Present-Day Cybersecurity
Actual Challenges and Solution Directions

van den Berg, Jan

DOI
10.5772/intechopen.1007021

Publication date
2024

Document Version
Final published version

Published in
Key Issues in Network Protocols and Security

Chapter

Present-Day Cybersecurity: Actual Challenges and Solution Directions

Jan van den Berg

Abstract

Currently available cyberspace services offer all kinds of possibilities for individuals, businesses, and organizations to arrange their lives and to improve their e-enabled business processes. However, next to the numerous benefits, we are aware of many less desirable developments in cyberspace. In other words, the security of cyberspace (i.e., cybersecurity) is at stake, and we have to act in this (relatively new) domain. In this chapter, we first provide a condensed overview of existing and upcoming cyber activities and cyber processes in various cyber subdomains, hereby using the terminology of a holistic cyberspace model. We also introduce a general cyber risk management model. Next, we present an overview of a series of (mostly) recent cyber incidents, based on which we formulate related cybersecurity challenges. In order to understand how we currently deal with these challenges, we then describe the current efforts of various cyberspace actors to enhance cybersecurity to a sufficient resilience level and evaluate the limitations of their endeavors. By putting together all findings, we draw our conclusions in an overview of actual cybersecurity solution directions, that is, an overview of the efforts needed to bring the security in all cyberspace subdomains at acceptable levels.

Keywords: cyberspace, cyber activities and processes, information technology & operational technology, cybersecurity governance, cybersecurity and information security, cyber risk management

1. Introduction

In this introduction, we sketch current developments in cyberspace leading to the basic goals of this paper, we introduce the fundamental concepts describing cyberspace and cybersecurity, we dwell on the chosen methodological approach, and present the structure of the remainder of this chapter.

1.1 Emergence of cyberspace and related cyber risks

Suddenly, in the last decade of the previous century, all kinds of Internet services started to become available for “everyone,” and to grow exponentially. This revolution in *cyberspace*, sometimes termed the 5th domain (next to the physical domains of land, water, air, and space [1]), is still going on. This makes cyberspace a very dynamic space offering lots of challenges for individuals to better arrange their lives by executing all kinds of so-called *cyber activities* (i.e., *digital* or *information technology (IT)-enabled activities*) like e-mailing, e-(re)searching, e-chatting, e-streaming, e-navigating, e-shopping, e-planning, e-booking, e-paying, e-dating, e-socializing, e-gathering, e-consulting, e-matching, e-learning, e-gaming, e-gambling, e-crowd-funding, e-voting, e-protesting.

Along the same line, new challenges for businesses and other organizations emerged for improving their profits or functioning by optimizing their *cyber processes* like e-marketing, e-warehousing, e-banking, e-tracking, e-tracing, e-procuring, e-selling, e-renting, e-transporting, e-meeting, e-negotiating, e-participating, e-cooperating, e-supervising, e-teaching, e-governing, and e-crowd sourcing. Similarly, technology-driven companies and organizations in industry and (critical) infrastructures started their *operational technology (OT)-enabled activities* and *processes* like e-producing, e-supplying drinking water and energy, e-building, e-transporting, e-telesurgery performing, e-data acquisitioning, e-mining, e-monitoring, e-controlling, e-steering, e-supplying, and e-networking.

However, next to all these (growing) benefits, cyberspace suffers from existing and upcoming cyber threats due to our growing dependence on IT and OT. After all, both IT and OT, can unintentionally fail, or natural disasters can take place like hurricanes, floods, and earthquakes. Moreover, malicious people and organizations, from script kiddies, hackers, criminal gangs, to even state actors, can choose from a huge variety of e-means (including those available in the dark web [2]) to execute all kinds of annoying, odious, disruptive, criminal, et cetera e-activities, and e-processes like e-bullying, e-fraud committing, e-sexting, e-pornography distributing, e-fake news spreading, e-illegal goods selling, e-cyberattack services renting, e-espying, e-influencing, e-stealing, e-intelligence collecting, e-attacking, e-sabotaging, and even e-warfare operating.

As a consequence of the cyber threats related to cyber activities and processes, *cyber incidents* of all kind (can) occur with (potentially) high negative impact for individuals, businesses and organizations, up to governments, states, and in the darkest scenario's (e.g., due to a huge electricity blackout, or the shutdown of crucial Internet exchanges), even parts of continents. So, the *security of cyberspace*, that is, *cybersecurity* is at stake, and we have to deal with the existing and upcoming cyber risks in order to get the related *cybersecurity risk levels* at sufficient levels.

Based on these considerations, the *goals of this paper* are to more precisely define the present-day cybersecurity challenges, to analyze our current cyber resilience levels, and, finally, to sketch the cybersecurity solution directions needed to guarantee sufficient cybersecurity levels in all cyber subdomains.

1.2 Conceptualizing cyberspace and cybersecurity

To reach the goals defined above, we need to use a clear conceptualization of the domain at stake, that is, of cyberspace. In addition, we need to have a clear understanding of what cybersecurity entails. Both cyberspace (in which several billion people are active, facilitated by the worldwide Internet and other IT & OT) and cybersecurity are complex notions. Fortunately, we can use earlier research outcomes here. Due to various reasons, we were forced to come up with the first ideas around precisely defining cyberspace and cybersecurity almost fifteen years ago, which resulted in the first (best paper award-winning) publication on this subject [3]. Actually, the terminology used in subsection 1.1 above is completely in line with the concepts introduced in that paper.

Later on, we elaborated these first ideas, resulting in a series of additional papers published, the last, most extensive one being [4]. Meanwhile, the Dutch National Coordinator for Counterterrorism and Security (NCCS) of the Ministry of Justice and Security almost completely adopted our conceptualizations; see, for example, the "Cyber Security Assessment Netherlands (CSAN) 2013" report [5]. The elaboration of the first ideas resulted later in a set of additional *mental models* that more precisely define cyberspace and cybersecurity [4]. Here we confine ourselves to present the basic cyberspace model and basic cybersecurity model, and to briefly describe the set of additional mental models needed to understand the rest of this chapter.

The basic *three-layer Cyberspace Model* is shown in **Figure 1**. The middle layer is the *socio-technical layer*, that is, the layer of cyber activities and cyber processes. This middle layer concerns the most crucial layer (!), namely, that of the *key assets* of cyberspace, since it concerns the cyber activities and processes that people execute in order to achieve their specific goals, so it concerns *human behavior*. When acting in cyberspace by means of e-enabled cyber applications, users utilize IT & OT services of the "underlying" *technical layer* shown as the inner layer in **Figure 1**.

The choice of making a separation between the technical layer and the socio-technical layer has severe consequences—when we talk about *cybersecurity*, we mean the security of the cyber activities and cyber processes of the socio-technical layer, while if we speak about *information security*, we mean the security of the technical (inner) layer. The latter concerns the security of data that are being stored and processed in terms of the preservation of their confidentiality, integrity, and availability (CIA) (see, e.g., the famous ISO/IEC) 27,000-series on information security: [6] and its successor publications). Within this framework of thinking, it should be clear that information security incidents that take place in the technical layer pose threats to the cyber security of the socio-technical layer. This all implies that *information security management* is fundamentally different from *cyber security management*, both needing specific, complementary attention.

