‘Bismarck 4.0’: A Cross-Disciplinary Thought Experiment on Cyber Pacifism

Michael FUNK[a,1], Peter REICHL[b], and Bernhard DIEBER[c]
[a] *Philosophy of Media and Technology, University of Vienna, Austria*
[b] *Cooperative Systems Research Group, University of Vienna, Austria*
[c] *Institute for Robotics and Mechatronics, JOANNEUM RESEARCH, Klagenfurt, Austria*

Abstract. This essay summarizes the claims on IT security that have been presented and discussed during the workshop “YuMi in Action! Ethics and Engineering as Transdisciplinary Robotics Performance”. As a sort of “Ems Telegram” in the era of digital transformation, this essay aims to be a cross-disciplinary thought provocation on IT security and what Bismarck, Prussian’s 19th-century militarism and industrial quality ‘Made in Germany’ may teach us in this respect, such as values of technical functionality like accuracy, precision, standardization, resilience, accessibility, simplicity, autarchy, and reliability. What we definitely not want to take over are ideologies which have contributed to the horrible 20th-century world wars, war crime, antisemitism or racism in any fashion. Joining the perspectives of a philosopher of technology, a computer scientist and a robotics researcher, our goal is to work towards a (maybe utopian) world where IT security as a problem disappears. To this end, we propose the concept of ‘Bismarck 4.0’ as an alternative draft in times of cyber warfare and social robots that overrun our firewalls like herds of next generation Trojan horses. Basic elements of this approach include strategic de-networkification as well as a clear emphasis on strengthening IT autarchy and resilience. The resulting position of newly gained strength will allow to increase network- and user-centric quality (including security) as well as, eventually, to go for a sustainable openness and neutrality by design. In this away, we arguably introduce some historical experimental evidence into a current debate that, ironically, refers to almost identical problem settings.

Keywords. Social robots, IT security, Otto von Bismarck, Prussia, made in Germany, Trojan horse, war, quality of experience, quality of life

1. Robophilosophy and (the Next) Downfall of the Occident

In this essay written for the proceedings of the Robophilosophy 2018 / TRANSOR 2018 conference our goal is to describe a cross-disciplinary (and probably controversial) thought experiment at the meeting point between computer sciences, robotics engineering and philosophy of technology. We start from the buzzword ‘Industry 4.0’ as the latest of a series of constantly upraising concepts that have also shaped the Robophilosophy conference, including social robots, social relations 4.0, androids and linguistic interaction 4.0. Based on that, this paper points towards one of

[1] Michael Funk, Institut für Philosophie, Universitätsstraße 7 (NIG), A-1010 Vienna, Austria. Email: funkmichael@posteo.de

Author’s manuscript. This paper has been published as
M. Funk, P. Reichl, and B. Dieber, “‘Bismarck 4.0’: A Cross-Disciplinary Thought Experiment on Cyber Pacifism,” in Envisioning Robots in Society – Power, Politics, and Public Space, Proceedings of the Robophilosophy 2018 / TRANSOR 2018, 2018, vol. 311, pp. 357–365.
http://ebooks.iospress.nl/volumearticle/50821

the many possible results of the joint transdisciplinary workshop "YuMi in Action! Ethics and Engineering as Transdisciplinary Robotics Performance" and, at the same time, is also the consequence of an overarching intellectual trajectory that would not have been possible if this workshop had not been embedded in the broader horizon of the conference.

Within the YuMi workshop, we have been trying to go some possible ways of transdisciplinary engagement with a concrete focus on the collaborative robot ABB "YuMi", the VDI *Fundamentals of Engineering Ethics* and current EU reports for the legal regulation of robotics and human-machine-interaction (see [1], this volume). Within the workshop and also during a series of subsequent discussions, we started experimentally reversing the up-taking trajectory of robotic developments, asking questions like: Why always being so 'up to date'? Why not alternatively trying to think in 19th century categories?[2] And more specifically: as it seems more and more problematic to use current technologies for solving today's problems in IT, maybe there are fruitful perspectives which are rooted in the very past?

