Cyborg networks: freedom through data with open source and implantable devices

Kevin Rändi

ANNALS of the University of Bucharest
Philosophy Series

Vol. LXXI, no. 1, 2022
pp. 87– 110.

ANALELE UNIVERSITATII BUCURESTI

CYBORG NETWORKS: FREEDOM THROUGH DATA WITH OPEN SOURCE AND IMPLANTABLE DEVICES

KEVIN RÄNDI[1]

Abstract

Implantable computing technologies are the blueprint for the ongoing process of cyborgization. Already with the present devices, design decisions and computational issues blend together with a living organism, so that our health, for example, depends on well-adjusted information security, which requires constant work and decisions by many actors of different expertise. This means that implantable technologies form important sociotechnical systems. I will explore cyborg vulnerabilities found in sociotechnical systems, but take seriously the proposed development model of open-source technologies, promising existing and future cyborgs more autonomy and freedom. However, I want to take this vision further. Given the number of technologies that matter in the context of cyborgs, it becomes necessary to look at a wider application of open source, needing more experts and quicker data exchange. While offering a technological solution to make the data exchange possible, granting the users freedoms and autonomy, I also find it important to address how the debates around open source move from software to a large-scale social consideration, should the solution be implemented.

Keywords*: cyborg, open source, sociotechnical systems, implantable technologies, data exchange*

Introduction

In the first half of 2022, following an article published in *IEEE Spectrum*, news spread about people risking losing their sight for a

[1] PhD Student in Studies of Cultures, School of Humanities, Tallinn University.
Email: <kevin.randi@tlu.ee>

second time due to a company going bankrupt (Strickland & Harris 2022). Evidently, the company behind valuable implantable retinal and brain technologies had faced financial difficulties, discontinuing any further support for the parts, and thus causing uncertainties for its users. This is only one example of what could be called a cyborg problem with implantable technologies. However, it is an important issue that should make us think about such technologies beyond the interaction between the user and the machine. The relevant questions concerning our health, well-being, and vulnerabilities are also questions about development and design processes of technologies. In such cases, I take the view that dependency on technologies is at the center of a complex interplay between several actors and forces, including clinical experts and engineers, together with those who maintain, manufacture, design, use, and live in this complexity. All these human and technological actors, but also regulations and rules form what is known as sociotechnical systems (Cooper & Foster 1971; Franssen & Kroes 2009).

A view from sociotechnical systems, where the focus is on existing implantable technologies and its stakeholders, uncovers vulnerabilities with implantable technologies in more detail, but it also discloses why we need to give more philosophical attention to the development of computing devices. Due to the surgical nature of such technologies, the wearers may wish, for example, that they had more certainty about its maintenance and access, if needed. Furthermore, as in the example above, the way technologies are manufactured, raises concerns about autonomy for the wearers. One possibility is to design technologies with the principles of open source, important in the field of software and computing. I commit to this view. However, by assuming that implanting wireless and networked computational devices with both software and hardware will continue to be relevant on the path to our cyborg future, I want to further examine the use and the ethos of open source. If we remain true to both sociotechnical systems and open source, having an open-source piece of hardware and software in our bodies might not be enough. We would require different communities of experts together with quick and reliable ways of exchanging a large amount of data. While I propose an existing technological solution, able to co-join private and public institutions as an example, I will show how some new

philosophical issues and considerations might emerge. Implantable technologies already make information security an integral part of our understanding of health. With the changed understanding of health, both novel vulnerabilities and possible mitigations need only look to the existing debate between closed and open source having an impact on social and political matters once the decision is made.

Cyborgization Now

Cyborg, a portmanteau for a cybernetic organism, refers to a deeper technological embodiment forming a hybrid that is a "self-regulating human-machine system" (Featherstone & Burrows 1995, 2). The term "cyborg" was first coined by Clynes and Kline (1960) to propose a new way for humans existing in space by incorporating "exogenous components" that extend "the self-regulatory control function of the organism in order to adapt it to new environments." This entity has become an eminent figure in today's academic literature that captures ways we should rethink our being in the existing technological world, as famously proposed by Donna Haraway (1991). For others, like Ray Kurzweil (2005), cyborg also denotes one possible posthuman outcome of the ongoing technogenesis. Reconceptualization of the human with cyborg ontology is often attributed to posthumanism, whereas the view of cyborg as the outcome is more closely aligned to transhumanist ideas. Due to different ontological and anthropological assumptions, both are seen in many respects as irreconcilable. Without seeking any unification of the two, there is, nevertheless, a question concerning technology that requires attention from both. Namely, what could be significant for the future of cyborgization once we start from the lifeworlds of those currently needing cyborg technologies?