The third outer layer of the Cyberspace Model is the *governance layer,* the layer of rules and regulations that should be put in place to properly organize the two other

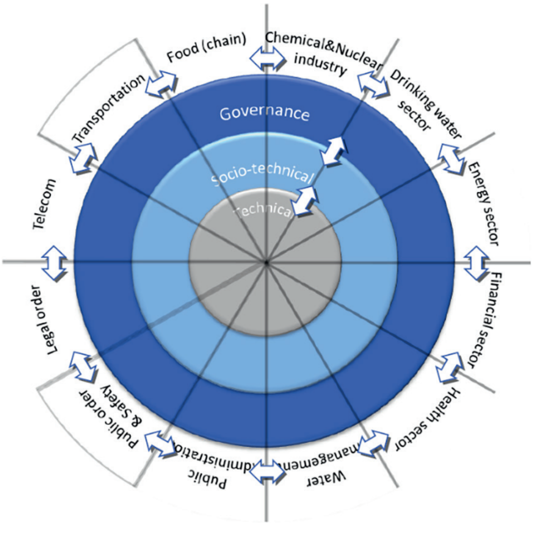

Figure 1.
Basic 3-layer cyberspace model [3, 4].

layers, including their security. This relates, for example, to the Internet governance issues related to the functioning of the World Wide Web and the Internet as a whole, next to rules and regulations that influence human cyber behavior, that is, the way people execute cyber activities and cyber processes in the middle layer.

Next to the separation into three layers, the cyberspace model of **Figure 1** shows a division in pie slices mentioning various *cyber subdomains*. This is done to emphasize that cyber activities and processes in different subdomains often have different characteristics and thus different cybersecurity challenges.

For each cyberspace layer, a specific *mental model* can be used to concisely describe its fundamental characteristics [4]. For the socio-technical layer, the basic challenge for people is to act “unconscious cyber competent” as “homo digitalis,” that is, to show continuously and consistently adequate cyber(security) behavior. For the technical layer, the key issues relate to the two protocol stacks used to describe computer networks, namely the OSI and TCP/IP protocol stacks [7]. For the governance layer, the chosen mental model concerns the four modalities of regulation in cyberspace [8] (1) laws, rules, policies, & regulations, (2) norms, that is, informal societal rules, (3) markets, and (4) architecture, that is, physical or technical constraints on cyber activities. This framing of these four modalities of regulation of the governance layer is precisely in line with the three-layer model of cyberspace: the modalities of laws, norms, and markets steer cyber activities and processes, that is, steer cyber behavior from a direct governance perspective, while the modality architecture puts constraints on the cyber activities and processes by measures taken in the technical layer. For more digressions about these three specific mental models of cyberspace, we refer to [4].

Having visualized cyberspace, we now present the *basic bowtie model of cybersecurity*. Going from left to right in **Figure 2**, the model shows (intentional and unintentional) threats, incidents, and the impact of the latter. Threats may result in (sometimes interdependent) cyber incidents. Incidents occur with a certain probability or likelihood, and the risk of a cyber incident is defined as the expected impact of this incident, that is, *risk = likelihood x impact*. In cyberspace, the bowtie model can be used to model cyber threats, cyber incidents, and their (negative) impact, and thus cyber risks. To avoid cyber incidents happening, preventive measures can be taken to reduce the probability of their occurrence. To reduce the impact of occurring incidents, repressive measures should be taken. For more details on (the use of) the bowtie model, we refer to reference [9].

Cybersecurity is actually a risk management challenge. For proper risk management, a risk management process should be implemented (basically a responsibility

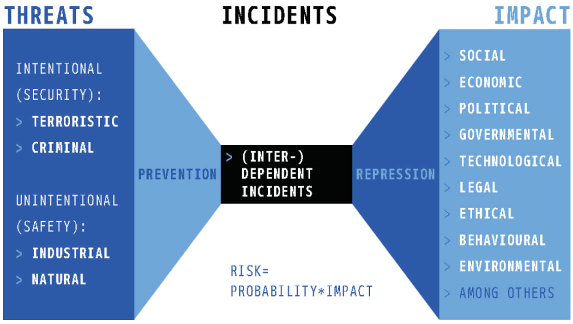

Figure 2.
Basic (bowtie) model of cybersecurity [3, 4]. (adapted from [9]).

of the governance actors). This process can be implemented as a *cyber risk management cycle* of six basic steps and can be described by the following pseudo-code: "Repeat forever, in all cyber subdomains, (1) identify critical cyber activities and processes (sometimes termed the "crown jewels"); (2) identify & assess their cyber risks (potential gains & losses); (3) define acceptable cyber risk levels; (4) decide way(s) of dealing with the risks; (5) design & implement relevant cyber risk measures; and (6) monitor the effectiveness of measures taken." Once again, we emphasize here that within our framework of thinking, cybersecurity primarily entails risk management of cyber activities and cyber processes. Since the characteristics of these activities and processes often vary substantially in different cyber subdomains and, therefore, the related cyber risks vary as well, cyber risk management cycle processes should be adapted to the actual context in which they are executed.

Like the cyberspace model, the bowtie cybersecurity model can be specified in more detail by means of a set of (additional) mental models [4]. These additional mental models will be briefly summarized here and relate to the six steps of the risk management cycle: (1) the "crown jewels model" (to describe the critical cyber activities and processes at stake), (2) the "cyber situation awareness" model (to know and understand goal and progress of actual cyber activities and processes) and the "unified kill chain model" (to identify the related intentional and unintentional cyber threats and the ways in which cyberattacks take place), (3) the "risk matrix model" (to assess the related cyber risks), (4) the "risk response strategies model" (to select the proper way(s) of dealing with the established cyber risks), (5) the "Swiss cheese model," the "institutional design" model and the "cyber social contract model" (to select the concrete measures of dealing with the cyber risks), (6) the "cyber situational awareness model" again (to understand the behavior changes of running cyber activities and processes as a result of the measures taken). For more contemplations about these additional mental models for implementing the cyber risk management cycle, we refer again to [4].

1.3 Methodological remarks

The first group of remarks concerns the domain focus of the research executed or, more precisely, concerns the cyberspace areas in the world we selected to focus on. Since the ways cyberspace is managed and governed often very differ in various countries (mainly due to existing distinct political opinions and structures), we observe that (a) cyber activities and processes in the world differ, and (b) what is considered cybersecurity and the way it is implemented certainly differs. In this book chapter, we mainly focus on countries having a so-called "open society" [10]. This choice is also motivated by the fact that sources with recent information about current cyber(security) developments and practices are easier to find in these countries.

A second group of remarks concerns the chosen research approach. As already mentioned in the introduction, we used the earlier developed concepts of cyberspace and cybersecurity as a "*lens*" to sketch and analyze current cyber and cybersecurity developments. By using this lens, we actually apply a *transdisciplinary* [11] research strategy crossing various disciplinary boundaries (e.g., we talk about human behavior, technologies, and legislation) and based on both scientific and practical sources. Especially the latter enabled us to use information sources describing very recent developments. Other characteristics of our research approach are a socio-technical view (i.e., considering the interrelation of social and technical aspects) and a multi-actor view (we include all actors in cyberspace, in possibly various roles), which altogether results in a holistic picture [11] ("the whole is greater than the sum of the parts").

