Humanities and Social Sciences **2022**
Research Journal 29, No. 1 (2022), pp 87-95 **January-March**

Karsten WEBER[1]

CYBERSECURITY AND ETHICAL, SOCIAL, AND POLITICAL CONSIDERATIONS: WHEN CYBERSECURITY FOR ALL IS NOT ON THE TABLE

The text aims to demonstrate that establishing cybersecurity is not only a technical challenge, but that legal, economic, or organizational aspects also play at least an important role. The provision of cybersecurity raises ethical questions, since cybersecurity can affect moral values such as autonomy, freedom, or privacy. If measurements necessary for the provision of cybersecurity shall be accepted, it is essential to find a balance between the different claims of all stakeholders involved. This aim is achieved through a detailed ethical analysis accompanied by an extensive literature study. As the most important result of this analysis, it becomes obvious that cybersecurity is in competition or even conflict with other values and interests, and that establishing cybersecurity always involves a trade-off. Not only can there be no 100 percent cybersecurity for technical reasons, but if other values and interests are to be considered, this inevitably leads to compromises in cybersecurity.

Keywords: cybersecurity, computer security, information security, cyberattacks, cybercrime, cyber espionage, cyber terrorism, cyberwar, ethics, values, competition, conflict, economy, policy, ethical evaluation.

1. INTRODUCTION: DEFINITION AND HISTORY

Today, one can read it in almost every newspaper nearly every day: computers or any other networked devices are potential targets for a hacker attack. 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. 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; Coventry and Branley, 2018; Woods, 2017). Some attacks are carried out because the people running them want to show that they are able do it. 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; Nadir and Bakhshi, 2018). Sometimes,

[1] Karsten Weber, Prof. Dr., Institute for Social Research and Technology Assessment, Ostbayerische Technische Hochschule Regensburg, Galgenbergstraße 24, 93053 Regensburg, Germany; e-mail: Karsten.Weber@oth-regensburg.de. ORCID: 0000-0001-8875-2386.

attacks must be understood as terrorist acts; this is called "cyberterrorism" (cf. Chen et al., 2014; Jarvis and Macdonald, 2015). If such attacks are carried out by state authorities or groups that are in close relationship 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).

It is rather curios that the Hollywood blockbuster "War Games" allegedly was instrumental in raising awareness among political and military leaders in the US about the vulnerability of military computer systems (Kaplan 2016). The 1980s are characterized by the speedy dissemination of home and personal computers followed by the first large-scale attacks by computer viruses (e.g. Szor 2005). Due to the Internet, since the 1990s malicious programs (or malware) were no longer spread mainly through the exchange of data storage media such as floppy discs. That computers can be targets for attacks probably became generally accepted by this time at the latest.

Although at the beginning the terms "computer security" or "information security" were used rather than "cybersecurity", the basic issues and perspectives were shaped very early. Probably two texts published by Ware (1967a and 1967b) mark the beginning of the debates and are still relevant nowadays. Computer technology has changed significantly since 1967, but the descriptions regarding attack vectors, threats, and motives for attack as well as the human factor still hold true.

As soon these debates gained momentum, normative questions were raised that have shaped the discussion regarding the extent to which the widespread use of computers will have an impact on individuals, groups, and entire societies; one of the most important contributions was certainly Alan F. Westin's book "Privacy and Freedom" (1967). Since then, scholarly work linking computer security or cybersecurity to ethics has continued to appear (e.g. Campbell 1988; Cooper, 1995; Leiwo and Heikkuri, 1998). 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 cybersecurity and ethics. For some years now, scholarly work has been published that deals with such issues (e.g. Christen et al. 2017; Christen et al., 2019; Domingo-Ferrer and Blanco-Justicia, 2020; Loi et al., 2019; Manjikian, 2018; Pattison, 2020).