Cyborg technologies are often discussed in the light of human enhancement, with the emphasis on RFID chips, and brain-computer interfaces that move beyond the species-typical biological functioning (See, *e.g.*, Barfield & Williams 2017). However, it cannot be assumed that current wearers of prostheses and medical implants are able to see their lives merely having the species-typical functioning restored. Much

about their lives becomes different, as do certain meaningful concepts about their bodies. As Nelly Oudshoorn has argued, instead of equating cyborg technologies with human enhancement or emergent technologies, we need to also consider the lives of the already existing "and more familiar" cyborgs for whom technology is a matter of life and death (Oudshoorn 2015). Medical implantable devices, to begin with, are the clearest instance of how the future of humanity could be dependent upon the design and how all the relevant actors come to affect us, revealing already novel forms of vulnerabilities from which to re-think the cyborg future.

Also, by mentioning vulnerabilities next to existing medical devices and "familiar" cyborgs, I do not mean that the latter need to be taken as more vulnerable because of a person's condition, or because of some specific medical function of these devices. Rather, these devices help to reveal already existing vulnerabilities that could characterize other implantable technologies of the future. The idea that vulnerabilities form our unwanted companion for the whole road to the future has been explicitly stated by Mark Coeckelbergh (2011, 2013). Even the currently imagined posthumans would be relational, embodied within something and, as such, dependent on other factors; only the form of vulnerability is apt to change (Coeckelbergh 2011).

Implantable Technologies and Sociotechnical Systems

Wireless and networked implantable medical devices (IMDs) have been used for years. Without referring to any specific device now, these devices within the overall e-healthcare systems, including also the Internet of Medical Things (IoMT), have provided medical professionals better data monitoring, and remote access to health. Moreover, some devices, like implantable cardioverter defibrillators (ICDs), save lives with an automated monitoring and regulating system to shock and pace the heart to avoid the worst. As it is with many technologies, while there are benefits, there are also trade-offs. With all the connectivity and software in a wireless IMD, biomedical considerations have also become cybersecurity concerns. Signals, databases, and the device itself can be

exposed to malicious actors (Pycroft & Aziz 2018). Because of the cybersecurity issues, people with IMDs might need the extra layer of protection from other (wearable) technologies, such as wristbands, UV-visible tattoos, centralized databases (See, Denning *et al*. 2014). Furthermore, to satisfy utility, safety, security, and privacy goals, IMDs need to meet a broad body of criteria, from software updates to data protection (Halperin *et al*. 2008). Not only is (medical) cybersecurity a relational matter of persons, devices, and professionals, but a successful mitigation of such issues requires even more actors, such as cybersecurity experts, and their constant work on innovation. Furthermore, technology itself is not the only thing that constitutes all the factors and vulnerabilities. An unexpected shock, and at the wrong time, from an ICD, as I will briefly show, sets many relevant sociotechnical practices in motion. The wearers of ICDs are the stakeholders who are impacted by the design, but also dependent on medical professionals who interact with these technologies by referring to the existing regulations. What this all means is that networked devices form a complex interaction and interdependencies between technologies and many actors, highlighting what we should mean by sociotechnical systems. To solve emerging problems of implantable technologies, or even cast light on overall emerging cyborgization, we should investigate these interactions and interdependencies as such.