A third group of remarks concerns *validation*—is the applied methodology a correct one? We do think so, because our conceptualizations of cyberspace and cybersecurity have already been successfully applied in designing and implementing an executive master's program cybersecurity, in many master's thesis research projects (for examples, see ref. [4]), and in cybersecurity research resulting in scientific papers published (see [3, 4], and the references in [4]). Also, the adoption in 2021 of our conceptual framework by the Dutch Ministry of Justice and Security for creating the yearly CSAN reports underpins the effectiveness of our way of thinking.

Our final methodological remarks are also validation-related. Using the terms of our conceptualizations of cyberspace and its security, we searched on the Internet for information sources. To double-check the validity of factual findings, we often searched for additional sources. The resulting conclusions in Sections 5 and 6 followed mostly from logical inferences in the text and have, as much as possible, been checked using information from additional trustworthy sources.

1.4 Structure of the remainder of this chapter

In order to create a more complete overview of present-day cyberspace dynamics, Section 2 presents additional examples of currently widely used, new, and emerging cyber activities and processes. Section 3 then first provides a series of mostly recent cyber incidents (and related cyber threats and impact), from which we next derive present-day cybersecurity challenges. We continue by sketching actual cyber resilience levels in Section 4. By combining all this information, we present in Section 5 a set of solution directions needed to create desired cyber risk levels in the various cyber subdomains. Finally, Section 6 summarizes our findings by means of a few main conclusions.

2. Present-day cyber activities and processes

In the introductory section, we already sketched examples of various (IT- & OT-based) cyber activities and processes. Based on various (other) sources, we here elaborate on this to create a more complete, up-to-date picture of cyberspace developments by sketching currently widely used, new, and emerging e-activities and processes as executed by various stakeholders.

a. Considering *individual end-users* in cyberspace, we first provide a set of *key statistics* (i.e., estimations of their Internet-based activities) [12]: "There are (currently) 5.35 billion Internet users worldwide," "On average, Internet users spend six and a half hours online every day," "75% of people aged 15–24 have access to the Internet across the world," "7.5 million blog posts are published each day," and "5.04 billion people are on social media as of 2024." Especially (free of charge) social media like Facebook, TikTok, Twitter, and Instagram are extremely popular, since they enable user-friendly "multimodal communication, simultaneously with many members" [13]. They are mostly used for private information exchange, but sometimes also for more professional reasons, as in the case of LinkedIn and YouTube. Another important motivation is financial: content creators or influencers (i.e., persons with a large group of followers) are contacted by large companies to promote their products or apply affiliate marketing. It is further important to note that in many cases these social media are used anonymously, for example, by adopting a nickname or various fake names.

Talking about Internet use, we should also briefly discuss the existence of the *surface web* ("representing about 5% of its total content"), the *deep web* ("representing about 90% of its total content" and concerns the websites "used by entities such as corporations, government agencies, and nonprofits"), and the *dark web* ("representing about 5% of its total content" and concerns "an area of the Internet that is only accessible by users who have a Tor browser installed") [14]. The original goal of using the Tor browser was to enable Internet users to privately browse without tracking, surveillance, or censorship. It is currently mostly known as a cyber area where illegal goods and services can be obtained.

Another Internet source [15] mentions the currently *"ten most-used" general cyber activities* of end-users being social networking, online shopping, online banking, e-education and upskilling, e-gaming, e-trading, e-dating, e-mailing, e-newspaper reading, and e-researching. Going into more detail of cyber activities, we observe the still great popularity of e-trade in cryptocurrencies like Bitcoin, Ethereum, Tether USDt, BNB, and Solana, among almost 200 others [16]. Maybe somewhat less-known, we observe Internet of Things-(IoT-) based cyber activities and processes like e-monitoring of personal health, water and energy use at home, e-tracking of solar energy production [17], and e-controlling distant home temperatures and security. Note that for quite some cyber activities, end-users do not communicate with human beings but just with "intelligent servers," for example, when performing e-transactions or talking with chatbots. The latter Artificial Intelligence (AI)-based service relates to the recent revolutionary growth of generative AI-based ("human creativity empowering") products and tools [18] enabling the e-creation or adaption of images, music, video's, text, and computer code, with probably the most well-known example tool ChatGPT [19]. The latter can be used for answering questions, generating content, translating languages, writing computer code, engaging in conversations, and providing explanations, among others.

b. Considering *businesses and other organizations* acting in cyberspace, we observe (and experience) that the digitization of business processes also continues and deepens, often driven by financial motives. When searching for present-day *e-commerce trends*, we found 12 trends that are "powering online retail forward" like augmented reality in online shopping, voice search facilities, chatbot-enabled personalized product recommending, chat-marketing, mobile shopping services, flexible payment solutions, e-shopping via social media platforms, personalized price offerings, and more [20]. But also in other sectors like finance, agriculture and livestock farming, public and commercial transporting, water supply, and other critical infrastructures (just to name a few), we see all kinds of new Internet-enabled solutions related to enhancing efficiency, convenience, quality control, sustainability, or security.

In industrial contexts, digitalization is further developing using technologies like IoT and cloud computing. Examples of IoT-based applications in subdomains like agriculture, logistics, retail, and transportation include e-monitoring and e-management of micro-climate conditions in greenhouses, e-tracking of products from their start on the factory floor to their placement in the destination store, e-controlling warehouse automation and robotics by (online and in-store) shopping sales figures, e-steering of self-driving cars, and (sensor data-based) e-improving of fleet vehicle driving behavior resulting into optimized performance, fuel use reduction, and reduced pollution generation [17]. Note that also here more and more AI-based solutions have been adopted.

Examples of present-day cloud-based applications in industry and beyond include big data storage, management & analysis, corporate solutions for e-commerce, marketing & sales, scalable and adaptable cloud services for software testing, e-services for presentation and video-conferencing, and real-time daily accounting services [21].

c. Considering the digital transformation in *governments and state actors*, it refers to processes of utilizing technology and digital solutions to modernize and enhance the delivery of public services and to streamline internal operations (both in the socio-technical layer of the cyberspace model) and to improve overall governance [22]. This of course also concerns intense transformation processes. It aims to facilitate data-driven decision making, to realize citizen-centric servicing, to promote transparency and accountability in day-to-day operations, and to safe costs and enhance operational efficiency, among others [20]. More specifically, we observe e-based measures to streamline public and private mobility, to accelerate the energy transition, and to improve biodiversity, sustainability, and other environmental-related affairs, often within the context of creating smart cities and environments.

Considering the governmental task of creating and maintaining a safe and secure "open society" [10], lots of e-enabled initiatives are being taken, from managing the safety of large crowds and high traffic volumes, protecting critical infrastructure, law enforcement on the street, reducing trade in hard drugs, unmasking financial fraud, and enhancing national intelligence efforts for detecting intellectual property stealing, fake news spreading, and terrorism and warfare-related attacks. In non-open societies, those in power interpret their safety and security role usually very differently and use their IT-enabled capabilities (also) to impose a single ideology, suppress individual freedoms, detect and prohibit critical organizations, and track, trace, arrest, and convict dissidents, among others.