2. THE LACK OF CYBERSECURITY AND ITS NEGATIVE IMPACT ON SOCIETIES

Different types of threats, whether cybercrime, cyberterrorism, or cyberwar, can have different ramifications measured with different scales (cf. Gandhi et al., 2011). If a power plant is attacked (cf. Chhaya et al., 2020; Mazzolin and Samueli, 2020), this may cause malfunctions that could trigger the collapse of the power supply; this can 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 might result in political instability, increase distrust of citizens in state institutions, or limit a government's ability to act (cf. Gross et al., 2016; Iasiello, 2013). Attacks on computers may affect different dimensions of individual, societal, corporate, or political life. This makes it difficult to compare the amount of damage. For this reason, reports highlighting the consequences of computer attacks generally refer to economic damage or costs. While this facilitates comparisons, for instance, between different sectors of the economy (cf. Tripathi and Mukhopadhyay, 2020), countries, or defender and adversary (e.g. Derbyshire

et al., 2021), it also obfuscates 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 grown to orders of magnitude that pose significant challenges to even high-performing economies. 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 […] to $226 billion […]". Nearly a decade and a half later, the Center for Strategic and International Studies (CSIS 2018: 4) writes "[…] that cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP".

Two years later, the cybersecurity company McAfee (2020: 3) reports that it "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". As the Center for Strategic and International Studies put it (CSIS, 2018): "Cybercrime is a business with flourishing markets offering a range of tools and services for the criminally inclined". One can hire cybercriminals to do the job or might find all tools needed on the Internet to carry out cyberattacks, without needing expert knowledge; one simply buys "cybercrime-as-a-service".

Yet, despite the seemingly dire situation, Odlyzko (2019: 4) suggests that beyond the aim of ensuring cybersecurity, there are other objectives that are at least as important: "[E]ven 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 shall therefore demonstrate that it makes little sense to set cybersecurity as an absolute, while ignoring that there are other economic and/or social goals which are at least as important as cybersecurity. Making cybersecurity an absolute would pose a threat to moral values as well as to design requirements for technology.

3. BALANCING COMPETING AND CONFLICTING AIMS AND VALUES

Analysing the existing scholarly literature on ICT in general and particularly on cybersecurity regarding moral values (cf. Christen et al., 2017; Yaghmaei et al., 2017), one will find, among others, privacy and trust, freedom and (informed) consent, fairness, and equality, as well as dignity and solidarity (see also Weber and Kleine, 2020). 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. When considering ICT in healthcare as a paradigmatic use case, 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 than healthcare as well. Adherence to these values and principles must guide professional behaviour because they constitute the core of the respective profession. They should guide the professional behaviour of, for instance, physicians, computer scientists, or engineers – especially when they are concerned with ensuring cybersecurity. Yet, that means there may be circumstances in which the core moral values of a profession may compete or even conflict with technical or other requirements.

Aggregating 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 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 reveals that they already cannot always be realised together: The establishment of a very strict security architecture to protect confidentiality of data and communication often cause the usability of corresponding systems to suffer (cf. Garfinkel and Lipford, 2014), from the user's point of view, efficiency and quality of service may also decline (e.g. Al Abdulwahid et al., 2015); strong encryption of communication to provide confidentiality, particularly in the case of mobile and IoT devices, may compete with available energy and thus ultimately with availability of services and systems. Since research and development are being carried out in this regard, it is to be expected that appropriate solutions might be found. Nevertheless, this illustrates how, at certain point in time, technical requirements might compete or even collide.

Moral values and technical requirements do not exhaust the factors shaping ICT and thus influence the question of what level of cybersecurity can be achieved; economic considerations also 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: 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. Ekelund and Iskoujina, 2019; Wirth, 2017). Even if the utility of cybersecurity measures can be demonstrated, it is still true that resulting costs must 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).

Political aspects 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; Liebetrau and Christensen, 2021). Strong encryption methods have often been associated with export restrictions (e.g. Buchanan, 2016; Manpearl, 2017), or governments demanded that encryption methods having backdoors allowing law enforcement or intelligence agencies to break the encryption (cf. Ahmad, 2009). In these cases, the respective actors pursue interests at the expense of the interests of other stakeholders. However, such measures reduce cybersecurity because criminals or terrorists 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.

4. 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 even if one tries to consider other stakeholders and their interests. Judgement about the morally appropriate design of technology depends on numerous aspects: Which conception of human beings is presupposed? Which ethical theory is being considered, which normative assumptions are being made regarding 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 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. (2018b) 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 there 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 could the various interests and perspectives be adequately taken into account (e.g. Reijers et al., 2018a; Schuijff and Dijkstra, 2020; Thorstensen, 2019).