I want to emphasize that in the context of existing IMDs, it is the wearer who is ultimately affected by the overall "setup". Oudshoorn (2016) has analyzed and highlighted how people experience and attempt to handle an inappropriate shock—the one not needed, and often unexpected—from their defibrillators. According to her study, both the technicians and technomedical culture determine whether an inappropriate shock could be likely. A technician, under uncertainty, might tune the machine to have more agency, and risk an inappropriate shock (noted in the USA and previously in the Netherlands), or disable a couple of functions on the device, and allow the heart to attempt to regain itself (as it is in the Netherlands now) (Oudshoorn 2016). She then further points out how frustration with the technology and technicians has led some people to use magnets to tame the device, having learned it themselves or suggested to do so by medical professionals or other

users. In case of an emergency, physicians may use round-shaped clinical magnets to bypass the programming and wait for an appropriate professional to analyze it. However, there are risks involved with using magnets (Rodriguez-Blanco *et al*. 2013), and even more so when used outside medical institutions. These technologies reveal just how interdependencies generate the need for more artifacts as well as the need to modify the existing technology because the medical device itself depends on certain actors. But it is also the opposite. The technology itself, programmed and accessed in a certain manner and by certain professionals, generates the layout for how actors are involved.

Besides devices and medical practitioners, we also must account for the software and, more importantly, the code that the device uses. Karen Sandler's story and research shows why it is such an important matter for IMDs. Sandler, formerly in the GNOME Foundation, and currently an executive director of Software Freedom Conservancy, highlights an inappropriate shock experience with her ICD. In her "cyborg-to-cyborg" interview with Marie Moe (2021), she mentions her hypertrophic cardiomyopathy being the reason for having an ICD, and tells of an instance during pregnancy. When the ICD registered the heart palpating as worthy of a shock, it made her take countermeasures to calm it down. As ICDs are computing devices, Sandler sees the fault in software, which is usually owned by manufactures, and as a result, closed for patients and medical professionals to access and test its features (Sandler *et al*. 2010). Closed source means that software makers have decided not to provide the code which can be read and modified by others (third parties). It is very often the case with the so-called propriety licensing where the authors function as the owners, setting the restrictions.

Instead, Sandler argues for open-source software that allows others to review and modify the code. It is mainly because some essential technical problems might be overlooked, and the closed source is potent to vulnerabilities as the only ones able to investigate and mitigate are the owners (Sandler *et al*. 2010). There is another benefit, according to Sandler, besides having more eyes and hands on technical problems. Open source would not ultimately mean that wearers themselves access it, but that they have the freedom to choose the professionals and

companies that have access to the device (Sandler & Moe 2021, 105). Moreover, as she mentions, because of proprietary software in the ICD, there is no way to ensure that the device can adapt to the changes in her life—this technology is meant to last for years, however, in a world with rapid technological changes (Sandler & Moe 2021, 103). What Sandler proposes here, is a distinct concept of freedom, applicable to implantable technologies. It is the freedom of relationality, important for our sociotechnical systems' context. This gives one the choice to decide the assemblages between actors. It implies that an individual should have the freedom to decide among the professionals by allowing them also to access and, if needed, modify the device. To generalize, this could become relevant for all kinds of implantable technologies in the process of cyborgization. If such freedom presupposes the development model of open source, it deserves further investigation.

From Open-Source Software to Clinical Engineering

The previous section provided a look into some problems we need to face with implantable technologies. However, it also uncovered open source as a development model that could be needed for existing and emerging cyborg technologies. Furthermore, without open source, cyborgs could face further difficulties to their quality of life if, by having an implantable technology, one is tied to a closed relation in terms of actors, technicians, or a company's decisions. Nevertheless, an account for software might not be enough to argue for the need and value of open source that needs to include many elements of cyborg technologies. Furthermore, particularly when it comes to other aspects of biological life where open-source development could be used or is needed, there are already worries and benefits pointed out. This section and the following one will examine the development model across relevant human and technology realms.

Drafted by Bruce Perens, and later modified by his colleagues, the Debian Free Software Guidelines (Debian Project 2004) became "The Open Source Definition" of the Open Source Initiative (OSI). The document states the terms according to which software counts as open

source (Open Source Initiative 2007). Anyone should be allowed to access the source code for software, and be able to study, use, modify, and distribute in under numerous licenses available. Eric S. Raymond, in his famous essay *The Cathedral and the Bazaar* (2001) examined the development model of Linux's operating system kernel that happened via the internet. According to Raymond, before and outside the development of the Linux operating system, software with open-source code reached only a small group of developers. It resembled people building cathedrals. However, the development model of Linux took advantage of the internet. The latter indicated that everyone could see and access the development early on. Thus, Linux took the open-source development to the public, resembling something of a bazaar.

