IoTs and the need for digital norms – A global or regional issue?

Maria Bada
Cambridge Cybercrime Centre
University of Cambridge
maria.bada@cl.cam.ac.uk

Abstract

Internet technologies have continued to advance over the last few decades, which led into the development of Internet of Things (IoTs). There has been a lot of debate at an international level on IoTs and the new threats and new forms of cyber-attacks that could emerge from new technologies. IoTs and 5G connectivity imply faster speeds and tools for citizens but also for criminals. Additionally, lack of awareness or unwillingness of devices owners to update and fix devices' security flaws, and the lack of compatibility among communication standards makes it hard addressing the security challenges of IoTs. In terms of legislation there have been many developments at an international level as well as at regional level. However, challenges remain in the implementation of regulation. This study aims to a) review current research and policy developments on regional and international norms and IoT security considerations and b) identify if and how IoTs are discussed within underground forums. The methodology used is based on a) a thorough literature review and b) the use of CrimeBB Dataset from the Cambridge Cybercrime Centre. The results provide useful insights on potential use and exploitation of IoTs and stress the need for international cooperation and multi-stakeholder engagement to address interoperability, as well as security and safety issues especially in light of emerging developments and the advent of 5G.

Keywords: IoTs, AI, cyber norms, cybersecurity, cybercrime, awareness

1. Introduction

The Internet has drastically transformed the way that we as a society communicate, interact and trade. At the same time, it has also opened new opportunities for criminals. Internet technologies have continued to advance over the last few decades, which led into the development of Internet of Things (IoTs). There has been a lot of debate at an international level on IoTs and the new threats as well as new forms of cyber-attacks that could emerge from new technologies (Radanliev, et al., 2019, Europol IOCTA, 2019). IoTs and 5G connectivity imply faster speeds and tools for citizens but also for criminals.

IoT security refers to steps that are taken to secure or enhance the safety of internet-connected devices. It can mean anything from requiring a unique password on devices to ensuring that devices use only password-protected internet connections. However, we see that manufacturers of IoT devices do not provide publicly information to consumers about the security features of the devices before they purchase the product, while little information on cyber hygiene is also provided (Blythe, et al., 2019).

Additionally, lack of awareness (Bada et al. 2015) or unwillingness of devices owners to update and fix devices' security flaws, and the lack of compatibility among communication standards makes it hard addressing the security challenges of IoTs (Mannilthodi & Kannimoola, 2017).

Policies and practices developed in an analogue world are clearly inadequate, and every day there are attempts to write new rules, or challenge existing ones, that relate to privacy, freedom of expression, intellectual property protection and national security. Policy makers, businesses, NGOs, users, face immense challenges (WEF, 2013).

In terms of legislation there have been many developments at an international level as well as at regional level. However, in regions such as the Gulf Cooperation Council (GCC) states or African states, the absence of legislation or lack of implementation of regulation can undermine international collaboration, even within the same territory. Therefore, the issue arises of some jurisdictions not being able to wait for others in developing IoT and 5G regulations.

Additionally, at a European level, policies and regulations have been already in place and new ones suggested to set the foundations of cyber norms. Also, organisations such as ENISA and Europol[1] collaborate in order to identify more proactive and efficient ways for preventing cybercrime.

The importance of establishing a cybersecurity ecosystem has been acknowledged by all sectors. Cybersecurity experts have acknowledged the need to focus more attention on the attitudes, beliefs and practices of end-users (Dutton, 2017). Rather than following a learned set of practices or habits, individuals could internalise this goal in ways that it motivates them to prioritise security in their online behaviour. Dutton (2017) has defined a cybersecurity mindset as "*a pattern of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users*". This can lead to creating a cybersecurity culture manifested at different levels, at the level of observable behaviour in different social contexts, at the deeper levels of self-construction of personal identities and at the fundamental level of cognition and perception of the world (Badrudin, 2019).

Imposing security to users has proved not effective (Bada, 2015). Also, creating a culture of fear is problematic. Cybersecurity is no longer in the purview of computer science departments, and technical experts in security, but more multidisciplinary (Dutton, 2017). Users might not necessarily realise the risks associated with the use of smart devices (Houses of Parliament, 2019), therefore awareness initiatives should continue in order to increase baseline cybersecurity and nurture the skills and expertise needed to ensure a safer cyber-space (De Zan, 2019).

Setting digital norms is essential (Garriga, 2019, Luke, 2018) to fight against online disinformation. Access to information has as a prerequisite morality of access in information, however, due to a misconception between freedom of expression and freedom of malicious manipulation and bias between the right to privacy versus the right to non-discrimination we often see fake news being spread online.

This study aims to review current research and policy developments on regional and international norms and IoT security considerations, as well as identify the ways IoTs are discussed within underground forums. The paper is structured as follows. Section 2 describes the methodology followed and the data used. In Section 3, the current literature is reviewed.

[1] https://www.enisa.europa.eu/events/3rd-europol-enisa-iot-security-conference

Section 4 presents the legal and regulatory frameworks related to IoTs. Section 5 presents the findings from underground forum data, while in Section 6 findings are discussed.

2. Methodology

This study aims to a) review current research and policy developments on regional and international norms and IoT security considerations and b) identify if and how IoTs are discussed within underground forums. The methodology used is based on a) a thorough literature review and b) the use of CrimeBB Dataset from the Cambridge Cybercrime Centre[2] (Pastrana, Thomas, Hutchings, & Clayton, 2018).

This dataset includes data 'scraped' from several underground forums with more than 48 million posts. The datasets were created via queries using keywords related to IoTs and their use for malicious purposes. CrimeBB was created to allow large scale, longitudinal analysis of underground forums and cybercriminal communities. The dataset provides a means for researchers to conduct an analysis of cybercriminal activities without the need to write their own scraper. CrimeBot, the scraper tool, provides regular updates and users can access the dataset through a legal agreement via the CCC. This dataset has been used for previous work in analysing activities in underground forums (Pastrana, et al., 2018, Caines, et al., 2018).

Qualitative Methods

A thematic content analysis was conducted in order to analyse the randomly drawn posts from the CrimeBB dataset. The main aim of using this methodology was to categorize the data by searching for themes with broader patterns of meaning (Zhang & Wildemuth, 2005). Due to the size of the extracted data it was not feasible to perform manual qualitative analysis and coding for all data, thus initially 600 posts were selected randomly from 2013-2019.

Quantitative Measures

Additionally, in order to complement our findings from the qualitative analysis, a search was performed in order to identify the hash tags used when users discuss this topic on Twitter. For this an AI-based Twitter tracking tool was used, Trackmyhashtag[3]. The following keywords were used: "*IoT AND cybercrime*" and "*AI AND cybercrime*". The search was conducted on the 12th October 2019.

3. Literature Review

In this section the different aspects related to IoTs are being described. Concepts such as cyber norms and ethics, the emergence of new threats and risks associated to smart devices as well as the security features of products are discussed. Additionally, examples of smart devices having been hacked are being presented.

