Grasping cybersecurity

A set of essential mental models

van den Berg, Jan

Publication date
2019

Document Version
Final published version

Published in
Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019

Citation (APA)
van den Berg, J. (2019). Grasping cybersecurity: A set of essential mental models. In T. Cruz, & P. Simoes (Eds.), *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019* (Vol. 2019-July, pp. 534-543). IARIA / Curran Associates.

Grasping Cybersecurity: A set of Essential Mental Models

Jan van den Berg
Delft University of Technology, Delft, The Netherlands
j.vandenberg@tudelft.nl

Abstract: For most people, cybersecurity is a hard to grasp notion. Traditionally, cybersecurity has been considered as a technical challenge and still many specialists view it equivalent with information security, with the notions of confidentiality, integrity and availability as starting points of thinking. And although others searched for a broader perspective, the complexity and ambiguity of the notion still thwarts a common understanding. While developing and executing a MSc cybersecurity program for professionals, the lack of a common understanding of what cybersecurity entails was again observed. Stimulated by this, we started to look for and define a new, transdisciplinary conceptualization of cybersecurity that everyone can agree upon. It resulted in two scientific papers published. This paper describes the outcomes of the continuation of our research journey. It turned out that the earlier introduced description of two key notions, namely that of *cyberspace* and that of *cybersecurity*, can still be considered as adequate starting points. Here, we describe a set of additional mental models that elaborates them and provides more detail to the meaning of the two key notions. In practice, it turned out that the additional mental models strongly support the description and analysis of existing and upcoming cybersecurity challenges and helps to understand how everybody, in his or her various roles, can or should contribute to reducing the related cyber risks to adequate levels. We further discovered that for certain cybersecurity challenges, especially those related to efficient cyber risk mitigation, we could not yet identify an adequate sub-set of mental models. This defines the agenda for near future cybersecurity research.

Keywords: cyberspace, cyber activities, cybersecurity, cyber risk management, mental models, holistic view, cyber situational awareness, cyber risk assessment, cyber risk mitigation

1. Introduction

For most people, including those responsible for it, cybersecurity is a hard to grasp notion. Traditionally, cybersecurity has been considered as a technical challenge and still many specialists view it equivalent with Information or IT Security, with the notions of Confidentiality, Integrity and Availability (CIA) as starting points of thinking. Also in information security standards like the (famous) ISO/IEC 27000-series (ISO/IEC JTC 1, 2018), (ISO/IEC JTC 1, 2005), the key asset chosen is 'information' and the 'preservation of the confidentiality, integrity and availability' of information is defined as the key information security challenge.

This conceptualization maybe rather clear to IT specialists (like those working in hardware and software R&D), for policy makers, strategic managers and end-users, among others, this cybersecurity framing is difficult to grasp and does not invite for proper actions from their side. As a consequence, many actors in cyberspace have difficulties in defining what their role can and should be in securing the digital environment. It leads to the situation that in many cyber sub-domains, a coherent cybersecurity approach is missing. Based on this, we argue that there is need for a re-conceptualization of what the cybersecurity challenge entails. More precisely we claim that there is a need for a broad view on cybersecurity that (a) everybody can grasp, and (b) enables that everybody understands how he/she can contribute to securing cyberspace, in each of his/her cyber activity roles.

While developing and executing an executive MSc Program Cybersecurity for professionals (Cyber Security Academy, 2019), we worked on the creation of a holistic view on cybersecurity and discovered that mental models turn out to be very useful to create a common conceptualization, understanding, and language about what cybersecurity essentiality is. Our work resulted in two papers (Van den Berg et al., 2014), (Van den Berg, 2018), in which we brought forward (the) two key elements of cybersecurity being (*i*) a clear *conceptualization of cyberspace*, and, (*ii*) a basic *definition of* what cybersecurity, i.e. *securing cyberspace,* encompasses.

During further cybersecurity research as well as continued execution of the MSc program, we elaborated these ideas by collecting all kinds of additional models and best practices in attempts to deepen the new conceptualization. This paper describes how far we have reached now by sketching the set of mental models that are thought to be most essential. In addition, we describe in which part of the cybersecurity challenge we are still missing some basic mental models. In a way to validate the proposed set of essential mental models, we also describe some examples of cybersecurity research in which these models have been applied.

The remainder of this paper is structured as follows. In section 2, we describe the basic model of *cyberspace* (consisting of three layers) and three supportive mental models, one for each layer. This creates the basics for describing in section 3 what the *cybersecurity challenge* essentially is using again one basic model (related to a cyber risk management cycle), supplemented by a series of supportive mental models. We here also identify some gaps in our body of cybersecurity knowledge (inviting for 3 key topics of cyber research to be performed in the near future). In section 4, we provide, in an attempt to validate the proposed set of mental models, the results from recent research, in which these models have been applied. Finally, in section 5, we draw conclusions and summarize future research topics.

2. Cyberspace and its security concerns

2.1 Three-layer model of cyberspace

The ISO/IEC standard 27032 (ISO/IEC JTC 1, 2012) - having the aim 'to clarify the terms and demonstrate global leadership with this and the other cybersecurity standards projects now in progress' - defines cyberspace as 'the complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks.'