To answer these questions, the remainder of the essay is structured as follows: We start illustrating the problem space with two prominent application-oriented examples, i.e. IT security and care robots, with a special focus on the issues of complexity and responsibility. It turns out that 19th century militarism provides a unique ideal of technological quality which, paradoxically, is as relevant as neglected in this context. Our thought experiment in this essay follows the method of eclecticism: for both ethical and methodic reasons we don't adopt all the ideas from militarism, but select certain aspects that might be worth to rethink today. Here, the historical figure of Otto von Bismarck serves as inspiration in his attempt to achieve political *equilibria* through technological autarchism, and leads us finally to a first draft formulation of our 'Bismarck 4.0' concept, based on five pillars: de-networkification, autarchy, resilience, quality, and equilibrium alliances (sustainable openness and neutrality by Design).

Before we go on with our argument, we want to insist that we refuse any form of violence, wars, war crime, discrimination, antisemitism or racism. In addition we are aware of the fact that 19th-century nationalism and militarism also led to two horrible world wars and the holocaust with millions of victims worldwide. Anything like this must not be repeated at any time. We possibly touch taboos out of bounds by trying to learn from Prussianism.[3] But this essay is neither intended to be a full postmodern provocation where the authors try to generate attention with shocking slogans. Nor do we intend to play with history as if nothing bad had ever happened. Instead we belief that tabooing contributes to an undifferentiated and uncritical treatment of things. In contrast, reflecting possible taboos from an unusual point of view is a form of critical enlightenment. It contributes to differentiated learning processes—also from the history

[2] Note that this essay refers in a deliberately speculative way to historical facts which can be easily obtained from current historical literature. For Bismarck see: [2]; for 19thcentury history see: [3-5]; for history of technology and industrialization see: [6]. On the other hand experimental interpretations are given which relate primarily the 19th century to current questions of IT security in Internet and robotic applications. Those interpretations include speculative elements and go beyond the pure historical facts. Hence, we admit there could also be different interpretations and counter arguments which might falsify our thought experiment, without doubting the historical facts. It's a thought experiment—no more, no less.

[3] One reviewer of this paper pointed out that tries to learn from 19th-century militarism or nationalism after the disasters of the 20th-century could be perceived as a break of taboo which might personally affect some readers. We are thankful to have received this and other critical remarks, which have contributed to enhance the quality of this text. Personally we respect the thematic borderlines that might be accepted by some readers. But it is also a chance for critical philosophy to sometimes focus even uncomfortable topics.

of mankind. In conclusion, this text is intended to be an arguable and falsifiable, yet somehow differentiated, contribution to critical philosophy and freedom of speech.

2. Key Examples: IT Security and Care Robotics

It seems that the field of IT security is especially accessible to this type of approach, despite, or maybe because, we currently have such a plethora of problems there (just think of the spectacular cyber attack on the German government in early 2018 which has been receiving a lot of media attention and, on the other hand, is only one of millions of similar attacks happening every single day). This applies of course also to robotics, where the danger of hackings and other cyber operations cannot be denied at all. On the contrary, robots are computers as well, embedded in IT networks, they are collecting sensor data and can be conquered on the software basis like every IT system in the world (as it has been summarized in [7]). Thus, cyber war is by no means limited to computers and the Internet only, moreover it is the military fate of all current robotic applications worldwide—even of 'civil' robot applications ([8]).

As another example, consider medical systems and care robots in hospitals and elderly care houses. When those systems are hacked, not only sensitive personal data might be stolen and misused for blackmailing etc. Also the danger of physical harm is pretty significant. Whoever hacks a care robot on the non-physical software level, is able to cause physical harm to the weakest persons in our societies. In the discussions during Robophilosophy 2018 and beyond, but also in the literature, in this context sometimes the metaphor of a Trojan horse is used: the doors are open, we create the critical infrastructure ourselves, and terrorists or criminals use it to conquer what has been thought to be the IT fortress. If we have a closer look at the many doors we keep open today, then we might also talk about a stud farm, a whole Trojan herd which endangers our 'civil' life with military and criminal means. While the authors readily confess to be pacifists, this still seems to be a harsh reality that cannot be denied: if we think about IT security, in the case of YuMi or in the case of androids or other robotics systems, then we are forced also to think about war. In other words: No social robots without social robotic warfare.