[2] https://www.cambridgecybercrime.uk

[3] https://www.trackmyhashtag.com

IoTs, 5G and societal implications

The technological advancements that come along with a fully developed 5G network will be life-changing. 5G has the potential to drastically improve the quality of life in many ways such as in healthcare (WEF, 2019). However, obstacles such as cost and regulatory oversight will need to be resolved before the capabilities of 5G can open up a new world of possibilities.

Developed cities will be the first to experience 5G, as rural areas currently lack the infrastructure to support the network, and it will take years before the whole world is connected (WEF, 2019). Consequently, the pace of growth is expected to also become greater between developed and developing countries, increasing the digital divide (Nurse & Bada, 2017). The digital divide can lead to digital inequality, which refers not just to differences in access, but also to inequality among persons with formal access to the Internet (DiMaggio et al., 2004). Digital inequality can be defined in terms of access, usage, skills and self-perceptions (Robinson et al., 2015). This is where we can begin to witness the impact on cybersecurity as some nations will naturally be better at protecting themselves given their experience, while others (particularly their citizens) may lack the aptitude, skills and knowledge in security (Gamreklidze, E., 2014).

An additional issue is that the current generation of IoT devices' security is often not inherently included in their design (Liyanage, et al., 2018). A study (ARR Group, 2017) concluded that 20% of designers do not consider security at all in their design and more than 40% of the developers do not encrypt their communications, mostly because of cost constraints.

Moreover, although developed countries have access to the latest technologies, inadequate education and ineffective awareness-raising efforts cause inequality in user skills (Tagert, 2010). For example, there is a lack of basic skills and knowledge for activities such as regularly updating software and apps, avoiding threats such as phishing attacks, and avoiding weak passwords in their use of devices.

The impact of the digital divide can also impact cybercrime at an international scale because it constantly provides a ripe group of victims for attackers. For instance, attackers may first target the more developed countries with attacks (e.g., spam or spear-phishing emails) and then, as their success rates begin to drop, they could target less developed nations with the same attacks (Nurse & Bada, 2017).

In a report from Microsoft, we can see an example of this, since Asia Pacific countries were among the most vulnerable to malware threats (Microsoft, 2017). A similar argument may also be made in terms of cybercriminals and the law, with smart criminals choosing a base of operations where law enforcement is incapable of tracking them down.

The issue here is also whether society as well as business are prepared for 5G connectivity and new technologies. Research from Barclays (2019) has found that just 15% of business decision makers are thinking about how they can utilise the new technology. Also, a study conducted by Repeater Store (2018) showed that the demand for 5G was not high and that participants would prefer providers to deliver rural areas with consistent 4G service first.

Cyber Norms and Ethics

Cyber norms vary widely across regions and evolve rapidly. For example, according to a WEF (2013) report, over 50% of users surveyed in China, prefer to receive targeted ads based on personal Internet activity, while only 20% to 30% of Europeans want to see such ads. There is a rapid change in norms and perceptions across countries and regions, and the wide range of opinions on issues such as the right to online anonymity, targeted online advertising, and the extent to which Web access itself is a right or a service (McKinsey's iConsumer survey).

Organizations operating across borders must recognize that the users of that information, and their governments, often have different cultural norms and expectations. And those norms themselves are changing as "digital natives" come of age and challenge old orthodoxies (WEF, 2013).

Governments and regulatory bodies tend to take the lead in bringing order to the digital word (Dunn Cavelty 2016). While state-related efforts such as the United Nations Group of Governmental Experts (UNGGE), G7, G20, and OSCE have sought to promote norms for responsible state behaviour in cyberspace (Maurer 2011), often it is technology companies who contribute in a steady and prime way in the stability and security of cyberspace (Hurel & Lobato, 2018). The private sector can support in promoting and advocating for international norms but also in the setting of a new norm by adopting it as best practise but also by engaging with organisations supporting the norm (Flohr et al. 2010, 19).

There have been different practises that have emerged over the years in an effort to create cyber norms and ensure national level security and stability. Among these, legislation supported by businesses and rights holders is prominent, as are laws designed to protect minors or prevent the dissemination of illegal material such as child pornography. There are, of course, differences in approach across regions. However, it is often the case that existing laws do not adequately address these issues.

Another practise that has emerged over the years, is the increased monitoring of online activity by governments to limit access to provocative content or disrupt organized protests that might present challenges to national security or stability. For example, there have been content bans in China, monitoring and surveillance of social media in the United Kingdom to identify terrorist and illegal activity, while countries such as Morocco and Tunisia have set up public entities to control and regulate personal data on the Web (WEF, 2013).

Cultures are very much related to how artefacts and instruments themselves are regarded and how their use is circumscribed by socio-cultural norms and specific meanings given to them. Culture manifests itself at different levels—for example: a) at the level of observable behaviour; b) at the deeper levels of self-construction of personal identities; c) at the fundamental level of cognition and perception of the world (Badrudin, 2019). As described by UNESCO (1997) "*In every human society there are networks of values and attitudes, customs and behavioural patterns that define the way of life*".

The great diversity among stakeholders and interests involved necessarily pushes the search for common values and norms towards a high level of abstraction (Iacovino, 2002). Often, statements of principles or values are based on abstract and vague concepts, for example commitments to ensure AI is '*fair*', or respects '*human dignity'*, which are not specific enough to be action-guiding (Mittelstadt, 2019).

The issue of ethics falls often upon developers, who need to translate principles and specify essentially contested concepts as they see fit, without a clear roadmap for unified implementation. Thus far, it is assumed that norms and normative practical requirements can be successfully embedded in development and established in design requirements. However, these assumptions cannot be taken for granted (Mittelstadt, 2019).

These systems are much more fragile and error-prone than marketing materials tend to present (Cattekwaad, et al., 2019). For example, IBM's self-learning algorithms have suggested erroneous medical interventions that could have fatal consequences (The Verge, 2018). Additionally, after the launch of Tesla's self-driving technology, there were several fatal accidents and delays in projected development (The New York Times, 2019).

Self-learning algorithms make mistakes, are sensitive to manipulation, and often poor at coping with outliers. Moreover, algorithmic systems make decisions based on historically biased and flawed data and embed the assumptions of their developers. These dynamics, in turn, can lead to unintended yet discriminatory outcomes, as societal biases are encoded into AI systems (West, et al., 2019).

The Ethics Guidelines for Trustworthy Artificial Intelligence (European Commission, 2019) is an effort towards setting the key requirements that AI systems should meet in order to be trustworthy. These are: a) human agency and oversight; b) technical robustness and safety; c) privacy and data governance; d) transparency; e) diversity, non-discrimination and fairness; f) societal and environmental well-being; g) accountability. Aiming to operationalise these requirements, the Guidelines present an assessment list that offers guidance on each requirement's practical implementation. According to these guidelines, AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights, and AI systems need to be resilient and secure while adequate data governance mechanisms must also be ensured. Additionally, the data, system and AI business models should be transparent while unfair bias must be avoided.

