may just make them choose other, easier targets (Russon 2019).

With the advent of driverless cars, a breach of cybersecurity may result in even more serious and complicated consequences. For example, the computer system of a driverless, autonomous or self-driving car may communicate various attributes to a central server to improve autonomous system performance for all other cars made by the same manufacturer. If a hacker breaks into and damages the central service, there may be safety implications for the entire fleet. For example, when the hacker hacks the radar sensor of cars from the central server, this may cause the radar sensor to misrecognize certain types of hazard, so that there is no signal issued for the necessary braking, or a signal is issued for false braking. For example, the signal from a radar sensor is reflected by a metal object much more strongly than a wood or plastic object, thus, an overhead metal road sign may at first appear a major hazard to this sensor, but, when compared against the sensor data and subsequent car behaviour from other cars in the fleet at that location, the autonomous system can understand the road sign is not a hazard and therefore braking is not required (Tesla 2016).

In addition, hacking of a central server of self-driving cars may also pose a potential threat to privacy. The centrally stored vehicle-generated data can include vehicle location and speed. The hackers may use the stolen data to spy on car owners in order to break into their houses or conduct other intended harm. It was reported that Tesla is recording short video clips from the car's external cameras for lane lines, street signs or other necessary surrounding information to perform self-driving functions (Muller 2019). However, the unauthorized access to such data may enable the offender or hacker to use the data to publish identifiable individuals' personal information.

In response to cybersecurity challenges at the national level, countries and regions have been establishing public–private partnerships to tackle issues of cybersecurity. This partnerships initiative originates from the USA. For over 25 years, the USA has considered the development of public–private partnerships as key to tackling cybercrime. In 1997, a

Commission for Critical Infrastructure Protection was established by President Clinton to assess threats to infrastructure. However, there are opposing views as to the benefit of public–private partnerships (Chatterjee and Lefcovitch 2016: 4). In practice, a degree of mistrust towards public sectors may result from concerns over increased regulatory measures.

At the international level, global efforts have been made to address cybersecurity, which is now a global issue. For example, in 1983, the Organisation for Economic Co-operation and Development (OECD) initiated a study on the possibility of an international application and harmonization of criminal law for computer-related crime and abuse, which subsequently published 'Computer-Related Crime: Analysis of Legal Policy' in 1986. In 1992, the OECD finally issued 'Guidelines for the Security of Information Systems' to encourage cooperation between public and private sectors. In 2012, the OECD published a report on 'Cybersecurity Policy Making at a Turning Point', discussing a new generation of cybersecurity strategies in several countries (OECD 2012). Following OECD initiatives, in recent years, the International Organization for Standardization (ISO) has also been working with nations and companies such as Tesla to develop the new international standards for consumer protection via 'privacy by design' for consumer goods and services (ISO/PC 317).

With regard to transnational cooperation and coordination among governments, the establishment of cooperation between the EU and US in 2000 to create a safer information society (COM (2000) 890 final), which was subsequently enhanced after the EU–US summit in 2010, was considered to be the first major transatlantic cooperation in security (Fahey 2014: 55). In order to enhance the coordination, it was suggested that the Court of Justice of European Union should look to how the European ombudsmen deal with EU privacy complaints, while the US authorities should prompt more searching inquiry into the ombudsmen's practice (Margulies 2017: 495).

Moreover, specialized international organizations, such as the International Telecommunication Union (ITU), an agency of the United Nations (UN), have also issued recommendations for governments to take preventative action against Cybercrime. It is noted that the nature of threats has changed significantly since the inception of the ITU in 1865 (Chatterjee and Lefcovitch 2016: 6). Nonetheless, the approach of international cooperation should be enhanced, as the level of international cooperation often affects the level of the success of preventing cybercrime, given the global nature of cyber-related criminal activities. In 2007, to improve

international cooperation, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA). The legal framework of the GCA recommends harmonization of cybercrime legislation, in conjunction with the ITU.

This article aims to aid the understanding of cybersecurity, cyber threats, cyber-attacks and cyber defence from both legal and technological perspectives. It discusses the most recent EU cybersecurity legislative movements (2013-2019) and considers whether current legal and technical measures, including the newly adopted EU Cybersecurity Act (March 2019), have provided efficient solutions to respond to radically changed cyber threats and attacks, in particular in critical services in the EU. Additionally, it offers insights into the scope and limitations of technical measures in achieving the highest possible level of cybersecurity due to the unpredictable nature of certain cyber-attacks.

[B] EU CYBERSECURITY LEGISLATIVE MOVEMENTS

General EU Cybersecurity Strategies

As described above, cyber-attacks have become a very serious issue in Europe, targeting essential services such as national health systems, banks, electoral campaigns or mobile services. In recent years, the EU has issued strategy, communications, action plans and legislative proposals to assess new challenges and review the ENISA Regulation (Regulation (ECU) No 526/2013).

For example, in 2013 the EU set out a cybersecurity strategy (Joint Communication 2013) providing five strategic priorities:

1. achieving cyber resilience;
2. drastically reducing cybercrime;
3. developing cyber defence policy and capabilities;
4. developing the industrial and technological resources for cybersecurity; and
5. establishing a coherent international cyberspace policy (JOIN (2013) 1 final: 4-5).

In the same year, Europol established the European Cybercrime Centre (EC3) to strengthen the law enforcement response to cybercrime in the EU, focusing on three types of cybercrime:

1. cyber-dependent crime;
2. online child sexual exploitation; and
3. payment fraud (European Cybercrime Centre n.d.).

In 2017, the Council of the EU adopted these three areas as Europol's priority crime areas under the 2018-2021 EU Policy Cycle. It recommends fighting cybercrime by:

> (1) disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, by (2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by (3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities (EU Policy Cycle—Empact 2017).

