Introduction: Safety and Security

This chapter explores the meaning of, and ways of managing and responding to, issues surrounding safety and security in digital systems and how these need to be considered from a technical perspective when trying to understand knowledge landscapes. Digital health information has a range of risks and challenges as seen in earlier chapters in this book: here we discuss risks associated with the development and use of the Internet of Things (IoT) and in particular the Internet of Medical Things (IoMT), devices and systems increasingly seen in healthcare. The chapter draws on

D. Simunic (✉)
Wireless communications, Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia
e-mail: dina.simunic@fer.hr

P. Pale
Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia
the authors’ disciplinary expertise in electrical engineering and computing. As with the other two chapters in this section, it offers some practical ways forward in regard to managing risks.

In spite of the fact that many languages do not in practice differentiate between ‘safety’ and ‘security’, it is crucial that we clarify their difference. This is especially important in the context of information and communications technologies (ICT) and their role in health systems. In broad terms, ‘safety’ covers events caused by the environment, technology or unintentional accidents caused by people, while security relates to incidents intentionally caused by people (M-W Dict, safety 2020a). For example, a user may accidentally erase a digital file and in most cases it will be possible to recover the content. This can also happen through disc malfunction, computer malfunction, water spillage, and so on. These unintentional events are covered by the term ‘safety’ and procedures that help avoid them. In contrast, a malicious attack by a hacker can erase a file on purpose and in such a way that it cannot be recovered by any means (except if backed-up): such attacks can be prevented by appropriate ‘security’ measures (M-W Dict, security 2020b).

The IoT gathers pace across many societies and, related to IoT wireless security, surveys show that a high percentage (39%) of respondents think that it ‘remains a huge concern’ (Weissman 2015) as is amply demonstrated by the recent fallout over the use of Facebook data. The European Union seeks to develop a legal solution to this problem, at least in regard to key concerns which are to be addressed through new provisions in the General Data Protection Regulation (e.g. developing privacy by design) (GDPR 2016). However, policing and enforcing these policies calls for considerable financial and human resources that have to be effectively planned and harmonized at all the levels, involving both strategic and tactical domains. While ‘pure’ IoT sensors will in general be oriented mostly to the broad human environment, the IoMT system (Marr 2018) is built on improved precision to facilitate effective interaction between medical expertise and the human body. An example would be remote health monitoring for illness, diagnostics and prevention. Another example is remote surgery that enables precision medical care outside a shared geographical location for the medical expert and patient. Unfortunately,
all these devices and their communication systems and structures, enabling their ‘connectivity’, can be extremely vulnerable.

As a result, the possibility of individuals or organizations hacking the IoMT could have a significant impact on the health of an individual or even of a wider population, raising crucial ethical, legal and technological issues. In this context, a multi-stakeholder discussion between the four most important parties—citizens, medical professionals, government and private industry—on the governance of the ‘smart human society’ and its related connectivity has to be pursued, aiming to create a consensus over the meaning of connectivity security. The most powerful defence against and prevention of abuse is to educate users, especially younger people, about the possible risks and threats they may have to deal with. As noted above, this chapter explores the dangers, risks and threats in the existing and near-future healthcare environments, related to digital systems.

**Some Basic Principles**

Measures to achieve safety are based on three pillars: (i) backing-up data at two or several remote locations and in different types of media; (ii) building redundancy into solutions, systems and infrastructures; and (iii) closely monitoring systems, components and activities and promptly alerting users/others about risk-related events or discrepancies. However, measures to achieve desired security level are much more complex.

Security depends on three different stakeholders: (a) designers, developers and producers, (b) solution and maintenance providers and (c) end users.

(a) Designers of devices and systems are focused on functionality, flexibility, ease of use and cost-effectiveness. These are in direct opposition to security, because security and comfort are reversely proportional—the more a system is secure, the more cumbersome and slower it is to use it.

Developers should be given time, resources and knowledge to implement a ‘security by design’ concept. Industry should be forced by
regulation and standards to deliver safe and secure devices from the beginning. For example, every device delivered should have a globally unique identifier and authentication token(s).

(b) Those who design, install and maintain custom solutions should have an in-depth knowledge of both ICT and a client’s local domain needs and processes. They are struggling in particular with equilibrium of usability and security. They need to monitor their devices and networks for any sign of vulnerability or accident and quickly respond to them. Especially they need to patch, update and replace software or their components in order to reduce their vulnerability.

(c) Users also have the responsibility to purchase secure products, to wisely choose competent consultants and trainers, to update software and licenses, to promptly respond to requests and instructions from technical personnel and above all not to share their credentials with anyone. They are also responsible for their own awareness and competence in computer security.

While social media reports the growth of hacking and cybercrime, many users neglect more common issues involving damage to data and/or financial risk which are in fact due to safety incidents. Quite a significant proportion of information-related safety incidents are caused unintentionally by people, due to their lack of awareness or competence or mere mistakes.

Security incidents in contrast are believed to be predominantly caused by hackers and other malicious sources outside of any organization. IBM defines an attack as ‘malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself’. However, in reality the majority of attacks (c.60%) are executed by insiders: current or recent ex-employees (IBM X-Force Cyber Security Index 2016). IBM X-Force studies, monitors and reports on the latest threat trends. The first goal of the X-Force’s activity is to understand the threats in order to provide a higher security content to its customers but also to warn customers and the general public about emerging and
critical threats. It is also important to keep in mind the observation that the ‘typical hackers sit inside a network for 254 days before they make themselves known’ (Joy 2019).