As a means to creating an environment of trust for the successful development, deployment and use of AI, the European Commission encouraged all stakeholders to implement the seven key requirements of the Guidelines. Moreover, the Commission will bring the Union's human-centric approach to the global stage and aims to build an international consensus on AI ethics guidelines.

New threats and new forms of Cyber-attacks

As discussed in a report from Deloitte[4], a smart home with the garage door having the functionality to deactivate the home alarm upon entry, could potentially become a target for cybercriminals who will need only to compromise the garage door opener to enter the house. The broad range of connectable home devices creates a myriad of connection points for hackers to gain entry into IoT ecosystems, access customer information, or even penetrate manufacturers' back-end systems.

Cyberattacks enabled with the use of AI are already taking place. All the required tools for the use of offensive AI already exist, such as highly sophisticated malware and open-

[4] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in an-internet-of-things-world-emerging-trends.html

source AI research information available in the public domain (WEF, 2019). For example – the Emotet trojan[5] – is a prime example of a prototype-AI attack. Emotet's main distribution mechanism is spam-phishing, usually via invoice scams that trick users into clicking on malicious email attachments. Also, in 2017, the WannaCry ransomware attack hit organizations in over 150 countries around the world and that was the beginning of a new era in cyberattack sophistication (WEF, 2019). Its success lay in its ability to move laterally through an organization in a matter of seconds while paralysing hard drives, and the incident went on to inspire multiple copycat attacks.

New threats continue to emerge from vulnerabilities in established processes and technologies. Moreover, the longevity of cyber threats is clear. Some threats of yesterday remain relevant today and will continue to challenge us tomorrow (Europol IOCTA, 2019).

Cyberattacks can have bigger effect and less technical skills will be required. Offensive AI will have the potential to achieve the same level of sophistication faster and at bigger scale. In the case of Emotet and other malware that can impersonate users, these will be able to learn the nuances of an individual's behaviour and language by analysing email and social media communications. They will be able to use this knowledge to replicate a user's writing style and crafting messages that appear highly credible. Messages written by AI malware will therefore be almost impossible to distinguish from genuine communications. As the majority of attacks get into our systems through our inboxes, even the most cyber-aware computer user will be vulnerable. AI malware will also be able to analyse vast volumes of data at machine speed, rapidly identifying which data sets are valuable and which are not (WEF, 2019).

A smart home for example can be even more vulnerable depending on the time of day and what types of devices someone uses. Apparently, security camera systems are the least secure, accounting for 47% of attacks, due to the fact that they are built on similar models, thus making it easier for hackers to access them (SAM Seamless Network, 2019).

Although international bodies like the European Union and the governments of many countries have started to examine and rectify the threat posed by insecure IoT devices, more needs to be done. Continuous and in-depth investigations are needed, to understand where the vulnerabilities stem from.

As we begin to see AI become part of the cyber attacker's toolkit, the only way that we will be able to combat this malicious use of AI is with AI itself. Therefore, incorporating the technology into this ecosystem is crucial (Cunningham, et al., 2018).

In terms of security and privacy considerations, users are often willing to accept (multi-user) security and privacy risks posed by usage of the smart home because of the convenience and utility it provides (Zeng & Roesner, 2019). According to Zeng and Roesner (2019) smart home transparency features do not provide significant benefits for users. Users are generally indifferent to the information provided by the activity and discovery notifications, though some users find them useful for other reasons such as home security and verifying that their automations are working.

[5] https://www.malwarebytes.com/emotet/

These findings reinforce the fact that smart home control interfaces need to be more accessible to users. If a user does not have the skills to install a mobile app or not all members of a household install it, then the benefits of this app will be limited.

Security features of products

There are many consequences to insufficient IoT device security, such as that the devices can be taken over by cybercriminals and used against their owners. For example, internet-connected devices that have cameras or microphones could be used to record or listen to their owners without permission. Additionally, internet-connected devices such as a webcam, digital video recorders and home routers can be strung together and used in botnets for distributed denial-of-service attacks launched by cybercriminals (Süddeutsche Zeitung, 2019).

The last few years we have witnessed deep fake algorithms making it easier to fake video and audio. For example, in 2019 it was the first time a criminal took money by synthetically imitating the voice of a CEO (Süddeutsche Zeitung, 2019). Lyrebird[6] for example, is an application that allows anyone to save his or her voice so that a robot speaks typed sentences and sounds like the tuner. For that fraud the criminals had to use recordings with the voice of the real person for training of Lyrebird and they had to have someone who could type very fast - because Lyrebird speaks only typed. This could also apply to video manipulation with methods of "deep fake". "Fake President" has come to be used as a term for cases in which alleged CEO enforced the transfer of funds.

Additionally, Zao, a free deepfake face-swapping app that's able to place your likeness into scenes from hundreds of movies and TV shows after uploading just a single photograph, has gone viral in China (The Verge, 2019). A user created a 30 second clip of their face replacing Leonardo Dicaprio in famous moments from several of his films. What once required hundreds of images to create a rather convincing deepfake video now requires just a single image with better results. Research has already shown technology that is able to turn a single photo into a singing portrait (Vougioukas K., Petridis, S. & Pantic, M., 2019). This demonstrates how quickly the underlying technology has evolved.

A recent report (Deep Trace, 2019) also showed that currently there are 14,678 deepfake videos online, 96% of which are pornographic, while most deepfake targets are women.

Considering the above, it comes by surprise that manufacturers of IoT devices do not provide publicly information to consumers about the security features of the devices while little information on cyber hygiene is also provided (Blythe, et al., 2019). Shoppers should be given high quality security information in order to make choices at the counter for smart devices (ZDNet, 2018). However, again it would depend on the consumer's awareness and knowledge regarding cybersecurity which will define the purchase decision.

[6] https://www.descript.com/lyrebird-ai?source=lyrebird

Examples of Smart Devices Hacked

Below some examples of smart devices, which have been hacked, are presented. These are a small number of examples, randomly selected to illustrate the risk landscape related to IoTs.

- **Gas Pumps:** There's a lot of discussion in underground forums about compromising internet-connected gas pumps. Like any unsecured connected device, there's the possibility that internet-facing gas pumps could be roped into botnets for use in Distributed Denial of Service (DDoS) attacks, with attackers using them to help overload online services (ZDNet, 2019). However, there are ways to help protect gas pumps and similar devices, even if they're connected to the internet, including ensuring that devices have their default passwords changed, so brute-force attacks aren't as effective.