This framing is somewhat related to Enterprise Resource Planning (Jacobs, F.R., Weston Junior, F.C.T., 2007) type of thinking where, in a layered approach, business processes, as executed by people and machines, are enabled by supportive IT services. The framing also relates to the purport of the well-known 'People, Process, Technology' triangle, where – in the context of software applications – people are split into end-users (of the applications) and application creators (i.e., IT specialists), where (business) processes relate (and should be aligned) to the strategic business goals of the organization (to be fixed by the strategic management), and where the supportive software applications enable better business-decisions by relevant decision makers (Halo Business Intelligence, 2009).

Based on an analysis of existing information security approaches and inspired by the above-given frameworks of thinking, we have provided a new conceptualization of cyberspace (Van den Berg, 2018) consisting of a three layer model, shown in figure 1, left side. It concerns the basic cyberspace model. The *middle layer* concerns the *socio-technical layer* of *cyber activities* as being executed by people and smart IT, in attempts to reaching their personal, business, or societal goals. Examples of cyber activity behavior include searching on the world wide web, execution of financial transactions, manufacturing goods and products, controlling critical infrastructures, law enforcement pursuits (around, for example, privacy breaches and selling illegal products in the dark web), up till criminal cyber activities of all kind, and cyber warfare operations. The *inner layer* of the cyberspace model concerns all IT that enables the cyber activities. So, in other words we can say that *cyber activities* are, basically, *IT-enabled activities*. The *outer layer* of the model concerns the *governance layer of rules and regulations* that should be put in place to properly organize the two underlying layers, including their security. The three layer model visualization further shows a sub-division of cyberspace in example *cyber sub-domains* to emphasize that cyber activities in different domains have often different characteristics and, as a consequence of that, different security requirements.

Due to the continuous process of strong digitization in almost all domains of society, the amount and variety of cyber activities we currently execute at home, when traveling, at work, and beyond, is enormous, and is still growing. For many of us, it is quite challenging to adequately cope with the rapid digitization developments and to stay competent as 'homo digitalis'. The basic challenge for *adequate cyber behavior*, which include secure cyber behavior, maybe therefore be formulated as becoming *unconscious cyber competent*. This is visualized in the middle at the right side of figure 1: the basic challenge is that every cyberspace actor, regarding all his/her cyber activities, takes the path from the state of being 'unconscious incompetent', via 'conscious incompetent' and 'conscious incompetent', to the final state of being 'unconscious competent'.

To clarify the key issues of the governance layer, we have chosen as mental model the picture shown at the top of the right side of figure 1. It concerns the *four modalities of regulation* in cyberspace as proposed by Lawrence Lessig (Lessig, 1999) being *laws* (next to rules, policies, and regulations), *norms* (informal societal rules), *markets* (to create the right incentives for stakeholders), and *architecture* (which concern physical or technical constraints on cyber activities). It should be clear that this framing of the four modalities of regulation is precisely

in line with the three layer model of cyberspace: the modalities laws, norms and markets steer cyber activities (in layer 2) from a governance perspective (in layer 3), while the modality architecture (in layer 1) put constraints on cyber activities using a technical approach.

For the *technical layer*, the key issues relate to the two protocol stacks that are in use to describe computer networks, namely, the OSI and TCP/IP protocol stacks. These stacks are in the core of what every cyberspace actor should understand to a certain extent.

