An uncommon yet indispensable combination of issues

Karsten Weber

If there is anything we can now regard as solidly established, it is that we don’t know how to build secure systems of any real complexity.

(Odlyzko 2019: 4)

Introduction: from dangerous computers to endangered computer systems

Today, one can read it in almost every newspaper nearly every day: computers or any other devices that are programmable and can be connected to the Internet are potential targets for a hacker attack. In a rather harmless case, such an attack might allow access to the camera and microphone of a laptop or smartphone, so that images and sound recordings can be made without the user’s knowledge. However, the potential damage an attack on computers might cause can be increased to virtually any degree. Examples of attacks might be illegal access to financial data, encryption of important data and extortion for a ransom, theft and misuse of personal data or trade secrets, purposeful sabotage of industrial plants, damage to or destruction of computer systems, shutdown, malfunction or destruction of critical infrastructures such as energy or water supplies. One even finds reports on the hacking of live supporting implantable devices like pacemakers or insulin pumps (e.g. Baranchuk et al. 2018: 1285ff.; Coventry and Branley 2018: 48ff.; Mohan 2014: 372; Ransford et al. 2014: 158ff.; Woods 2017). The list of threats and assaults likely could be extended almost indefinitely. Some attacks are carried out because the people running them want to show that they are able to do it – this was probably the original starting point for many hackers. Many committing these assaults have a criminal background; the attacks, then, represent the virtual version of a bank robbery or extortion and are usually referred to as cybercrime and, at times, cyberespionage (c.f. Connolly and Wall 2019; Dunn Cavelty 2014; Nadir and Bakhshi 2018). Sometimes, attacks on computer systems must be understood as terrorist actions; the term for this is cyberterrorism (see, for instance, the papers in Chen et al. 2014; Jarvis and Macdonald 2015; Weimann 2005). If such attacks are carried out by state authorities or by groups that are in close relationships to state actors, we would have to speak of state terrorism or even of a virtual variant of war – often called cyberwar or cyberwarfare (e.g. Liff 2012; Robinson et al. 2015).
In public perception, however, because there was hardly any information about the actual capabilities of computers readily available to the public in the early years of computer development, computers were not always seen as targets of attacks, but as the starting point of a threat. In the 1960s and 1970s, when computers were increasingly visible to the public but laypeople were poor at assessing their capabilities, stories were circulated, especially in the science fiction genre, in which giant “electronic brains” subjugated humans and sought world domination – the movie Colossus: The Forbin Project from 1970 can be seen as paradigmatic here (Weber 2018a). More recent films, such as the Terminator franchise with its Skynet computer unleashing a global thermonuclear war against humanity, tie in with such threat scenarios.

The discussion about the security of computer systems underwent a major change with the 1983 film War Games. In his book Dark Territory (2016), which provides an excellent account of the history of cyber threats, journalist Fred Kaplan writes that this film was instrumental in raising awareness among political and military leaders in the US about the vulnerability of military computer systems. The public, or at least parts of it, particularly in Germany and the US, probably first became aware of the hacking of (military) computer systems through Clifford Stoll’s book, The Cuckoo’s Egg (1989).

As far as computers are concerned, the 1980s are characterised by the speedy dissemination of home computers and the first personal computers. This is associated with the first large-scale attacks on these devices by computer viruses, which also attracted public attention. In fact, computer viruses appeared several years earlier (for the history of computer viruses, see Szor 2005). With the rapid spread of the Internet in the 1980s and 1990s, these malicious programs (or malware) were no longer spread through the exchange of data storage media such as floppy discs, but increasingly occurred because many computers were networked with each other locally and globally. The recognition that computers can therefore be targets for attacks probably became generally accepted by this time at the latest. Today, it is most likely that almost everybody living in an industrialised country has heard about some sort of cyberattack, since these are ubiquitous. As Fred Kaplan (2016: 5) puts it:

Once the workings of almost everything in life were controlled by or through computers – the guidance systems of smart bombs, the centrifuges in an uranium-enrichment lab, the control valves of a dam, the financial transactions of banks, even the internal mechanics of cars, thermostats, burglary alarms, toasters – hacking into a network gave a spy or cyber warrior the power to control those centrifuges, dams, and transactions: to switch their settings, slow them down, speed them up, or disable, even destroy them.