As a final remark related to present-day cyber activities and operations, it is important to note that the underlying, enabling transnational IT & OT services of the technical layer are often under the control of a small group of providers, ranging from basic Internet communication services (like satellite-based Starlink [23]) to cloud-based services and applications in the possession of big companies (like the five Tech Titans and big Chinese IT companies [24]).

3. Actual cybersecurity challenges

Having sketched above an updated picture of the current cyber activities and processes, we here continue by presenting the related cybersecurity challenges. We first present an overview of recent cyber incidents in various cyber subdomains, including the related (un)intentional threats and impacts (remember the bowtie model). Secondly, we derive from this a list of actual cybersecurity challenges.

3.1 Recent cyber incidents

When searching on the Internet for recent cyber incidents, you can easily find large numbers of websites, papers, and reports presenting a wide variety of incidents. To structure our search efforts, we first looked for information about single incidents with (potentially) big impact. Next, we searched for sources providing more structured information in terms of overviews and trends.

Let us start with a very recent, truly "wake-up call" incident: July 19, 2024, a defect CrowdStrike content update hit over 8.5 million Windows hosts impacting a range of industries with flights grounded, health services affected, and payment services unavailable; see Reference [25] for details, and its Internet links. This cyber incident is considered one of the worst cases ever due to its enormous impact. Maybe surprising—it was an unintentional attack. The same source also mentions details of another big incident named "RockYou2024," where a hacker exposed nearly 10 billion passwords. The potential harm (impact) of this incident is huge since threat actors could use the information in the RockYou file "to conduct brute-force attacks and gain unauthorized access to various online accounts used by individuals who employ passwords" [25]. To refresh our memory (occurred cyber incidents are often quickly forgotten), we also looked for the biggest cyber incidents ever and their impact. We found a list of ten incidents [26] and describe here six of them: (1) 1999 Melissa virus incident (causing widespread disruption of operations at major companies and the US Army), (2) 2023 MOVEit incident (the related zero-day vulnerability-based attack in question affected over 2000 organizations and exposed the data of 60 million people), (3) 1999 NASA cyber incident (a 15-year-old computer hacker caused a 21-day shutdown of NASA computers that support the International Space Station and invaded a Pentagon weapons computer system), (4) 2007 Estonia Cyber Attack (a Russian state-based Distributed Denial-of-Service (DDoS) attack against critical infrastructures of Estonia disrupted essential services like online banking, media communication, and government functions), and (5) 2011 PlayStation Network incident (hackers infiltrated Sony's PlayStation Network resulting in the theft of personal information from about 77 million user accounts), and (6) 2015 Ukraine Power Grid incident (the related malware based attack is considered the first successful cyberattack to cause a power outage on a national grid, resulting in power outages for around 230,000 customers). During the ongoing Russo-Ukrainian War (started in 2022), there have been multiple cyberattacks targeting Ukraine's national infrastructure. For more details about these and other big incidents, we refer to Reference [26].

Since social networking is the greatest cyber activity (see above), we also searched for cyber incidents that occur in this cyber subdomain. It is easy to find information sources discussing cyber activities like cyberbullying, cyberstalking, cyber harassment, and victimization leading to incidents related to poor workplace performance, psychological distress, and social isolation, among others (see ref. [27] for example). Social media are often also used in other undesirable ways, for example to spread misinformation, fake news, and unwanted pornographic videos, to create social media addiction, to distract and create productivity losses, and to compromise user privacy and expose users to fraud [28]. Moreover, we found that Internet-enabled social networks not only directly suffer from cyber incidents; the related social media are also exploited as a "social engineering" channel, that is, as a means, to cause cyber incidents in other cyber subdomains by means of (enhanced spear-) phishing attacks [29].

We already mentioned the existence of the notorious dark web that enables, by allowing anonymous acting, all kinds of illegal activities. It is quite easy to find (on the normal surf web) horror stories with details on dark cyber incidents with big impact related to criminal activities like buying and selling illegal drugs, weapons, passwords and stolen identities, and trading illegal (child) pornography.

Having presented this overview of cyber incidents, we observe that (a) the numbers are high, (b) most incidents occur due to intentional attacks, (c) attacker types (still) range from script kiddies to cybercriminals and state actors, (d) impacts range from personal harm to disruptions of critical infrastructures, which can affect thousands of people, and, therefore, (e) the impact of a single incident is sometimes enormous.

In order to check and validate the findings presented in this subsection, we also inspected information sources discussing general cyber security developments and trends. First, we reread the developments and trends as reported in the recent CSAN reports earlier mentioned ([5] and other versions). They confirm our observation that cybercriminals and state actors (notably Russia and China) create the biggest threat for open societies. The primary motive for cybercriminals is financial gain, and for state actors, geopolitical and economic gain. Both types of actors permanently invent new ways and apply new (sometimes in the dark web hired) tools to execute their attacks. Especially ransomware-based attacks are a big threat for national security in terms of the continuity of vital processes and for keeping sensitive and private information secure. The reason that cybercriminals can be so sophisticated in their cyber-attacks is that they are usually well organized, often by acting in the dark web, where they can make use of cyber-as-a-crime services and communicate unnoticed. Next to ransomware, Distributed Denial-of-Service (DDOS) software is used as an attacking tool within the context of current geopolitical tensions and warfare operations. These and other general findings are illustrated in the CSAN reports by means of lists of occurred cyber incidents. In a categorization of these, we observed, as remarkable types of cyber incidents, cyber espionage incidents, cyber sabotage incidents, website defacement incidents, supply chain information disruption incidents, and process disruption incidents. The incidents and types reported are largely in line with the cyber incidents mentioned earlier and in the first paragraphs of this subsection.

In a final attempt to get improved insights about recent cyberspace incidents, we used the Google browser with the key words "general cyber developments and trends." The first results presented information about cyber war trends and technologies with discussions on cyber warfare operations (intelligence, defense, and attack) and hybrid warfare (merging traditional military action with cyberattack operations) [30]. Another paper [31] presents the results of analysis of around 15 million cyberattacks mentioning trends like "cyber espionage is most likely aiming government, media, and law enforcement sectors," "cyber espionage, cyber war and hacktivism techniques, cyber-crime target all business sectors," and "there is a continuous increase in the mobile attacks" (i.e., attacks resulting into unauthorized access to smart phones).

As a side-remark at the end of this subsection, we observe that the inspected information sources use the concepts of cyberspace and cybersecurity usually with a meaning different from ours and from each other, or not define them at all. For example, cyberspace is seldom defined, the terms cyber activities and cyber processes are rarely found, while cybersecurity and information security are often treated as synonyms (then having the classical meaning of the "security of data," as promoted by the famous ISO/IEC-27000-series [6]). More in general are cyber concepts often used in sloppy ways: cyber risks are regularly correctly considered as risks, but often (also) as probabilities of an incident, and malware like ransomware is often termed an attack, or even an incident, instead of a means to execute an attack that may result in a cyber incident.

3.2 Cybersecurity challenges

Having presented an updated image of occurring cyber incidents, we can derive from these the related cybersecurity challenges, both general and specific ones. To structure the information presented below, general challenges will be numbered by adding a single number x, written in the text as (x), with $x = 1, 2, ...$, while more specific challenges will be numbered with more numbers and written like (2.1), (2.2), ... and (3.1.1), (3.1.2)....

