Cyber Security, Cyber Hygiene or Cyber Fiction of our Time

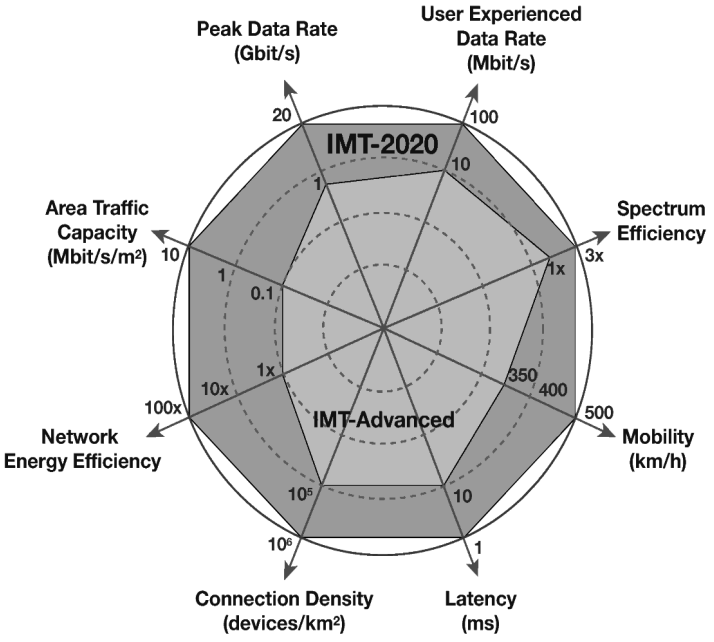
Tomasz Chomicki

1. Introduction

The moment we start thinking about how the world will look like in five, maybe ten years, the image of "The Matrix" or other sci-fi movies comes to mind. Is it possible to predict business processes and technologies that will become our everyday life in a few years? The answer is not simple, but in the technical literature you can read about what functions the future 5G or maybe even 6G network will have. Many pseudo-experts define the new, fifth-generation network as one that will give us extremely high speeds. This is just one of many parameters that only gives us a slight understanding of the technology. Standardization bodies ITU, International Telecommunications Union and 3rd Generation Partnership Project (3GPP) have defined in formal documents, technical parameters of the fifth-generation network. The most important of these are, first of all, 1 million devices per 1 km2, minimum latency of up to 1 millisecond, sending speed to the edge of the network is 10Gbps, about 10 times longer battery life, operation of the network when devices move at 500 km/h, and great reliability described as six nines (or 99.9999). The technical document describing these assumptions is IMT-2020 (Figure 1).

What does this mean for the common man or the well-educated lawyer? The set of these enigmatic technical parameters shows that mobile communication technology is born, which means no less than "the new Internet". The Internet, to which, according to the theory, we will connect all devices. The Internet that will be a kind of oxygen of our modern life. Questions may arise: So do these services already exist? Do the technologies that realize the above described standard and advertisements of the operators tell us that we live in this technological mature world? Well, no. The development of this new technology is still ahead of us. Is it possible to stop or delay it? Probably not, because even the times of COVID-19 pandemic show how indispensable reliable communication is for today's functioning. The essence of the new tomorrow are autonomous cars, drones delivering packages, or Da'Vinci medical robots, whose operators-doctors perform complex medical procedures. This is still the future,

Figure 15: Specification of the technical standard described in the ETSI IMT-2020 documents



Source: IMT-2020 - Wikipedia, <https://en.wikipedia.org/wiki/IMT-2020> 'accessed 29 March 2021'.

although not very distant; such projects can already be found on the map of international implementations.

A surgeon in China has already performed the world's first remote surgery using 5G technology, PC Mag reports, citing local news reports from China. The doctor from the southeastern province of Fujian used next-generation networks to control robotic arms at a location 30 miles away. The operation was made possible by the extremely low latency of 5G..[1]

1 China Performs First 5G Remote Surgery, <www.pcmag.com/news/china-performs-first-5g-remote-surgery> accessed 29 March 2021.

2. *Cybersecurity*

The great array of technological challenges is at the same time a rising tide of cyber threats. Analyses of the digital crimes occurring in our country made by cybersecurity companies indicate that the number and intensity of cyber attacks are invariably increasing. In 2019, DDoS attacks (those that overloaded websites) and ransomware attacks (software that encrypts for ransom) were the main problems in Polish companies. Organizations in Poland also noted data destruction, leakage or damage primarily due to malware infection. According to experts' analysis, the number of reported incidents after ransomware attacks increased by 20 % and the number of so-called botnets, which, among other things, spread other malware or sent spam, increased by 28 %. Analysts also observed an increase in the installation of special programs to secretly generate cryptocurrencies .[2] The number of tools that embed special scripts on websites and are used to steal financial data also increased by 200 %. In addition, the number of banking trojans that steal customers' payment data has increased in 2019.