Compared to 2015, when the healthcare sector was globally most likely to be hit by data breaches, by 2019 the sector was the tenth most targeted industry, accounting for 3% of all attacks within the top ten sectors (IBM X-Force Threat Intelligence Index 2020). The most usual motivation of cybercriminals is financial with the aim to steal and sell medical records, or to disrupt activity of hospitals and nursing home networks for ransom. In the summer of 2018, what was known as ‘Ryuk’ attacks started to appear in a public malware repository with the aim of targeting enterprise environments. In 2019 Ryuk attacks in the USA demanded more than $7.5 billion from at least 966 government agencies (113 state and municipal governments and agencies, 764 healthcare providers and 89 universities, colleges and school districts, with operations at up to 1233 individual schools potentially affected) (Taylor 2019). Thus, the healthcare sector has a clear interest in improving security within current and emerging medical systems. The Herjavec Group in its 2019 Official Annual Cybercrime Report (Herjavec 2020) estimates that healthcare companies will experience approximately $6 trillion in damages (e.g. data loss) in 2021.

Safety and Security Navigating Knowledge Landscapes

There is a whole range of information safety and security risks, threats and vulnerabilities, while navigating knowledge landscape [Svalastog et al. 2020]. Most commonly these relate to outdated, incomplete, damaged, poorly transformed, inadequately stored, poorly described or inappropriately structured data. Then there is user’s inability to find the source of information, root data, evaluate trustworthiness, validate, verify, attribute or simply identify who said something, to whom, why and in which context. Finally, there are cases of intentional misinformation, lies, spin, fake news, deep fake videos, plagiarisms and logic violations.
Each of these problems deserves at least a whole chapter. The above-mentioned problems have one common denominator: the individual user as the one most likely to encounter the problem. Thus, intuitively it is often hoped that if effective and trustworthy machines were the source of data, we would have no or much less information security problems.

The Internet of Things (IoT)

In 2018 more than 8.4 billion ‘things’ joined the ‘Internet of Things’ (IoT), making the total worldwide number of active IoT devices in 2019 to 26.66 billion [Statista 2019]. Projections say that by 2025 there will be 75 billion of IoT devices worldwide.

Every second, 127 new devices are connected to the Internet. The majority of healthcare providers have increasingly become engaged with IoT in the medical world, hence referred as the ‘Internet of Medical Things’ or sometimes the ‘Internet of Health Things’ (IoHT). By 2020, 40% of all IoT devices will be used in the healthcare industry. Estimates from Deloitte (Deloitte 2019) are that the global IoT market will reach $7.1 trillion and within it the global IoMT market a ‘$158 billion valuation in 2022, up from $41 billion in 2017’. Thus, all the theories of ‘big data’ hold (Mayer-Schönberger and Cukier 2013).

Internet of Medical Things (IoMT)

The IoT changes almost any object into a source of information (‘thing’) that can be used for further processing. Since IoMT comprises only devices that are used in medical assistance, IoMT is clearly a subgroup of IoT that covers almost all activities of human society.

This means that the IoMT consists of medical devices, software applications, health systems and services connected by a communication infrastructure. The IoMT ecosystem is very special due to its enabling role of remote patient monitoring with sensor-based tools and the possibility of coupling gathered patient data with patient information. The
rise of IoMT is driven by ‘an increase in the number of connected medical devices that are able to generate, collect, analyze or transmit health data or images and connect to healthcare provider networks, transmitting data to either a cloud repository or internal servers’, as noted by Deloitte (2019).

Ultimately, this connectivity between medical devices and sensors is streamlining clinical workflow management and leading to an overall improvement in patient care, both inside care facility walls and in remote locations.

The following IoMT examples show the full spectrum of existing applications that is growing every day. One of the most important features of the current IoMT world is the possibility of tracking in the operational area of healthcare, where, for example, tags are used to prevent baby theft or their misplacement (Centrak 2019). The IoMT is also used in regard to smart beds with the purpose of monitoring vital functions and preventing common patient problems such as bedsores (Wellsensevu 2019). Some applications (e.g. AutoBed by GE Healthcare) have helped to reduce emergency waiting times in New York hospitals by 50%. Some other applications take care of patient medications and blood samples (e.g. SensorMetrix 2019) to ensure that they are exposed to a required accurate temperature. No less important is a system of remote patient monitoring by sending an alert if the patient does not move or if he/she falls (e.g. Zanthion 2019). Even in an intensive care unit in a hospital, IoMT enables the responsible senior doctor on duty to have an immediate notification of any change in the vital parameters of his/her patient with all the required details without being close by. This is also the case while a doctor is ‘on-call-duty’, that is, not in the hospital (Binkowski 2016).

The IoMT contributes to a network of connected medical devices, which enables patients and healthcare providers access to data, and thus also to important information. In the information and communication society, there is a difference, as noted in other chapters, between data as information and how this can be processed to form tractable forms of knowledge. Data are unprocessed facts or figures, whereas knowledge represents the processed data. Furthermore, data doesn’t depend on information, whereas the knowledge depends on data. Actually, data represent a single unit, whereas knowledge is based on data that carries news and
meaning. For example, in IoMT, the ‘Medical Thing’ (MT) can be a medication, a wheelchair, a heart monitor or any sensor on or in the human body (Mole 2018; Meola 2020; Tung et al. 2015). Sometimes, when it is really of urgent importance to get a complete ‘picture’ of the patient and thus have a full and continuous flow of patient data, as for example in the smart city scenario, all the sensors and devices (so-called patient ‘body area network(s)’, BAN(s)) are connected to an internal hub. In this case, the hub of the patient can be considered as MT (Hammi et al. 2017). The main aim of IoMT is to increase the quality of life for all the citizens, but especially for the elderly and disabled, who often require specially designed healthcare (Chen et al. 2017). At the same time, the IoMT makes possible preventive care and improvement thereby in patient outcomes. In addition, it opens entirely new space for medicine and medical personnel given it is possible to identify higher health risk individuals in patient populations. This latter is the objective in the near future, where it is expected that IoMT systems will utilize not only sophisticated sensor technology and classical wireless communications systems but also artificial intelligence and novel wireless communications systems, as planned in the quickly growing smart cities (United Nations Department of Economic and Social Affairs 2018; European Smart Cities 2015; EC 2020). Finally, the IoMT makes the costs of healthcare lower due to the efficient management of medical assets.