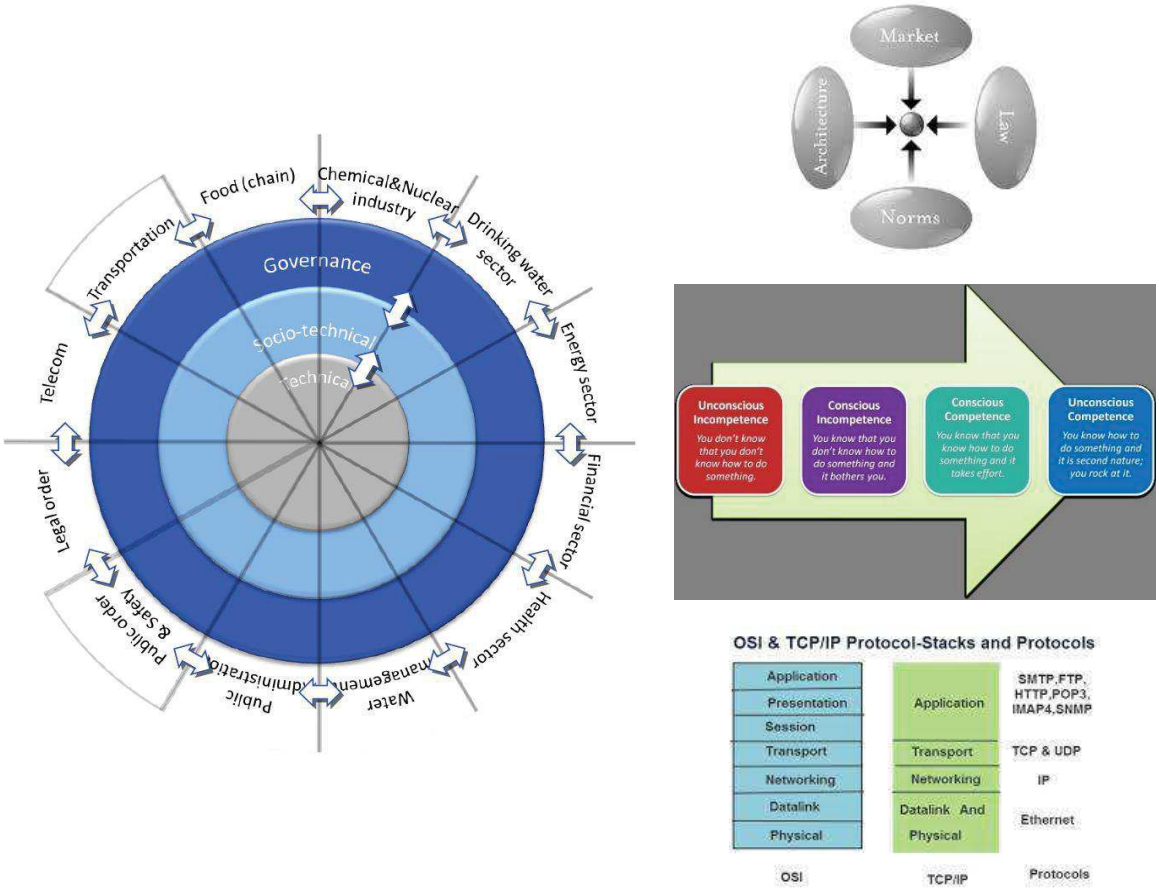


Figure 1: The 3-layer model of cyberspace (left), and three models describing the key cyberspace issues per layer (right)

2.2 Security concerns of cyberspace layers

Having conceptualized cyberspace in three layers, we can determine the *security concerns per layer*. To do so, let us start considering the key assets in cyberspace being the cyber activities. We may say that *cyber security* basically concerns the *security of cyber activities*, which actually is about the *security of cyber behavior!* It is easy to see that the security requirements of a cyber activity strongly depend of the type of the activity and its context. For example, the requirements related to the execution of a financial transaction in a public environment relate to secure payment behavior: careful use of debit/credit card, checking the amount before paying, shielding the keyboard of the payment equipment while typing your pin number, and inspection of the correctness of the receipt. When considering the automatic control of a critical infrastructure like water supply, the cyber security requirements are very different and are basically about guaranteeing continuous automatic supply of clean water to recipients, monitoring of this process, and committing necessary interventions 'through SCADA systems attached to distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs) and field devices' (ISACA, 2016). More in general, we can say that issues of secure cyber activity behavior (also) relate to minimization or no use of USB-sticks, to always choosing strong passwords, to never clicking on a URL in an email, and to very limited (or no) downloading of files from the Internet, among others.

Looking at the technical layer, we can use the classical requirements of information security being *confidentiality, integrity, and availability* (CIA) (ISO/IEC JTC 1, 2018). For the financial payment example just mentioned, all the three CIA requirements are relevant, while more refined technical requirements might be added here like secure identification, authentication and access (IAA) control, and non-repudiation. Note that, as a consequence of separating cyberspace in layers, we explicitly *discriminate between cyber security* (being the security of cyber activities in layer 2) and *information security* (being the security of IT of layer 1), a distinction that is quite different from the current practice.

Continuing our way of thinking, we further make the observation that incidents in the technical layer (often termed information security breaches) are actually (cyber) threats for the cyber activities executed in the socio-technical layer. If such cyber threats, emerging as information security incidents in the technical layer, result into incidents in the socio-technical layer, we can term these incidents cyber security incidents or cyber security breaches, which again shows an important difference in meaning of 'cyber' and 'information'. In short, within our conceptualization of cyberspace and cyber security, information security is truly something else than cyber security.

Finally, the security concern of the governance layer encompasses the fixation of rules and regulations (using the governance modalities mentioned above and in accordance with the chosen 'risk appetite': see below) for both the socio-technical and the technical layer. So, these governance rules and regulations should be related to both secure cyber activity behavior (in layer 2) and secure IT (in layer 1).

3. Modeling the cybersecurity challenge

Before diving into the cyber security challenge (which, as we will argue, basically concerns a risk management challenge), it is relevant to put forward the modern notion of risk. According modern standards, risk is the potential of gaining or losing something of value, or, according (ISO/TC 262, 2018), the (positive or negative) 'effect of uncertainty on objectives'. In the financial world, this phenomenon is well-known since investments can result into an actual return on an investment that is higher (opportunity) or lower (potential loss) than the expected return. In cyberspace we observe similar symptoms since digitization usually offers expected opportunities like efficiency, cost reduction, convenience, et cetera, but at the same it enhances the 'cyberattack surface' creating higher cyber risks. While for decision makers on cyber security it is always wise to take this two-sided view on cyber risk into account, the focus of our discussion in the remainder of this paper is mostly focused on the negative part of it.

3.1 The bowtie and the cyber risk management cycle

A well-known basic model used in safety and security science is the bowtie model. Basically, it reasons from (intentional and unintentional) threats to incidents next to the impact of the latter. Incidents occur with a certain probability or likelihood, and risk of a threat is defined as the expected impact of this threat, i.e., Risk = Likelihood times Impact. In cyberspace, the bowtie model can be used to model cyber threats, cyber incidents and their impact. To prevent cyber incidents from happening, preventive measures can be taken to reduce the probability of their occurrence. To reduce impacts of a given incident, repressive measures can be taken like measures related to detection and recovery. For more details on (the use of) the bowtie model, we refer to (Zipp, 2015). In figure 2, at the left side, a visualization of the bowtie is provided.