We could also see interesting developments in 2020, when the COVID-19 pandemic took hold for good. Bitdefender's survey of IT staff published in July shows intimidating data - the number of IT security incidents has increased dramatically. The attacks that dominate have become whailing - a fishing attack on decision-making personnel (26 %) and ransmomeware (22 %). According to the survey described above, criminals were hitting financial institutions (43 %), healthcare (34 %) and the public sector with full force. However, the imagination of criminals knows no bounds.

From the information published on 10.2.2020 in the portal Niebezpiecznik, we can learn about an "interesting" and at the same time disturbing incident that could threaten the life and health of several thousand people, which was reported by a sheriff from Florida. "On Friday, someone broke into the water supply in Pinellas County and increased the concentration of sodium hydroxide a hundred times."[3]. Sodium hydroxide is used by Florida water utilities to control the acidity of water. The burglar managed to influence its concentration, which he altered to a value of 11,000 ppm, but luckily a waterworks employee noticed the change and

2 Check Point Data, 'Raport Cyberbezpieczeństwa' (2020).

3 Piotr Konieczny, 'Haker zatruł wodę w wociągach, przez Internet' (Niebezpiecznik.pl, 10 Fabruary 2021) <https://niebezpiecznik.pl/post/ktos-przez-internet-zatrul-wode-w-wodociagach//> accessed 31 March 2021.

promptly restored the correct parameters. Authorities reassure that even if the employee had not manually restored the settings, other safety systems would have worked, including one that monitors the pH of the water. They also add that the water with the changed parameters would be delivered to the residents the next day at the earliest.[4]

What does all this mean? The answer is quite simple: there is no longer a space in which we can feel safe. Critical infrastructure protection, including industrial networks, is becoming an important part of our security and thus a new area for deeper analysis by legal teams.

With this in mind, on December 11, 2020, a political agreement was reached at the European level to establish a European Cyber Security Competence Centre and Network. The seat of the Centre became Bucharest. This is not the only solution - in other countries there is also a heated debate on the law related to the implementation of new regulations related to cyber security. On the eve, when we stand at the stage of implementing new technologies, it is worth to stop and think about what to improve to avoid these threats and what systemic changes to introduce to minimize the effects of attacks and threats. Naive people may say that the law and emerging regulations will protect us. However, experts make it clear - the person responsible for protecting our security is us. Here are some rules that you should always pay attention to:

1) download and use applications always from authorized sources (stores like Play or Apple Store);
2) making regular copies of data in an independent cloud infrastructure;
3) active remote deletion function on the device (e.g. phone, tablet);
4) use of anti-virus systems, or applications with ongoing code analysis type MTD;
5) limiting trust in unknown links and attachments sent via email;
6) securing devices with password or biometric systems;
7) using unique passwords for each online account;
8) use of authentication;
9) keeping system software up to date;
10) using VPN services on open Wi-Fi networks;
11) separating professional and private work environments (containerization);

4 Andy Greenberg, 'A Hacker Tried to Poison a Florida City's Water Supply, Officials Say' (Wired.com, 2 August 2021) <www.wired.com/story/oldsmar-florida-water-utility-hack/> accessed 29 March 2021.

12) verifying the sender (carefully checking the email address) whenever you receive information about an amazing bargain, promotion, or win; messages sometimes contain minor character details, i.e., substituting the letter L for a capital I;
13) Paying attention to text messages, as it is not uncommon to receive shipping manipulation or impersonation of a store or contractor;
14) avoid using seemingly "free" applications or services (because they are not always free).

Is it enough? Of course not, but it will significantly reduce potential problems. Lack of knowledge does not release us from the consequences, and lawyers from responsibility, e.g. disciplinary. We must learn to build knowledge about cyber dangers, although Poles have more and more knowledge and awareness of threats and consequences of identity theft.

According to the study, 53 % of respondents are concerned about the security of data, 20 % of them used or use the services that provide data protection online[5]. According to a report prepared by the Insurance Information Institute (iii.org), identity theft continues to challenge consumers as criminals develop new mechanisms to commit fraud.