The World Health Organization (WHO) acknowledges the arrival and application of new technologies by organizing regularly WHO Global Fora on Medical Devices (WHO 2019). While many are working towards ease of workflows and transformation of healthcare in practice, the IoMT is vulnerable to various cybersecurity threats as all the other ICTs. Unfortunately, the ICT in the medical sector (mostly IoMT, connected to the networks) is in general less protected, because of the wish and the need for simple and easy-to-use systems for non-ICT personnel and/or patients (Lynch and Farrington 2018).

It seems that IoMT already plays an important role, but it will play an even more important role in the near future, since the majority of relevant data can be collected via IoMT external to clinics. Recent studies (e.g. Pandor et al. 2015) show that some European clinics are piloting a system to remotely monitor patients to reduce re-admission rates. This
could be very important in monitoring chronic conditions, shortening hospital stays and improving medication adherence.

Mobile health (mHealth), as a sub-area of eHealth, covers medical and public health practice supported by mobile devices (see also Chap. 10). mHealth uses applications and sensors connected to mobile communication devices for monitoring health and well-being of the individuals, that is, mHealth uses IoMT for remote monitoring of health status. This combination enables patients to actively monitor and manage their own health and, thus, a higher quality of life due to fewer required visits to a medical doctor or to a hospital. On the other hand, mHealth also enables healthcare professionals more efficient treatment of patients. As a consequence, patients are getting healthcare of a higher quality enabling them longer life, with less burden on the healthcare system. Consequently, the more precise determination of a patient’s current health status opens the door to the possibility of providing tailored health recommendations and prediction of potential future issues (EC 2004). Examples of devices used in remote monitoring include glucometers, electrocardiography devices, wearable healthcare devices, smart pill boxes, insole sensors, smartwatch applications, activity trackers of patients’ ambulatory abilities after surgery and fall detection devices. All these devices generate patient data that enable precious and precise clinical care external to clinics, often the best place for such a chronic patient, that is, in the home (such as a medically ‘smart’ home). Thus, the aim of the IoMT concept is to enable longer lives of a higher quality for all, allowing significantly shorter patient stays in hospital, enabling at the same time more efficient use of the existing health system for all users.

In spite of the increasing enthusiasm with the dawn of the ongoing IoMT revolution, society should not fall into the trap of believing that IoMT is a completely secure and safe system. On the contrary, as noted above, IoT and particularly IoMT actually create a completely new realm of information security problems.
IoT Threats, Vulnerabilities, Risks and Mitigations

Today a global awareness exists of the many possible threats to systems, especially to medical systems that are connected to the information and communication infrastructure, as is the case of the IoMT. Therefore, it is necessary to understand these threats. The definition of threat in Merriam-Webster dictionary is that it is an event with the potential to have a negative impact (M-W Dict, threat 2020c). In the context of IoMT, three main types of threats can have a negative impact on its operation:

(a) Natural threats (e.g. floods, hurricanes, earthquake, COVID-19)
(b) Unintentional threats (by a mistake of an employee who accidentally disrupts an IoMT)
(c) Intentional threats (by a virus arriving through exposure to automated attacks)

In this sense, our discussion on safety and security from the beginning of the chapter is related to unintentional threats and intentional threats, respectively.

The Merriam-Webster dictionary defines vulnerability as a quality of the environment that allows a realization of the threat [M-W Dict, vulnerability 2020d]. In our case, it means that it is a known weakness of the IoMT that can be exploited by hackers and succeed in their attack(s).

According to the Merriam-Webster dictionary, risk is the potential for loss or damage when a threat exploits a vulnerability. In the IoMT case, risks include loss of privacy in terms of a personal medical record or any other data and loss of connection that enables transfer from the patient to the medical doctor.

Therefore, the threat is outside of anyone’s control. However, the weak points of the system can be assessed and the action plan for minimization of the impact on the system can be developed. If such a plan is not developed, this creates vulnerability. The risk is then, for example, the loss of a personal medical record. However, the risk can be prevented (or
mitigated, if the prevention is not possible) by identifying potential threats and addressing vulnerabilities, that is, by developing a risk mitigation plan.

The IoMT consists of hardware and software systems, which means that the systems are vulnerable to a diversity of threats. As explained above, system functionality is based on understanding both: threats and vulnerabilities. In this game of balancing threats and ensuring safe and secure systems, three options are possible:

1. The system is not protected enough (so-called under protection).
2. The system is just-enough protected (optimum protection).
3. The system is over-protected (over protection).

Of all the options, the third option takes too many resources (often system memory and users’ time), so the users may well be minded to disregard it. Therefore, the system has to be designed more towards the direction of providing optimum protection.