The term is now wide-spread, and open source has become an ethos that captures more than software development. Without mapping out all of them, many producers are using the main idea and its licensing strategies to produce the goods. In the context of technological hardware, the Open Source Hardware Association (OSHWA) provides its definition and statement of principles in which hardware design is open source if the blueprints are available to the public. However, it also adds the specifics for hardware, including a plea to use readily available components, materials, and open infrastructure for the exchange of blueprints (Open Source Hardware Association 2022). While distributed version control—the visible bazaar of open source on the web— such as GitHub is known for the open-source software distribution, a website called Thingverse is an example of a hardware bazaar that provides the design blueprints.

The field of clinical engineering brings together both hardware and software with the emphasis on open source as valuable for our current needs (See, *e.g.*, De Maria *et al*. 2018, 2020). The situation, however, is complicated due to the function and nature of bionic and implantable medical devices. De Maria *et al*. (2020) nevertheless argue for the open-source medical devices (OSMD) because the current healthcare requires more accessible and affordable technologies for everyone—valued by Sustainable Development Goals and the World Health Organization. The challenge, however, is how to make open-source clinical engineering safe. The developers of OSMDs need to include and consider innovation

along the lines of all that makes up these technologies: software, hardware, safety regulations of a medical device. Thus, De Maria *et al*. propose the following definition. The first half consists of the requirements for open-source software as well as hardware. Such technologies should be built with interchangeable and interoperable parts and depend on more open e-infrastructures for information (De Maria *et al*. 2020, 9). It then proceeds by asking engineers to consider international safety standards. For the development of medical technologies, many legislation acts exist, and these are not hindering the commitments to open-source in the given area. The problem is rather about harmonizing different legislations across the globe so that those who are in need would benefit from the accessibility and affordability of OSMDs designs and products (De Maria *et al*. 2018).

Data Exchange Layer: A Bazaar for Cyborgs

Recently, some transhumanist scholars have started to see existing technological solutions and models as a viable option for certain ideas that we have about the future. Take, for example, Melanie Swan's idea on how blockchain technologies with smart contract applications could be able to support the idea of a cloudmind, defined as an individual's access to parts of his or her cognitive resources for the benefit of collaborative tasks (Swan 2019). In one commentary, Swan also explores the role of a distributed version control software and hosting site GitHub—essential for software developers to keep track of changes in code—to extrapolate how people who use cloudminds could be able to access earlier versions of their cognitive data, like memories in case of its loss (Swan 2015). GitHub, or Git-like version control software, in general, explicitly illustrates Raymond's idea of the bazaar for open-source development and its communities. Analogical to this well-controlled distribution database, others have been proposed, seen as beneficial for a safe progression towards a posthuman future. Stefan Sorgner promotes the second one by examining the usefulness of gene analysis, and the role of regulated distribution control on a governmental level. According to him, gene analysis—a promising path towards a posthuman

future—benefits from big data collection but is being troubled by the problem of privacy as many actors and companies have their interest in collecting and keeping the data to themselves (Sorgner 2017). In his later work (2021), however, Sorgner suggests a model that could be able to distribute gene data efficiently without letting interested parties centralize our data, and as a result, gene data can be used for greater innovation. Furthermore, in his vision we should think about the inescapable situation of total surveillance and reconsider the government as a democratic hosting service for distributing our data in a manner that we still have the freedom and control in this, *e.g.*, one can use data or other currencies to pay for medical necessities (Sorgner 2021, 42–46). In this scenario, since the government is the distributing host, private (pharmaceutical) companies lose the ability to overcharge for the goods as it then depends on whether people provide the data to the government to further distribute it to the company (Sorgner 2021, 44). While our investigation of human-technology interlinkages and open source differs from the ones above, the idea of regulating distribution models and technologies remains relevant. Two existing philosophical and technical explorations make use of distribution service support to mitigate the issues with data chaos and unorganized management. Considering our focus on the open-source devices and development, a technological infrastructure, providing similar benefits, should be asked for. In other words, what kind of "bazaar" architecture do we require so that we can have sociotechnical systems where open source is beneficial for:

- innovative and open clinical engineering so that certain parties do not make the device (meant to last for a long time) obsolete;
- people who use IMDs can take advantage of the freedom of relationality, *i.e.*, they have the option to choose among technicians and other professionals in hopes of avoiding uncertainties and unpleasant experiences;
- all the data required for this process to work across sociotechnical systems, nevertheless, can be safely managed, and used to improve the lives of those who either need IMDs or decide to wear any implantable device for any choice of cyborgization?