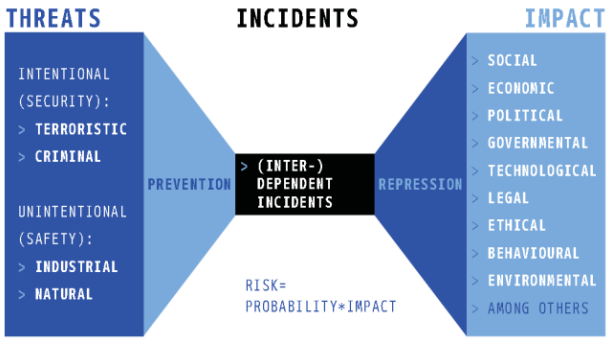


Figure 2: The bowtie model (left), and the basic cyber risk management cycle (right)

Since cyber activities are threatened, related cyber incidents may occur, sometimes with high impact. This clarifies why cyber security is actually a risk management challenge. Here, again, standards can help like the ISO standard (ISO/TC 262, 2018) mentioned above. It mentions that for proper risk management a risk management process should be executed. Here we provide this risk management cycle on the right in Figure 2, in the context of securing cyberspace. Within our framing, this concerns risk management of cyber activities.

Repeat 'forever'
(in all 'relevant' cyber sub-domains)
1. Identify the *critical cyber activities*
   (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 *cyber risk measures*
6. *Monitor effectiveness of measures taken*.

3.2 Additional mental models

Having defined and visualized the basic mental cyber security model in Figure 2, we can now sketch a set of additional models that provide background details. This is done by considering each of the six steps of the basic cyber risk management cycle. The first step concerns the identification of the critical cyber activities as executed by a person, organization or society. The critical cyber activities are the IT-enabled activities we mostly depend on and are, in case of being disrupted, expected to create the highest impact. In society, critical cyber activities are related to critical infrastructures like transport (of goods and people), supply of water & energy (electricity, oil, gas), as well as the financial, healthcare, and first aid services. In a digitalized corporate environment, data are often considered as critical and sometimes termed the 'crown jewels' (Fredriksen, 2018). Within our framing, we consider not its data but the critical cyber activities of a corporation as its crown jewels (which usually relate to its critical business processes) and they need to be cyber secured with the highest priority. For a visualization of the crown jewels, we refer to Figure 3 (left). But before being able to think about their security, they should be first identified and defined, which is still not common practice in many organizations as we have often observed.

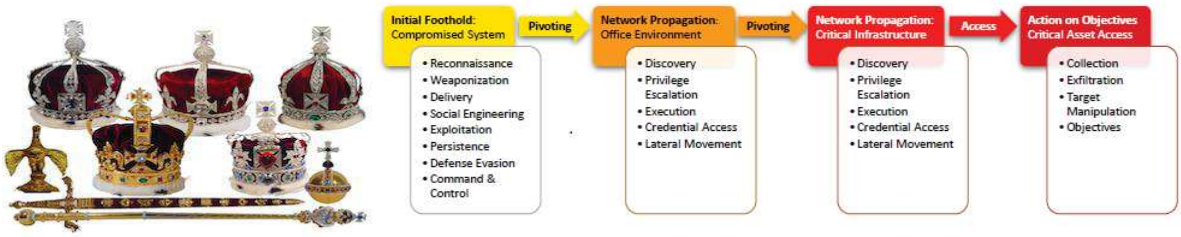


Figure 3: Two additional mental models related to the first two steps of the basic cyber risk management cycle: crown jewels (left) and the unified kill chain (right)

Once a person, organization or society has identified his/her/its critical cyber activities, the second risk management cycle step of identifying and assessing their cyber risks can be taken up. In case of considering intentional attacks, the 'unified kill chain' model can be applied for analyzing and defending against possible attack behavior: this model (visualized in Figure 3, right) describes in detail all possible steps an attacker can choose in attempts to disrupt (y)our critical cyber activities (Pols, 2018).

Such an analysis is of course only possible if we carefully monitor the cyber activities taking place on (y)our IT systems connected to the Internet or, in other words, we need to create sufficient 'cyber situation awareness'. The general notion of situation awareness was introduced in 1995 by Micah Endsley (Endsley and Jones, 2016) and is here applied in the context of securing cyberspace (Figure 4).