The fact that the IoMT encompasses many devices (as part of the hardware) and programs (as part of the software) opens the door to a high number of possible threats. The decision that has to be taken is whether every potential threat and corresponding vulnerability will be treated separately, or as a ‘threat bulk’. One of the further procedures is based on understanding the potential vulnerabilities without a specific corresponding threat (e.g. media failure). The complete risk assessment process comprises a detailed approach to both the views; it is an intermix of threat and vulnerability of the digital asset.

In general, risk assessment is oriented towards the identification of hazards. The risk assessment tries to understand who/what is a possible cause, who/what is a possible ‘victim’ and how can the ‘victim’ be harmed.

In the case of IoMT, the risk assessment is oriented to the environmental, site-support, physical and technical issues that are given below with examples.

Environmental issues of the IoMT security are reflected in any undesirable environmental activity, being a hazard (Halkos and Zisiadou 2018), such as lightning, or sprinkler activation. The other environ-
mental concerns include, inter alia, fire, tsunami, earthquake, flood, lightning, smoke, insects, dust, volcanic eruption, severe weather, chemical fumes, rodents, sprinkler activation, water leakage, vibration, electromagnetic interference, electrostatic discharge, explosion and nuclear disaster.

**Site-support** issues are related to the site aspects, such as electrical power or air conditioning. The other physical nature encompasses personnel action, such as vandalism or theft. A more detailed list comprises the following: site-support concerns include power outage, extreme or unstable humidity, extreme or unstable temperatures, facility inaccessibility, unsafe environment, electrical noise, improper maintenance, personnel unavailability, inappropriate fire suppression, inability to cut power during fire or flood, inappropriate trash disposal or telephone failure.

**Physical** issues (GlobalSecurity 2001) of the IoMT security encompass personnel action, such as vandalism or theft. They also include unauthorized facility access, sabotage, extortion, war, spillage or droppage, magnets or magnetic tools, collision, trip hazards, improper transportation, labour unrest, fire hazard, terrorism or improper mounting or storage of the equipment.

**Technical** concerns include specific events as a part of the technical system, and they include both the design and the use of the system. The fact that most of the technical devices and systems are typically thoroughly tested before arriving on the market is the basis for very few real threats. Interestingly, the most important threats are untrained users. The definition of ‘untrained user’ includes all the employees in an organization, who can, for example, typically click on a phishing email (Morin 2016). Therefore, it can be stated that the technical security concerns include improper operation, improper hardware and/or software configuration, improper or inadequate procedure, unauthorized software or hardware or their modification (Meidan et al. 2020), unauthorized logical access, unauthorized software duplication, unsanctioned use or exceeding licensing, malfeasance, malicious software, hardware and/or software error or failure related to functionality and/or security, communications error, data entry error, media failure, accidental software and/or data modification and/or deletion, over- or
under-classification, repudiation, message flooding, electronic emanations, accidental data disclosure, message playback, data remanence, geo-location, masquerading, object reuse, line tapping and communications failure or overload. These are generic concerns, but they are often used in the system design. System-specific vulnerabilities can be treated only by automated tools that identify operating system-, application- and middle-ware-specific vulnerabilities.

All the risk assessments must be evaluated for the specific system, with extensive calculation of the probability of their occurrence, projected event impact and mitigation costs.

The US FDA recently issued (1 October 2019) ‘URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication’, with the conclusion that there are no any currently confirmed adverse events related to the given vulnerabilities, but the software to exploit these vulnerabilities is already publicly available. Therefore, ‘these vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function’ [FDA 2019].

IoT Risks and Mitigation Techniques for the Special Case of IoMT

Even though the IoT has to provide a constant seamless connection, meaning that the security should always satisfy the highest standards, the special case of IoMT in the world of IoT has even higher security demands. This is the case, because the IoMT is directly related to human health and any kind of security compromise, especially in the case of connection of, for example, a breathing machine, can possibly lead instantly to a fatality for the individual under treatment. Thus, here are identified five IoT risks, together with the mitigation techniques for the risks removal. The identified risks with their description and mitigation are
device discovery; processes of identification, authentication and authorization; IoT botnets, DDoS attacks and IoT and IoMT passwords; encryption and network security.

Let us start with the first risk and its mitigation.

1. Device Discovery

In a nutshell, there should be no IoMT powered and attached to the network that is not known and not included in tracking, updating and checking. Devices no longer used should be powered down and disconnected from the communication network. Their decommission needs to be promptly communicated with all systems they were exchanging data with.

The very first task related to the IoMT risk and mitigation is device discovery. For example, port scanning, protocol analysis and other detection techniques support determination of the connected devices to a specific network. Examples are free tools, like Nmap (Nmap 2019), Shodan (Shodan 2019) and Masscan (Masscan 2019). After understanding which devices are connected, it is necessary to know the purpose of all the connected devices in order to distinguish between connected devices with approval and devices without approval with a possible malicious intention. If some of the devices from the approved list are stolen or lost, action has to be taken in the form of remote wiping or disabling their connectivity. This is very important, because sometimes an old login to a connected seemingly unimportant device like a refrigerator or a printer that should have been wiped long ago can be misused by a hacker and it can cause a data breach of the whole system.

Device Tracking and Updating

The core of security practices embedded in sound security policy is updating and patching devices. ‘Updating’ is the process of replacing a device’s software with a newer version. ‘Patching’ is the process where only a part of software is replaced with a newer component. The IoMT patching is very specific, because of the dispersed nature of the IoMT system. The
other good reason for the IoMT patching is the critical nature of the IoMT systems. The IoMT is very sensitive to the use of insecure or outdated software and firmware. Also, it is very sensitive to a system failure that can appear due to a possible corrupted update. Therefore, as suggested previously, all the devices should be listed in the asset registers, together with the versions of software and hardware. The updates should be tracked in relation to their publishing date, with the decision of the personnel dealing with the system operation whether the update will be automatic or on a periodic schedule. The IoMT devices should be tracked when retired to overcome and deny any kind of malicious activity.