3. Complexity and Responsibility

Aside from pure IT security aspects, we observe another general evolution these days: technology seems to become more and more overly complex and hence, in a certain sense, immature while its impact on our lives is exponentially increasing. In rather harmless cases, this means for instance that we have to perform a software update on our latest gadget before we can even use it, since it was produced and shipped before the software was finished. Hence, it seems that we are readily accepting 'quick and dirty' as the standard programming paradigm of our time, instead of insisting that software engineers have entirely thought through their product before releasing it to the market. We tend not to think about what this says about the creators of our technology—as well as about ourselves. The notion of quality has lost its traditional significance, while economic success has become the only relevant metric, and thus it is much more important to sell products than to prevent discomfort or harm to users. Note that this dominance of business over value has appeared also in other context

during the discussions of the conference, for instance following Hiroshi Ishiguro´s talk when he was asked to define his metric for robots being 'better' than humans.

After all, this boils also down to questions of responsibility, and here many examples are raising big concerns: for instance, traditional space agencies, like NASA or ESA, with their proven and well-established processes of building rock-solid space technologies are nowadays overtaken by private space start-ups which seem to have a much looser relationship to reliability standards, like, e.g., Space X, with Elon Musk confessing that they "started off with just a few people who really didn't know how to make rockets" (see Elon Musk's presentation at the International Astronautical Congress, Sept. 29th 2017, at about 12:00 [9]).

This is even more relevant if it comes to the latest wave of Artificial Intelligence, which is currently impacting the tech world and has become a standard feature in almost any 'smart' product (ranging from smartphones and loudspeakers over self-driving cars up to e-government applications). Being overwhelmed by the claims and promises it brings along, we tend to overlook that AI still is more of an experiment than the application of a mature technology, and not only since Chris Anderson has proclaimed the 'End of Theory' due to Big Data [10], which eventually means: the end of the scientific paradigm, or—as we put it nowadays—the beginning of the 'post-factual era'. We know that AI seems to work for some specific cases, but suffers from a fundamental problem: we have close to no idea where its limits are since the current generation of AI cannot always explain why it took a certain decision (just take a look at the aftermath of recent Tesla and Uber crashes). The reason for that is straightforward: machine learning, and especially neural networks, are able to identify merely correlations between data, but in no way causality between facts, and hence lack reasonable explanatory power. In this sense, the extent to which AI (or at least certain directions within it) are still consistent with generally acknowledged forms of scientific approaches is at least disputable, and in any case requires a carefully chosen ethical position.

This potential lack of responsibility is alarming, but, on the other hand, if an Austrian-German cross-disciplinary team of authors reflects about the robotic cyber war with the motivation to learn from the past, the situation morally might easily become rather sophisticated. No doubt, two horrible world wars as well as the holocaust are part of the Austrian and German history, and, as a matter of course, avoiding anything like this in the future will remain the completely indisputable top priority for once and ever. But, apart from that, we can also learn that basic technical innovations have been realized in the two world wars, which enable the robotic systems we have today. Clear examples for this claim include, for instance airplanes in WWI or RADAR technology as well as early computers and rockets in WWII.

4. What we can learn from Bismarck 1.0

However, we would like to extend this historical perspective, go back even farther and rather consider 19th century developments. While WWI has been perceived as the first industrialized war, bringing along a broad range of political, social and technological changes, we would like to point out that this is just the European perspective. In fact, already the US-American civil war (1861-1865) can be interpreted as the first industrialized war: railways have been used to speed up logistics, canned food and standardized mass production of weapons, mortars (cannons), ammunition and medical

products. At roughly the same time, in Europe it has been Otto von Bismarck (1815-1898) who started playing a very important role as historical figure. In German history, he is well known as first 'Imperial Chancellor' of the German Reich from 1871 to 1890, during which period he succeeded in creating a carefully balanced system of international alliances (e.g. with Russia, France) in order to politically stabilize Europe. Unfortunately, his clever system of international alliances has not become sustainable—one of many reasons that caused the beginning of WWI in 1914.

What can we learn from him with respect to our current IT security problems? To begin with, let us have a closer look at the German history of technology at that time. Compared e.g. to England, industrialization in the early 19th century was on a pretty poor level in Germany. The developments that lead to the founding of the German Reich in 1870/71 have not been only political processes; rapid urbanization, social and technical changes played an important role as well. And not to forget: this was also the time of two class systems that have been analyzed and criticized by Marx and Engels, the ideological beginning of communism and the founding of socialist working class parties. While this is less important in our context, we have to focus on the development which is today called 'rapid industrialization of Germany' (ca. 1870-1914). Here, in a very short period of time, Germany became one of the most advanced players of industrialization, including export of machines and other products world-wide. As a consequence, the British government (which was leading a large transcontinental empire at that time) started stigmatizing the German export products by using the slogan 'Made in Germany'. With this strategy they aimed to diminish the reputation of new German products and to protect their own industry production. 'Made in Germany' was intended to be a sign for poor quality, but in fact quickly the opposite happened: it became a hallmark of excellence.