In 2014, the EU cyber defence policy framework was adopted by the Council of the EU. This framework, which was updated in November 2018, calls in particular for restrictive measures for cyber-attack response and deterrence (Council of the EU, Press Release: 19 November 2018). The updated framework set out six priorities, including encouraging further protection through common security and defence policy communication, information systems and networks and promoting civil–military cooperation and international cooperation with significant international organizations, such as the UN and North Atlantic Treaty Organization (Council of the EU, Press Release: 19 November 2018).

In 2016 the European Commission (EC) adopted a Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM (2016) 410 final). In the same year, Directive (EU) 2016/1148 concerning measures for a high common level of security for network and information systems across the EU (known as the EC Directive on Security of Network and Information Systems) was adopted, which continues to strengthen the role of the ENISA. Directive (EU) 2016/1148 established the first mechanisms to enhance strategic and operational cooperation among member states (Position of the European Parliament, 12 March 2019). It also set up requirements for national capabilities and member states' obligations for dealing with cybersecurity measures and incident notifications.

In December 2016, the ENISA published a report on Cyber Hygiene Practices (ENISA Review 2016b). Cyber hygiene is considered a fundamental principle of information security, which is equivalent to the 'personal hygiene' of establishing simple daily routines, good behaviours and occasional check-ups to maintain good online health, increase immunity and minimize the risks from attacks (ENISA Review 2016b: 6, 14).

This review called for a standard approach with minimum baseline requirements for cybersecurity which should be flexible enough to support cross-border and cross-industry recognition across Europe (ENISA 2016b: 5). In this report, the ENISA reviewed the fundamental guidelines for small business information security by the US National Institute of Science and Technology, published in November 2016 (US Department of Commerce 2016). According to the findings in this report, there are no unified European cyber hygiene programmes (ENISA 2016b: 12). The UK appeared to be the strongest nation across Europe in terms of a relevant cyber hygiene programme, however, it was only mandatory to public-sector contracts (ENISA 2016b: 13). This report recommended employing an attainable, accreditable and affordable approach to set up cyber hygiene programmes and identified five main areas to establish their compliance regimes: '1) Protect the perimeter; 2) Protect the network; 3) Protect individual devices; 4) Use the cloud in a secure manner; and 5) Protect the supply chain' (ENISA 2016b: 15). It further provides ten corresponding action points:

> 1) Have a record of all hardware so you know what your estate looks like; 2) Have a record of all software to ensure it is properly patched; 3) Utilise secure configuration/hardening guides for all devices; 4) Manage data in and out of your network; 5) Scan all incoming emails; 6) Minimise administrative accounts; 7) Regularly back up data and test it can be restored; 8) Establish an incident response plan; 9) Enforce similar levels of security across the supply chain; and 10) Ensure suitable security controls in any service agreements (including cloud services). (ENISA 2016b: 15)

Subsequently, in December 2018, the ENISA further published Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, providing various contextual understanding of how human aspects of cybersecurity behaviours within organizations can affect organizational cybersecurity and how to plan and implement changes to improve security for organizations. Based on the findings, the Guidelines promoted cybersecurity adherence (active participation) rather than compliance (in particular threats and punishments) within organizations to raise cybersecurity awareness.

Regulatory Developments for EU Cybersecurity

In Autumn 2017 the EC proposed a regulation on cybersecurity (known as the EU Cybersecurity Act), which builds on previous actions and sets out measures to reinforce objectives. This is the first time that definitions of various key concepts have been provided in the EU cybersecurity legislative framework (COM (2017) 477 final/2), for example:

- ‘cybersecurity’ comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats (Article 2(1));
- ‘cyber threat’ means any potential circumstance or event that may adversely impact network and information systems, their users and affected persons (Article 2(8));
- ‘European cybersecurity certification scheme’ means the comprehensive set of rules, technical requirements, standards and procedures defined at EU level applying to the certification of information and communication technology products and services falling under the scope of that specific scheme (Article 2(9)).

On 27 June 2019, the European Cybersecurity Act came into force. It provides detailed provisions for the establishment of an EU-wide cybersecurity certification scheme and the enhancement of the role of the EU cybersecurity agency—ENISA.

In December 2018, the European Parliament, Council and Commission finally reached a political agreement on the Cybersecurity Act (EC 2018). On 12 March 2019, Members of the European Parliament adopted the European Cybersecurity Act giving it the effect of an EU regulation that applies automatically and uniformly to all EU countries when it enters into force, without the need of being transposed into national law (EC March 2019). This regulation serves two main aims as follows.

First, to reinforce the ENISA’s role as a centre of expertise and advice for cybersecurity matters, facilitating operational cooperation among member states, and strengthening capacity building in both their technical and human capabilities and skills in response to cyber threats (Position of the European Parliament, 12 March 2019).

Second, to implement a common cybersecurity certification approach through the establishment of the EU-wide cybersecurity certification framework. The certification schemes are key to increase trust and security in digital products (Position of the European Parliament, 12 March 2019).

Other Complementary Legislative Initiatives

Despite all the legislative movements to tackle Europe’s cybersecurity problem, it appears that Europe continues to face big challenges. In 2017 there was a series of high-profile cyber-attacks which hit Europe with ransom demands targeting governments and key infrastructures (Roth and Nakashima 2017). Sophisticated cyber-attacks can happen without

any notice before being launched. Where the software vendor has no previous knowledge of the particular vulnerability, the attack is known as a zero-day exploit (Kaspersky n.d.). A documentary called *Zero Days* (Gibney 2016) explained how Stuxnet, a state-sponsored computer malware, targeted an Iranian nuclear facility without any pre-warning signs. This shows that the knowledge to carry out such an attack with no defence is highly valuable to criminals. The nature of high-profile cyber-attacks is often cross-border and unpredictable.