  But, why would attackers target electronic gas-tank-monitoring systems? Attacker motivations for targeting gas-tank-monitoring systems vary for different types of threat actors. An experiment conducted by Wilhoit and Hilt (2015) showed that hackers can simply be testing their skills against ATG systems, experimenting and checking what level of access they can get and what they can do with it. Pranksters can, for instance, change the tank labels to something menacing. Additionally, threat actors can use the information visible on Internet-facing ATG systems to perform preliminary reconnaissance for highly industry-specific targeted attack campaigns. Lastly, attackers can hold the console hostage and ask for ransom to restore owner access.

- **Bluetooth Connected Hair straightener:** The Bluetooth connected hair straightener launched by a UK firm allows users to link the device to an application, which lets the owner set certain heat and style settings. The application can also be used to remotely switch off the straighteners within Bluetooth range. Researchers tested the device and found that it was easy to send malicious Bluetooth commands within range to remotely control an owner's straighteners (PenTestPartners).

  Because the straighteners have no authentication, an attacker can remotely alter and override the temperature of the straighteners and how long they stay on — up to a limit of 20 minutes. However, the straighteners only allow one concurrent connection. If the owner hasn't connected their phone or they go out of range, only then can an attacker target the device.

  Looking at the user manual of the device, it does not include security related details or any reference in how this can be used for illegal purposes and cause harm.

- **The Jeep Hack:** In 2015, researchers Miller and Valasek explained during the Black Hat USA Conference how they hacked a Jeep Cherokee using the vehicle's CAN bus (IBM Security Intelligence, 2015). By exploiting a firmware update vulnerability, they hijacked the vehicle over the Sprint cellular network and discovered they could make it speed up, slow down and even veer off the road. This is another example of how IoTs do have vulnerabilities and these might stem from peripheral devices or networks.

- **The WiFi Baby Heart Monitor:** Another example is the Wifi baby heart monitor. These devices have been developed in order to alert parents when their babies experience heart defunctions. However, the connectivity element makes these devices exploitable (IBM Security Intelligence, 2015).

- **AI used to Mimic Voice:** Law enforcement authorities and AI experts have predicted that criminals would use AI to automate cyberattacks. Earlier this year, we have seen that criminals used Lyrebird, an artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of a large amount (Süddeutsche Zeitung, 2019). The software successfully mimicked the voice of the German executive. Thus, this might be a serious challenge for the private or public sector.

- **DIY keys for Luxury Cars:** Researchers have already identified vulnerabilities of key fobs of modern cars (Francillon, 2011). By cloning a Model S key fob, researchers were able to unlock and drive a vehicle.

- **Public Wi-Fi:** It is well known for quite some time now that using an open public Wi-Fi can lead to serious risks. One of the dangers of using a public Wi-Fi network is that data over this type of open connection is often unencrypted and unsecured, leaving you vulnerable to a man-in-the-middle (MITM) attack. Essentially, this gives a hacker access to sniff out any information that passes between the user and the websites they visit — details of browsing activities, account logins, and purchase transactions. Sensitive information, such as passwords and financial data, are then vulnerable to identity theft.

4. Legal and regulatory frameworks related to IoTs

While the Internet of Things technological shift will require clear legal frameworks, alternative approaches also need to be developed (Weber & Studer, 2016). In terms of legislation there have been many developments at an international level as well as at regional level. At an international level, governments are investing in cybersecurity, developing national cybersecurity strategies and policies as well as agreements on international collaboration to fight cybercrime (e.g. UNODC, Interpol). Additionally, at a regional level different legal and regulatory developments have initiated or are already in place.

Europe

At a European level, the last few years the focus has shifted towards data protection and privacy. The General Data Protection Regulation-GDPR (2018), the Directive on the Security of Networks and Information Systems (NIS Directive, 2016) and recently the EU Cybersecurity Act (2019) have been drafted to promote resilience, ensure user privacy and serve as countermeasures for cybercrime. Recently, we have also seen new online risks emerging such as fake news, deep fakes but also online self-harm, which led the UK Government to a White Paper on online harms, (DCMS & Home Office, 2019) which sets out the government's plans for a package of measures to keep UK users safe online.

Some data handled by IoT devices is also covered by the General Data Protection Regulation (GDPR, 2018). It emphasises privacy by design and states that personal data must be handled securely. GDPR applies to the personal data of all EU residents.

Industry standards for internet-enabled devices were recently issued by the European Telecommunications Standards Institute (ETSI) Technical Committee on Cyber-Security. These standards are the first to apply to a range of devices globally and are based on the UK's Code of Practice.

To address cybersecurity concerns, one of the most ambitious initiatives introduced in Europe is the establishment of a cybersecurity certification framework (European Commission, 2018). Under the proposed EU Cybersecurity Act (European Commission, 2019), the EU Agency for Network and Information Security would establish an EU-wide voluntary certification framework for ICT products and services. Furthermore, the recent Cybersecurity Act is a European Commission proposal that strengthens the role of the European Union Agency for Network and Information Security (ENISA) for the definition of this framework, by providing additional guidelines and challenges for its realization (Matheu et al. 2019). As mentioned above, the Ethics Guidelines for Trustworthy Artificial Intelligence (European Commission, 2019) was also presented earlier this year presenting key requirements that AI systems should meet in order to be trustworthy.

- **United Kingdom:** The UK Government advocates for strong security to be built into internet-connected products by design. In October 2018, the Government published the Code of Practice for Consumer IoT Security to support all parties involved in the development, manufacturing and retail of consumer IoT. In addition, the Government also published the consumer guidance for Smart Devices. This describes how to support people with setting up and managing their smart devices to keep their home and their information safe (DCMS, 2018).

  In addition, the Department for Digital, Culture, Media and Sport (DCMS) is also developing a consumer IoT security labelling scheme to help inform consumers' purchasing decisions (DCMS, 2019). This will show customers how secure an IoT device is at the point of purchase. To gain a security label, a device must: a) use unique passwords by default; b) clearly state how long security updates will be available; c) offer a public point of contact for cybersecurity vulnerabilities. Global manufactures may, therefore, need to ensure their products meet UK standards before they can be sold in the UK.

- **France:** A recently passed "5G bill" in France means service providers now need to obtain approval from the government before deploying foreign hardware (Senat, 2019).

- **Netherlands:** In Rotterdam, the city is developing a "data-driven youth policy". Instead of relying on the experience and judgement of youth workers, algorithms determine what vulnerable children need in terms of care. Decisions are made based on sensitive and unstructured data from a variety of systems and sources. The experimental nature of the policy is invoked to minimize legitimate privacy concerns. The system should set the example for other cities and other policy areas (TNO Policy Lab, 2019).

United States of America

In September 2019, California became the first state to pass a law addressing the security of connected devices (California IoT law, Senate Bill No. 327, CHAPTER 886). The law will go into effect in 2020 and requires that manufacturers of any internet-connected devices to equip them with "reasonable" security features.