Cybersecurity begins and ethics (more or less) follows suit

However, the discussion about the security of computer systems started much earlier. Although at the beginning of the corresponding debates the terms “computer security” or “information security” were used rather than “cybersecurity”, the basic issues and perspectives were shaped very early. With regard to cybersecurity, probably two texts published by Willis H. Ware (1967a and 1967b) mark the beginning of the debates. Both papers are titled “Security and privacy” – the first text was written for the Rand Corporation (which primarily advises the US Air Force), and the second text was presented at an ACM conference. The ACM paper includes Figure 30.1, which presents possible attack vectors and threats:
Figure 30.1 Typical configuration of resource-sharing computer system

Source: Republished with permission of Association for Computing Machinery, from Ware 1967b; permission conveyed through Copyright Clearance Center, Inc.
It is also worth taking a closer look at the text even today, as Ware lists key challenges, as early as 1967, which arise in connection with the protection of computer systems against unauthorised access and which are still relevant nowadays (Ware 1967b: 281f.):

To summarize, there are human vulnerabilities throughout; individual acts can accidentally or deliberately jeopardize the protection of information in a system. Hardware vulnerabilities are shared among the computer, the communications system, and the consoles. There are software vulnerabilities; and vulnerabilities in the system’s organization, e.g., access control, user identification and authentication. How serious anyone of these might be depends on the sensitivity of the information being handled, the class of users, the operating environment, and certainly on the skill with which the network has been designed. In the most restrictive case, the network might have to be protected against all the types of invasions which have been suggested plus many readily conceivable.

Certainly, computer technology has changed significantly since Willis Ware wrote that paragraph, but the comments he makes in this very early paper regarding attack vectors, threats and possible motives for attack as well as the human factor still hold true. Actually, the definition of cybersecurity, provided by the International Telecommunications Union (2008: 3), somehow echoes the list of vulnerabilities Willis Ware mentions by enumerating the “collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organisation and user’s assets” as means to provide cybersecurity.

Almost as soon as the debates concerning cybersecurity gained momentum, moral, legal and political questions were raised that have shaped the discussion up to the present day regarding the extent to which the widespread use of computer systems will have an impact on individuals, groups and entire societies. In this regard, one of the most important contributions was certainly Alan F. Westin’s book *Privacy and Freedom* (1967), which established the connection between the protection of personal data and the preservation of individual freedom. Since then, scholarly work explicitly linking computer security or cybersecurity to ethics has continued to appear (e.g. Campbell 1988; Cooper 1995; Leiwo and Heikkuri 1998). Quite prominently, Diffie and Landau (1998) pointed out political aspects of computer system security in the late 1990s; Dittrich et al. (2011) called for the formation of a (scientific) community that should deal with computer security or cybersecurity and ethics. For some years now, more and more papers and books have been published that deal with such issues (see, for instance, the papers in Christen et al. 2019; see also Christen et al. 2017; Domingo-Ferrer and Blanco-Justicia 2020; Loi et al. 2019; Manjikian 2018; Pattison 2020).

**The lack of cybersecurity and its negative impact on societies**

Since there are many different types of threats to computer systems, whether attacks of cybercrime, cyberterrorism or cyberwar, that can have very different ramifications, these consequences can be measured with different scales (cf. Gandhi et al. 2011). For example, if SCADA systems of a power plant are attacked (cf. Chhaya et al. 2020; Mazzolin and Samueli 2020), this may cause malfunctions that could trigger the collapse of the power supply; this in turn may result in economic losses, but also in ecological damage, injury to people or, in the worst case, loss of life. Attacks on computers belonging to a country’s administration or government, in turn, can result in political instability, increase distrust of citizens in state institutions or limit
a government’s ability to act (for psychological and political effects of cyberattacks see, for instance, Gross et al. 2016; Herzog 2011; Iasiello 2013).