5. 'Made in Germany' Reloaded

Why did the British strategy fail, and why became 'Made in Germany' a somehow legendary slogan which stands for outstanding technical quality till today? Amongst the manifold reasons, in the context of our story regarding IT security in social robotic applications we want to point out one important issue. The 19th century was (also) a decade of nationalism and militarism. In no way it can be denied that the establishment of the German Reich was also the result of warfare. The German-French war 1870/71 played a major role, as did also the Napoleonic wars at the beginning of the 19th century. After early defeats against Napoleon—e.g. 1806 in the battle of Jena-Auerstedt—Prussia had started several reforms that also included economic, technical and military processes of modernization. Industrialized technologies have been related to values of strict and efficient (governmental and societal) administration, military functionality, rules, accuracy, order and autarchy. On the other hand, processes of nationalism and militarism created values of technical functionality like precision, standardization and normalization, easy handling and robustness. Note that these military technologies needed to be stable, to remain sufficiently operational even under hardest external conditions, easy to handle in stress situations, to be quickly learned and trained by recruits, and of course military technologies should be as simple as possible because of maintenance, autarchy (being independent from foreign resources), standardized mass production, and the reduction of possible sources of error (which could cause horrible trouble in combat situations). In principle, this should not have

changed until today: weapons need to precisely operate under worst conditions, and they are forced to be the perfect mean for whatever aim is given by the authorities. Drilled soldiers need drilled tools and most efficient organization—especially when an enemy (like, at the time, for instance Napoleon) is stronger in terms of strategic and numerical superiority.

6. Equilibrium and Quality

There are two remarkable issues: (I) First of all, our current approach to fighting IT security issues is mainly following a comparable idea of achieving a certain balance between attacking and defending forces, which leads to a game-theoretic analysis and interpretation ([11]). However, this becomes more and more difficult with an increasing speed of the corresponding strategic moves. It is no coincidence that for instance with Bitcoin technology, it has been decided to build in a 'proof of work' aspect that deliberately slows down transaction speed in order to avoid uncontrollable automatic high-speed interactions between the mining computers. While we won't comment on the apparent ecological absurdity of using highest available computing power for the basically useless guess-based calculation of cryptographic hash functions, not to speak from the current hype around 'blockchain technology' in general which is about to become the enchanting 'blue flower' of a 21st century digital romanticism [12], nevertheless it is interesting to note that the chosen time-scale (in the order of minutes) represents a major step towards a paradigm change that has been called 'Anti-Copernican Revolution', putting back the human horizon into the center of technological evolution [13]. Related to warfare a second post-Clausewitz logics is established with current acceleration of high speed cyber war. Carl von Clausewitz (1780-1831) is a well-known pioneer in the theoretical foundation of modern military sciences. His argument that "war is the continuation of politics by other means" (see the German original passage: [14]) became a *topos* of later conceptualizations of war till today. The first technological development which reduced this slogan to absurdity was the development of nuclear weapons: when human use a weapon which can destroy human life on earth, then war is not the continuation but the total ending of any politics. The second post-Clausewitz logic is caused by IT and cyber war. If algorithms 'autonomously' perform strikes and counter strikes on the software level worldwide and in real time, then, again, war is no more continuation of politics by other means. A temporal microcosm is technologically generated which cannot be cognitively accessed by humans. Things are too fast for rational decision making. The temporal post-Clausewitz structure of IT acceleration is another logical ending of politics and ethics. Deceleration becomes an imperative in order to (at least) make ethical decisions possible in terms of temporal access [15, 16].

The second remarkable issue, which is almost ironic, concerns the fact that the quality requirements of the Prussian military stand in a strong contrast to today's economic, profit oriented values of planned obsolescence. Light bulbs or nylon stockings are examples for technologies that have been intentionally strongly limited in their lifetime. From a profit-oriented perspective of producers, this makes sense as consumers are forced to replace more often and to spend more money for it. But this is not the source for 'Made in Germany', as here—ideologically—quality and success in any (even seemingly adverse) situation is considered more important than profit. From our pacifist point of view it might sound like a harsh conclusion, but it seems that the

military ideals of reliability, efficiency, resilience and durability are basic reasons for the success of 'Made in Germany'—and so even in civil technical developments. As a consequence, we hence would like to raise the question: Where is the new 'Made in Germany' or—even better—'Made in Europe' hallmark of excellence in times of 21st century IT security? In other words: what about struggling for a European 'Bismarck 4.0' in order to address this problem?