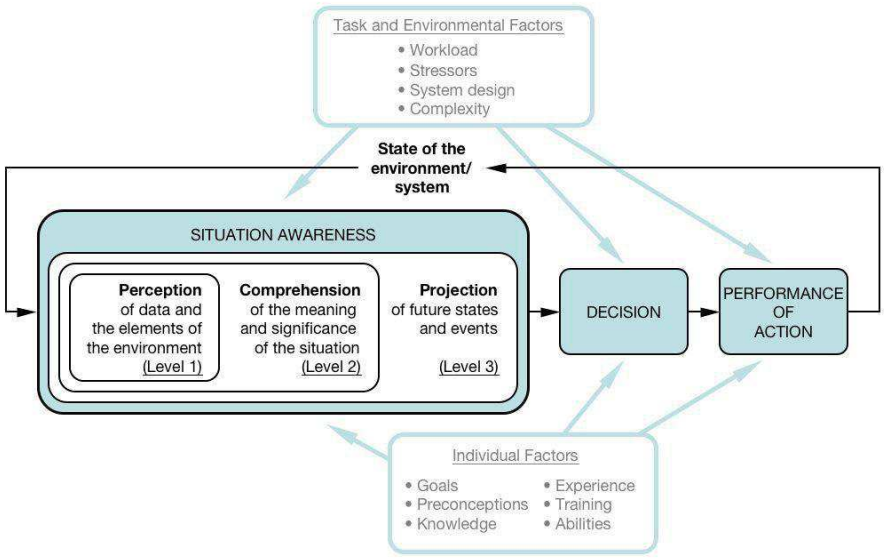
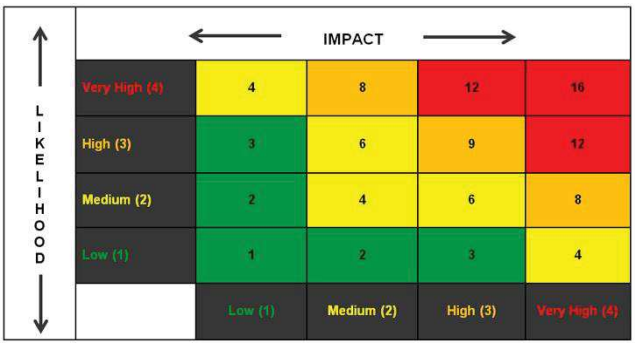


Figure 4: Another additional mental model related to the second step of the basic cyber risk management cycle: (cyber) situational awareness (Endsley and Jones, 2016)

Having organized adequate cyber situational awareness, one can try to assess the risk related to possible cyber activity incidents in terms of likelihood times impact. There are numerous methods available to make such assessments (for an overview we refer to (ISO/IEC TC 262, 2009)), but a picture showing the principle ideas is shown in Figure 5. The risk values found are shown with a color and range from low risk (green) to very high (red). This picture completes the set of four additional mental models related to the first two steps of the basic cyber risk management cycle.



Risk Score	Rating
0 – 3	Low
4 – 6	Medium
6 – 9	High
10 – 16	Very High

Figure 5: Yet another mental model related to the second step of the basic cyber risk management cycle: cyber risks assessment

The next step of the basic cyber risk management cycle concerns the fixation of acceptable cyber risk levels for each of the critical cyber activities. This relates the so-termed risk appetite of an individual, organization or society. Defining the risk appetite falls for the larger part outside the scope of science since it concerns mostly a choice and is often based on personal judgements. However, some remarks are of relevance here. For critical infrastructures, governments often determine the required risk levels as is common practice in the worlds of, for example, finance, energy supply, flood defense and (also) IT systems. Being not compliant with the related rules and regulations can result in severe penalties, which of course influences the risk appetite of an organization. Similarly, shareholders do have their ideas about managing (cyber) risk and the related risk appetite, so their voice is often decisive in the risk appetite choice of an organization.

Having assessed the relevant cyber risks and having chosen the acceptable cyber risk levels, the fourth step concerns the decisions how to deal with the assessed risks. A well-known principle from safety & security science tells us that there exist basically four response strategies to negative risk (Dorfman, 2007). The first one is *avoidance* by stopping the risky cyber activity at stake. The second one is *transfer* by making another party responsible for the risk through insurance or outsourcing. The third option is simply *accepting* the risk in case it is within your risk appetite. And the final response strategy is *mitigating* the risk to the defined acceptable risk

level by reducing the probability and/or impact of the cyber threat. The four possible risk response strategies have been visualized in Figure 6.

Figure 6: A mental model related to the fourth step of the basic cyber risk management cycle: risk response strategies

Step 5 of the basic cyber risk management cycle concerns the design and implementation of cyber risk measures, which is relevant in case you have adopted the strategy of risk mitigation in the previous step. This concerns a complex challenge since an abundance of preventive and repressive mitigation measures exist. Within our conceptualization of cyberspace, the challenge boils down to designing and implementing a 'balanced set of cyber risk mitigation measures' in the three layers. A simple example may illustrate the basic idea. Consider the case of using USB sticks, which is often a risky cyber activity since malware can be easily and fast transferred if sticks are used in different IT environments. Measures to mitigate such a malware infection risk at the socio-technical layer concern measures related to cyber activity behavior: someone, who feels herself a potential target for an infection attack via a USB-stick, might decide not to use such a device nor allow anyone else to use it on her PC or laptop. The identified USB infection threat might also be mitigated at the technical layer by disabling all USB ports in the IT environment at stake or, in a less restrictive approach, by monitoring USB stick injections and scanning on infections before allowing data retrieval from such sticks. Finally, at the governance layer, rules might be made official that USB sticks are not allowed inside a certain IT environment and, in case of a cyber incident occurrence due to a violation of this rule, the (financial or other) consequences are for the person who violated the rule.