2. Processes of identification, authentication and authorization

In order to prevent an unauthorized device to replace a legal device or a completely new device to penetrate the landscape, measures need to be taken. They should uniquely identify an IoMT device and assign it a predefined, strict set of authorizations.

**Identification** is a process of understanding the context of future interoperation by sending a mutually known identifier for a person or device, typically a username or device ID. According to Turner (2016), **authentication** is an electronic process for confirming or verifying the identity of an individual or device. **Authorization** is the process of giving the access to the individuals or devices with the confirmed identity.

In practice this means that any device included in the IoMT should have a unique identifier (e.g. in the form of a device ID). According to AIOTI (2018), an identifier is a pattern to uniquely identify a single entity (an instance identifier) or a class of entities (i.e. type identifier) within a specific context. The authentication is based on the user’s use of one or several credentials based on any one or combination of three possible factors: what they have (a device-token), what they are (biometrics: fingerprint, retina scan, etc.) or what they know (a password, an answer, an algorithm or a combination). While humans can use any of these three authentications, the devices can use only the knowledge-based technology. However, these passwords or algorithms can be much more complex than those for humans.
After the successful identification and authentication, the next step is the authorization. The authorization enables the exact operational management of the devices, that is, which devices are to be let in to work in the IoMT environment, what they can access and to whom they can communicate.

The first priority is to allow the IoMT devices to access only what is necessary for their full operation. The second priority is to change passwords in all devices that come with the factory-installed default passwords. The IoMT risks can be combatted by the strong passwords and by the two- or three-layered authentication, if we apply, for example, the device-token, fingerprint and a password. In principle, using cryptographic hardware together with digital certificates or biometrics issued from a trusted public key infrastructure (PKI) is the best solution. For the purpose of adjusting operations of the digital system for a specific need, the user or foreign device usually has initially to be identified, authenticated and authorized.

The Mirai attack in 2016 started with the connected cameras that had factory-default or hardcoded passwords, usually 1 from the 60 username-password combinations. Thus, it is of the utmost importance to understand that it is obligatory to update passwords by using strong passphrases or passwords. Manufacturers should also require changing default credentials before putting device into the function. Actually, manufacturers should be required to avoid using default passwords by any means.

3. IoT botnets, DDoS attacks and passwords

**Botnet** is a group of Internet-connected devices controlled by a central system. They usually all perform the same task controlled and synchronized by the botnet controller, the central system. The term is most often used in conjunction with malicious attacks, especially of the kind of Distributed Denial of Service (DDoS) attacks (Vishwakarma and Kumar Jain 2019). In DDoS, the Internet-connected devices in a large group flood a website or a network by sending many fake requests. The result is that the legitimate users cannot access it, since their requests are lost in the sea of the fake requests. Since hundreds or thousands of devices are involved trying to access the same number of unique IP addresses during
the attack, it is impossible or almost impossible to stop it. The IoT and, especially, the IoMT can easily become a part of the botnet and co-execute attacks, since the market is full of inexpensive devices (webcams, thermostats and many others), having small or zero built-in security. Therefore, they can be easily broken into and programmed to do harm or merely become a ‘home’ for the attacker. However, the users’ behaviour presents the most important vulnerability, because usually the users themselves are not paying any attention to the security. As an example, most of the users do not put any kind of password on their devices, which means that the devices are an easy target for any kind of attackers, especially for botnet specialists.

The impact of irresponsible user’s behaviour is huge. For example, an integral Internet infrastructure provider, Dyn, was partially offline in October 2016, because attackers used a botnet of approximately 100,000 unsecured IoT devices to take it down (Hammons and Kovac 2019). The direct consequence was that many high-traffic websites (i.e. Netflix, Amazon and Twitter) disappeared from the Internet for a while. Moreover, there was not one specific hacker who wrote a new code; instead the malware was assembled from existing code on the net and entitled Mirai. Mirai automated the process of coopting all the unsecured devices in the attack and used them until the owners removed these hacked devices from their network. Of course, when the attacker has so many devices at their disposal, they can be used for various kinds of purposes: speeding up password guessing, mining Bitcoins or any other kind of illegal service that can be rented by criminal organizations to perform whatever task they like. The only possible mitigation of these attacks is that all the IoT and, especially, IoMT devices run on a secure software, which is quite a difficult task. One of the options is to use Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) with DDoS features. The other is to take a partner with an Internet service provider that will detect and filter DDoS packets before reaching the considered network. Basic security hygiene encompasses changing default passwords. Nevertheless, it is quite important that all the users are aware of possible misuses, especially in the health sector, where any kind of misuse can cause hazardous consequences.
In relation to IoMT, privacy implies the need for legitimate data to be visible and readable only to those they are intended for. Privacy risks are usually mitigated by the encryption. The related cryptography protects the integrity of IoT and IoMT data. This is the crucial property required for the IoMT, having incorporated all the sensitive information of users. However, simple small sensors collecting data like environmental parameters are not equipped with processing and/or memory resources required for traditional encryption algorithms (e.g. Advanced Encryption Standard, AES). The IoT and IoMT with the aforementioned simple unsecured devices (such as cameras) must incorporate additional algorithms for high security and low computation (e.g. elliptic curve cryptography). The Public Key Infrastructure (PKI) can be embedded into devices at the manufacturing level, or later at the enterprise level. PKI can help in distributing and identifying keys that allow users and ‘things’ a secure exchange of IoMT data. PKI issues unique identity and digital certificate to ‘things’. In this case, it is also very important to have a ‘hygienic’ approach towards the encryption of a key lifecycle.