Although these are only two examples, it is probably already becoming apparent that the possible consequences that might arise from attacks on computer systems affect very different dimensions of individual, societal, corporate or political life. This makes it difficult to compare the amount of damage on a quantitative scale in these different dimensions. For this reason, the various reports that shed light on the consequences of computer attacks generally refer to economic damage in the sense of the costs incurred because of such attacks. While this facilitates comparisons, for example, between different sectors of the economy (cf. Tripathi and Mukhopadhyay 2020), between countries or even between the defender and adversary of an cyberattack (e.g. Derbyshire et al. 2021), it also hides the fact that a lack of cybersecurity not only causes monetary costs, but can also result in far-reaching damage that is difficult to measure.

The costs of cyberattacks worldwide have now grown to orders of magnitude that pose significant challenges to even high-performing economies. Moreover, these costs seem to know only one direction, increasing year by year. Cashell et al. (2004) report:

Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks).

However, the authors of this rather early report also emphasise that “the reliability of these estimates is often challenged; the underlying methodology is basically anecdotal”. Nearly a decade and a half later, the Center for Strategic and International Studies (CSIS 2018: 4) writes: “Our current estimate is that cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP”. Other metrics from CSIS used to measure the scope of cyberattacks are as impressive as they are worrisome:

One major internet service provider (ISP) reports that it sees 80 billion malicious scans a day, the result of automated efforts by cybercriminals to identify vulnerable targets. Many researchers track the quantity of new malware released, with estimates ranging from 300,000 to a million viruses and other malicious software products created every day.

Two years later, the cybersecurity company McAfee (2020: 3) writes that “we estimated the monetary loss from cybercrime at approximately $945 billion. Added to this was global spending on cybersecurity, which was expected to exceed $145 billion in 2020. Today, this is $1 trillion dollar drag on the global economy”. Now, the problem with such claims lies in not only the ambiguity of the methodology and thus the evidence on which these claims rest, but also in the fact that different reports seem to contradict each other, or at least operate with very different figures. For example, Klon Kitchen (2019), Director of the Heritage Foundation’s Center for Technology Policy, claims that “by 2021, cybercriminals are projected to cost the global economy more than $6 trillion annually, up from $3 trillion in 2015”. The figures he mentions are much higher than McAfee’s – but they, as well as probably all other statistics with regard to cybersecurity and threat analysis, are difficult or impossible to verify, at least for most parts of the audience (cf. Brito and Watkins 2011; Quigley et al. 2015; Stevens 2020).

From both a business and an economic perspective, not only direct costs (e.g. costs of repair, fraud-related losses) but also indirect costs (e.g. costs of preventive measures) and implicit costs (including lower productivity gains due to lower trust in digital transactions) are attributable to
cybersecurity breaches (Bauer and van Eeten 2009). Given the above-mentioned figures, it is hardly surprising when the Center for Strategic and International Studies writes (CSIS 2018: 12): “Over the last 20 years, we have seen cybercrime become professionalised and sophisticated. Cybercrime is a business with flourishing markets offering a range of tools and services for the criminally inclined”. If one knows where to look, one can hire cybercriminals to do the job, or one might find all the tools needed on the web to carry out cyberattacks, without needing any expert knowledge in this business; one simply buys “cybercrime-as-a-service”.

One can indeed draw radical conclusions from this rather convoluted situation, as Andrew Odlyzko (2019) does when he writes that

there is a rising tide of security breaches. There is an even faster rising tide of hysteria over the ostensible reason for these breaches, namely the deficient state of our information infrastructure. Yet the world is doing remarkably well overall, and has not suffered any of the oft-threatened giant digital catastrophes. This continuing general progress of society suggests that cyber security is not very important.