According to the 2019 Identity Fraud Survey from Javelin Strategy & Research, the number of consumers who were victims of identity fraud dropped to 14.4 million in 2018, down from a record 16.7 million in 2017. However, identity fraud victims bore a greater financial burden in 2018: 3.3 million, nearly triple the number in 2016. What's more, fraud costs more than doubled between 2016 and 2018 to $1.7 billion. Fraud losses on new accounts have also increased slightly, and criminals have begun to focus on a variety of financial accounts, such as loyalty and bonus programs and retirement accounts. In addition, criminals are becoming adept at thwarting authentication processes, particularly in seizing cell phone accounts. The number of these takeovers has nearly doubled to 680. The Consumer Sentinel Network, maintained by the Federal Trade Commission (FTC), tracks consumer fraud and identity theft complaints filed with federal, state and local law enforcement agencies and private organizations. Of the 3.2 million identity theft and fraud reports received in 2019. 1.7 million were fraud-related, about 900,000 were other consumer complaints, and about 651,000 were identity theft reports. Of the 1.7 million

5 According to research carried out by Credit Information Bureau – BIK, 'Cybersecurity of Poles 2020' (Biuro prasowe Grupy BIK, 26 January 2021) <https://media.bik.pl/informacje-prasowe/637189/dobre-praktyki-ochrony-danych-osobowych> accessed 31 March 2021.

fraud cases, 23 % of the reported money was lost. In 2019, consumers reported losing more than $1.9 billion due to fraud complaints, an increase of $293 million from 2018. Within the fraud category, impersonation fraud was the most frequently reported and ranked first among the top 10 fraud categories identified by the FTC. They resulted in losses of $667 million.[6]

The question arises why as many as 20 % of the respondents admitted that they do not protect their phone with a password at all, and 25 % never change the password they have? Internet users confirmed that antivirus programs are most often installed on computers (87 %), while 63 % use them on phones and tablets. Therefore, despite the growing awareness of threats, it is still necessary to intensively educate customers about cyber threats. KasperskyLab notes a 242 percent year-over-year increase in brute force attacks against protocols that support remote access to devices. Because a mobile device is not just a device from which we make phone calls, we are also increasingly "emailing," "banking" and working remotely. We must, therefore, almost re-learn the principles of cyber security.

3. *Cybers Hygiene – A Security Package*

The European Commission has unveiled a new cyber security package and a comprehensive set of rules for digital services operating in the EU. One of the postulates is the continuous deepening of knowledge from already well-established information websites like Niebezpiecznik, Zaufana Trzecia Strona, Rasmussen.edu, Itseccentral, Digitalguardian, Blog.feedspot or at technology seminars of various solution vendors. The governments of various countries are trying to talk a lot about it, organizing a wide range of courses and trainings and publishing more and more new information. It is worth realizing a great example shown by the Panoptykon Foundation. It shows what information can be obtained by connecting a smartphone to the network. As mentioned earlier, end devices, in order to ensure data security process, often connect to "cloud" services, creating copies of data, i.e. photos, recordings, contacts. It is worth taking care to secure this access with a strong password and carefully review the data storage policy and save very sensitive data on your own hardware.

---

6 See: Insurance Information Institute, 'Facts + Statistics: Identity theft and cybercrime' (iii.org) <www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> accessed 29 March 2021.

Another important piece of advice for users is to uninstall applications that are not being used, and to look carefully at access requests, e.g. if a flashlight application requests access to contacts it is a sign that the application is suspicious, and its developers may not necessarily have honest intentions. We know that the state institutions have the right to demand information about us from telecom operators, providing it to the appropriate services (e.g. phone records, location data). Operators, in accordance with generally applicable law, are obliged to keep such data for at least 12 months.

State authorities have also at their disposal solutions that enable partial or total surveillance. Recently there has been a lot of publicity about software from Israeli company NSO Group called Pegasus. The application allows to "infect" a device and in the next step to take full control over it, processing information, eavesdropping on messages, listening to conversations, collecting location data or listening to sounds coming from the environment without user's knowledge. According to research by Citizen Lab, the software has been purchased by at least 45 countries in the past two years, including Mexico, France, the United Kingdom and Switzerland, among others.[7]

4. AI and ML vs Internet Security

In the world of LegalTech, AI and ML have to be added to the world of cyber, as potentially risky situations can also occur with the tools they cover.

An interesting story involves Robert Julian-Borchak of Detroit, who was arrested on the basis of faulty facial recognition by a police algorithm and, according to the media, spent thirty hours in custody while completely innocent. When Williams was summoned by police, he was automatically screened by cameras, and the image-processing analytics that reside there concluded that he was the person seen in the 2018 robbery video.