The encryption is the key step towards privacy. However, the essential issue with cryptography is that it assumes a lack of resources, that is, there is often not enough processing power. The decryption is not possible without the proper key in a reasonable time-frame. However, detection of faults in encryption algorithms or their implementations as well as advances in the computer technology and principles (e.g. quantum computing) might create a possibility to break codes soon by exposing all the hidden content and rendering integrity of archived digital documents questionable. The hope is now seen in the quantum cryptography and the other advanced methods, but they are uncharted areas of science and there can be no realistic forecasts. Therefore, one of the important measures is to anonymize data referring to individuals as early as possible (GDPR 2016).
5. Network Security

Networks can be secured by traditional methods like the above-mentioned IPS and IDS programmes, anti-malware and firewalls. But, best practice suggests the separation of IoT devices in the network by segmenting them. In this way, the IoT devices are in one network and all the other systems are in another network segment. This is not always an easy task, because some of the non-replaceable legacy systems require different kinds of update and patching. The network segmentation offers a higher level of security, because different parts of networks are organized as subnetworks, with their own customized security policies. However, the nature of this kind of segmented network introduces additional latency and exposes the full system to more errors related to the connectivity, in comparison with the non-segmented network. The mitigation of the problem, especially related to the latency that is a critical parameter in every IoMT, but especially in the segmented IoMT, is use of a gateway. Thus, by using a gateway with more processing computing and memory power than the IoT devices in the network, the IoMT will be much more secure and without introduced much higher latency. Thus, a gateway can apply stronger security measures (like firewalls and antimalware), much closer to ‘things’. Except for the mitigations noted above, it is of crucial importance never to open IoT ports when not needed and to disable them for port forwarding, thus, ensuring port security. Blocking unauthorized IP address is always a must. One of the known issues and risks in the IoT and IoMT networks is a lack of the bandwidth, which causes a slowdown of productivity and efficiency in the network. Therefore, an important task is to perform regular capacity assessments in network planning, in order to avoid any kind of issues related to throughput.

The Digital Devices as Non-human Communicating Agents in the Knowledge Landscapes

The account above in regard to those technologies involved in the communication of the Internet-connected devices illustrates just how complex an interaction this is. These interactions are performed mainly by
machines, some of them were initiated at the request of a user, and some are completely independent of human influence. When discussing the knowledge landscapes, they are considered to be formed by the interactions of content, users and technology, where the users are people searching for knowledge (Svalastog et al. 2014, 2020). However, digital technology is far from offering a passive obedience in performing any given task. The levels of autonomy and independent interactions necessary to maintain the functionality of the system are in particular visible when discussing the issues of safety and security.

The human user is, in regard to safety and security, more a liability contributing to risks than an element allowing for the safe and secure functionality of the system. Consequently, the issues of safety and security depend mostly and substantially on the activity of the interconnected devices themselves. Ideally, especially in the near future within the environment of smart cities, digital systems should be able to confront threats automatically.

The functionality of all devices connected in the IoT depends on their ability to communicate. Subsequently they are part of the total communication within the digital environment involving all combinations of device-to-device, device-to-human, human-to-device and human-to-human interactions. When considering the digital society, the extent of digital communications and digital spaces where this communication occurs should recognize as well these non-human participants in the interactions. If we consider the whole of humanity to be connected in the very near future, the 8 billion humans will be in the communicating space with 26.66 billion communicating devices. Assuming the current growth of number of devices connected and the expected increase in their communicating and processing abilities, it becomes obvious that these digital entities are already members of digital society. With the onset of artificial intelligence, they would be further humanized with cognitive abilities (Hutter 2005). In Everitt and Hutter (2018) the ‘autonomous agents’ are presented in a way that they may have an ability to modify themselves but also that the ‘present AI [artificial intelligence] systems are not yet close to exhibiting the required intelligence or “self-awareness”’ (see also Luger and Stubblefield 2004).
Conclusions

It is currently predicted that urbanization, contributing to shifting the residence of the human population from rural to urban areas, will result with ca. 70% of the global population living in cities by 2050. Thus, it is necessary to plan the new paradigm of ‘smart city’. The definition of the smart city is ‘a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business’ (EC, Smart City). Therefore, ICT becomes a backbone of the smart city: it extends horizontally across all the building blocks or key fields of a smart city; it develops itself only to support development of the key fields of the smart city; it interconnects them. The six key fields of urban development are smart economy, smart mobility, smart environment, smart people, smart living and smart governance.

All the components of the triad IoT-AI-5G belong to the ICT area. They enable development of smart cities. Our common vision is that all the smart cities on Earth, managed by AI, will be one day interconnected. AI is generated by human endeavour, and one scenario is that this global interconnection creates some sort of trans-human ‘brain’: as Nikola Tesla, approximately 100 years ago argued, ‘When wireless is perfectly applied the whole Earth will be converted into a huge brain’ (Tesla 1926).

Digital devices are partners in the communications and interactions of digital society. Although they can be very simple, their number and distribution create a complex world of para-human interactions, which directly involve humans in the case of IoMT. Consequently, the issues of safety and security illustrate the interdependencies and challenges within digital ecosystems populated by humans and digital devices.