As these encompass both current and future difficulties, we must continue with the search for a "bazaar"—a distribution system able to accommodate the valuable world of open source: a decentralized system, rising from the need of human-technology interlinkage in a sociotechnical system with many actors involved. In this section, I will further provide a description of a technological model that could suit these needs, while in the next one, I will further analyze some related concerns.

Some countries are being recognized for taking the advantage of information and communication technologies (ICT) applied to government and other infrastructures. Estonia is considered a prime example having an e-governmental sociotechnical and information systems' solutions for running things. So, for now, I will consider a concrete example of the technology, called distributed data exchange layer (DXL), that runs behind the infrastructure of Estonia's e-Government (or e-Estonia, as it is sometimes called). A software-based ecosystem or a middleware, called the X-Road (officially "X-tee" in Estonian), is Estonia's open-source solution that is used to securely move data between different organizations (Estonian Information System Authority 2022)[2]. With this ecosystem, both the public and private sectors can exchange data without fragmenting collaboration and causing needless data duplication (Paide *et al*. 2018). Simply put, this means that all existing service providers of public and private sectors, who are members of X-Road, are linked together for easy data exchange by digitally signed contracts. Not going into all the technical details, I will lay out what it means for the existing residents within this ecosystem.

We could start with a concrete example of healthcare e-service. Residents can access all their data and histories concerning analyses, prescriptions, insurance, etc., on a patient web portal by authenticating themselves with a smartphone application or an ID-card. After some medical procedure, all the results go to the portal where both the patient and, for example, a family physician can access the data as it is. When the patient receives a prescription for medicine; the information goes to the database, and a pharmacist, entering the identification, can see it

[2] Available on GitHub: <https://github.com/nordic-institute>, last time accessed in September, 20, 2022.

together with other relevant information. While this forms interlinkage within healthcare infrastructure, the data exchange also reaches other institutions. To get a driver's license, one needs a medical certificate, and data goes from the patient portal to the road administration. To pay for the needed services, one exchanges data between the internet bank and, for example, the road administration. Suppose also that a car accident happens. After the phone call, an ambulance can quickly position the call, and the professionals can access, using a person's ID, all the real-time information, ranging from medicines currently used to allergies.

The open-source "cyborg" engineering and the users of these devices could benefit from a similar technological ecosystem that includes data exchange layer. This suggestion should be seriously and positively considered. The networked, software-based, yet at the same time health-related nature of implantable technologies, require better and quick-response connection within the complex sociotechnical systems to provide reliable and safe human-technology coupling. One could picture a working data exchange infrastructure that links together many bazaars or hubs of open-source developments. In case of a security issue or other bug, DXL would allow all the relevant parties to be aware of it, starting with patients, physicians, and technicians to engineers. The open-source code would be exchanged similarly in this case. Suppose, however, the update for the implant becomes available, the user and physicians would be able to consult about whether installation would be a good idea. The important factor in this case is also that all the other data in the system would give both the user and professionals a more personalized view over things to decide properly. A data exchange layer together with an ethos of open-source present a vision fit for cyborgs. A quicker and reliable data exchange and open innovation are both needed so that the technological part and the human part would continue to work in harmony. In short, this solution could help mitigate technical concerns we have with implantable technologies and would help us realize how open-source development could successfully work within sociotechnical systems, and further provide people the freedom and control over their health that is not limited by the pre-programmed device.