Remembering the introduced cyberspace model, we defined cybersecurity as the security of all cyber activities and processes (as initiated and executed by the various cyberspace actors in their different cyber roles), and the main goal of cybersecurity is to bring the security in all cyberspace subdomains at acceptable levels. This overall cybersecurity challenge can be better understood by considering each step of the cyber risk management cycle discussed in Section 1. Since cyberspace actors are very often unexpectedly surprised by occurring cyber incidents, we observe that a lot of them apparently not correctly (and sometimes not at all) implemented the cyber risk management cycle. This may relate to the relative novelty and high dynamics of cyberspace and related risks, as well as the lack of knowledge how to do or organize this. The latter is understandable since most steps of the cyber risk management cycle, actually from 2 till 6, are hard to do for an individual cyberspace actor, and support for doing so is often hard to find. Looking more specifically to step 3 (of defining acceptable cyber risk levels for all cyber activities and processes), we note that the latter is actually not a question that science can easily answer, but more a question that should be dealt with by all stakeholders themselves; for example, end-users should themselves define the acceptable cybersecurity risk levels for the cyber activities they execute in their private, work, school, and leisure time environment. For lots of businesses and other organizations, including governmental ones, especially the big ones, we experienced that a lot of them have already difficulties with step 1 of the cycle to define their digital crown jewels and therefore as well to precisely define in step 3 the acceptable cyber risk levels for these crown jewels. In addition, it is often hard to assess (in step 2) present-day cyber risks because, in order to do so, a lot of experience is needed. Related to this have many cyber actors difficulties in taking on (in step 5) the preventive and repressive measures needed, and just do whatever comes to mind. The fact that both people and organizations are often surprised by the sudden occurrence of high-impact incidents further suggests that lots of them paid too little attention to repressive measures (right-hand side of the bowtie), since such measures could have reduced the impact of such incidents. From these observations, it is clear that a first general cyber security challenge (1) is to provide cyberspace actors, in their various roles, with sufficient knowledge and skills to apply adequate cyber risk management.

Looking at the group of end-users, the general cybersecurity challenge (2) is the accomplishment of secure cyber behavior with respect to their cyber activities in various cyber subdomains. As a first example, we take a look at e-enabled social networking. The various incident types described in subsection 3.1 make clear that the e-enabled social networking environments are far from secure. The related challenge (2.1) is therefore to transform those environments into ones where people feel themselves safe and secure in all possible ways, which implies that they themselves behave according to agreed conventions, rules, and regulations. Similar challenges (2.2), (2.3), … can of course be formulated for a lot of other e-enabled environments related to school, work, traveling, and leisure.

Looking at businesses and other organizations, the main cybersecurity challenge (3) is to keep their e-business processes sufficiently secure and thus sufficiently resistant against intentional and unintentional, internal and external threats. These threats concern both malicious individuals and organizations (from their own employees to monetary motive-driven hackers and competitors) who execute cyber-attacks. But they also concern (information security) threats from the underlying IT & OT services that may themselves (un)intentionally be disrupted or fail. Actually, we talk here about large numbers of cyber subdomains with very specific characteristics, which results in specific cybersecurity challenges (3.1), (3.2), … for each cyber subdomain. It should be clear that the top managers of these organizations are the true responsible persons to formulate and deal with these domain-specific cybersecurity challenges.

We do not further elaborate here the cybersecurity challenges per cyber subdomain, simply because they are too numerous. Instead, we inspected again the (high-impact) cyber incidents described above and brought to mind here that, within the current geopolitical climate, cyber threats also come from abroad, both intentional, like in the context of international business competition or military conflicts, and unintentional, in the context of failures of global IT or OT services. So, we add, as a relatively general additional cybersecurity challenge for businesses and other organizations, the challenge (4) to adequately deal with the cyber threats from abroad with an aim to stay sufficiently cybersecure.

Thinking about cybersecurity challenges for government, we first observe that both for their internal operations and for critical infrastructures the same observations hold as those described in the previous two paragraphs, so this again concerns challenges (3.1), (3.2), …, and (4). But, in addition, we know that governments have the general governance task of making and keeping the relevant parts of cyberspace sufficiently secure (challenge (5)), based on their social contracts with citizens, companies, and other organizations [4]. This concerns again, like for businesses and other organizations, two complementary challenges, the first one (5.1) being the information security of all IT and OT infrastructures in use (layer 1 of the cyberspace model), the second one (5.2) the security of cyber activities and processes in cyber subdomains (layer 2).

Elaborating the two complementary challenges, we observe that the information security challenge (5.1) concerns the cybersecurity governance of both (the underlying) Internet (5.1.1) and the (higher level) IT- and OT-platform services, as made available by (mainly the big) IT companies (5.1.2). At the lowest level of the information security challenge (5.1.1), we should pay attention to the availability of sufficient, secure hardware. Also here, geopolitical tensions play a role related to the scarcity of certain essential raw materials, the production of microchips (see ref. [32] for example, the ASML case), and the potential insecurity of essential hardwired devices (like the controversy around 5G network devices coming from China [33]). With respect to the higher layers in the Internet protocol stack, we see that global Internet governance is conducted "by a decentralized and international multistakeholder network of interconnected autonomous groups." These groups aim "to create shared policies and standards that maintain the Internet's global interoperability for the public good" [34]. Originally, they (successfully) focused on technical issues like the establishment of unique domain names, IP addresses, and protocols. However, later on, other principles such as freedom of expression, freedom of information and human rights have been adopted by the multistakeholder network. These principles actually concern the cybersecurity challenges (2.1), (2.2), ..., where the bad news is that there exist huge international disagreements over what these principles practically mean and imply.

The information security challenge (5.1.2) of securing the (higher level) IT- and OT-platform services relates to cloud- and IoT-technologies. Concrete issues involve reducing dependency on services of the major IT companies, creating fair and transparent free market conditions for these (without monopolies), and enforcing compliance with the law (for example, related to privacy preservation and counteracting vendor lock-in).

The governmental challenge (5.2) of securing cyber activities and processes in all cyber subdomains is even a bigger one. It implies that citizens of all ages should become competent cybersecure actors, homo digitalis, and that governments have the task to design and implement a national cybersecurity strategy and related action plan (5.2.1) with concrete elaborations in terms of additional cyber education, stimulation, support, and enforcement. Similarly, and also part of the strategy and action plan, business and organizations (including the ones belonging to the government itself) should be supported and enforced to act and process cybersecurity (5.2.2). The four modalities of IT regulation [8] mentioned in Section 1 of this chapter certainly apply here.

The safeguarding of cyberspace also requires the creation of better cyber situational awareness (knowing and understanding what 24/7 is happening in relevant cyberspace subdomains [4]), based on which governments more continuously can assess actual cyber risks and inform the public about this. A final important governmental task concerns the institutional design of a cybersecurity governance ecosystem (with arrangements between actors that regulate cybersecurity tasks, responsibilities, costs, benefits, and risks [4]), with adequate governmental supervision.