IoMT represents a challenge within the health sector and its digital infrastructure, since it is expected that IoMT devices will be attached directly to a human body or they will be placed even within the body, in order to monitor or directly influence bodily functions. Any cyber-attack on them is an attack on human health. Here, we would like to stress that it is not only the IoMTs that control something that are at risk like pacemakers, brain stimulators, medicine-dispensing devices, breathing
machines and so on. Even those that only measure parameters of the human body are important. For example, if a hacker manages to forge measurement data about any bodily parameter, the user or his/her doctors could prescribe or apply a deadly lethal dosage or dangerous combination of medicines.

Therefore, some of the regulatory measures that have been and can be established should regard any attack on the IoMT as an attack against the human body, yielding the heaviest penalties and punishments as well as requiring the highest precautions and responsibilities by producers and distributors alike—very secure default settings, clear and understandable instructions about achieving security for users, mandatory training and certification of IoMT designers for security by design. Technical measures could lead towards the concept of a ‘personal health hub’ (PHH), a device ‘attached’ to a human body which would be the sole device communicating with all IoMTs of that person. PHH would then need to be highly secure and restrictive in communicating with the outside world. Finally, the PHH should never be integrated with general-purpose devices like smartphones.

We have shown in this chapter that the highest form of awareness needs to be achieved in IoMT developers, medical personnel and end users. Here elaborated interconnectedness between humans and digital devices, specifically sensitive in case of health-related devices, shows how the digital society and knowledge landscapes are a symbiosis of human and non-human participants.

References

[ehealth-hub]. Internet page: www.ehealth-hub.eu. Retrieved February 8, 2020.

AIOTI. (2018, February). Identifiers in internet of things (IoT), AIOTI version 1.0, AIOTI WG03 – IoT standardisation. Internet page: https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf, Retrieved February 18, 2020.

Binkowski, S. (2016). Medical IoT use case: I care about you ‘ICU’ – App, EMEA, 2016 SAP SE or an SAP affiliate company. Published: October 26th, 2016.
Internet page: https://open.sap.com/files/4bda64d8-1a14-4e00-b8b0-14b66046225a. Retrieved April 20, 2020.

Centrak. (2019). Internet page: www.centrak.com/solutions/newbaby-infant-protection/. Retrieved July 8, 2019.

Chen, T. L., Bhattacharjee, T., Beer, J. M., Ting, L. H., Hackney, M. E., & Rogers, W. A., (2017). Older adults’ acceptance of a robot for partner dance-based exercise. *PloS ONE, 12*(10): e0182736. https://doi.org/10.1371/journal.pone.0182736. Retrieved February 8, 2020.

Deloitte. (2019). Deloitte report. Internet page: https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html. Retrieved February 18, 2020.

European Commission. (2004). Green paper on mobile health (“mHealth”) (SWD(2014) 135 final), COM(2014) 219 final. *Brussels, 10*(4), 2014.

European Commission. (2020). White paper on artificial intelligence – A European approach to excellence and trust. *COM. 65* final. Brussels, 19.2.

European Smart Cities.4.0 (2015). Internet page: http://smart-cities.eu/?cid=2&ver=4. Retrieved April 20, 2020.

Everitt, T., & Hutter, M. (2018, January). Chapter 2: Universal artificial intelligence, practical agents and fundamental challenges. In Abbass, H. A., Scholz, J., & Reid, D. J. (Ed.), “Foundations of trusted autonomy”, *studies in systems, decision and control 117*. Springer. Internet page: http://www.hutter1.net/publ/uaitas.pdf. Retrieved April 20, 2020.

FDA. (2019). URGENT/11 cybersecurity vulnerabilities in a widely-used third-party software component may introduce risks during use of certain medical devices: FDA safety communication. safety communications. Date Issued: October 1, 2019. Internet page: https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce. Retrieved April 26, 2020.

Gehealthcare. (2019). Internet page: www.gehealthcare.com/about/healthcare-systems. Retrieved July 8, 2019.

Globalsecurity. (2001). Chapter 1: Physical security challenges. Field manual 3-19.30: *Physical security. Headquarters*, United States Department of Army. Archived from the original on March 13, 2013. Internet page: https://www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch1.htm. Retrieved February 18, 2020.

Halkos, G., & Zisiadou, A. (2018, July 7). Reporting the natural environmental hazards occurrences and fatalities over the last century. Munich personal
Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2017). Internet of Things (IoT) Technologies for Smart Cities. *IET Networks*. 7. 10.1049/iet-net.2017.0163.

Hammons, R., & Kovac, J. (2019). *Fundamentals of internet of things for non-engineers* (1st Ed.). Auerbach Publications, 430 Pages, ISBN 9780429274992, Published June 7.

Herjavec Group, Steve Morgan, Editor-in-Chief, Cybersecurity Ventures. (2020). 2019 official annual cybercrime report. Internet page: https://www.herjavecgroup.com/2019-official-annual-cybercrime-report/. Retrieved April 21, 2020.

Hutter, M. (2005). *Universal artificial intelligence*. Berlin: Springer.

IBM X-Force Cyber Security Index. (2016). Internet page: https://www.slideshare.net/KanishkaRamyar/the-ibm-x-force-2016-cyber-security-intelligence-index. Retrieved April 19, 2020.

IBM X-Force Threat Intelligence Index, IBM X-Force Incident Response and Intelligence Services (IRIS). (2020). Internet page: https://www.ibm.com/security/data-breach/threat-intelligence. Retrieved April 19, 2020.

Joy, A. (2019). CHIME fall forum 2019: Securing IoMT devices requires collaboration and a culture shift. *HealthTech Magazine*, CDW LLC 200 N. Milwaukee avenue, Vernon Hills, IL 60061. Internet page: https://healthtechmagazine.net/article/2019/11/chime-fall-forum-2019-securing-iomt-devices-requires-collaboration-and-culture-shift. Retrieved April 22, 2020.