The idea of negotiating a compromise among different stakeholders, their claims and other relevant factors also has the advantage that cultural and social aspects are automatically considered, as they will be included in the arguments of the stakeholders involved in the negotiation. However, this is also a decisive weakness because the result of such negotiations is contingent and 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.

5. CONCLUSION: CYBERSECURITY AS A MULTI-DIMENSIONAL CHALLENGE

Trying 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): "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)". Cybersecurity most obviously must 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 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 any such thing. In other words, cybersecurity in many cases, perhaps even most cases, will never be achievable to the same extent for all stakeholders at the same time. The interests of the stakeholders are too different for that, but so is their power to enforce these

interests. This is rather bad news particularly for citizens, as they are usually in the weakest position. On many occasions, compromises will therefore probably be at their expense.

6. 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. The paper at hand is a revised and much shortened version of Weber (forthcoming).

REFERENCES

Ahmad, N. (2009). *Restrictions on Cryptography in India – A Case Study of Encryption and Privacy. "Computer Law & Security Review", 25*(2). DOI: 10.1016/j.clsr.2009.02.001.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., Reich, C. (2015). *Security, Privacy and Usability – A Survey of Users' Perceptions and Attitudes* [In:] Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.), *Trust, Privacy and Security in Digital Business.* Heidelberg: Springer. DOI: 10.1007/978-3-319-22906-5_12.

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D. and Lakkireddy, D. R. (2018). Cybersecurity for Cardiac Implantable Electronic Devices. "*Journal of the American College of Cardiology", 71*(11). DOI: 10.1016/j.jacc.2018.01.023.

Beauchamp, T. L., Childress, J. F. (2019). *Principles of Biomedical Ethics.* 8th ed. Oxford: Oxford University Press.

Blythe, J. M., Johnson, S. D., Manning, M. (2020). *What is Security Worth to Consumers? Investigating Willingness to Pay for Secure Internet of Things Devices. "Crime Science 9*(1). DOI: 10.1186/s40163-019-0110-3.

Brito, J., Watkins, T. (2011). *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy.* Mercatus Center, Georg Mason University, Working Paper No. 11––24 [Access: 17.10.2021]. Access on the internet: www.mercatus.org/system/files/Loving-Cyber-Bomb-Brito-Watkins.pdf

Buchanan, B. (2016). *Cryptography and Sovereignty. "Survival", 58*(5). DOI: 10.1080/00396338.2016.1231534.

Campbell, M. (1988). *Ethics and Computer Security: Cause and Effect*. Proceedings of the 1988 ACM Sixteenth Annual Conference on Computer Science – CSC'88. DOI: 10.1145/322609.322781.

Cashell, B., Jackson, W. D., Jickling, M., Webel, B. (2004). *The Economic Impact of Cyber-attacks. CRS Report for Congress* [Access: 17.10.2021]. Access on the internet: https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf

Chen, T. M., Jarvis, L., Macdonald, S. (eds.) (2014): *Cyberterrorism.* New York: Springer. DOI: 10.1007/978-1-4939-0962-9.

Chhaya, L., Sharma, P., Kumar, A., Bhagwatikar, G. (2020). *Cybersecurity for Smart Grid: Threats, Solutions and Standardization* [In:] Bhoi, A. K., Sherpa, K.S., Kalam, A., Chae

G.S. (eds.), *Advances in Greener Energy Technologies.* Singapore: Springer. DOI: 10.1007/978-981-15-4246-6_2.

Christen, M., Gordijn, B., Loi, M. (eds.) (2019). *Ethics of Cybersecurity.* Cham: Springer.

Christen, M., Gordijn, B., Weber, K., van de Poel, I., Yaghmaei, E. (2017). *A Review of Value-Conflicts in Cybersecurity. "The ORBIT Journal*", *1*(1). DOI: 10.29297/orbit.v1i1.28.

Christensen, K. K., Liebetrau, T. (2019). *A New Role for "the Public"? Exploring Cyber Security Controversies in the Case of WannaCry.* "*Intelligence and National Security:,* 34(3). DOI: 10.1080/02684527.2019.1553704.

Connolly, L. Y., Wall, D. S. (2019). The Rise of Crypto-ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures. "*Computers & Security",* 87. DOI: 10.1016/j.cose.2019.101568.