This case is widely considered to be the first AI/ML error of its kind in history. This raises the question of whether algorithms can therefore be trusted and whether the technology is necessary to function. Data from

7 Bill Marczak and others, 'Hide and seek, Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (citizenlab.ca, 18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 29 March 2021.

the IoT report is presented below. According to research presented by Strategy Analytics Research services of 2019, the number of devices using the Internet will grow rapidly, and no longer only smartphones, tablets, TVs will be connected to the network, but autonomous vehicles, "smart" home devices, industrial IoT, etc. The scale of various vulnerabilities is constantly growing, so machine learning algorithms and artificial intelligence solutions will also have to be used to counter them.

As an interesting note, Researchers from Monash University and the Indian Institute of Technology Ropar have developed machine learning algorithms capable of detecting fake videos, for example, during video conferencing conducted by the ZOOM app. The researchers applied over-the-top analysis and search for differences between video and audio, breaking images into fragments and analyzing the unsynchronized differences, searching for details in unnatural facial movements, lips, or sound disturbances.[8]

According to the EC, the expenses related to the development of artificial intelligence in the public and private sector will amount to about 20 billion euros per year in the time forecast 2020-2030. An important indicator on which systems are to be built is trust, which will force a change in current regulations. It is proposed that in selected sectors, such as medicine or transport, digital systems created using artificial intelligence and machine learning algorithms should always be transparent, traceable and supervised by a human. Thus, the role of law and lawyers who will be able to work in interdisciplinary teams that understand the technology and use the tools is slowly becoming a requirement rather than a direction for a distant transformation.

5. The Forecast of the Future

In the White Papers[9] prepared by Samsung, we can read that applications using wireless communication, are expanding from connecting people to

8 See: Monash University, 'Deepfakes detect Zoom-bombing culprits' (monash.edu, 25 January 2021) <www.monash.edu/it/about-us/news-and-events/latest/articles/2021/deepfakes-detect-zoom-bombing-culprits> accessed 29 March 2021.

9 See: Samsung, 'Samsung's 6G White Paper Lays Out the Company's Vision for the Next Generation of Communications Technology' (Samsung Newsroom, 14 July 2020) <https://news.samsung.com/global/samsungs-6g-white-paper-lays-out-the-companys-vision-for-the-next-generation-of-communications-technology> accessed 29 March 2021.

connecting things. Wireless communication is becoming an important part of social infrastructure and people's daily lives. In addition, today's exponential growth of advanced technologies such as artificial intelligence (AI), robotics, and automation will cause an unprecedented paradigm shift in wireless communication. These circumstances lead to four major megatrends moving toward 6G: connected machines, the use of AI in wireless communications, the openness of mobile communications, and increased contribution to social goals. The number of connected devices is expected to reach 500 billion by 2030, about 59 times the projected world population by then (8.5 billion). Mobile devices will take many forms, such as augmented reality (AR) glasses, virtual reality (VR) headsets and hologram devices. Increasingly, machines will need to be connected via wireless communications. Examples of connected machines include vehicles, robots, drones, home appliances, displays, smart sensors installed in various pieces of infrastructure, construction machinery, and factory equipment. As the number of machines increases exponentially, data will become the dominant user of 6G connectivity.

Looking at the history of wireless communications, the technologies were developed with the premise of developing services targeted at people. That was and is their primary use. In 5G, machines and technology development have also been taken into account when defining requirements and technology development. It can be expected that new technologies, such as 6G, will need to be developed specifically to connect hundreds of billions of machines. To provide initial insight into the target performance required, the perceptual abilities of humans and machines were compared. For example, the ability of the human eye is limited to a maximum resolution of 1/150° and a viewing angle of 200° in azimuth and 130° in zenith. On the other hand, machine vision capabilities are highly developed and the elimination of such limitations occurs because it can use multiple cameras with different functions. Given the strong capabilities of machines, the performance requirements of a 6G system can be very high for relevant service scenarios that are still unknown today. In recent years, the development of AI has penetrated various fields such as finance, healthcare, manufacturing, industry, and wireless communication systems. The application of AI in wireless communications has the potential to increase efficiency improvements and reduce capital expenditures (CAPEX) and operating expenditures (OPEX).

The authors of the paper[10] show by example that AI can improve the efficiency of data relaying operations by taking into account the dynamic geographic deployment of networks and environments, and in a new way optimize network planning that includes the location of stations baseband (BS) and network termination. The advantages that will be achieved include reduced network energy consumption and prediction, detection and repair of network anomalies. In the case of 6G, the realization that AI technologies are available for practical applications can help develop a system that takes into account the possibility of embedding AI in the various entities that make up the wireless network and services. The vast amount of data associated with hundreds of billions of connected machines and people will need to be collected and used in 6G systems. Including AI early in the concept and technology development for 6G will therefore provide more opportunities to use AI to improve the overall network performance in terms of efficiency, cost, and ability to provide various services.

10 *ibid.*