The legislation predates federal legislation securing IoT devices, while the new law is expected to serve as a template for future legislation. One of the main issues here is what ''reasonable'' security features mean. California's IoT bill requires manufacturers to include specific features when producing these devices. Thus, it will likely set off a trend that is followed nationwide. This bill is also expected to lead into federal legislation, since manufacturers will have to produce all of their devices following the same requirements or even stronger than the California law.

Africa

In the GCC states or African states, the absence of legislation or lack of implementation of regulation can undermine international collaboration, even within the same territory. Also, different countries have a different level in data protection mechanisms (UNCTAD, 2019), or the personal data privacy values can be very different between different legislations. Therefore, currently it seems that cybersecurity and privacy norms might be more effective at a regional level. However, in 2018 the Commonwealth Cyber Declaration committed member states to cooperate on cybersecurity and to promote security by default for connected devices (Commonwealth, 2018).

Australia

Australia has proposed a certification for IoT devices to meet certain requirements. The requirements include using non-default passwords, software updates to fix vulnerabilities and to not expose ports to the wider internet (IoT Alliance Australia, 2017).

South America

- **Brazil:** Brazil works to grow its internet and digital networks. The Brazilian government launched a plan in 2017, to focus on expanding the Internet of Things in the country. Under the umbrella of Brazil's strategy "The Internet of Things: an action plan for Brazil" (Brazilian Government, 2017), new partnerships, higher education programs, and innovators will be promoted to make the most of new opportunities in Brazil's expanding digital market.

Japan

Japan recently launched a campaign to test 200 million devices by attempting to access them with default passwords. Once the campaign is complete, the Japanese government will inform IoT providers of the issues and instruct them to fix the vulnerabilities. According to a Ministry of Internal Affairs and Communications report, attacks aimed at IoT devices accounted for two-thirds of all cyber-attacks in 2016 (ZDNet, 2019).

India

The Government of India has taken key initiatives on IoT. In line with the Government's vision of a Digital India, the Department of Electronics and Information Technology (DEITY, 2016) launched India's first draft IoT Policy Document in 2016. The policy lays the foundation of a strong governance framework for holistic implementation and execution of IoT-related policies and campaigns.

Additionally, the National Digital Communications Policy (NDCP, 2018) has set futuristic goals and undertaken crucial policy initiatives to address the problem of communications and access of digital services in India. According to Internet and Mobile Association of India, the goals set for 2022 are crucial policy initiatives which will address the problem of access and are a welcome step to take India towards a vibrant digital economy. This policy aims to create a roadmap for the emerging technologies in areas like IoT and may result in improving the efficiency and economic benefits.

Overall, legislation to protect IoT devices and the data they hold will help regulate aspects that were originally beyond user control. But implementing effective regulation comes with many challenges. For regulation to be effective, it needs to be coordinated at an international scale. Legislation needs to cater for manufacturers, retailers and consumers. It must regulate but also educate them about data security at every stage of an IoT device's lifecycle. People often think and assume that the government will take care of it and that regulators should ensure privacy and security standards. Additionally, it is expected that it is the manufacturer's responsibility. However, it is a more holistic responsibility that remains with all relevant stakeholders, as well as users.

5. Findings from analysing underground forum data

The findings from the qualitative and quantitative data analysis are presented below.

Qualitative Data Analysis

As mentioned above, a thematic content analysis was conducted in order to analyse the randomly drawn posts from the CrimeBB dataset. In general, discussions within the underground forums analysed, ranged from news and attack tutorials to actual advertised malicious services.

One interesting finding is that since 2014 underground forum members were discussing the topic of automated cars and 3G.

A member of an underground forum wrote: *"all cars will have a GPS and 3G connection not to mention other alarming news concerning control of water and food supplies and electricity and even money supposedly for tax evasion so that all money will be controlled electronically through banks…."* (Quote 1).

The thematic content analysis of the underground forums was performed, which led into two main themes emerging:

1) Human behaviour

Quite interesting is the fact that forum members were discussing about human behaviour and how users fall victims of social engineering or spear phishing. A member noted:

"My hacking abilities greatly depend on my targets I.Q. and computer knowledge. If they click links or download files when suggested to them I can do anything from watch them undress via their webcam to empty their entire bank account. If they don't click things then I can't do much... Unless Google tells me different" (Quote 2).

While another member wrote:
"I'm good when it comes to analyzing human behavior enough to see the woman clicking on the link in her email may not necessarily be un-intelligent. Not that what she did was an indicator, but rather that she was just being selfish. She "wanted to see" what was there, and in a snap judgment, combined with dishonest rationalization, she did what most humans do when it comes to multimedia" (Quote 3).

2) Search engines

Additionally, it is identified that since 2014 members were discussing about the different tools they use for hacking. A member wrote: *"I'm a Google hacker. If I want to hack something, I head over to Google and search 'How to hack x"* (Quote 4).

It is interesting to see that later in 2018 and 2019, discussions included a popular search engine 'Shodan'[7], that scans the internet for connected devices and systems. Because of the way Shodan functions, cybercriminals can operate very efficiently, zeroing in on targets, based on certain criteria.

[7] https://www.shodan.io

A member wrote: “*I mostly use shodan exploits and exploit.db to find stuff, but if you can't find anything you can search on github for stuff. Sometimes researchers post their info on git services, and you can just download it*” (Quote 5).

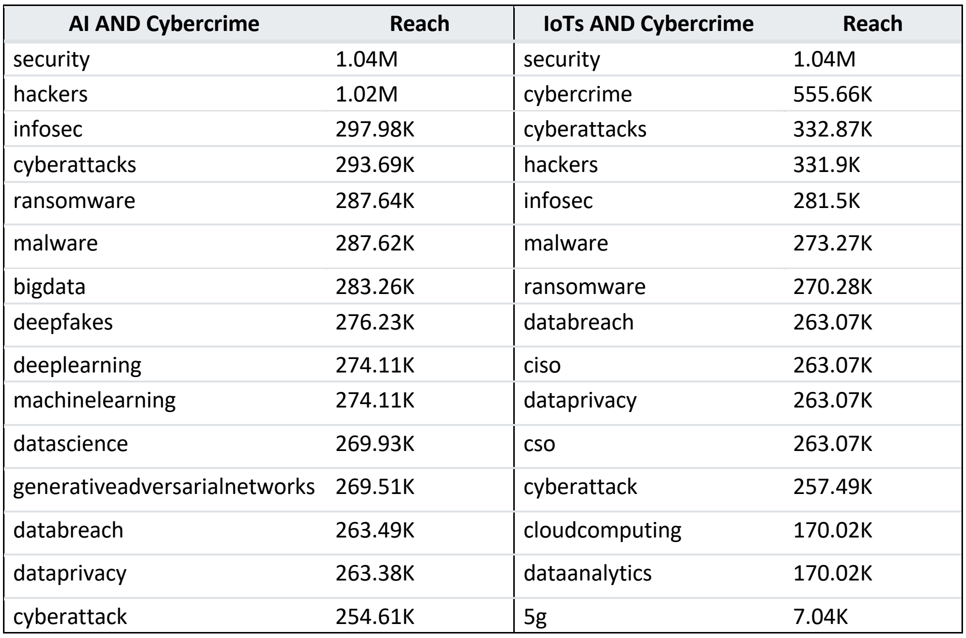
While another member wrote: “*Find yourself a vulnerable website, easily found with something like shodan. Do this though Tor, Upload your dos script and launch attack from there*” (Quote 6).