Cooper, H. A. (1995). Computer Security, Ethics, and Law. "*Journal of Information Ethics", 4*(1).

Coventry, L., Branley, D. (2018). *Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward.* "*Maturitas", 113*. DOI: 10.1016/j.maturitas.2018.04.008.

CSIS – Center for Strategic and International Studies (2018). *Economic Impact of Cybercrime – No Slowing Down* [Access: 17.10.2021]. Access on the internet: www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

Derbyshire, R., Green, B., Hutchison, D. (2021). *"Talking a Different Language": Anticipating Adversary Attack Cost for Cyber Risk Assessment.* "*Computers & Security", 103*. DOI: 10.1016/j.cose.2020.102163.

Diffie, W., Landau, S. (1998). *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, MA: MIT Press.

Dittrich, D., Bailey, M., Dietrich, S. (2011). *Building an Active Computer Security Ethics Community. "IEEE Security & Privacy Magazine", 9*(4). DOI: 10.1109/MSP.2010.199.

Domingo-Ferrer, J., Blanco-Justicia, A. (2020). Ethical Value-centric Cybersecurity: A Methodology Based on a Value Graph. "*Science and Engineering Ethics", 2*6(3). DOI: 10.1007/s11948-019-00138-8

Dunn Cavelty, M., Egloff, F. J. (2019). *The Politics of Cybersecurity: Balancing Different Roles of the State. "St Antony's International Review", 15*(1).

Ekelund, S., Iskoujina, Z. (2019). *Cybersecurity Economics – Balancing Operational Security Spending.* "*Information Technology & People", 32*(5). DOI: 10.1108/ITP-05-2018-0252.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P. (2011). *Dimensions of Cyber-attacks: Cultural, Social, Economic, and Political. "IEEE Technology and Society Magazine", 30*(1). DOI: 10.1109/MTS.2011.940293.

Garfinkel, S, Lipford, H. R. (2014). Usable Security: History, Themes, and Challenges. *Synthesis Lectures on Information Security, Privacy, and Trust", 5*(2). DOI: 10.2200/S00594ED1V01Y201408SPT011.

Gross, M. L., Canetti, D., Vashdi, D. R. (2016). *The Psychological Effects of Cyber Terrorism. Bulletin of the Atomic Scientists", 72*(5). DOI: 10.1080/00963402.2016.1216502.

Iasiello, E. (2013). *Cyber attack: A Dull Tool to Shape Foreign Policy.* 5th International Conference on Cyber Conflict (CYCON 2013).

Jarvis, L., Macdonald, S. (2015). *What is Cyberterrorism? Findings from a Survey of Researchers.* "*Terrorism and Political Violence", 27*(4). DOI: 10.1080/09546553.2013.847827.

Johnson, S. D., Blythe, J. M., Manning, M., Wong, G. T. W. (2020). *The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay*. *"PLOS ONE" 15*(1). DOI: 10.1371/journal.pone.0227800.

Kaplan, F. M. (2016). *Dark Territory: The Secret History of Cyber War.* New York: Simon & Schuster.

Kitchen, K. (2019). *A Major Threat to Our Economy – Three Cyber Trends the U.S. Must Address to Protect Itself* [Access: 17.10.2021]. Access on the internet: www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect

Leiwo, J. and Heikkuri, S. (1998). *An Analysis of Ethics as Foundation of Information Security in Distributed Systems*. "*Proceedings of the Thirty-First Hawaii International Conference on System Sciences", 6*. DOI: 10.1109/HICSS.1998.654776.

Liebetrau, T., Christensen, K. K. (2021). *The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces. "European Journal of International Security", 6*(1). DOI: 10.1017/eis.2020.10

Liff, A. P. (2012). *Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. "Journal of Strategic Studies", 35*(3). DOI: 10.1080/01402390.2012.663252

Loi, M., Christen, M., Kleine, N., Weber, K. (2019). *Cybersecurity in Health – Disentangling Value Tensions.* "*Journal of Information, Communication and Ethics in Society", 17*(2). DOI: 10.1108/JICES-12-2018-0095

Manjikian, M. (2018). *Cybersecurity Ethics: An Introduction.* New York: Routledge.