In practice, cyber risk mitigation is usually a much more complex challenge than the simple example shows. Considering for example again critical infrastructures in our digitized society, we immediately observe that usually many stakeholders (often a combination of public and private actors) are involved, each one with specific responsibilities for the risk mitigation challenge. This thwarts the design and implementation of balanced risk mitigation approaches that are both effective and efficient. Actually, we identify here a huge research topic for the near future, since, up to our knowledge, so far little attention has been paid to the cyber risk mitigation challenge of designing and implementing balanced sets of cyber risk mitigation measures. However, we are not completely empty-handed with respect to filling in this knowledge gap. For example, to implement the often-heard adage of public-private partnership (PPP) in cyberspace, models from institutional economics are of relevance. The first one, a visualization of which is given in Figure 7 (left), relates to the 'institutional design for complex technological systems' in such a way that 'socially desired objectives are realized' (Koppenjan and Groenewegen, 2005). It discusses 'arrangements between actors that regulate their relations: tasks, responsibilities, allocation of costs, benefits and risks', so we argue that this theory can be very helpful for institutional design around securing cyberspace. A second model refers to social contract theory (Bierens et al., 2017). In this paper it is argued that also for cyberspace (next to existing societal domains), an appropriate social contract has to be fixed where it discriminates between a direct social contract (between citizens and the government) and indirect social contract (between citizens and the government but via private organizations), a visualization of which is given in Figure 7 (right).

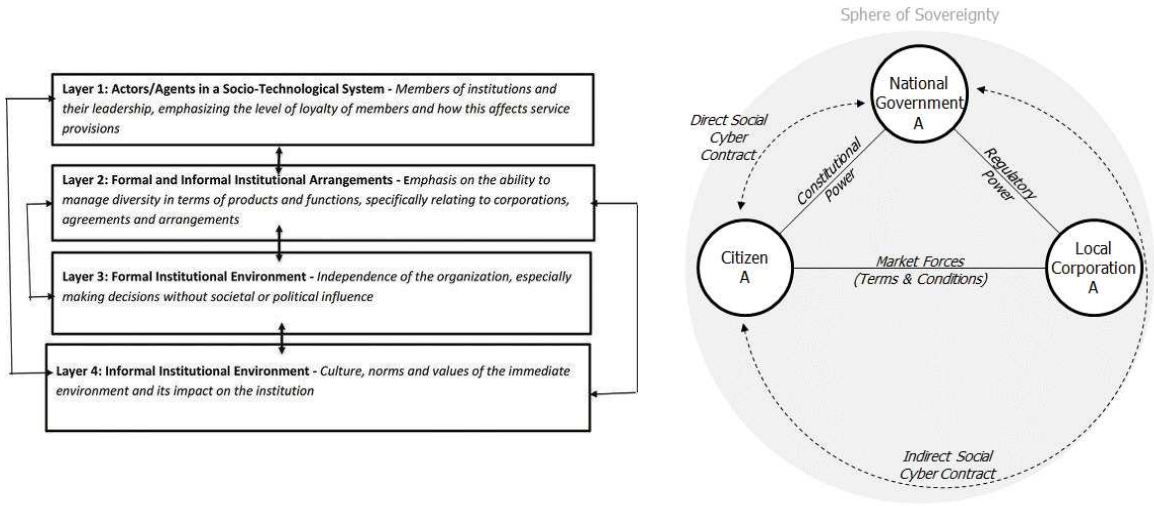


Figure 7: Two mental models related to the fifth step of the basic cyber risk management cycle: the four-layer diagram of institutionalization (left) and the direct and indirect social contract model (right)

Finally we consider step six of the basic cyber risk management cycle, where we have to take care of monitoring the effectiveness of the measures taken. We argue here that this strongly relates to the creation of cyber situation awareness discussed above. Measuring the effectiveness of measures taken is certainly not an easy task but through smart monitoring of cyber activities in the socio-technical layer and of IT-processes in the technical layer, we may create the necessary insights. And we are aware of certain examples. Currently, it has become commonplace to monitor and analyze real-time all kinds of financial transactions in attempts to prevent fraudulent ones, among other issues. In addition, national intelligence services are busy in monitoring cyber activities of foreign state (or state-sponsored) actors related to, for example, espionage or the distribution of fake news, and the police monitors the dark web on all kinds of illegal activities. And finally, researchers are monitoring and analyzing all kinds of Internet traffic to, for example, discover new threats based on new upcoming attack tools. Since such monitoring activities are strongly related to the creation of cyber situation awareness discussed above, we see no need to introduce an additional mental model here.

3.3 Three key challenges for the near future

Reconsidering the analysis results provided so far, we finalize this section by mentioning three key challenges for the near future in an attempt to arrive at adequate cyber security levels:

- *1. Creation of Cyber Situation Awareness:* although some progress has been made, the state of the art of understanding what happens in cyberspace is still insufficient. It is often heard that states, organizations and individuals have limited insights on the (in)correctness of relevant cyber activities and, as a consequence, the related cyber risks. Cyber Situation Awareness is crucial for understanding cyber risks, for measuring the effectiveness of cyber risk mitigation measures, as well as for dealing with fundamental dilemma's like between cyber opportunities and negative cyber risks (discussed above), and between privacy and cyber security. To illustrate the latter: if cyber risks are very high (e.g., societal disruptive), people tend to be more willing to accept privacy limitations to help law enforcement agencies to catch the perpetrators.
- *2. Methodologies for a Arriving at Balanced Sets of Cyber Risk Mitigation Measures:* being aware of the possibility to take all kinds of cyber risk mitigation measures in both the technical, socio-technical and governance layer of cyberspace, methodologies (or even a set of best practices) for selecting an balanced set of those measures that is both efficient and effective do not exist. This is considered to be an important research challenge for the near future.
- *3. Implementing Public-Private Partnerships (PPPs) for Securing Cyberspace:* although we observe a growing amount of emerging initiatives of increased cooperation in all kinds of cyber sub-domains, one might say that – compared to PPP implementations in physical world (land, water, air and space) domains – the development of those for securing cyberspace is still in its infancy. This may be caused by the enormous complexity of cyberspace with almost 4 billion people connected via the world-wide Internet on the one hand, and a few big players on the other (the famous 'Big Five' tech companies). However, governments