For the chapter at hand, however, another statement by Odlyzko (2019: 4) seems much more important, as he suggests that in addition to the aim of ensuring cybersecurity, there are other objectives that are at least as important:

There is another factor that is not discussed here, namely that even if we could build truly secure systems, we probably could not live with them, as they would not accommodate the human desires for flexibility and ability to bend the rules.

What follows will therefore attempt to demonstrate that it makes little sense to set the aim of ensuring cybersecurity as absolute, while ignoring that there are, for instance, other economic and/or social goals whose importance is at least as significant as cybersecurity. Moreover, it will be argued that making cybersecurity absolute would pose a threat to numerous moral values as well as to many design requirements for technology.

The challenge of cybersecurity: balancing competing and conflicting aims and values

This text will not serve as an introduction to the many aspects of cybersecurity, or as an introduction to (applied) ethics. Actually, this is not necessary, because there are many excellent textbooks for both purposes. Those who want to familiarise themselves with the subject area of cybersecurity might use, for example, Bruce Schneier’s Secrets and Lies (2000). Those who want to get acquainted with the theories of ethics can use, for instance, William K. Frankena’s book Ethics (1963), as it offers a very easy-to-understand approach. Yet, any introductory book would also be suitable; the same can be said with regard to applied ethics (cf. Morscher et al. 1998). In the end, however, dealing with the details of both cybersecurity and (applied) ethics will not be required to understand the following remarks; the coming sections place emphasis on showing that the provision of cybersecurity is accompanied by numerous conflicts of aims and values. These values are not necessarily only moral values but can also include, for example, economic values as well. The conflicting aims can be technical design requirements, organisational aspects or usability issues, to name but a few.

At the end of this chapter, an attempt will be made to at least give some hints on how such conflicts could be resolved. However, it must remain an attempt, because if conflicts of aims
and values are to be resolved, then one cannot avoid delving deeper into the fundamentals of both cybersecurity and ethics. As far as ethics is concerned, one then can no longer do without more precise statements about what one considers morally good or evil or which ethical theory one presupposes. The same applies with regard to cybersecurity, because without more precise knowledge of possible threats, attack vectors, risks and damage levels, as well as the respective technology, it is not possible to make any robust statements about a functioning balance between – in the broadest sense of the word – technical requirements and moral claims.

Finally, if cybersecurity is to be established while maintaining ethical standards, one lesson that has to be learned is that this can only be achieved through interdisciplinary cooperation among, for instance, software engineers, legal experts, computer scientists, economic experts and – indeed – ethicists.

**Moral aims and values in ICT**

An exhaustive enumeration of all relevant moral values in a society is, for many reasons, rather impossible, not least because it would first need clarification as to what is regarded as relevant. If one tries to develop a standard here, one will very quickly find that different moral values are considered relevant in different ways in different societies. Emphasis on social justice and equality, for example, is more pronounced in countries of continental Europe like France, Germany or the Scandinavian countries than in Great Britain or the US. In all Western societies, individual autonomy is highly appreciated as a moral value, but this value is moderated in different ways by the importance of social ties to, for instance, religious associations, the family and certain social groups as well as other institutions, organisations or associations. In short, it is difficult to draw up a generally accepted list of moral values across societies and cultures (cf. Barry 2001; Fleischacker 1999). Moreover, it has to be emphasised that, so far, we have only been talking about Western societies, but it must be understood that the value systems that actually exist there are not dominant in other parts of the world. We must therefore assume that there is a great pluralism of (moral) values worldwide.

If one wants to be a little more modest and just explore which moral values are relevant to cybersecurity, then one might examine the relevant scholarly debates to see which moral values are explicitly mentioned there (e.g. Kruger et al. 2011; Sawaya et al. 2017). However, it must be clear that this is an inescapably narrow perspective, as it does not take into account the various political or ideological attitudes towards the relationship between cybersecurity and ethics, which shape the ways cybersecurity is dealt with. This narrow focus, however, is unavoidable if one wishes to achieve some understanding of the topic at all.