Quantitative Data Analysis

In order to complement the findings from the qualitative analysis, a search was performed to identify the terms used on social media, as hash tags, when users discuss this topic on Twitter.

As seen in Table 1, the hashtags mainly used to describe topics about Artificial Intelligence and cybercrime are: security, hackers, infosec, cyberattacks, ransomware, malware, bigdata, deepfakes, privacy etc. The hashtags used mainly to describe topics about IoTs and cybercrime were very similar as expected. However, some new terms emerged such as 5G and CISO.

These findings show that Twitter users do have a broad understanding of what IoT and AI exploitation entails.



AI AND Cybercrime	Reach	IoTs AND Cybercrime	Reach
security	1.04M	security	1.04M
hackers	1.02M	cybercrime	555.66K
infosec	297.98K	cyberattacks	332.87K
cyberattacks	293.69K	hackers	331.9K
ransomware	287.64K	infosec	281.5K
malware	287.62K	malware	273.27K
bigdata	283.26K	ransomware	270.28K
deepfakes	276.23K	databreach	263.07K
deeplearning	274.11K	ciso	263.07K
machinelearning	274.11K	dataprivacy	263.07K
datascience	269.93K	cso	263.07K
generativeadversarialnetworks	269.51K	cyberattack	257.49K
databreach	263.49K	cloudcomputing	170.02K
dataprivacy	263.38K	dataanalytics	170.02K
cyberattack	254.61K	5g	7.04K

Table 1: Tweeter Hashtags

6. Discussion

The complexity and resulting cybersecurity challenges in relation to the IoT ecosystem call for a holistic, smart and agile approach. The multi-faceted nature of the challenges and risks demands an equally faceted response by all relevant stakeholders with a view to ensuring cybersecurity (Europol EC3, 2016).

Currently, there is a growing number of policy and legal measures regarding IoTs at an international level. However, when it comes to regulation, questions arise such as exactly whose risk should the regulator be reducing – the risk to a dominant industrial player, or to its millions of customers. Thus, there is need for strong leadership with a strategic forward-looking approach and with policymaking that is dynamic and responsive to the developments in technology.

Additionally, governments and regulatory bodies will need to monitor advances and make it easier for telecommunication companies to invest in upgrading technology. Policies will have to be enacted to enable new revenue models, like data monetization and content management (WEF, 2019). As seen in Section 4, at an international level, governments are investing in cybersecurity, developing national cybersecurity strategies and policies as well as agreements on international collaboration to fight cybercrime (e.g. UNODC, Interpol).

Although these developments are necessary, there lies the risk of nations having different policies at a regional level while we discuss about a global issue. This is why a global digital code is suggested by different stakeholders, which will enable collaboration, and co-innovation seamlessly into a digital world (WEF, 2019). Developing this code will require a collaborative effort from communications and technology providers around the world. But, in the meantime use of 5G will rely on having the necessary infrastructure in place. It is therefore, necessary to also close the digital divide gap among developed and developing countries by investing in cybersecurity capacity building initiatives for developing nations.

G7 countries are considering a coordinated action also on disinformation, following reflexions in international fora such as the OCDE and the Internet Governance Forum of the United Nations (European Parliament, 2019). The need for stronger international collaboration is also echoed in some of the recommendations of the UK DCMS Parliamentary Inquiry into online disinformation (DCMS report, 2018) and the UK Government's response (DCMS HC 1630, 2018).

Sharing threat data is also important, in order to understand the threat landscape and inform decisions to avoid future risks. Additionally, setting standards for sharing data and for exchanging threats with government and private sector is essential. Developing a secure ecosystem with trust among its members will help facilitate sharing of threat related information and enhancing each other's resilience.

Adapting existing standards might entail risks, since we have also seen inappropriate standards being adopted in the past (Anderson & Fuloria, 2010). Therefore, it is suggested that an organisation is established tasked to help monitor and encourage good security-by-design practice, and set out and document an approach to designing secure 5G networks, applications and services. Security-by-design and privacy-by-design should be the guiding principles when developing IoT devices and enabling services (Europol EC3, 2016).

To effectively and efficiently investigate the criminal abuse of the IoT, deterrence is another dimension that needs strong cooperation between law enforcement, the CSIRT community, the security community as well as the judiciary. This creates an urgent need for law enforcement to develop the technical skills and expertise to fight IoT-related cybercrime successfully (Europol EC3, 2019).

As discussed above, there is a need for transparency of the security of products, suggesting that the responsibility to achieve this should lie with the manufacturers and service providers. Transparency is essential and begins with tracking and publicizing where AI systems are used, and for what purpose (West et al., 2019). The field of research on bias and fairness needs to go beyond technical debiasing to include a wider social analysis of how AI is used in context. This necessitates including a wider range of disciplinary expertise.

From a more technical perspective, measures such as monitoring and patching are crucial. It is important for users as well as developers to understand the implications of new technologies. Employees as well as contractors will need to understand the risks and consider security during their work. One important measure suggested is to include security risks in manuals of smart devices. Currently, no security related details or any reference in how a device can be used for illegal purposes and cause harm are mentioned. As shown in Section 3, smart devices have vulnerabilities that cybercriminals already have identified. Additionally, the underground data analysis showed that popular search engines have been used for malicious purposes, such as Google and Shodan.

Data literacy of the population as well as education and awareness around IoTs is also required (Bada et al., 2015). As described in Section 5, the underground forum data analysis revealed that members take advantage of human behaviour and the tendency of users to click on links or attachments sent by email. Additionally, consumer surveys report that poor cybersecurity practices such as using default, weak, or reused passwords are common (Norton, 2017). Also, consumers may underestimate the risk and severity of cybercrime that targets devices and believe that security is not their responsibility (Cyber Aware, 2018). The UK Government has also highlighted that consumers lack the information needed to assess security when buying devices, saying that cybersecurity should not rely on users and that devices should be designed to be secure and easy to manage (Houses of Parliament, 2019).

As shown in Section 5, the hashtag analysis from Twitter showed that users do discuss cybercrime and IoTs or AI, using terms such hackers, ransomware, malware, bigdata, deepfakes, privacy, 5G, CISO etc. Therefore, there is a broad understanding around the exploitation of smart devices or new technologies. But this does not necessarily mean that users personalise risks or realise the severity of cybercrime.