In response to mass cyber-attacks and alongside the legislative developments of the EU Cybersecurity Act, in 2017 the Council of the EU agreed to develop a framework called the 'cyber diplomacy toolbox' for a joint EU diplomatic response (Council of the EU, 29 June 2017). The proposed EU cyber diplomacy toolbox introduced several measures to tackle malicious cyber activities, including crucial initiatives, such as 'shared situational awareness' and 'restrictive measures' (sanctions) (Draft Council Conclusions 2017). Some researchers have raised concerns over such a mechanism, i.e. it is argued that it 'will be dysfunctional from the get-go and might actually produce counter-productive results' because there is inequality in capacity and capability for collective attribution and also for attribution assessment in different member states (Soesanto 2018). Research data also showed that sanctions may not be effective for the deterrence of cyber-attacks because, in 2018 despite cybercrime activities from 59 individuals and 28 companies in Iran, North Korea and Russia being sanctioned by the US Treasury Department's Office of Foreign Assets Control, there was no reduction in these activities (Soesanto 2018). There was also concern over the implementation of sanctions based on inaccurate assessment of attribution, which may violate international law (Moret and Pawlak 2017).

In January 2018, the EC initiated a communication concerning the Digital Education Action Plan (Communication from the Commission 2018). This Action Plan reinstates the importance of education and training systems to improve the competency of using innovation and digital technology. It calls for EU-wide cooperation to develop relevant digital skills and competence. It also calls for improving education systems through better data analysis and foresight.

In July 2018, concerns over the reality of the EU's lack of operational and legal capacity to respond to major cyber-attacks and prosecute the attackers was raised by the Centre for European Reform (Mortera-Martinez 2018). In that report, it urged the EU to work with other nations to agree on international rules (i.e. a transatlantic treaty), in particular to

improve access to cross-border digital evidence to respond to attacks (Mortera-Martinez 2018). It also called for the EU to work with other nations and technological companies to better understand cyber threats and support member states to invest more in cyber security, implement the cyber diplomacy toolbox and thus combat these attacks more effectively (Mortera-Martinez 2018).

In September 2018, the EC also proposed a regulation to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM (2018) 630 final). Apparently, the aim of this Centre is to provide complementary efforts to support the ENISA's capacity-building work, but with a different focus and to stimulate the development and deployment of technology in cybersecurity. At the same time, the ENISA will act as a permanent observer on the Governing Board of the new Centre (COM (2018) 630 final: Article 12(7)). Although their relationship and functions are provided for in the proposed regulation, it still appears that some of their responsibilities may overlap. This requires further clarification, in particular stakeholders, data subjects or any other rights-holders need to be made aware as to which authority they should report any incident of cyber breach or attack. The reporting structure should be made clear and straightforward because rights-holders may not be able to define the nature of the attacks and the specific responsibilities of different authorities in order to know which one they should approach. It may be helpful to have one single point of contact for incident notifications for cyber-attacks or breach emergencies across sectors in the EU.

In addition, during the movements of the general EU cybersecurity legislative developments, specific areas and sectors, such as cybersecurity in the financial sector, which are more susceptible to cyber-attacks have also been emphasized. Corresponding measures have been proposed and reviewed in order to tackle continued cyber threats to the security of the digital financial markets.

[C] SIGNIFICANT THREATS TO CYBERSECURITY IN THE FINANCIAL SECTOR

As noted above, payment fraud has already been recognized as one of the three priorities of cybercrime areas that need to be tackled in the EU policy cycle from 2018 to 2021. With the continuing technology innovation in financial industries, cyber threats to global financial markets are reaching new heights due to the expanding scale of attacks and the growth of advanced methods.

It is known that Fintech has been a driver for current financial innovation. Fintech is understood as promoting 'technology-enabled innovation in financial services', which involves a variety of technological solutions to provide services, e.g. digital identification, mobile applications, cloud computing, big data analytics, artificial intelligence, blockchain and distributed ledger technologies (Fintech 2018).

Fintech has also been advancing global financial services. However, the cybersecurity of Fintech is of great concern, because the largest users of digital technologies are located in the financial sector (Fintech 2018). There is understandably a growing fear of cyber risks in the financial sector. According to the World Bank, there was a 29% increase in cyber-attacks in the financial sector from 2015 to 2016, whilst there were 65% more cyber-attacks in 2016 on customers of financial services than customers from other industries (World Bank 2018). In 2017 the EU report on the assessment of the risks indicated that the level of threat to a variety of attacks concerning virtual currencies, money laundering and terrorist financing was most often considered as very significant—namely level 4, the highest (COM (2017) 340 final). It is noted that the 'terrorists financing threat related to cash couriers/unaccompanied cash movements shows that terrorist groups have made use of various techniques to move physical cash across the external borders, particularly in the case of larger organisations' (COM (2017) 340 final). In December 2018, it was reported that cybercrime continues to increase in global financial sectors—one of the most common methods of cyber-attack is to steal funds from victims by using phishing emails that appear to come from legitimate financial organizations (McAfee 2018).

Fintech has digitally transformed the economy and society globally and increased the efficiency of financial services. This has changed the business models of established financial institutions and other companies offering financial services and has had an impact on trust from consumers and businesses using new financial services, in particular with the fear of cybersecurity compromise in financial institutions.