4. Actual cyber resilience levels

When cyberspace for everyone suddenly emerged at the end of the previous century, cyber skills were generally low and cyber resilience a nonexistent term. But shaken awake by a growing number of incidents, cybersecurity awareness started to increase gradually and, supported by campaigns, trainings and discussions, cybersecurity behavior to improve little by little. Actually, a kind of cybersecurity rat race emerged where attackers enhanced and refined their attacks (see ref. [4] for eaxmple, the "unified kill chain model"), and, as a reaction, cyber actors improved their defensive cybersecurity practices (which, in their turn, stimulated attackers to further sophisticate their attack strategies, and so on and so on). As a consequence of these dynamics between cyber attackers and defenders, we note that cyber resilience levels are not fixed but change over time. So, it is hard to know precisely how high these levels are today. Therefore, we decided not to assess their precise levels but, instead, to just describe observed trends in the efforts defenders make to secure their digital activities and processes.

The rat race mentioned above is certainly visible for the group of end-users. Supported by the availability of various defense tools (like advanced virus detection tools) and the enforcement of two-factor authentication and other security practices by e-services providers, end-users now more regularly install software updates, backup their data, and show improved cyber behavior. Being better aware of the risks, end-users also act more cautious, for example, when reading emails (with possibly phishing intentions), participating in social networks, performing transactions during e-shopping or e-booking activities, or being called by a supposedly bank employee who asks for login details. When surfing via open communication channels, growing numbers of people (especially those living in countries without freedom of speech and press) make use of a Virtual Private Network (VPN) connection (to hide their cyber activities from others). In addition, they pay more security attention when installing IoT devices or uploading handy smart phone apps.

On a larger scale, the same trends are visible for businesses and other organizations, including governmental institutions, where the bigger ones usually do better. The related cyber security endeavors are not only motivated by their own cyber risk assessments but also through enforcement by national and internal rules and regulations. In Europe, for example, the 2016 General Data Protection Regulation (GDPR) set strong guidelines for the collection and processing of personal information from individuals. These guidelines are compulsory for businesses and other organizations acting in one of the European Union (EU) countries and have a huge impact. Probably even more influential is the 2023 Network and Information Security Directive 2 (NIS2). It obligates medium-sized and large companies, as well as organizations working in one of seven essential sectors, to "strengthen the security requirements, address the security of supply chains, streamline (cyber incident) reporting obligations," among others. More specifically for companies that produce devices with digital elements, the 2022 Cyber Resilience Act (CSR) is of importance. It prescribes that digital devices should be designed in such a way that those receiving automatic updates should also receive automatic security updates. Those companies should furthermore conduct cyber risk assessments for their products and report occurring cyber incidents. For more details about these and many other cybersecurity regulations, mostly of western countries, we refer to [35] and its numerous references.

With respect to governmental institutions, similar trends as described in the previous paragraph hold for their e-enabled processes. With respect to NIS2, national governments do have additional obligations like adopting a national cybersecurity strategy and action plan (for an example see ref. [36]), participating in coordinated vulnerability disclosures by fixing them in a European registry, ensuring that measures of supervision or enforcement are effective, proportionate, and dissuasive, and ensuring the imposition of administrative fines, among others. This also involves the monitoring of the big IT companies and the requirement to act in cases they transgress the applicable cyber rules or regulations. Concrete cases, for example, related to the GDPR legislation [37], show that governments do enforce cyber legislation, but the fines issued are mostly incomparable and small compared to the (huge) profits of those companies.

With respect to the governmental task of creating cyber situational awareness that helps to enhance cyber resilience, complications exist since governments should themselves behave compliant with existing cyber legislation [35], for example with respect to the privacy of people. This creates limitations to what extent governments can track and trace people. Another complication here is that illegal and criminal activities are often executed on the dark web. Of course, national intelligence services and other security companies are very active here, but they are generally not very transparent in what they know and discover, which, in turn, thwarts citizens and business organizations from understanding actual cyber risks.

A very recent development concerns the governmental effort to deal with generative AI-related security problems. Next to the many benefits (see also Section 2) generative AI may "affect public values such as non-discrimination, privacy, and transparency. If it leads to the deterioration of our information ecosystem, it thereby affects democracy and our rule of law" [38]. We are also aware of many discussions on the relationship between intellectual property rights and generative AI. Reference [38] of the Dutch Ministry of Internal Affairs further provides a list of six action lines to deal with generative AI, like "closely monitoring all developments," "shaping and applying laws and regulations," and "strong and clear supervision and enforcement," which actually shows that governments still struggle with the control over this new cyber development.

More generally, we may conclude from this and other examples that, due to the fast emergence of new cyber activities and processes and the much lower speed of new cyber law adoption, cyber security legislation is at various stages of implementation and often not yet adapted to the newest cyber security challenges.

5. Cybersecurity solution directions

Having created updated pictures of actual cybersecurity challenges and cyber resilience levels, we can now sketch cybersecurity solution directions. Remembering the list of recent cybersecurity incidents, we start by bringing to mind that solutions that guarantee 100% security are not available and that we always should prepare for unexpected cybersecurity breaches. This is often compactly framed as "expect the unexpected." So, solutions always have their limitations.

To formulate our set of solution directions, we return to the cybersecurity challenges of Section 3 and analyze to what extent they are dealt with by the actual cyber resilience efforts presented in Section 4. In the background, we also keep in mind the various cyber incidents mentioned in subsection 3.1.

The first general cyber security challenge (1) was formulated as "to provide cyberspace actors, in their various roles, with sufficient knowledge and skills to apply *adequate cyber risk management.*" Analyzing the actual cyber resilience efforts, we observe that, although much progress has been made in awareness and skills, cybersecurity risk capabilities and practices of people need to be further improved. This might be achieved to stimulate them, both at home, work or whatever environment, to better think through the kinds of cyber risks they may face when executing their cyber activities. This should result in *internalized cybersecurity behavior,* like installing antivirus software, always locking your computer when leaving your workplace, prompt installation of critical software updates, and making regular backups with a frequency adapted to the identified cyber risks. And for those installing IoT devices, they should automatically pay attention to the related cybersecurity risks.

Also, businesses and other organizations are doing better nowadays, but many of them do not have a sufficiently developed corporate culture around cybersecurity management, with clear responsibilities for the various employees under the umbrella of a companywide cybersecurity strategy. In addition, we observe that governments are now taking up the cybersecurity risk management challenge (more) seriously, but the implementation of a cybersecurity governance ecosystem serving the whole country with clear cybersecurity responsibilities and supportive laws and regulations is far from complete. Regarding the design and implementation of a trustworthy cyber social contract between governments and civilians (which anchors what cybersecurity responsibilities governments take upon for companies and civilians in exchange for certain obligations of the latter), we only observe first attempts. We conclude that cybersecurity challenge (1) still holds and requires action in all cyber subdomains by all cyber actors in the three layers of cyberspace.