can not escape from their responsibility, as part of their social contract with their citizens, to take together the lead in creating public-private partnerships in the benefit of a more secure (fifth domain of) cyberspace. Researchers can support this development by suggesting suitable looking relation arrangements between relevant cyberspace stakeholders.

4. Use of mental models

As already mentioned above, the set of mental models introduced in this paper has been collected based on discussions and research collaboration with cyber security professionals while following an executive master's program (Cyber Security Academy, 2014). In attempt to validate the choice of models presented, we here briefly review the use of a few mental models during the execution of the research of some students when composing their final thesis. The cyberspace model of three layers has been often applied, for example, to structure the results of an analysis of the security of eHealth services of Dutch General Practitioners (Willems, 2017), or to structure a large set of requirements for designing a multi-stakeholder roadmap for implementing consumer vulnerability management (Bastiaanse, 2018).

In another thesis, the model of Lessig on cyber regulations modalities was applied to analyze policy strategies to make smartphone Virtual Private Networks (VPNs) available for consumers (Ghaoui, 2017).

As a final example, we mention here a thesis written on the design of a model for cyber security supervision of 5G in the Netherlands (Wazir, 2019). In this thesis, both the bowtie model and the three-layer model of cyberspace have been applied and have been integrated in one conceptual supervision model, which is shown in Figure 8. For more details, we refer to the related Master's theses, most of which are already available on line.

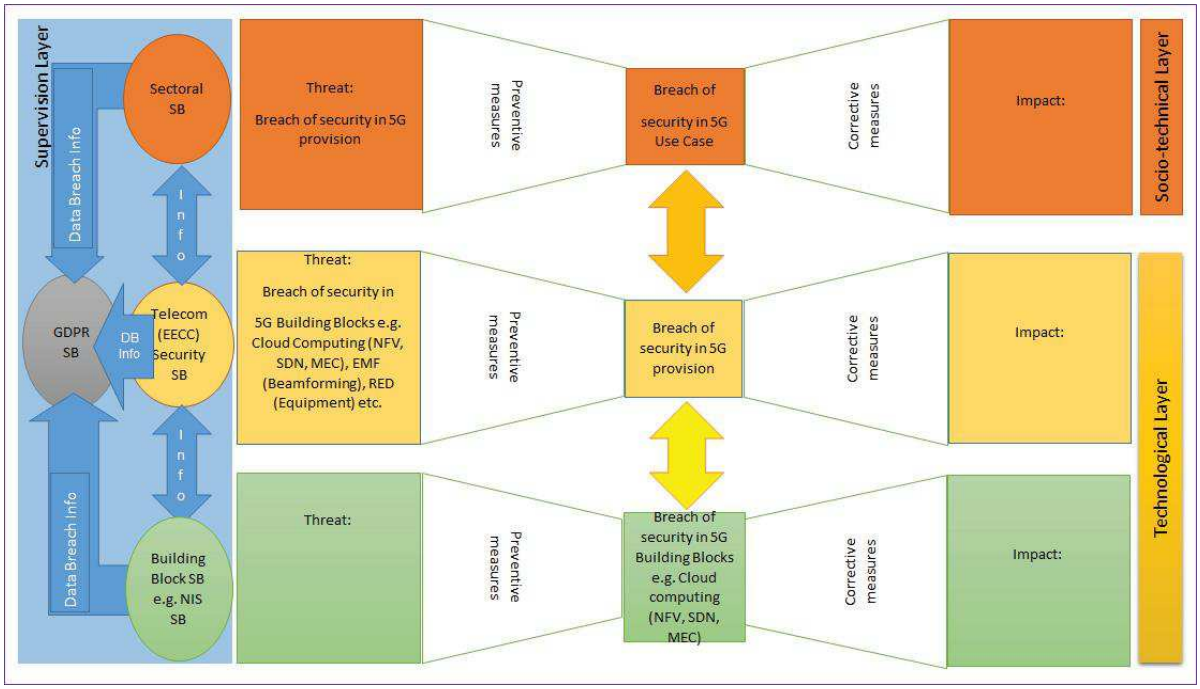


Figure 8: The Triple Bow Tie Cyber Security Supervision model with the 5G use case layer, the 5G provisioning layer and the 5G building blocks layer (Wazir, 2019).