On 8 March 2018 the EC launched the 'Fintech Action Plan: For a More Competitive and Innovative European Financial Sector' (the Fintech Action Plan) (COM (2018) 109 final). This action plan interacts with the EU's cybersecurity strategy (JOIN (2017) 450 final) and initiates specific cybersecurity actions for digital financial services to fill gaps in general EU cybersecurity legislative developments. The European Parliament has also called on the EC 'to make cybersecurity the number one priority in

the Fintech action plan' (Motion 2016/2243 (INI)). There are three main objectives in the EU Fintech Action Plan as follows:

1. to support innovative business models to scale up across the single market;
2. to encourage the uptake of new technologies in the financial sector; and
3. to increase cybersecurity and the integrity of the financial system (EC Memo 2018).

Correspondingly, the EU Fintech Action Plan has initiated various measures to build up the resilience and integrity of the financial sector, in particular in response to the cross-border nature of cyber threats. The measures include: reinforcing ENISA's Cyber Hygiene Practices and the Commission's Digital Education Action Plan; and recommending digital services to incorporate a 'security by design' approach to minimize cyber-attacks (COM (2018) 109 final) in line with the EU Cybersecurity Act (Recital 12). The EU Fintech Action Plan stresses the fundamental importance of 'access to threat intelligence and information sharing' to improve cybersecurity and identifies difficulties of accessing intelligence due to potential conflicts with the General Data Protection Regulation 2016/679.

In order to enhance cybersecurity and encourage Fintech developments, countries have been establishing global or regional Fintech Hubs to combine different elements (such as capital, markets, talent, government support and regulation), in particular to bring together people with different skills to interact and encourage learning between regulators, innovators and established players (Institute of Chartered Accountants in England and Wales and Institute of Singapore Chartered Accountants 2018). It was reported in 2018 that there were seven global Fintech Hubs in the world: four in China, two in the US and one in the UK (Global Fintech Hub Report 2018). This shows that European countries have made limited progress in establishing global Fintech Hubs. Nevertheless, there are currently six regional Fintech Hubs in Europe (Switzerland, Ireland, Netherlands, Germany, France and Sweden) (Global Fintech Hub Report 2018).

In March 2018, the European Banking Authority (EBA) published a Fintech Roadmap, setting out its five priorities of work and also initiating the establishment of a Fintech Knowledge Hub to enhance knowledge sharing and develop technological-neutral regulatory measures (EBA 2018). One of EBA's priorities is 'promoting best supervisory practices on assessing cybersecurity and promoting a common cyber threat testing

framework' (EBA's Fintech Roadmap 2018). Another priority also involves establishing regulatory sandboxes and innovation hubs. It is not clear in this roadmap about the differences or relationships between a Fintech Knowledge Hub and an innovation hub. It is also unclear whether the Fintech Knowledge Hub is to serve as a global Fintech Hub in the EU. In the roadmap, it appears that the Fintech Knowledge Hub is just a forum for competent authorities to share knowledge and engage with other stakeholders, whilst the innovation hub (together with 'regulatory sandboxes') is for regulated or unregulated entities to engage with competent authorities (EBA's Fintech Roadmap 2018: 4-5). 'Regulatory sandboxes' are defined as 'safe spaces in which innovative products, services, business models and delivery mechanisms can be tested without being subject to the full set of regulatory or supervisory requirements that would otherwise apply' (EBA's Fintech Roadmap 2018: 4-5). There is a need for further clarification of why two different hubs are required and how these two hubs can liaise with each other to achieve the common goals of knowledge sharing and security enhancement. It would also be helpful to clarify why there is the need for both the innovation hubs and regulatory sandboxes, as well as what the differences are between these two models in terms of functions and features. In April 2019, the European Forum for Innovation Facilitators was launched by the EC and the European Supervisory Authorities (ESAs) to act as facilitators (in the form of innovation hubs and regulatory sandboxes) to improve cooperation on technological innovation (EC April 2019). It further clarifies that 'innovation hubs' provide a dedicated point of contact for financial firms to engage with competent authorities on Fintech issues, whilst 'regulatory sandboxes' are schemes for competent authorities to allow firms to test innovative financial products and services (EC April 2019).

In some countries, sandbox mechanisms or frameworks are regulated through national Fintech laws. For example, the Mexican Fintech Law, effective in March 2018, has set out relevant provisions on the sandbox mechanism, which provide a trial period of up to two years (with a potential one-year extension) for tech firms to implement new technology financial services for a limited number of clients within a certain geographic area (Baker Mckenzie 2018). In other countries, sandboxes are implemented by national monetary authorities. For example, in Hong Kong, a regulatory sandbox is also called a supervisory sandbox. The Hong Kong Fintech Supervisory Sandbox, launched in 2016 by the Hong Kong Monetary Authority, is a forum with a chatroom for tech firms to test their new Fintech products and services (including cross-sector products) and seek feedback without the need for full supervisory

requirements or going through a bank (Hong Kong Monetary Authority 'Sandbox' n.d.). The Hong Kong Monetary Authority also hosts the Fintech Facilitation Office (FFO). The innovation hub proposed by the EBA in the EU appears to intend to serve similar functions to the FFO in Hong Kong, which provides a platform for exchanging ideas among stakeholders, bridging understanding between market participants and regulators, and initiating industry research (Hong Kong Monetary Authority 'FFO' n.d.).

Although cybersecurity in the financial sector has been considered as one of the priorities in the EU Fintech Action Plan and the EBA Roadmap, unfortunately, there are still no specific security measures or technical measures identified in the roadmap, and the ESAs most recent joint report on regulatory sandboxes and innovation hubs (ESAs Joint Report 2019). It is noted that ESAs include three authorities: the European Securities and Markets Authority, the EBA and the European Insurance and Occupational Pensions Authority. Technical measures are of fundamental importance from the initiations of the trial period of financial products and services to safeguard users, in particular due to the vulnerability of new products and services. It should be the joint responsibility of supervisory authorities and innovation facilitators to work with the ENISA to make sure that appropriate technical measures are built into pilot projects. For example, the 'moving target security' approach is often employed by sensitive services and products such as stock exchanges, banks or robotic firms. The purpose of the moving target security approach is to move around the names, locations and references of files and software applications, so that the system is not configured in the same way each time. However, there is always a trade-off between usability and security because the more secure a computer is, the less practical it is (Russon 2019). Thus, it is important to define a set of standards for security by design, as proposed in the EU Fintech Action Plan, and set out realistic and appropriate security-by-design approaches for financial services and products.