Of course, especially from a German and Austrian point of view, after the 20th century and two world wars it seems to be forbidden to argue in favor of any sort of 19th century Prussian militarism. Moreover, of course there is always the counterargument of historical distance: 21st century IT and our societies today are very different to what happened technologically in the centuries before, and maybe our analogy of 'security' is simply failing. Also the understanding of warfare changed dramatically since the end of the 20th century: 'symmetric wars' in which nations fight against nations received a dinosaur status, and could be maybe termed a 'September 10th' concept, while our wars today ('September 11th' style) become more and more asymmetric. Terrorists, warlords, mercenaries or child-soldiers are the new actors which do not belong to the classical group of military combatants that is part of the international law of war. In current debates the slogan 'new wars' is used in order to describe the dramatic changes of warfare [17]. But there is not only the political and societal, but also a genuine technological asymmetry. In cyber war, we already situated the Trojan horses (4.0) in our civil societies. The smartphones, computers and social robots of civil owners with civil motivations are abused for war-like purposes, and, as a matter of fact, between software and hardware there is no military symmetry to be found. In contrast, 19th century national armies with regular combatants stand for a different symmetric form of warfare, which by itself seems to forbid a comparison between today's situation and the 19th century. Of course this does not render it useless to formulate a thought experiment about 'Bismarck 4.0'!

7. Autarchy or Anarchy?

The situation is somewhat comparable with about the current discussion on 'Industry 4.0', a concept, which indicates our need to integrate historical roots into the current discourse. Technologies follow developmental paths: without nukes and rockets no strategic nuclear rockets, without computers no smartphones, without radar no autopilots, etc. Hence, any technology is strongly historically shaped, and similarly our ways to culturally use tools are historically grown. Like with astronomy where we know about the cosmic background radiation, in philosophy (and even more philosophy of technology) we depend on an analogous historic-cultural background radiation. This leads us eventually to our proposal to try learning from the past also for these current challenges which, on first sight, do not have many similarities.

In times of world-wide communication networks, drones and social robots, a first characteristic of 'Bismarck 4.0' would concern establishing IT autarchy as a fundamental security requirement. How can we use safe computers or robots when they are produced in foreign countries? Nobody knows which additional spy chips are added in the factory, and moreover, outsourcing and profit-oriented ideologies of planned obsolescence (always a new need to buy a new device) make up the oat with which we ourselves feed our Trojan horses today. Hence, it is not about warfare, but about the 19th century's ideal of technology (which has also been shaped by military demands)

that could become a strict imperative for 21st century robotics and IT security. On the other hand, in the course of the Internet evolution since the 1970th, security was not the highest value (if it has been considered at all). While this did not seem to be necessary at the very beginning, where the Internet was conceived as an experimental collaboration platform between benevolent and trustworthy scientists, the commercial turn this development has taken since has caused a disastrous structural deficit which, despite of all attempts, could not be closed till today, and even worse: there is not yet a generally accepted strategy available that could resolve this issue. Therefore, we doubt that 'the Internet is broken, and we have to fix it' as has been recently claimed by the influential online journal *Wired* in its January 2018 edition. The Internet is as it is, but it has lost its virginity, and instead of serving any longer as a fascinating playground for enjoying and experimenting with all sorts of more or less innocent toys, it has turned into both the most critical infrastructure on our planet and, at the same time, an ubiquitous market forced to obey brutal economic laws and harsh business logics. We won't be able to fix this, instead we have no other choice than to accept these deficiencies and to look for a *Punctum Archimedis* outside. Historic reflection may help us in this respect, and hence substantiates our proposal to stop further pushing our technological advancements towards 4.0s and 5.0s, but first of all address our societal needs and allow us a decent period for rethinking our position and then decide. Mankind has made the mistake to invent nuclear power once without any chance of getting rid of it now—and we should avoid repeating such faults from now on. Thus, it is not too late to start a 'Bismarck 4.0' movement!