Open Source for Cyborgs as a Technical Problem

The solution is so far only partially examined. It might allow the experience of greater autonomy, a variety of choices and assurances regarding their device. However, the implementation of open source from a design perspective, and even more so in the context of cyborgization, is far from an easy decision-making. Both closed source and open source as methodologies for developing technologies are, besides the complicated economic decisions, also decided regarding assumptions about security and human factors susceptible for breaking the technology. Furthermore, while the previously mentioned idea could offer a technological solution to the people needing implantable devices for medical purposes to restore biological functioning and sustain their health, open source is also an ethos already applicable to various technological and scientific pursuits and needs, which can be used to reflect on wide-range cyborg developments. Beyond the development of computing devices, cyborgization also demands scientific materials, such as genetic information, body monitoring, and tools, to be opened to the public. As such, it is especially important for the question concerning a variety of cyborg practices and the current concerns with the latter. Here, such openness introduces a public concern about unregulated uses of information and technology. These are demanding challenges. Nevertheless, if technologies can potentially pose certain threats to cyborg or human lives and freedoms, and if open source could be seen as the remedy for these new vulnerabilities, which could also illuminate challenges for the future of cyborgs, it is worth addressing both technological and political issues. In this section, I will consider the technological ones because the implementation of a data exchange layer presupposes that open-source technologies are without fundamental errors or, in our case, life-threatening.

The problem of a company going bankrupt is a serious one for the wearers of implantable technologies. Nevertheless, while it could be a good reason for adopting open source, the proponents of closed source, especially in terms of software, might be right to argue that without the visibility of source we will have better security. Malicious actors are known to take advantage of bugs and overlooked instances of the

program to cause harm. The advocates of open source rely on the idea that a peer-review process of the community can assess and address these issues quickly (Payne 2002). One of Raymond's musings is that "[g]iven enough eyeballs, bugs are shallow" (2001, 19), emphasizing the role of community for greater security. Proponents of closed source might, nevertheless, claim that if bugs cannot be seen and known, there is no security problem (Payne 2002, 67). Furthermore, given that bugs in open-source software are always visible, it is a problem because it is not guaranteed that enough eyeballs mean enough skilled minds (Payne 2002, 70), or that good developers are quick enough to reach these vulnerabilities in an instance of a new version (Schryen & Kadura 2009, 2018). Besides removing bugs, security might be achieved with system integrity, which means that both hardware and software are designed as if meant for each other. Apple's closed source devices could be an excellent example of system integrity, having all the parts necessary for another so that the security cannot be compromised on any level of the system. While these are valid points for our computers, it is questionable if closed source in implantable technologies could be argued for from the same grounds. For example, is a perfect system integrity possible in the case of implantable technologies? It might be in the future. Nevertheless, it would require greater knowledge and data about humans, and it could mean that we still need open source on a level of biological science for a quicker innovation and access. This is the consideration for the next section. Here, we need to continue with the argument on open-source technology.

Where closed source advocacy might make a plausible input for implantable technologies against open source is about the latter being unable to reach bugs and errors quickly enough. But the same could be said about closed source, especially in the context of implantable technologies. On everyday computers, the user can use an alternative program until the problem is solved, upload the data elsewhere and switch the computer. To a living being, an overlooked bug could be fatal (Sandler *et al*. 2010), and there would be no quick alternative (shutting the device down with a magnet is a temporary solution, not beneficial for the whole being). Thus, any cyborg would need not only the largest set of eyes and skilled minds to access the information, but also the

quickest measures. The latter would require both existing data about the person, technology, and other information necessary. Having a data exchange layer technology over our open-source cyborgization could offer this. Moreover, a human wearer of technology would need a collaboration transcending one field of expertise: a bazaar for cyborgs.

My proposal is not without further difficulties. With a sort of data exchange layer technology, we would completely materialize our being within the Internet of Things (IoT). For people with wireless IMDs it already is the case. But with more and more data about biology, different technologies on top of the existing ones (especially with future technologies), and more actors could become involved. Such exploration shifts from the matter of accountability from technologies and cyborgs to sociotechnical systems: the accountability of cyborgs as networked beings. This would now mean a greater dependency on a single technological system to exchange everything. A malicious attempt is then an even greater risk. It is not only even about the attacker shutting down the data exchange layer system, or stealing a large amount of valuable data, but using the large-scale data exchange technology to literally get into a person's body, having now perhaps a greater variety of instances to attack. Open source is argued to be highly efficient for the IoT (Rayes & Salam 2022), and if we again use Estonia as an example, X-Road is also open source. If cyborgization means being more within the IoT than ever, then open source, based on the previous arguments on software, poses a serious concern. While distributed ledger technologies, such as blockchains and many other cryptographical means have proven to be safe enough, the solution in our case might not lie in the answer of adding more technology to make our existing and coming cyborg world a safer place. Rather, open source could perhaps benefit from social endeavors for the ideas proposed here. Besides technological problems, public acceptance tends to have differences regarding wide-spread open source as a valuable ethos.