[D] IMPROVING LEGAL AND TECHNOLOGICAL MEASURES ON CYBERSECURITY IN THE EU

As shown above, in the EU cybersecurity legislative movements in recent years, there have been numerous new creations in the form of authorities, facilitators, centres, hubs, institutions and public organizations. These have been set up to work on regulatory developments on cybersecurity issues in the EU. It can be observed that one of the common goals of these new establishments is to facilitate continuing dialogues among different

competent authorities and stakeholders to set out appropriate legal and technical measures to enhance cybersecurity in both public and private sectors in the EU. While it is helpful to have a variety of establishments which share their special skills and knowledge in cybersecurity legislative developments, it may be more effective if these establishments were set out in a logical structure and with clear and non-duplicated functions. It is vital that these establishments are not established spontaneously, but rather that they are carefully thought out in terms of definitions, functions, responsibilities, connections and relationships with one another.

In addition to a lack of integrated strategic working plans across numerous establishments relating to cybersecurity-related issues in the EU, it appears that technical measures have also been under-researched by these establishments. It is essential that best practices for minimum technical standard and measures for security are established for both public and private sectors. Moreover, minimum technical standards and measures for sensitive public services and national infrastructures should be regulated and implemented harmoniously across the EU. Setting up appropriate technical-neutral measures for security can be the most challenging task for regulators because it requires regulators to understand current technologies, technological developments and their potential implications in law. There is certainly no one single solution to the need to improve cybersecurity, but a wide range of collective and far-reaching technical and legal measures may make it as hard as possible for those who want to attack the security of infrastructures, services and products.

Moreover, the Council of Europe Convention on Cybercrime (also known as the Budapest Convention 2001) was the first international treaty to foster international cooperation to deal with cyber-related criminal activities such as computer-related fraud, child pornography and network security violations. However, it appears that the current EU cybersecurity legislative movements, including the EU Cybersecurity Act, have made no clarification about the conceptual connection and differences between cybersecurity and cybercrime as defined in the Budapest Convention. It would be helpful to define in what circumstances breach of cybersecurity constitutes tortious (civil), administrative or criminal liability. For example, Article 65 of the EU Cybersecurity Act gives member states discretion to lay down the rules on penalties and necessary measures. Such penalties are required to be effective, proportionate and dissuasive. However, there is no harmonized standard as to what is considered as effective, proportionate and dissuasive penalties or sanctions across member states.

Generally speaking, there are two main types of legal and technical measures for cybersecurity: namely forward-looking measures and backward-looking measures. Forward-looking solutions may be arguably much more efficient and effective than backward-looking solutions. However, forward-looking solutions may be more challenging as they require an ability to foresee potential harms and anticipate future trends of technological developments.

Prevention is one of the main forward-looking measures in law and technology. Legal measures for prevention mean that law-makers, regulators and competent authorities need to enhance their understanding of potential hazards, risks and dangers in technologies and establish best practices or legal requirements of minimum standards to minimize risks. Technical measures for prevention mean that computer coding needs to be reviewed and updated periodically and that engineers need to implement best practices in industries.

For example, in the automotive domain, software development guidelines, such as MISRA C (Motor Industry Software Reliability Association) are commonly followed to ensure code is written with safety and reliability in mind. Standards have also been created for the entire safety lifecycle, such as the international standard for functional safety of electrical systems in production of road cars (ISO26262). Such standards provide a necessary foundation of safety and reliability, upon which security resilience can be built.

Automotive cyber-security is now taken increasingly seriously, as many new vehicles have an always-on connection to the internet. Vehicle manufacturers perform threat analysis and develop attack models to test the resilience of their systems. Road vehicles commonly have dozens of networked electronic components, from engine control to electric seat movement. Nowadays, the vehicle is not considered a closed system, but a system at risk of attack from the outside, either by direct physical access or by virtual access over the internet. Communications between components (i.e. engine control units and anti-lock brake systems) are now increasingly being encrypted and segregated into distinct sub-networks. For example, components responsible for critical safety systems may be kept separate from components responsible for the infotainment system. Thus, a successful attack on less critical parts of the vehicle infrastructure cannot spread to a critical part.

The battle against hackers may be a challenging one for vehicle manufacturers to win. The embedded systems have limited resources compared with a desktop personal computers, making anti-virus software

impractical. Where software patches previously had to be installed at a main dealer, over-the-air (OTA) updates from the internet are becoming more common. These have traditionally focused on updating non-safety critical areas of the vehicle due to the risk of rendering the vehicle undrivable in the event of a failed update or bug in the update. As OTA updates become the standard method of patching all components in the vehicle, manufacturers will have to, firstly, ensure hackers cannot gain widespread access to critical components and, secondly, that updates are well validated to minimize disruption.

Public awareness can also be considered as part of prevention measures. The EU Cybersecurity Act sets out guidelines to increase and enhance public awareness on cybersecurity. It provides that such public awareness is:

> to promote safer online behaviour by individuals and digital literacy, to raise awareness of potential cyber threats, including online criminal activities such as phishing attacks, botnets, financial and banking fraud, data fraud incidents, and to promote basic multi-factor authentication, patching, encryption, anonymisation and data protection advice (Position of the European Parliament 12 March 2019).