Basic steps such as updating a password or checking that the computer's firewall is active are crucial for using IoT devices as well. Users share also the responsibility for implementing secure configuration and setup of their IoT devices to reduce the risk of these devices being used for criminal means. However, establishing a cybersecurity mindset, is a long-term process because it requires a change in attitudes, beliefs and practices of end-users (Dutton, 2017). Users will need to prioritise cybersecurity in all aspects of their online behaviour to ensure they take the necessary steps to reduce risks.

Setting international cyber norms requires the promotion of best practises and the support of the private and public sector (Flohr et al. 2010, 19). However, for these norms to be part of a culture need to protect and respect the values of a democratic society. Understanding the values needed and ensuring that information shared online is real challenging though, since the Internet is buzzing from disinformation and rumours.

In conclusion, there is a need for digital norms and this is a global issue. However, actions such as leveraging existing initiatives and frameworks, regionally and internationally, following a multi-pronged approach combining and complementing actions at legislation, regulation and policy, standardisation, certification/labelling and technical level are required to secure the IoT ecosystem.

Acknowledgments
Many thanks to Dr Ildiko Pete for assisting in exploring the CrimeBB dataset.

References

Anderson, R., Fuloria, S. (2010). Security Economics and Critical National Infrastructure. In: Economics of Information Security and Privacy. Springer US.

ARR Group (2017). Embedded Systems Safety and Security Survey.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society, CSSS. 2015, pp. 118-131.

Badrudin, A. (2019). Culture, the process of knowledge, perception of the world and emergence of AI. AI & SOCIETY, 1-14. https://doi.org/10.1007/s00146-019-00885-z

Barclays (2019). Is your business 5G-ready? https://home.barclays/news/2019/04/preparing-your-business-for-5g/

Blythe J. M., Sombatruang, N., Johnson, S.D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?, Journal of Cybersecurity, Volume 5, Issue 1, tyz005. https://doi.org/10.1093/cybsec/tyz005

Brazilian Government (2017). Internet of Things, An Action Plan for Brazil. http://www.funag.gov.br/images/2017/Novembro/Dialogos/Claudio_Leal-Internet-of-Things.pdf

Dunn Cavelty, M. (2016). Cyber-security and Private Actors. In Routledge Handbook of Private Security Studies, edited by Abrahamsen Rita and Leander Anna, 89–99. New York: Routledge.

Caines, A., Pastrana, S., Hutchings, A. & Buttery, P. (2018). Automatically identifying the function and intent of posts in underground forums. Crime Science, 7(19), 1-14.

California IoT Law (Senate Bill No. 327, CHAPTER 886). https://gcn.com/articles/2018/12/14/faq-california-iot-legislation.aspx

Cattekwaad, C. Dobbe, R., Cath-Speth, C. (2019). Politicians and administrators: Don’t expect. Miracles from artificial intelligence. Oxford Internet Institute. https://www.oii.ox.ac.uk/blog/politicians-and-administrators-dont-expect-miracles-from-artificial-intelligence/

Commonwealth (2018). Commonwealth Cyber Declaration.

CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale, Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton. ACM The Web Conference, 2018 (WWW), Lyon, France, April 2018.

Cunningham, C., Blankenship, J., Balaouras, S., Sridharan, S. Barringham, & B., Dostie, P. (2018). Using AI For Evil. A Guide To How Cybercriminals Will Weaponize And Exploit AI To Attack Your Business. https://www.forrester.com/report/Using+AI+For+Evil/-/E-RES143162

Cyber Aware (2018). A Call to Action: the Cyber Aware Perception Gap. https://www.gov.uk/government/publications/cyber-aware-perception-gap-report

Department for Digital, Culture, Media & Sport-DCMS (2019). Plans announced to introduce new laws for internet connected devices. https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices

DCMS and Home Office (2019). Online Harms White Paper. https://www.gov.uk/government/consultations/online-harms-white-paper

Deep Trace (2019). The State Of Deepfakes: Landscape, Threats and Impact. https://deeptracelabs.com/resources/

Department for Digital, Culture, Media and Sport (2018). Secure by Design Report.

Department of Electronics and Information Technology of India (DEITY) (2016). IoT Policy Document. https://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf

Deloitte. Cyber risk in an Internet of Things world. Flashpoint edition 4: More data, more opportunity, more risk. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html

De Zan T. (2019). Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions. https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf

DiMaggio, P., Hargittai, E., Celeste, C. & Shafer, S. (2004). Digital Inequality: From Unequal Access to Differentiated Use. In Social Inequality. Edited by Kathryn Neckerman. New York: Russell Sage Foundation. pp. 355-400.

Dutton, W. H. (2017). Fostering a cyber security mindset. Internet Policy Review, 6(1). DOI: 10.14763/2017.1.443

European Commission (2018). The EU Cybersecurity Certification Framework.

European Commission (2019). Ethics Guidelines for Trustworthy Artificial Intelligence (AI). https://ec.europa.eu/futurium/en/ai-alliance-consultation

European commission (2016). The Directive on security of network and information systems (NIS Directive). https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European commission (2019). EU Cybersecurity Act. http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#BKMD-20

European Parliament (2019). Automated tackling of disinformation. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

Europol (2019). Internet Organised Crime Threat Assessment (IOCTA). https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Annegret, F., Rieth, L., Schwindenhammer, S. & Wolf, D.K. (2010). The Role of Business in Global Governance: Corporations as Norm-entrepreneurs. London: Palgrave Macmillan.

Francillon, A., Danev, B. & Capkun, S. (2011). Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February – 9th February.

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue. The Journal of International Communication Vol. 20, Iss. 2.

Garriga G. (2019). A short guide to ethics in AI. https://www.linkedin.com/pulse/short-guide-ethics-ai-gemma-garriga-phd/?trackingId=hadNBGPpsP1%2BAQ9h%2FqudqA%3D%3D

General Data Protection Regulation-GDPR (2018). The European Parliament and the Council of the European Union. https://eugdpr.org

Government of India (2018). National Digital Communications Policy (NDCP). http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

Houses of Parliament. Cyber Security of Consumer Devices. Number 593 February 2019.

Hurel, L.M. & Lobato, L.C. (2018). Unpacking cyber norms: private companies as norm entrepreneurs, Journal of Cyber Policy, 3:1, 61-76, DOI: 10.1080/23738871.2018.1467942 https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1467942

Iacovino, L. (2002). Ethical Principles and Information Professionals: Theory, Practice and Education, Australian Academic & Research Libraries, 33:2, 57-74, DOI: 10.1080/00048623.2002.10755183

IoT Alliance Australia (2017). Strategic Plan to Strengthen IoT Security in Australia. http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf

Liyanage, Ma., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 10.1109/5GWF.2018.8516981.

Luke, A. (2018). Digital Ethics Now. Language and Literacy, 20(3), 185-198. https://doi.org/10.20360/langandlit29416

Maurer, T. (2011). Cyber Norm Emergence at the United Nations—an Analysis of the UN's Activities Regarding Cyber-security. Cambridge, MA: Belfer Center for Science and International Affairs.