The general cybersecurity challenge (2) was formulated for end-users and expressed as "the accomplishment of *secure cyber behavior* with respect to their cyber activities in various cyber subdomains." Although also here improvements are visible (see Section 4), we see that cyber behavior in various contexts, like social networking, is far from inherently secure. To compare, if persons nowadays participate in traffic as pedestrian, biker, car driver, or whatsoever, most of them are very aware of the risks in all kinds of circumstances and show secure traffic behavior adapted to the actual situation; they internalized secure behavior in traffic. This level of security behavior should also be achieved in cyberspace and should be stimulated, and often even enforced in the various cyber subdomains. As an enforcement example let us assume, in a (unfortunately unrealistic) thought experiment, that we could get global agreement on a ban on anonymous cyber participation in social networks or other worldwide cyber environment, then their adoption would certainly substantially reduce the number of cyber incidents for individuals, companies and even states. The assumption of getting global agreement is unfortunately not feasible for such global cyber environments, but in other, smaller cyber subdomains, agreement might be reached and could a ban on anonymous cyber behavior be an effective enforcing measure.

The cybersecurity challenge (3) for business and other organizations was expressed as "to keep their *e-business processes sufficiently secure*, and thus sufficiently resistant against intentional and unintentional, internal and external threats." This challenge *also holds for governments* with respect to their internal operations. And again, we observe that progress is being made here, certainly regarding security awareness, but issues like the realization of internalized cybersecure behavior and cybersecure business processes, and law compliance are still often not sufficiently dealt with. Actually, we observe here also doubtful developments like the outsourcing of IT services to (what are sometimes termed) "hyperscalers" that offer large-scale data processing and data storage services [38].

The state-of-the art concerning general cybersecurity challenge (4) "to adequately deal with the *cyber threats from abroad* with aim to stay sufficiently cybersecure," which was formulated for both business and governments, may considered as probably one of the most disturbing. The underlying reason is that most of the cyberattacks are being executed by state actors and internationally organized criminals, and the amount and intensity of these attacks is expected to only increase in the coming years. The very up-to-date information on significant cyber incidents actually substantiates this claim; see reference [39, 40] and similar sources.

Cyber security challenge (5) for governments was decomposed in an information security challenge (5.1) concerning the *governance of national and international IT & OT infrastructures*, and the governmental challenge (5.2) of *securing cyber activities and processes in all cyber subdomains*. These concern both huge challenges, which can only successfully be dealt with in an international context. It would be of great value if the United Nations organization could get a leading role here, for example, as mediator in international cyberwar-related conflicts and in efforts to reduce international crimes (for example, with respect to what happens in the dark web), but we should notice here that this solution direction is currently also difficult to achieve due to geopolitical tensions.

A prerequisite for challenge (5.1) is to intensify the efforts in international forums to get agreement on how the dependence and power of the big IT companies (for example, in the ways they retain customers, stimulate screen addiction, and deal with their personal data) should be kept within acceptable limits. The good news is that the EU is taking these challenges seriously and often starts new initiatives, for example, by adopting and enforcing new cybersecurity legislation and by taking action against big companies who break the rules. The bad news, however, is that the current geopolitical tensions also here thwart global agreements regarding these challenges and actually invite for all kinds of new cyber conflicts. Governmental challenge (5.2) involves as the very first step the adoption and true implementation of a national cyber security strategy and related action plan, next to many more initiatives as described above.

6. Conclusions

In this final section, we confine ourselves to providing *a few main conclusions* concerning the goals of this chapter and some additional findings.

The choice of using the three-layer Cyberspace Model and the Cybersecurity Bowtie Model to frame our thoughts and observations appeared again to be very effective. Especially the *separation between the concept of information security* and *that of cyber security is crucial* to formulate challenges and solution directions in *behavioral and technical terms* that *everybody can understand*. This is actually in stark contrast to the conceptualizations used in the popular ISO/IEC 27000-series on information security [6], where the security of data and information (in the abstract terms of confidentiality, integrity, and availability) is the starting point. The latter results into information security management solutions that are almost solely understandable for specialized IT-security management persons. Our first conclusion is therefore:

- The ISO/IEC 27000-series [6] need to be rewritten, where cyber activities and cyber processes are defined as the key assets to be sufficiently secured.

The choice of adopting a multi-actor approach in the Cyberspace Model helped to formulate *actual cybersecurity challenges* for *three groups of cyber actors* being end-users, businesses and other organizations, and governments. These challenges can be framed in terms of behavioral influence toward internalized secure cyber behavior, and toward adequate cyber risk management (at home, work, school, …), the creation of a corporate cyber security culture (in companies and other organizations including governmental institutions), and the development and implementation of a national cyber security strategy with accompanying action plan, where much attention is paid to international cyber threats. In this chapter, we have only been able to sketch the actual cybersecurity challenges in relatively general terms. We, therefore, formulate our second main conclusion as:

- The actual cybersecurity challenges described should be further concretized by the different cyber actor groups.

In the section on *cyber resilience*, we observed that in general all cyberspace actors are showing improvements; individuals do show more awareness and improved cybersecurity behavior, so do business and other organizations. Also, governments are taken cyberspace as new fifth domain seriously nowadays, and started to implement cybersecurity related regulations that are highly needed. But because of the sometimes still very unexpected occurrence of new cyber incidents, it is clear that the enhancement of cyber resilience levels still needs our attention, where taking repressive measures to limit the impact of occurring incidents should not be forgotten. We therefore also conclude that.

- Cyber resilience capabilities of all actors in cyberspace need to be further refined toward fully internalized cyber resilience behavior.

In the previous section on solution directions, we observed that these involve the continuation of the efforts of taking on the cybersecurity challenges of all cyber actors. Compared to say 10–20 years ago, we observe a society that is (a) much more active in cyberspace because of its benefits, but also (b) much more aware of (potentially) negative aspects. What we possibly mostly need to do now is to organize more discussions on what is happening cyberspace, what we think is correct and incorrect behavior, what cyber threats exist and related risks are, and what cybersecurity measures everyone can and should take to deal with these risks. This leads to the final conclusion formulated as:

- Let us all take cyberspace as separate fifth domain very seriously and organize more discussions, both nationally as internationally, on how we wish and should (securely) behave ourselves in this exciting domain.

Acknowledgements

I would like to express here my sincere thanks to IntechOpen for their kind invitation to compose this chapter and for their active funding support.

Author details

Jan van den Berg[1,2]

1 Faculty of Electrical Engineering, Mathematics and Computer Science and Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands

2 Faculty of Governance and Global Affairs, Leiden University, The Hague, The Netherlands

*Address all correspondence to: j.vandenberg@tudelft.nl

References

[1] Pagamini P. NATO officially recognizes cyberspace a warfare domain [Internet]. 2017. Available from: https://securityaffairs.com/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html [Accessed: July 19, 2024]

[2] Dark web [Internet]. Wikipedia. 2024. Available from: https://en.wikipedia.org/wiki/Dark_web [Accessed: July 27, 2024]

[3] Van den Berg J, Van Zoggel J, Snels M, Van Leeuwen M, Boeke S, Van Koppen L, et al. On (the emergence of) cyber security science and its challenges for cyber security education. In: Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium; 13-14 October 2014; Tallinn, Estonia (Winner of the Best Paper Award)

[4] Van den Berg J. A basic set of mental models for understanding and dealing with the cybersecurity challenges of today. Journal of Information Warfare. **19**(1):26-47. Available from: https://www.jinfowar.com/journal/volume-19-issue-1/basic-set-mental-models-understanding-dealing-cybersecurity-challenges-today [Accessed: July 28, 2024]