Luger, G., & Stubblefield, W. (2004). *Artificial intelligence: Structures and strategies for complex problem solving* (5th ed.). San Francisco: Benjamin/Cummings.

Lynch, R., & Farrington, C. (2018). *Quantified lives and vital data: Exploring health and technology through personal medical devices*. Basingstoke: Palgrave.

Marr, B. (2018). Why the internet of medical things (IoMT) will start to transform healthcare in 2018. Internet page: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#4e7405c24a3c, Forbes.com. Published: January 25, 2018. Retrieved February 18, 2020.

Masscan. (2019). Internet page: manpages.org/masscan/8. Retrieved July 8, 2019.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.
Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2020). Detection of unauthorized IoT devices using machine learning technique, Researchgate. Internet page: https://www.researchgate.net/publication/319736005_Detection_of_Unauthorized_IoT_Devices_Using_Machine_Learning_Techniques. Retrieved February 18, 2020.

Meola, A. (2020). IoT healthcare in 2020: Companies, devices, use cases and market stats, business insider. Published: February 13, 2020. Internet page: https://www.businessinsider.com/iot-healthcare?op=1. Retrieved April 20, 2020.

Merriam-Webster Dictionary. Internet page: https://www.merriam-webster.com/dictionary/safety. Retrieved February 18, 2020a.

Merriam-Webster Dictionary. Internet page: https://www.merriam-webster.com/dictionary/security, Retrieved February 18, 2020b.

Merriam-Webster Dictionary, Internet page: https://www.merriam-webster.com/dictionary/threat. Retrieved February 18, 2020c.

Merriam-Webster Dictionary, Internet page: https://www.merriam-webster.com/dictionary/vulnerability. Retrieved February 18, 2020d.

Mole, B. (2018). With ingestible pill, you can track fart development in real time on your phone. Internet page: https://arstechnica.com/science/2018/01/with-ingestible-pill-you-can-track-fart-development-in-real-time-on-your-phone/. Published: September 1, 2018. Retrieved February 18, 2020.

Morin, D. (2016, February 19). Untrained IT users: Who they are might surprise you. Global-ICT 2015, Article: 7. Internet page: https://connect-world.com/untrained-it-users-who-they-are-might-surprise-you/. Retrieved April 20, 2020.

Nmap. (2019). Internet page: https://nmap.org. Retrieved July 8, 2019.

Pandor, A. T., Gomersall, J. W., Stevens, J., Wang, A., Al-Mohammad, A., Bakhai, A., Cleland, J. G. F., Cowie, M. R., & Wong, R. (2015, April 28). Remote monitoring after recent hospital discharge in patients with heart failure: A systematic review and network meta-analysis. Internet page: heart.bmj.com (published on Researchgate). Retrieved February 8, 2020.

GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.
SensorMetrix. (2019). Internet page: www.sensormetrix.com. Retrieved July 8, 2019.

Shodan. (2019). Internet page: https://www.shodan.io. Retrieved July 8, 2019.

Statista. (2019). Internet page: www.statista.com. Retrieved July 8, 2019.

Svalastog, A. L., Allgaier, J., Martinelli, L., & Gajović, S. (2014). Distortion, confusion, and impasses: Could a public dialogue within Knowledge Landscapes contribute to better communication and understanding of innovative knowledge? Croatian Medical Journal, 55, 54–60.

Svalastog, A. L., Gajovic, S., & Webster, A. (2020). Navigating knowledge landscapes. Basingstoke: Palgrave.

Taylor, H. (2019, December 13). The state of ransomware in the US: Report and statistics 2019, Emsisoft, security blog. Journal of Cyberpolicy. Internet page: https://journalofcyberpolicy.com/2019/12/13/state-ransomware-us-report-statistics-2019-emsisoft-security-blog/. Retrieved March 21, 2020.

Tesla, N. (1926). When woman is boss, (1926) an interview with Nikola Tesla by John B. Kennedy, colliers. January 30, 1926. Internet page: http://www.tfc-books.com/tesla/1926-01-30.htm. Retrieved July 8, 2019.

Tung, C. E., Su, D., Turakhia, M. P., & Lansberg, M. G. (2015). Diagnostic yield of extended cardiac patch monitoring in patients with stroke or TIA. Frontiers in Neurology, 5, 266.

Turner, D. (2016). Digital authentication: The basics. Cryptomathic. Archived from the original on 14 August 2016. Retrieved February 18, 2020.

United Nations Department of Economic and Social Affairs. (2018). 68% of the world population projected to live in urban areas by 2050. 16 May 2018, New York. Internet page: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html. Retrieved April 28, 2020.

Vishwakarma, R., & Kumar Jain, A. (2019, April). A honeypot with machine learning based detection framework for defending IoT based Botnet DDoS Attacks. The 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 23–25. IEEE 2019.

Weissman, C. G. (2015). Survey: We asked executives about the internet of things and their answers reveal that security remains a huge concern. http://www.businessinsider.in/We-Asked-Executives-About-The-Internet-Of-Things-And-Their-Answers-Reveal-That-Security-Remains-A-Huge-Concern/articleshow/45959921.cms. Published January 21, 2015. Retrieved February 18, 2020.
Wellsensevu. (2019). Internet page: www.wellsensevu.com. Retrieved July 8, 2019.
WHO. (2019). Internet page: www.who.int. Retrieved July 8, 2019.
Zanthion. (2019). Internet page: www.zanthion.com. Retrieved July 8, 2019.