Manpearl, E. (2017). *Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate. "University of Florida Journal of Law & Public Policy", 28.*

Mazzolin, R., Samueli, A. M. (2020). *A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence*. 2020 IEEE International Systems Conference (SysCon), 1–7. DOI: 10.1109/SysCon47679.2020.9275828

McAfee (2020). *The Hidden Costs of Cybercrime.* [Access: 17.10.2021]. Access on the internet: www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Nadir, I., Bakhshi, T. (2018). *Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques.* 2018 International Conference on Computing, Mathematics and Engineering Technologies (ICoMET), 1–7. DOI: 10.1109/ICOMET.2018.8346329.

Odlyzko, A. (2019). *Cybersecurity is Not Very Important. "Ubiquity"*. DOI: 10.1145/3333611

Pattison, J. (2020). *From Defence to Offence: The Ethics of Private Cybersecurity. "European Journal of International Security", 5*(2). DOI: 10.1017/eis.2020.6

Reijers, W., Koidl, K., Lewis, D., Pandit, H. J., Gordijn, B. (2018a). *Discussing Ethical Impacts in Research and Innovation: The Ethics Canvas* [In:] Kreps, D., Ess, C., Leenen, L., Kimppa, K. (eds.), *This Changes Everything – ICT and Climate Change: What Can We Do?* Cham: Springer. DOI: 10.1007/978-3-319-99605-9_23.

Reijers, W., Wright, D., Brey, P., Weber, K., Rodrigues, R., O'Sullivan, D., Gordijn, B. (2018b). *Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations. "Science and Engineering Ethics", 24*(5). DOI: 10.1007/s11948-017-9961-8.

Robinson, M., Jones, K., Janicke, H. (2015). *Cyber Warfare: Issues and Challenges. "Computers & Security", 49*. DOI: 10.1016/j.cose.2014.11.007.

Schuijff, M. and Dijkstra, A. M. (2020). Practices of Responsible Research and Innovation: A Review. *Science and Engineering Ethics* 26(2), 533–574. DOI: 10.1007/s11948-019-00167-3.

Szor, P. (2005). *The Art of Computer Virus Research and Defense.* Hagerstown, MD: Addison--Wesley.

Thorstensen, E. (2019). *Stakeholders' Views on Responsible Assessments of Assistive Technologies through an Ethical HTA Matrix. "Societies", 9*(3). DOI: 10.3390/soc9030051.

Tripathi, M., Mukhopadhyay, A. (2020). *Financial Loss Due to a Data Privacy Breach: An Empirical Analysis. "Journal of Organizational Computing and Electronic Commerce", 30*(4). DOI: 10.1080/10919392.2020.1818521.

Ware, W. H. (1967a): *Security and Privacy in Computer Systems.* RAND Corporation.

Ware, W. H. (1967b): Security and Privacy in Computer Systems. *Proceedings of the April 18–20, 1967, Spring Joint Computer Conference – AFIPS'67 (Spring).* DOI: 10.1145/1465482.1465523

Weber, K. (forthcoming). Cybersecurity and Ethics. An Uncommon Yet Indispensable Combination of Issues [In:] Kurz, H. D., Schütz, M., Strohmaier, R. and Zilian, S. (eds.), *Handbook of Smart Technologies.* New York: Routledge.

Weber, K., Kleine, N. (2020). Cybersecurity in Health Care [In:] Christen, M., Gordijn, B. and Loi, M. (eds.), *The Ethics of Cybersecurity.* Cham: Springer. DOI: 10.1007/978-3-030-29053-5_7.

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Wirth, A. (2017). *The Economics of Cybersecurity.* "*Biomedical Instrumentation & Technology",* 51(s6). DOI: 10.2345/0899-8205-51.s6.52.

Woods, M. (2017). *Cardiac Defibrillators Need to Have a Bulletproof Vest: The National Security Risk Posed by the Lack of Cybersecurity in Implantable Medical Devices. "Nova Law Review", 41*(3).

Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M., Morgan, G., Weber, K. (2017). *Canvas White Paper 1 – Cybersecurity and Ethics.* DOI: 10.2139/ssrn.3091909.

DOI: 10.7862/rz.2022.hss.07

The text was submitted to the editorial office: November 2021.
The text was accepted for publication: March 2022.