McKinsey iConsumre Survey results. http://reports.weforum.org/norms-values-digital-media/consumer-survey/?doing_wp_cron=1570182232.6711440086364746093750

Mannilthodi, N., & Kannimoola, J. M. (2017). Secure IoT: An Improbable Reality. In IoTBDS (pp. 338-343).

Matheu G., Nieves, S., Hernández-Ramos, J., & Skarmeta, A. (2019). Toward a Cybersecurity Certification Framework for the Internet of Things. IEEE Security & Privacy. 17. 66-76. 10.1109/MSEC.2019.2904475.

Microsoft Report (2017). Asia Pacific countries among the most vulnerable to malware threats: https://news.microsoft.com/apac/2017/01/26/asia-pacific-countries-among-the-most-vulnerable-to-malware-threats-microsoft-report/

Mittelstadt, B. (2019). AI Ethics – Too Principled to Fail? SSRN: https://ssrn.com/abstract=3391293 or http://dx.doi.org/10.2139/ssrn.3391293

Norton (2017). 2017 Norton Cyber Security Insights Report. https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

Nurse, J. R. C. & Bada, M. (2017). Connected Life: Digital Inequalities. MIND THE GAP: How Digital Inequality Impacts Cyber Security. Oxford Internet Institute, Oxford, UK, 19th June 2017.

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018). Characterizing Eve: Analysing cybercrime actors in a large underground forum. Heraklion: The 21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID).

PenTestPartners. https://www.pentestpartners.com/security-blog/burning-down-the-house-with-iot/

Radanliev, P., De Roure, D.C., Maple, C., Nurse, J.R., Nicolescu, R., Ani, U. (2019). Cyber Risk in IoT Systems. Preprints, 2019030104 (doi: 10.20944/preprints201903.0104.v1).

Repeater Store (2018). Consumer's Views on 5G Rollout, LTE Coverage, and Health Effects of Cellular Radiation. https://www.repeaterstore.com/pages/consumer-perspectives-on-5g-october-2018

Robinson, L., Cotten, S.R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, J., Hale, T. M. & Stern, M.J. (2015). Digital inequalities and why they matter. Information, Communication & Society 18(5).

SAM Seamless Network (2019). New Research Exposes the Vulnerabilities of Smart Home Networks Through Security Cameras and Smart Hubs. https://www.prnewswire.com/il/news-releases/new-research-exposes-the-vulnerabilities-of-smart-home-networks-through-security-cameras-and-smart-hubs-300866213.html

Sénat, Loi (2019). 5G: Députés et Sénateurs s'accordent Sur Un Texte Équilibré. http://www.senat.fr/presse/cp20190703a.html.

Senate Bill No. 327, CHAPTER 886. An act to add Title 1.81.26 (commencing with Section 1798.91.04) to. Part 4 of Division 3 of the Civil Code, relating to information privacy. [Approved by Governor September 28,

2018. Filed with Secretary of State September 28, 2018.] Legislative Counsel's Digest. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Süddeutsche Zeitung (2019). Betrüger erbeutet 220 000 Euro mit gefälschter Stimme by Herbert Fromme. https://www.sueddeutsche.de/wirtschaft/betrug-mit-synthetischer-stimme-1.4493902!amp?__twitter_impression=true

Tagert, A.C. (2010). Cybersecurity challenges in developing nations. PhD Thesis. Carnegie Mellon University.

The New York Times (2019). Despite High Hopes, Self-Driving Cars Are 'Way in the Future'. By Neal E. Boudette. https://www.nytimes.com/2019/07/17/business/self-driving-autonomous-cars.html

TheSecuirtyCompany (2019). How new regulations could shape the future of the Internet of Things (IoT). https://www.thesecuritycompany.com/infosec-news/how-new-regulations-could-shape-the-future-of-the-internet-of-things-iot/?utm_source=SASIG+distribution+list+-+2018&utm_campaign=d59ce8ad7d-THE_INSIDER_2019_21_05_COPY_01&utm_medium=email&utm_term=0_72508cb181-d59ce8ad7d-98741733

The Verge (2019). Another convincing deep fake app goes viral prompting immediate privacy backlash. By Jon Porter. https://www.theverge.com/2019/9/2/20844338/zao-deepfake-app-movie-tv-show-face-replace-privacy-policy-concerns

The Verge (2018). IBM's Watson gave unsafe recommendations for treating cancer. By Angela Chen. https://www.theverge.com/2018/7/26/17619382/ibms-watson-cancer-ai-healthcare-science

UNCTAD (2019). Cybercrime legislation worldwide. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

UNESCO (1997). Culture and technology. A study. Prof. Andrew O. Urvebu, Doc./DEC/PRO-1997

Vougioukas K., Petridis, S. & Pantic, M. (2019). Realistic Speech-Driven Facial Animation with GANs. CoRR. https://arxiv.org/pdf/1906.06337.pdf

Weber, R. & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review. 32. 10.1016/j.clsr.2016.07.002.

West, S.M., Whittaker, M. & Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute. Retrieved from https://ainowinstitute.org/discriminatingsystems.html.

Wilhoit, K. & Hilt, S. (2015). The GasPot Experiment: Unexamined Perils in Using Gas-Tank-monitoring Systems. TrendLabs, 2015.

World Economic Forum (2019). 5G isn't just a buzzword. It will change the world. By CP Gurnani. https://www.weforum.org/agenda/2019/01/here-s-how-5g-will-revolutionize-the-digital-world

World Economic forum (2019). 3 ways AI will change the nature of cyber-attacks. William Dixon and Nicole Eagan. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

World Economic forum (2013). Norms and Values in Digital Media Shaping Solutions for a New Era. http://reports.weforum.org/norms-values-digital-media/wp-content/blogs.dir/16/mp/uploads/pages/files/norms-values-digital-media-final-170113.pdf

Zhang, Y. & Wildemuth, B. M. (2005). Qualitative Analysis of Content by. Analysis 1 (2):1-12.

ZDNet (2019). IoT security: Now dark web hackers are targeting internet-connected gas pumps. https://www.zdnet.com/article/iot-security-now-dark-web-hackers-are-targeting-internet-connected-gas-pumps/

ZDNet (2019). Japanese government plans to hack into citizens' IoT devices. By Catalin Cimpanu. https://www.zdnet.com/article/japanese-government-plans-to-hack-into-citizens-iot-devices/

ZDNet (2018). IoT security warning: Your hacked devices are being used for cybercrime says FBI. By Danny Palmer. https://www.zdnet.com/article/iot-security-warning-your-hacked-devices-are-being-used-for-cyber-crime-says-fbi/

Zeng, E. and Roesner, F. (2019). Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In the Proceedings of the 28th USENIX Security Symposium, August 14–16, 2019, Santa Clara, CA, USA 978-1-939133-06-9 https://www.usenix.org/system/files/sec19-zeng.pdf