If one analyses the existing scholarly literature on information and communication technology (ICT) in general and on cybersecurity in particular as comprehensively as possible with regard to moral values (cf. Christen et al. 2017; Yaghmaei et al. 2017: 9–17), one will find, among others, privacy and trust, freedom and (informed) consent, fairness and equality (which can be translated to social justice), as well as dignity and solidarity (see also Weber and Kleine 2020: 145f.). Although this list is by no means complete, it is already clear that a wide range of moral values is involved in the development and use of ICT and the provision of cybersecurity. In particular, when considering ICT in healthcare, one can expand these values to include the principles of Beauchamp and Childress (2019): autonomy, beneficence, non-maleficence and justice. While these principles originate in biomedical ethics, they can be applied in other professional domains as well.

This means that the above-mentioned values and principles should guide the professional behaviour of, for instance, physicians, computer scientists, or engineers – especially when they

614
are concerned with ensuring cybersecurity. In fact, it can be argued that the adherence to these values and principles must be the focus of respective professional behaviour, because they constitute the core of at least some professions. Accepting this last statement, the implication is that there may be circumstances in which the core moral values of a profession may compete or even conflict with technical or other requirements.

**Technical aims and values in ICT**

If we try to aggregate the numerous technical requirements for ICT, the list might look as follows: efficiency and quality of services, privacy of information and confidentiality of communication, usability of services, safety, integrity, availability (Yaghmaei et al. 2017). Some of these aims or requirements for ICT relate to cybersecurity, while others are more general in nature.

Regardless of whether these technical objectives compete or conflict with moral values and principles, even a cursory examination of the aforementioned requirements reveals that they already cannot always be realised together. For example, the establishment of a very strict security architecture to protect the confidentiality of data and communication often has the consequence that the usability of corresponding systems suffers (cf. Garfinkel and Lipford 2014). Thus, from the user’s point of view, the efficiency and quality of the service may also decline (e.g. Al Abdulwahid et al. 2015; Dhamija and Dusseault 2008; Kainda et al. 2010). Another example would be the strong encryption of communication to provide confidentiality, which in the case of mobile devices, and particularly IoT devices, may compete with available energy and thus ultimately with availability of services and systems. In fact, a considerable amount of research and development is being carried out in this regard (cf. Elhoseny et al. 2016; Gupta et al. 2020; Pranit Jeba Samuel et al. 2020), so it is to be expected that, adapted to the respective requirements, appropriate solutions might be found. Nevertheless, this example in particular illustrates how different, in the narrower sense of the word, technical requirements might compete with each other.

**Other factors, aims and values in ICT**

Without doubt, moral values and technical requirements do not exhaust the factors effective in shaping ICT and thus influence the question of what level of cybersecurity can be achieved. Even a brief look at the scholarly literature shows that economic considerations in particular play a crucial role. Cybersecurity is expensive and, like all preventive measures, its benefits are difficult to quantify – if cybersecurity is successful or cyberattacks are not successful or even do not occur at all, then damages or costs prevented can at best be credibly estimated, but not quantified unequivocally. To put it somewhat bluntly: successful cybersecurity is no good advertisement for more cybersecurity. In any case, however, there must be an economic payoff to investing in cybersecurity (e.g. Anderson and Fuloria 2010; Dynes et al. 2007; Ekelund and Iskoujina 2019; Moore 2010; Wirth 2017). Nevertheless, even if the utility of cybersecurity measures can be demonstrated, it is still true that the resulting costs have to be paid. Often, attempts are made to pass these costs on to the end users, which can only succeed if they are willing to pay and to bear these costs (cf. Blythe et al. 2020; Johnson et al. 2020; Rowe and Wood 2013).