[5] NCTV, Ministry of Justice and Security. Cyber Security Assessment Netherlands (CSAN). The Hague, The Netherlands. 2023. Available from: https://english.nctv.nl/documents/publications/2023/07/03/cyber-security-assessment-netherlands-2023 [Accessed: July 28, 2024]

[6] ISO/IEC JTC1. ISO/IEC 27001. Information Technology—Security Techniques—Information Security Management Systems—Requirements. Geneva, Switzerland: ISO; 2005

[7] Tanenbaum AS. Computer Networks. 3rd ed. New Jersey, USA: Prentice Hall; 1996. 795 p

[8] Lessig L. Code and Other Laws of Cyberspace. New York, USA: Basic Books; 1999

[9] UN International Civil Aviation Organization (ICAO). BowTieXP, bowtie methodology manual [Internet]. Revision 39. 2019. Available from: https://www.icao.int/safety/SafetyManagement/SMI/Documents/BowTieXP%20Methodology%20Manual%20v15.pdf [Accessed: July 28, 2024]

[10] Popper KR. The Open Society and its Enemies. 4th ed. Routledge & Kegan Paul Ltd; 1962. 735 p

[11] Transdisciplinarity [Internet]. Wikipedia. 2024. Available from: https://en.wikipedia.org/wiki/Transdisciplinarity [Accessed: August 6, 2024]

[12] Pelchen L. Internet users statistics in 2024 [Internet]. ForbesHOME. 2024. Available from: https://www.forbes.com/home-improvement/internet/internet-statistics/ [Accessed: July 30, 2024]

[13] Musiał K, Kazienko P. Social networks on the internet. World Wide Web. 2013;**16**:31-72. DOI: 10.1007/s11280-011-0155-z

[14] Tulane University, School of Professional Advancement. Everything you should know about the dark web [Internet]. Available from: https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web [Accessed: July 31, 2024]

[15] Atria Convergence Technologies Ltd. Top 10 uses of the internet [Internet].

2023. Available from: https://www.actcorp.in/blog/top-10-uses-of-the-internet [Accessed: July 31, 2024]

[16] CoinMarketCap. All cryptocurrencies [Internet]. 2024. Available from: https://coinmarketcap.com/all/views/all/ [Accessed: August 1, 2024]

[17] Terra J. Real-world IoT applications in 2024 [Internet]. SimpliLearn. 2024. Available from: https://www.simplilearn.com/iot-applications-article [Accessed: August 2, 2024]

[18] Bersani S. How generative AI can empower human creativity [Internet]. COLIBRYX. 2024. Available from: https://colibryx.com/en/blog/how-generative-ai-can-enhance-human-creativity

[19] Elegent Themes. What is ChatGPT & 10 creative ways to use it in 2024 [Internet]. 2024. Available from: https://www.elegantthemes.com/blog/business/what-is-chatgpt#10-generating-ai-art [Accessed: August 1, 2024]

[20] BIGCOMMERCE. 12 E-commerce trends that are powering online retail forward [Internet]. 2024. Available from: https://www.bigcommerce.com/articles/ecommerce/ecommerce-trends/ [Accessed: August 2, 2024]

[21] Chadha M. 15 cloud computing applications [Internet]. 2024. Available from: https://www.shiksha.com/online-courses/articles/cloud-computing-applications/ [Accessed: August 2, 2024]

[22] Wavetec. 2024. Available from: https://www.wavetec.com/blog/public/digitizing-public-services/ [Accessed: August 2, 2024]

[23] Abels J. Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. European Journal of International Relations. 2024. DOI: 10.1177/13540661241260653 [Accessed: August 10, 2024]

[24] Big Tech [Internet]. Wikipedia. Available from: https://en.wikipedia.org/wiki/Big_Tech [Accessed: August 10, 2024]

[25] World Economic Forum. CrowdStrike content update causes global IT outage, and other cybersecurity news to know this month [Internet]. 2024. Available from https://www.weforum.org/agenda/2024/07/crowdstrike-global-it-outage-cybersecurity-news-july-2024/ [Accessed: August 11, 2024]

[26] Stewart E. Top 10 biggest cyber attacks in history [Internet]. EM360Tech. 2024. Available from: https://em360tech.com/top-10/top-10-most-notorious-cyber-attacks-history [Accessed: August 11, 2024]

[27] Bussu A, Pulina M, Ashton S-A, Mangiarulo M. Exploring the impact of cyberbullying and cyberstalking on victims' behavioural changes in higher education during COVID-19: A case study. International Journal of Law, Crime and Justice. 2023:75. DOI: 10.1016/j.ijlcj.2023.100628 [Accessed: August 11, 2024]

[28] Raghavan R. Top 20 advantages and disadvantages of social media [Internet]. 2024. Available from: https://webandcrafts.com/blog/social-media-advantages-and-disadvantages [Accessed: August 13, 2024]

[29] Mondo Insights. Types of cyberattacks on social media & how to prevent them [Internet]. Available from: https://mondo.com/insights/social-cyberattacks/ [Accessed: August 11, 2024]

[30] Trifunović D, Zoran BZ. Cyber war—Trends and technologies. NSF Volumes.

2021;**21**:65-94. DOI: 10.37458/nstf.21.3.2 [Accessed: August 12, 2024]

[31] Bendovschi A. Cyber-attacks—Trends, patterns and security countermeasures. Procedia Economics and Finance. 2015;**28**:24-31. DOI: 10.1016/S2212-5671(15)01077-1

[32] Robinson D. US wants ASML to stop servicing China-owned chip equipment [Internet]. The Register. 2024. Available from: https://www.theregister.com/2024/03/07/us_asml_china_restrictions/ [Accessed: August 15, 2024]

[33] Concerns over Chinese involvement in 5G wireless networks [Internet]. 2024. Available from: https://en.wikipedia.org/wiki/Concerns_over_Chinese_involvement_in_5G_wireless_networks [Accessed: August 15, 2024]

[34] Internet governance [Internet]. Wikipedia. 2024. Available from: https://en.wikipedia.org/wiki/Internet_governance [Accessed: August 14, 2024]

[35] Cyber-security regulation [Internet]. Wikipedia. 2024. Available from: https://en.wikipedia.org/wiki/Cyber-security_regulation [Accessed: August 16, 2024]

[36] NCTV, Ministry of Justice and Security. The Netherlands Cybersecurity strategy 2022-2028 [Internet]. The Hague, The Netherlands. 2022. Available from: https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028 [Accessed: August 15, 2024]

[37] Husain O. 52 biggest GDPR fines and penalties (2018-2024) [Internet]. 2024. Available from: https://www.enzuzo.com/blog/biggest-gdpr-fines [Accessed: August 17, 2024]

[38] Hyperscale computing [Internet]. 2024. Available from: https://en.wikipedia.org/wiki/Hyperscale_computing [Accessed: August 20, 2024]

[39] Center for Strategic and International Studies (CSIS). Significant cyber incidents [Internet]. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed: August 30, 2024]

[40] Kondruss B. Cyber attack news today [Internet]. KonBriefing. Available from: https://konbriefing.com/en-topics/cyber-attacks.html [Accessed: August 30, 2024]