5. Conclusions and future research

In this paper, a set of essential mental models have been presented that together cover the key elements of cyberspace and those of securing cyberspace, i.e., cyber security. They provide an overview on what cyberspace entails and what the related cyber security challenges encompass. In day-to-day discussions between cyber security professionals and during the execution of cyber security research, these models and the related frameworks of thinking have turned out to be useful and effective. The choice of making an explicit distinction between IT (the enabling technology of cyberspace in layer one) and the use of it (in terms of cyber activities in layer two) is crucial for understanding the difference between classical information (or IT) security and cyber

security. Cyber security is the new notion and concerns the challenge of sufficiently securing our cyber activities, the things we *do* using modern IT. The consequence of this framing is that everybody can now understand what cyber security is about since cyber activities are human-based and avoid the one-sided focus on (for many difficult to grasp underlying) IT. The second model with underling mental models emphasizes that cyber security is essentially a cyber risk management challenge. Here, risk is being considered as a two-side notion of being both an opportunity (positive risk) and a potential loss (negative risk). This invites for discussions on assessing at the same time potential advantages and disadvantages of (further) digitization. In this way, cyber security is not just only a cost factor but also a factor of potential profit, which, for sure, facilitates discussions on cyber security at board level. Finally, it is argued that, in one way of another, the design and implementation of the basic cyber risk management cycle is crucial for trying to create a sufficiently secure cyber environment in the cyber sub-domain at stake.

During our research journey we encountered three key challenges related to the implementation of the cyber risk management cycle that need soon further investigation, namely, *(i)* the creation of well-established cyber situation awareness in all kinds of cyber sub-domains, *(ii)* the design of methodologies for arriving at a balanced set of cyber risk mitigation measures in all cyber sub-domains, and *(iii)* the implementation of public-private partnerships in cyberspace.

References

Bastiaanse, H. (2018), "Multi-stakeholder roadmap for implementing consumer vulnerability management", *Master's thesis*, Cyber Security Academy, The Hague.

Bierens, R., Klievink, B., and Van den Berg, J. (2017), "A social cyber contract theory model for understanding national cyber strategies". In Jansen, M. et al., editor, Proceedings of IFIP EGOV-EPART 2017 Conference (EGOVEPART2017), volume 10428 of *Lecture Notes in Computer Science*, pp 166 - 176, St Petersburg.

Cyber Security Academy (2014), "About the CSA", https://www.csacademy.nl/en/about-csa (last access: 2019-02-03).

Dorfman, M.S. (2007), *Introduction to Risk Management and Insurance* (9th ed.), Prentice Hall, Englewood Cliffs.

Endsley, M. and Jones, D. (2016), *Designing for Situation Awareness* (Second ed.), CRC Press.

Fredriksen, G. (2018), "Protecting the Crown Jewels", Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/08/13/protecting-the-crown-jewels/#3eb2ba30a5a9 (last access: 2019-02-17)

Ghaoui, N. (2017), "Policy strategies for VPN for consumers in the Netherlands", *Master's thesis*, Cyber Security Academy, The Hague.

Halo Business Intelligence (2009), "People Process Technology, The Golden Triangle Explained", *white paper,* https://halobi.com/blog/people-process-technology-the-golden-triangle-explained/ (last access: 2019-02-03)

ISACA (2016), "The Merging of Cyber Security and Operational Technology", *white paper*, ISACA.

ISO/TC 262 (2018), *ISO* 31000:2018*, Risk Management, Guidelines*, ISO, Geneva, Switzerland.

ISO/IEC JTC 1 (2018), *ISO/IEC* 27000:2018, *Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*, ISO, Geneva, Switzerland.

ISO/IEC JTC 1 (2005), *ISO/IEC* 27001:2005, *Information Technology - Security Techniques - Information Security Management Systems - Requirements,* ISO, Geneva, Switzerland.

ISO/IEC JTC 1 (2012), *ISO/IEC* 27032:2012, *Information Technology - Security Techniques - Guidelines for Cybersecurity,* ISO, Geneva, Switzerland.

ISO/IEC TC 262 (2009), *ISO/IEC* 31010:2009, *Risk Management - Risk Assessment Techniques*, ISO, Geneva, Switzerland.

Jacobs, F.R. and Weston Junior, F.C.T. (2007), "Enterprise resource planning (ERP) - A brief history", *Journal of Operations Management*, vol. 25, No. 7, pp 357 - 363.

Koppenjan, J. and Groenewegen, J. (2005), "Institutional design for complex technological systems", *Technology, Policy and Management*, vol. 5, No. 3, pp 240 - 257.

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, Basic Books, New York.

Pols, P. (2018), "The Unified Kill Chain, Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks", *Master's thesis*, Cyber Security Academy, The Hague.

Van den Berg, J. et al., (2014), "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education", Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium, Tallinn, Estonia, October 13–14. (Winner of the Best Paper Award).

Van den Berg, J. (2018), "Cyber Security for Everyone". In Stefanie Frey and Michael Bartsch, editors, *Cyber Security Best Practices*, pp 571 – 583, Springer Vieweg, Wiesbaden.

Wazir, F. (2019), "Can NL trust 5G? A conceptual model for cyber security supervision of 5G in the Netherlands", *Master's thesis*, Cyber Security Academy, The Hague.

Willems, D. (2017), "Caring for security: an analysis of the security of eHealth services of Dutch General Practitioners", *Master's thesis*, Cyber Security Academy, The Hague.

Zipp, A. (2015), "BowTieXP, Bowtie Methodology Manual", *white paper*, preliminary version, IP Bank.