8. Towards Bismarck 4.0

Having said this, how could a 'Bismarck 4.0' IT security doctrine look like? We believe that, at least, the following five principles should be included, which—at the same time—may be understood as roadmap proposal ('five-point plan') for achieving a new level of IT security by rethinking the Internet from scratch:

1. Strategic *de-networkification*, i.e. reduction of our dependency from the Internet and/or Internet services/applications (this is the initial operation which enables the following points and could also lead in the worst case to a total cut from the Internet for a period of several months).
2. Operational *IT autarchy*, including PC architectures, infrastructure, software development and hardware production (e.g. in a trans-European IT and robotics industry).
3. *Resilience* in crisis situations, referring to the ability of sustaining basic system functionality also in a state of severe disorder—and, moreover, the ideal of turning weaknesses into strengths in crisis situations.
4. Focus on (user-centric) *quality* instead of mere bandwidth, ubiquity, obsolescence etc.
5. *Sustainable Openness and Neutrality by Design* through a balanced system of international alliances (equilibrium) avoiding any sort of totalitarian control (no more Gleichschaltung).

These principles aim at defining a new type of Internet in the sense of an 'Inter-natio-net' or 'Inter-conti-net', and can be summarized as follows: kicking out the Trojan herd (4.0), going back to old-fashioned military ideals of robust, precise, easy to handle and

non-obsolescent technologies without social drill and military ideologies, nationalist or racist behavior in the heads of the people, supporting enlightenment, music, arts, literature and political liberalism[4] and thus creating a confident autarkic negotiation position, and last not least recurring to the original conception of the Internet as a 'network of networks'. On a more global level, such a confident negotiation position could then be used to start a reform of the UN in order to make it become an employable transnational institution. Note that, of course, even with IT autarchy in Europe, robotic technologies would still be developed and applied in a globalized world, and hence any efficient and realistic ethical and legal regulation can only be realized on a global scale, while, nevertheless, a powerful and enlightened transnational institution without any Trojan horses will be the fundamental requirement.

9. Time for New Utopias!

Realistic proposition or wild dream of some crazy utopians? We are happy to face this critique, as, maybe, in a world of profound pragmatism, only dreams and utopias may have the potential to show us new ways out of the various dilemmas we are constantly facing these days. What could be more to the point if we consider today's digital revolution—which is almost unequivocally hailed or at least announced as something that is about to arrive, or already there anyhow—without ever having asked our society about its opinion at all? What a democratic nightmare in the cold light of day…? And, after all, such an attempt is but a positive version of what e.g. Günther Anders had in mind when he postulated the "exaggeration towards the truth" as a proper methodology for philosophy of technology [18]. Hence, we believe that the sketched 'Bismarck 4.0' approach, together with enlightenment, arts and education could provide at least a hint into the right direction. And, of course, this is not depending on a Prussian or German perspective—instead, it is the idea (of accurate resilient technical functionality which can support enlightenment and liberty) and the chance that matters, not so much the national or historic tunnel view, and this can easily be achieved by learning from your own history, as, after all, robots don't have a specific history at all…

In this essay we performed a cross-disciplinary thought provocation on IT security and what Bismarck, Prussian's 19th-century militarism and industrial quality 'Made in Germany' may teach us in this respect. We argued that processes of nationalism and militarism created values of technical functionality (accuracy, precision, standardization and normalization, easy handling and robustness, to be quickly learned and trained by users, at the same time as simple as possible because of maintenance, resilience, autarchy, and the reduction of possible sources of error) which should be applied to current IT and robots in order to enable real security and safety. Therefore our (maybe utopian) thought experiment leads to 'Bismarck 4.0' roadmap proposal as an alternative draft in times of cyber warfare and social robots that overrun our firewalls like herds of next generation Trojan horses: (i) strategic *de-networkification* (reduction of dependency from the Internet and linked services/applications), (ii) operational *IT autarchy* (PC architectures, infrastructure, software development and hardware production in a trans-European IT and robotics industry), (iii) *resilience*

[4] Which, by the way, also has been a part of Prussian history, as the notion of Germany as "Land der Dichter und Denker" (attributed to Madame de Staël) indicates. Insofar, in terms of enlightenment, education, arts, music and culture, the Bismarck 4.0 allegory can be combined with a Friedrich II. 4.0 allegory as well.