In order to build up strong cyber resilience, effective training and awareness-raising activities are required. Subsequently, in January 2018 the EC adopted its Digital Education Action Plan to improve digital skills throughout Europe, including for an action plan (in Action 7) for cybersecurity (COM (2018) 022 final). Action 7 includes two initiatives: one is to initiate an EU-wide awareness-raising campaign on cyber culture to promote online safety, media literacy and 'cyber hygiene' for children, parents/carers and teachers; and the other is to provide a course (online and offline) to teach cybersecurity in primary and secondary education (EC Education and Training n.d.). Although these two initiatives sound promising, the challenging part is how to implement them effectively. In other words, whether this action plan can be effectively conducted, relies on more appropriate programmes and strategies for different levels of teachers and learners: for example, what level of knowledge and awareness is expected for all levels of learners including children, and how it is possible to know whether the desired outcomes are delivered and achieved among learners.

Correct response is another example of forward-looking measures in law and technology. Legal measures for correct response make a great difference in minimising aftershocks and impacts. For example, legal measures should provide well-defined responsibilities for each responsible authority and also provide clear information and single contact for all

types or nature of security breach notification. This is because it is not reasonable to expect harmed parties or entities to be able to identify the nature, scale and scope of breach or harms immediately when reporting incidents. Correct response also relies on a harmonized cyber defence framework, which enables cooperation and information-sharing between civilian and military incident response communities.

Technical measures for correct response mean that the harmed parties, entities or their agents and competent representatives are capable of implementing the required emergency circumvention measures without undue delay. For example, a Norwegian aluminium company with 35,000 staff in 40 countries, Hydro, was hit by malware in March 2019, which has cost it at least £25.6m (*BBC News* 27 March 2019). However, note that Hydro adopted the best incident representation response plan to the cyber-attack and did not pay a ransom. The company was able to put up a temporary website up and remain open to the press and its staff. Hydro even had daily webcasts, with the most senior staff talking through what was happening and answering questions from webcast watchers. Hydro also used its backup data, utilized recovery support from Microsoft and other companies, and engaged with national cybercrime bodies, industry groups and police authorities (Beaumont 2019). In the EU, there are no specific guidelines on correct response to cybersecurity breaches for public and private entities. This is an area that needs to be strengthened. Raising awareness of correct response can be partially enhanced within the general Digital Education Action Plan. Providing correct response to cyber threats or attacks requires more than just awareness: specific skills and knowledge are also needed. Thus, specific training may be required for engineers who are responsible for taking correct technical response action and for leaders who are responsible for taking correct administrative response action.

In addition, there is also a need to establish an efficient mechanism for reporting cyber threats, attacks, security breaches or cyber-related criminal activities. Providing a single point of contact in each state will allow the public, business or organizations to report any cybersecurity concerns without undue delay. However, an internal reporting structure or management plan for gathering and passing information to relevant authorities should also be established and be ready to respond to cybersecurity issues concerning one state across multiple states or multiple sectors.

Collective efforts are a crucial forward-looking solution. It has been noted that the collective securitization of cyberspace among member

states is crucial to the function of EU governance (Christou 2019: 294). There are various levels at which collective efforts can be made. Firstly, collective efforts can be made among member states in the EU and with other non-EU countries and international organizations. For example, member states should work together to provide the most accurate assessment of the situation of cyber threats or attacks and share relevant intelligent evidence.

Secondly, collective efforts can also be made through bilateral agreements or multilateral agreements among countries towards an effective and collective response to cross-border cyber threats or attacks. Such agreements can be made to facilitate cooperation among nations in terms of intelligent evidence-sharing, administrative procedures, investigation procedures or even prosecution procedures.

Thirdly, collective efforts have been made among stakeholders to protect the public. For example, software vendors are keen to gain advance knowledge of security vulnerabilities so that they can provide software patches to circumvent the intended attack. Microsoft offers a bounty programme to reward individuals and groups of researchers who can provide advance information concerning security vulnerabilities. For example, Microsoft currently offers a bounty of up to $100,000 for unreported critical or important vulnerabilities in Microsoft Identify services that can bypass user authentication (Microsoft n.d.). Governmental organizations can also make use of a bounty programme to issue social and public recognition in addition to monetary awards to motivate public collective efforts in combatting cybersecurity breaches.

Fourthly, collective efforts can also be made among non-governmental organizations and communities. For example, the Global Forum on Cyber Expertise comprises various non-governmental organizations, the tech community and members from academia. The Forum aims to develop practical initiatives to build cyber capacity amongst stakeholders. In this Forum, No More Ransom, a public–private initiative, was launched on 25 July 2016, providing a common portal. This web portal provides free decryption tools to victims, prevention advice and links to report a crime online.

Legal sanctions are often considered as backward-looking measures, though certain measures under legal sanctions may also be considered as forward-looking, such as deterrence, rehabilitation and incapacitation (Cutler and Nye 1983: 2). In the context of backward-looking measures, legal sanctions mean penalties, punishment or other law enforcement procedures. Under the UK Serious Crime Act 2015 (Part 2 Computer

Misuse, amending the Computer Misuse Act 1990), if the cyber-attack causes serious economic or environmental damage or social disruption, the offender can be sentenced to up to 14 years' imprisonment (UK Serious Crime Act 2015, Part 2, section 41). Punishment may not be an effective measure if cyber attackers think they are unlikely to be caught, in particular when the attack has been instigated in another jurisdiction. In these cases, legal sanctions will not have a positive effect. Thus, legal sanctions need to be strengthened in the areas that may make a difference, for example, if private or public entities have not complied with the required technological standard for cybersecurity, or if private or public entities have not followed legal procedures during the very limited and crucial response period when an incident happens.