Securing Biology, Freeing Information

Here we have concern for our security on two levels. One is security vulnerabilities reaching us through the technology, if we are to require a technological and open-source development solution. The second is the vulnerability of our very biological and bodily being at risk due to the ethos of open-source in the first place. Again, there is a concern about the possibility of malpractices when our biological information is freed. We need to address this, because information about biological matters and the development model for sharing the latter could prove to be useful for designers and other professionals working to contribute to the "cyborg bazaar".

As there is an "irresistible analogy between software and molecular biotechnology," (Hope 2008, 18) there is also a possible case for open source in bioscience where we move from software bazaar to a biobazaar, explored by Janet Hope with the hopes of innovation and faster progression. However, all the innovative work in open-source biology could be curtailed by malicious actors, unsafe practices outside the laboratory, and overall societal concerns (Evans and Selgelid 2015). While Evans and Selgelid argue that the ubiquitous spread of information by open-source biology is good for society and for advancements of our well-being, they nevertheless emphasize the role of regulations and biosecurity awareness in open-source biology communities. Their argument, however, is not simply a proposal for further enforcement of existing regulations on an innovative approach, but regulations themselves need to become innovative in the presence of potential malpractices. The threat lies greatly in the fact that, by allowing the radical openness of science and information, all the equipment and knowledge of genomics and synthetic biology gets thrown into the uncertain wilderness of actors with very different intentions. However, the future of open-source biology could benefit, if we do not conceptually or otherwise place the radical openness of science outside its initial context of software development but keep it in the successful model of open-source software (Hessel 2006). As Andrew Hessel says, if open-source software "works, and DNA is software, don't reinvent: adapt" to point out that genetic engineering should be done on

computers like software engineering, using open-source software for the task (Hessel 2006, 290). This re-thinking and re-making open-source biology back into open-source software, a collaborative online "bazaar" is found, for instance, in the project of Cambia.[3] More recently, SynBioHub[4] rose as a repository for engineered biological systems that allows downloading and uploading, for example, DNA and protein designs for sharing and storing within the repository (McLaughlin *et al*. 2018). Open source within biology and clinical engineering, although having ongoing challenges with security and regulations, are seen to benefit from the openness—its ethos, licensing, and technologies (CAD-programs, versioning repositories, free and open-source software, 3D-printers etc.)—that grant it its success. If taken separately, these various commitments could be seen to regulate their own sciences and devices, allowing them further success.

However, and in many ways, the concern with our genetic information and other scientific tools is about its uses for everyone, about the practitioners of the so-called "citizen science" (Irwin 1995). The body itself is something "hackable", and arguably open source, for body hacking "grinder" and biohacker communities in the hacker culture of the cyberworld.[5] Self-experimentation that goes beyond restoration, and thus explores with reconfiguration and enhancement through implantable RFID, magnetic, etc., technologies, is for some significant way to identify themselves as cyborgs. Instead of tackling the ethical issues about the safety, control, and freedom of these practices (See generally, Greguric 2014, 2022), I want to problematize these practices considering our data exchange layer proposal.

---

[3] Available on <https://cambia.org/> last time accessed December 17, 2022.

[4] Available on <https://synbiohub.org> last time accessed December 17, 2022.

[5] Nowadays, the term "hacker" has a negative meaning of a person engaging in malicious activities. However, in the context of open source and hacker culture, hackers have been technology-savvy people that enjoy challenges and solving problems and are opposite to those "crackers" (Raymond 2020). In other words, instead of malicious hackers, we should talk about malicious crackers.