(ability of sustaining basic system functionality also in a state of severe disorder—and the ideal of turning weaknesses into strengths in crisis situations), (iv) focus on (user-centric) *quality* instead of mere bandwidth, ubiquity, obsolescence etc., and (v) *sustainable openness and neutrality by design* through a balanced system of international alliances (equilibrium) avoiding any sort of totalitarian control (no more Gleichschaltung).

References

[1] M. Funk & B. Dieber, "We Are Living in a Social Submarine! Children Are still the Better Adults" in: M. Coeckelbergh, J. Loh, M. Funk, J. Seibt & M. Nørskov (eds.), *Robophilosophy 2018: Envisioning Robots in Society – Politics, Power and Public Space. Proceedings of Robotphilosohy 2018 / TRANSOR 2018*, IOS Press, Amsterdam a.o., 2018.

[2] E. Kolb, *Bismarck*, C.H. Beck, München, 2014.

[3] E. Fehrenbach, *Vom Ancien Régime zum Wiener Kongress. Oldenbourg Grundriss der Geschichte 12*, Oldenbourg, 1992.

[4] L. Gall, *Europa auf dem Weg in die Moderne 1850-1890. Oldenbourg Grundriss der Geschichte 14*, Oldenbourg, 2009.

[5] G. Schöllgen & F. Kießling, *Das Zeitalter des Imperialismus. Oldenbourg Grundriss der Geschichte 15*, Oldenbourg, 2009.

[6] W. König (ed.), *Propyläen Technikgeschichte*, Propyläen, Berlin, 2000.

[7] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, & P. Schartner, „Security for the Robot Operating System", *Robotics and Autonomous Systems **98** (2017)*, 192-203.

[8] M. Funk, "Tacit Security? Roboethics and Societal Challenges of 'Social Robotic Information- and Cyberwar'" in: J. Seibt, M. Nørskov & S. S. Andersen (eds.), *What Social Robots Can and Should Do. Proceedings of Robophilosophy 2016 / TRANSOR 2016. (Frontiers in Artificial Intelligence and Applications, 290)*, IOS Press, Amsterdam a.o., 2016, 119-128.

[9] Musk, E. (2017). Becoming a multiplanet species/Making Live multiplanetary. https://www.youtube.com/watch?v=tdUX3ypDVwI [last visited on April 15, 2018]

[10] C. Anderson, „The End of Theory: The Data Deluge Makes the Scientific Method Obsolete", *Wired, 23.06.2008*. [https://www.wired.com/2008/06/pb-theory/ (15.04.2018)]

[11] P. Maillé, P. Reichl & B. Tuffin, „Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management" in: N. Gulpinar, P. Harrison & B. Rustem (eds.), *Performance Models and Risk Management in Communication Systems*, Springer, 2011, 33-53.

[12] M. Coeckelberg, *New Romantic Cyborgs. Romanticism, Information Technology, and the End of the Machine*, MIT Press, 2017.

[13] P. Reichl & A. Passarella, "Back to the Future: Towards an Internet of People (IoP), Invited Paper", *MMBNet 2015, Hamburg, Germany, September 2015*.

[14] C. v. Clausewitz, *Vom Kriege. Auswahl. Herausgegeben von Ulrich Marwedel*, Reclam, Stuttgart, 1994, p. 39.

[15] M. Funk, "Zeit als Element technologischer Kriegsführung" in: M. Funk, S. Leuteritz & B. Irrgang (eds.), *Cyberwar @ Drohnenkrieg. Neue Kriegstechnologien philosophisch betrachtet*, Königshausen & Neumann, Würzburg, 2017, 59-83.

[16] M. Coeckelbergh & M. Funk, "Data, Speed, and Know-How. Ethical and Philosophical Issues in Human-Autonomous Systems Cooperation in Military Contexts" in: J. Hodicky (ed.), *Modelling and Simulation for Autonomous Systems. Third International Workshop, MESAS 2016, Rome, Italy, June 15-16, 2016, Revised Selected Papers. (Information Systems and Applications, incl. Internet/Web, and HCI, 9991)*, Springer, 2016, 17-24. [(DOI) 10.1007/978-3-319-47605-6]

[17] M. Kaldor, *New and Old Wars: Organized Violence in a Global Era*, Polity Press, Cambridge, 1999.

[18] G. Anders, *Die Antiquiertheit des Menschen 1. Über die Seele im Zeitalter der zweiten technologischen Revolution*, C.H.Beck, München, 1956, p. 15.