[E] CONCLUSION AND REFLECTIONS

Cyberspace is classified as the fifth domain of operations after land, sea, air, and space in the EU (Council of the EU, Press Release, 19 November 2018). It is understood that the politics and strategies of cybersecurity are 'one of the most complex and diverse technical and political challenges of our contemporary world' (Stevens 2018: 1). Robust and resilient security in cyberspace is crucial for the healthy operation of public and private sectors in all member states. The EU has made efforts to build a harmonized cybersecurity legislative framework through the establishment and enhancement of cybersecurity strategies, regulations (i.e. the EU Cybersecurity Act 2019) and complementing initiatives. Numerous public organizations, non-governmental organizations, centres, hubs, agents, institutions and teams have been established to improve the level of cybersecurity in the EU. The ENISA appears to play a key role in offering expertise and advice on cybersecurity matters, implementing the EU-wide cybersecurity certification scheme and facilitating strategic and operational cooperation among member states.

Enhancing cybersecurity is an ongoing process due to the ever-changing and unpredictable nature of technologies used in cyber threats and attacks. Legal measures and technical measures need to be continuously reviewed and improved in response to such challenges. Minimum technical measures on cybersecurity need to be established for all sectors, in particular for sensitive infrastructures and services. Legal measures can be further established to facilitate cooperation and intelligent evidence-sharing among member states and to implement the required standard of technical measures in all sectors.

It is essential to build up a set of both forward-looking measures and backward-looking measures in order to combat cyber threats and attacks and increase cybersecurity. Prevention, public awareness, collective efforts and correct response are the key set of forward-looking measures. These four main forward-looking measures are interlinked and intertwined with one another. Prevention is a key goal. Legal measures for prevention can be through best practices, whilst technical measures for prevention are through reviewing and updating computer coding and complying with a set of coding standard guidelines. The requirements of general technical measures, such as privacy by design and security by design, need to be further clarified in the current EU legislation. Although technical measures may be limited (e.g. it is possible for even air-gapped computers to be hacked), implementing a set of minimum standards will minimize the risk of being attacked. For example, for email services, it is good practice to employ TLS for messages to be encrypted in transit. For Fintech services, the moving target security approach should be further developed and implemented.

Although legal sanctions are usually considered as backward-looking measures, they also relate to forward-looking measures in terms of deterrence, rehabilitation and incapacitation. It would be beneficial for the EU to look into strengthening a harmonized standard in legal sanctions, in particular, for serious cybercrime across member states due to the cross-border nature of cyber-attacks.

Finally, all levels of cooperation are fundamentally important to build up strong cyber defences. National, regional and international cooperation needs to be established to enable collective, effective and correct response and increase the resilience of cybersecurity around the globe.

References

Baker McKenzie (2019) 'Fintech Law in Mexico: What to Expect, How to Prepare and What Comes Next' 9 March 2019.

BBC News (4 January 2019) 'German Politicians Targeted in Mass Data Attack'.

BBC News (8 March 2019) 'Security Holes Found in Smart Car Alarms'.

BBC News (27 March 2019) 'Aluminium Firm Cyber-attack Cost at Least £25.6m'.

BBC News (23 April 2019) 'More than Half of British Firms "Report Cyber-attacks in 2019"'.

Beaumont, Kevin (2019) 'How Lockergoga Took Down Hydro—Ransomware Used in Targeted Attacks Aimed at Big Business' *Double Pulsar* 21 March 2019.

Chatterjee, Charles and Lefcovitch, Ann (2016) 'Cyber Security, Diplomacy and International Law' 108 *Amicus Curiae* 2-12.

Christou, George (2019) 'The Collective Securitisation of Cyberspace in the European Union' 42(2) *West European Politics* 278-301.

COM (2000) 890 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26 January 2001.

COM (2016) 410 final, Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 5 July 2016.

COM (2017) 340 final, Report from the Commission to the European Parliament and the Council on the Assessment of the Risks of Money Laundering and Terrorist Financing affecting the Internal Market and relating to Cross-border Activities, 26 June 2017.

COM (2017) 477 final/2, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ('Cybersecurity Act'), 4 December 2017.

COM (2018) 022 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan, 17 January 2018.

COM (2018) 109 final, 'Fintech Action Plan: For a More Competitive and Innovative European Financial Sector', 8 March 2018.

COM (2018) 630 final, Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 12 September 2018.

Council of the EU (29 June 2017) 'Cyber Attacks: EU Ready to Respond with a Range of Measures, including Sanctions'.

Council of the EU (19 November 2018) Press Release 'Cyber Defence: Council Updates Policy Framework'.

Cutler A and D Nye (1983) 'Forward and Backward Approaches to Criminal Law' *in Justice and Predictability* London: Palgrave Macmillan.

'Draft Council Conclusions (2017) on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)' 7 June 2017.

EBA's Fintech Roadmap (2019) *Conclusions from the Consultation on the EBA's Approach to Financial Technology (Fintech) EBA*, 15 March 2018.

EU Policy Cycle—Empact (2017) 'Robust Action to Target the Most Pressing Criminal Threats'.

European Banking Authority (EBA) 2018 'EBA Publishes its Roadmap on Fintech' 15 March 2018.

European Commission (EC) (2018) 'Cybersecurity Act' 11 December 2018.

European Commission (EC) Memo (2018) 'Frequently Asked Questions: Financial Technology (Fintech) Action Plan' 8 March 2018.

European Commission (EC) (March 2019) 'The Cybersecurity Act Strengthens Europe's Cybersecurity' 19 March 2019.

European Commission (EC) (April 2019) 'Financial Technology: European Commission and European Supervisory Authorities Launch New Platform to Improve Cooperation on Technological Innovation in the Financial Sector' 2 April 2019.