Political aspects undoubtedly also play a role in the design of computer systems and thus in the question of what measures are taken to strengthen cybersecurity (cf. Christensen and Liebetrau 2019; Dunn Cavelty and Egloff 2019; Harknett and Stever 2011; Liebetrau and Christensen 2021). For example, strong encryption methods have often been associated with
export restrictions (e.g. Buchanan 2016; Diffie and Landau 2007; Herr and Rosenzweig 2016; Manpearl 2017; Sundt 2010; Swire and Ahmad 2012), or governments demand that encryption methods contain backdoors that allow law enforcement or intelligence agencies, for example, to break the encryption (cf. Ahmad 2009). In these cases, the respective actors pursue interests at the expense of the interests of other stakeholders. The problem here, however, is that such measures reduce cybersecurity in general, because actors with criminal intentions, for instance, can also use backdoors. Export restrictions, in turn, lower the level of protection that can be achieved for all stakeholders, which makes attacks easier and can lead to mistrust among stakeholders.

Cybersecurity as a multi-dimensional challenge

If one now tries to draw some tentative conclusions from what has been mentioned up to now, it is well worth listening to those who professionally work on the analysis of cyberattacks and the establishment of cybersecurity (Wirth 2017: 52):

The world is facing a growing prevalence of increasingly sophisticated, targeted, and malicious cyberattacks. This new reality forces us to continually evolve our understandings of our cyberenvironment and to re-evaluate and update our security posture in ways that minimize the growing cyberrisks to ourselves, our infrastructure, and our businesses. In doing so, we must recognize that any comprehensive cybersecurity strategy includes more than just technical elements. It must include aspects of leadership, societal, and corporate culture and encompass larger economic and even sociopolitical elements (e.g. national security).

With Quigley et al. (2015) as well as Stevens (2020), there are sound arguments to at least critically examine the first part of the quoted statement, but the conclusion that establishing cybersecurity is not a solely technological challenge, or that technology does not even come first, appears more than plausible based on what has been said so far. Cybersecurity has to be understood as a multi-dimensional task. Without claiming to be exhaustive, one can at least identify moral values, technical requirements and other factors that influence the design of ICT and thus have a tremendous impact on the conditions under which cybersecurity can be provided. The assignment of existing values, aims, requirements and factors to the above-mentioned categories is of course arbitrary. For example, it would be conceivable and presumably reasonable to place aspects such as usability, acceptance or willingness to pay in an additional category that could be called “human factors”. Similarly, political and social conditions could be subsumed into a category of their own. Ultimately, however, such categorisations do not really matter, because the decisive consideration is that the chance or impracticality of the provision of cybersecurity depends on numerous values, aims and requirements that are interrelated but also in competition or even conflict with each other. If one accepts this finding, the question that remains to be answered is how it is then possible to strike a balance and combine these values, aims and requirements in such a way that all stakeholders can agree to the compromise that eventually is found – if there is actually any such thing.

Methods to balance competing and conflicting aims and values

The question of what should be morally required or forbidden when technology is developed usually does not find easy answers if one is willing to broaden one’s view and not only take
one's own interests into account. However, even if one tries to consider other stakeholders and their interests, judgement about the morally appropriate design of technology depends on numerous other aspects. Which conception of human beings is presupposed? Which ethical theory is being considered, which normative assumptions are being made with regard to the relationship between different generations, which and whose normative claims are being prioritised, how should norm conflicts or norm competition (whereby these norms are not limited to moral norms) be resolved? Which understanding of the profession is present? All these and probably many more (normative) considerations already affect the ethical evaluation of technology at the theoretical level. Yet, if one wants to give an answer not only on an abstract or theoretical level, but for the actual use of technology in a (more or less) clearly defined environment, further influencing factors are added. Ethical considerations are “contaminated” by personal involvement of stakeholders and their interests and (mostly implicit and often unconscious) subjective attitudes as well as external constraints, which may make appear unfeasible what is normatively desirable, unsuitable for practice or inappropriate from a professional point of view.

Reijers et al. (2018a) describe a plethora of methods that could be used to first identify the competing and/or conflicting claims of the various stakeholders involved in the provision of cybersecurity, and then possibly find a solution in the form of balancing the different claims. Many of the methods mentioned by Reijers et al. are based on a central intuition drawn from discourse ethics: what is morally right or wrong cannot be answered by recourse to universal norms and values, some concept of utility or the idea of virtue, but must be negotiated among the stakeholders. Only in this way, so the argument goes, can the various interests and perspectives be adequately taken into account (e.g. Reijers et al. 2018b; Schuijff and Dijkstra 2020; Thorstensen 2019).