European Commission (EC) Education and Training (n.d.) 'Digital Education Action Plan—Action 7 Cybersecurity in Education: Raising Awareness of Teachers and Students'.

European Cybercrime Centre (EC3)

European Supervisory Authorities (ESAs) Joint Report (2019) 'Fintech: Regulatory Sandboxes and Innovation Hubs' JC 2018 74, 7 January 2019.

European Union Agency for Network and Information Security (ENISA) (2016a) 'Definition of Cybersecurity—Gaps and Overlaps in Standardisation'.

European Union Agency for Network and Information Security (ENISA) (2016b) 'Review of the Cyber Hygiene Practices' December 2016.

European Union Agency for Network and Information Security (ENISA) (2017) 'Phishing on the Rise'.

European Union Agency for Network and Information Security (ENISA) (2018) 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity'.

Fahey, Elaine (2014) 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' 5(1) *European Journal of Risk Regulation* 46-60.

Gibney, Alex (2016) *Zero Days*.

Global Fintech Hub Report (2018) 'The Future of Finance is Emerging: New Hubs, New Landscapes Hangzhou' 16 November 2018.

Global Forum on Cyber Expertise.

Google (n.d.) 'Email Encryption in Transit'.

Hong Kong Monetary Authority 'Fintech Facilitation Office (FFO)'.

Hong Kong Monetary Authority 'Fintech Supervisory Sandbox (FSS)'.

Institute of Chartered Accountants in England and Wales (ICAEW) and Institute of Singapore Chartered Accountants (ISCA) (2018) 'Fintech Innovation: Perspectives from Singapore and London'.

ISO/PC 317 (2018) 'Consumer Protection: Privacy by Design for Consumer Goods and Services' ISO 2018-2021.

JOIN (2013) 1 final, Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013.

JOIN (2017) 450 final, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, 13 September 2017.

Kaspersky (n.d.) 'What is Zero Day Exploit?'.

Kosseff, Jeff (2018) 'Defining Cybersecurity Law' 103(3) *Iowa Law Review* 985-1031.

LexisNexis Risk Solutions and ThreatMetrix (2019) 'EMEA Cybercrime Report: Q1 2019'.

Margulies, Peter (2017) 'Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy' 24(2) *Indiana Journal of Global Legal Studies* 459-95.

McAfee (2018) 'McAfee Labs Threats Report' December 2018.

'Microsoft Bug Bounty Program' (n.d.)

Moret, Erica and Patryk Pawlak (2017) 'The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?' EU Institute for Security Studies (EUISS) Brief 12 July 2017.

Mortera-Martinez, Camino (2018) 'Game Over? Europe's Cyber Problem' Centre for European Reform July 2018

Motion (2016/2243 (INI)) for a European Parliament Resolution on Fintech: The Influence of Technology on the Future of the Financial Sector, Committee on Economic and Monetary Affairs, Rapporteur: Cora van Nieuwenhuizen, 28 April 2017.

Muller, Joann (2019) 'What Tesla Knows about You' *Axios* 13 March 2019.

National Cyber Security Centre (n.d.) 'What is Cyber Security?'.

No More Ransom.

Organisation for Economic Co-operation and Development (OECD) (1986) Computer-related Crime: Analysis of Legal Policy (Information, Computer, Communications Policy) Paris: OECD.

Organisation for Economic Co-operation and Development (OECD) (1992) 'OECD Guidelines for the Security of Information Systems' Paris: OECD.

Organisation for Economic Co-operation and Development (OECD) (2012) 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy' Paris: OECD.

Ponemon Institute (2019) 'Cybersecurity in Operational Technology: 7 Insights You Need to Know' Traverse City: Ponemon Institute.

Position of the European Parliament adopted at first reading on 12 March 2019 with a view to the adoption of Regulation (EU) 2019/... of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Roth, Andrew and Nakashima, Ellen (2017) 'Massive Cyberattack Hits Europe with Widespread Ransom Demands' *Washington Post* 28 June 2017.

Russon, Mary-Ann (2019) 'Should Cyber-security be more Chameleon, Less Rhino?' *BBC News*, 9 April 2019.

Simmons, Dan (2019) 'Cyber-attacks "Damage" National Infrastructure' *BBC News*, 5 April 2019.

Soesanto, Stefan (2018) 'A Hammer in Search of a Nail: EU Sanctions and the Cyber Domain' (December) *Journal of International Affairs*.

Stevens, Tim (2018) 'Global Cybersecurity: New Directions in Theory and Methods' 6(2) *Politics and Governance* 1-4.

Tesla (2016) 'Upgrading Autopilot: Seeing the World in Radar' 11 September 2016.

ThreatMetrix (2018) 'The ThreatMetrix European Cybercrime Report: Q1 2018'.

US Department of Commerce (2016) 'Small Business Information Security: The Fundamentals' NISTIR 7621 Revision 1, November 2016.

Walder, Bud (2016) 'Gmail TLS Email Encryption—Is It Good Enough?' *Datamotion* 24 August 2016.

World Bank (2018) 'Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision' 24 February 2018.

Legislation Cited

Council of Europe Convention on Cybercrime (Budapest Convention 2001

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (known as 'EC Directive on security of network and information systems') OJ L 194, 19 July 2016

EU Cybersecurity Act 2019

General Data Protection Regulation 2016/679

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance

UK Serious Crime Act 2015

UK Computer Misuse Act 1990

Cases Cited

J Brazil Road Contractors v Belectric Solar Ltd (2018) 1 WLUK 294

Pisciotta v Old National Bancorp 499 F3 d 629, 638 (7th Cir 2007)

R v Connor Douglas Allsopp (2019) EWCA Crim 95