The idea of negotiating a balance or compromise among different stakeholders, their claims and other relevant factors also has the advantage that cultural preconditions and other social aspects are automatically taken into account, as they will be included in the arguments of the stakeholders involved in the negotiation. However, this is also a decisive weakness (similar arguments are also put forward against the moral principles of Beauchamp and Childress, e.g. Clouser and Gert 1990; Hine 2011; Sorell 2011) because the result of such negotiations is contingent and is not based on universally valid and accepted norms and values. However, good arguments can be given that in practice it is still better to find a compromise between the different (normative) stakeholder claims that can be accepted by all, rather than a solution based on a universal moral theory, but which only a few stakeholders would accept.

A well-tested tool, for example, is MEESTAR (Model for the Ethical Evaluation of Socio-Technical Arrangements; see Weber 2018b). The basic idea of this tool is that those stakeholders who might be affected by technology (MEESTAR was developed for the ethical evaluation of ambient assisted living technology) carry out their own ethical evaluation of the technology in question in a well-defined process. The results of this evaluation are then fed into the development process. At best, this would take place several times in an iterative process during the whole R&D process. As already mentioned, the ethical evaluation and development of solutions for moral problems caused by the respective technology ultimately represent some kind of negotiation process – MEESTAR thus represents a method based on discourse ethics. In the original version of MEESTAR, the evaluation of technology is carried out with regard to seven so-called moral dimensions. Six out of the seven moral dimensions can be mapped onto Beauchamp and Childress’ (2019) four principles (Table 30.1).

Yet, the seventh moral dimension, “self-perception of stakeholders”, finds no correlation in Beauchamp and Childress’ principlism. The idea behind this dimension is that the use of
technology alters the self-perception or self-image of stakeholders and is intended to encourage stakeholders to think about possible changes caused by technology, for example, with regard to their own profession or their own self-image and to evaluate these changes from a moral point of view. Most important, it is possible to modify MEESTAR in a way that dimensions can be added or removed, depending on the technology or application to be evaluated; this, of course, also applies to technology for the provision of cybersecurity.

It is crucial to note that MEESTAR, like presumably all tools based on discourse ethics, cannot provide a permanently valid answer to the question of how technology can be designed to meet all (normative) claims of all stakeholders; rather, this can only be stated for a concrete system or for an actual situation or application. This limitation can hardly be avoided without recourse to universally accepted moral theories, norms and values.

### Conclusion

Even though the term “cybersecurity” was not used at the beginning of computer development, the problems associated with this term already existed at a very early stage and became increasingly important in parallel with the rapid spread of computers, for example for economic, military or organisational purposes. At the same time, it also became clear that establishing cybersecurity is not only a technical challenge with technical solutions, but also that legal, economic or organisational aspects play at least as important a role. Finally, it turned out to be apparent, also very early in this development, that the provision of cybersecurity raises ethical questions, since cybersecurity can affect moral values such as autonomy, freedom or privacy – to name just a few. If one wants to achieve that the establishment of cybersecurity is accepted on an individual, organisational and societal level, then it is essential to find a balance between the different claims of the many stakeholders involved in the provision of cybersecurity. The aim of this chapter was to present this complex situation and to give at least some hints on how this balance could be achieved.

### Acknowledgments

This text could not have been written without the work done as part of the project “Constructing an Alliance for Value-driven Cybersecurity” (CANVAS, https://canvas-project.eu/). I am deeply indebted to my colleagues with whom I had the privilege of working on this project and whom I would like to thank for their excellent collaboration. CANVAS has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No. 700540; additionally, it was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052–1.
Cybersecurity and ethics

References


Karsten Weber


Cybersecurity and ethics