Open-Source Politics for Cyborgs

The question is about inclusion of those using the information but wanting the freedom to seek their own way of cyborgization, and together with it, their own communities for the further development of source code or blueprint. Here is an alluring analogy with the practice known as *forking*, known to the users of the Linux operating system and GitHub. In the software world, forking means separating a copy from an existing community's source base to pursue developing it independently or with another community, often competing with the original (Fogel 2005, 69). It could be pursued if there are conflicts with the community or visions in development. However, the ultimate problem with forking is that it might generate a situation where two versions cannot "exchange code" (Raymond 2001, 72). It is a "technological equivalent" to how DNA and evolution works in case of "speciation in genetics" (Weber 2004, 157). Data exchange layer, our technological vision, could be taken as a solution for this situation in case of "cyborg forking" where people, unsatisfied with current actors, approaches, and data, seek to form their own communities to develop and sustain as cyborgs. Nevertheless, data exchange also fails in this sense: the original community consists of scientists, developers, medical experts, etc., who cannot, due to the lack of understanding of technologies of the new community, or are not willing to help these cyborgs. Not to mention the situation where people decide to copy and develop their own data exchange layer, incompatible with the one offered by the government. An optimal hope lies in a larger set of information, provided by open source ethos across many sciences, to cover for all possibilities of forking. I contest, however, that the "right to fork" should be removed from the data exchange technology for the safety of cyborgs.

Code—the crux of the philosophy of open-source development and information freedom—generates both the cyborg world, and combines both technology and politics, requiring us to take freedoms within the software world seriously, as Samir Chopra and Scott Dexter have said (Chopra & Dexter 2007, 2008). "In the cyborg world," Chopra and Dexter moreover claim, "closed software threatens individual autonomy; the advocacy for, and the provision of, closed software is a

form of paternalism, diminishing cyborg autonomy as it controls and regulates the nature of human-machine interaction" (Chopra & Dexter 2007, 47). The freedom of information, code-based or otherwise, and other rights have been emphasized for the sake of "cyborg citizenship" even earlier, needing political protection and political technologies for that matter (Gray 2000, 28–29). Nevertheless, while open source and other technologies, in principle, can grant these freedoms, it would be wise to account what open source already entails in other areas, and what other political and social concerns might arise if our cyborg world is not just any human-machine interlinkage, but dominantly constituted by information and computing devices (Chopra & Dexter 2008, 148). The issue of forking is, thus, also relevant.

Forking, at least in software development, is undesirable and under social pressure (Raymond 2001, 73), but it is also an essential right in open-source projects (Fogel 2005, 5) if the latter is about autonomy and community work. Among software developers, major or hard forks have not been frequent (Weber 2004, 134). If we take seriously the idea that cyborgs with implantable and other technologies need both open-source developments and all the help with the IoT where relevant data and free information exists, forking becomes a question about societies, culture, and politics. Because of changes in open source policies, such as forking, it could lead to paternalism, or if such questions are overlooked, could bring harm to cyborgs. Thus, there would be a need for addressing technological development in-depth. Furthermore, we must look at how new vulnerabilities benefit from technologies, but also what other questions might rise on a social and political level.

Conclusion

Next to other pathways to the posthuman future, cyborgization is often seen as an ongoing process, in which we tamper with biology and evolution through technologies. Ray Kurwzeil's vision is well-known: computational devices move from desks to pockets, from pockets to our bodies, until there is more machine than human (Kurzweil 2005). The

question here has not been about the likelihood of such an event, but an exploration of what cyborgization means advanced from the current, computationally ubiquitous, present. Looking at the possibility of designing human advancement with technologies, we should be interested in both the nature of technologies and the design practices. In terms of technologies, some transhumanist scholars, I believe, are on the right track when they inquire about the significance of data and internet, raising philosophical problems on the way to the future (Sorgner 2017; Sorgner 2021); or when they attempt to situate the utopian idea of mind uploading into a concrete technologically secure solution (Swan 2015, 2019).

This paper focused on the open-source development model, found in software engineering and elsewhere. It adds to the process of cyborgization the idea that we are not only designing humans with technologies, but have ways of developing the technologies that count as a part of the former. This is just one way of seeing how the internet, and different actors, from developers to users, constitute a complexity of cyborgization. Open-source development, often associated with the Linux operating system, has, from early on, taken advantage of the internet, and development has been described as co-evolution, binding together communities and structures of social and technical (Tuomi 2002). Nevertheless, the proposal to take this model into consideration should not be merely based on its current success in innovation. As I have shown, the reason for taking open source seriously arises from (new) vulnerabilities, related to implantable technologies. Decisions made by companies and professionals live within people or are deeply attached to them. The argued solution could be open-source technologies, freely modifiable by the other, giving the wearer a sense of freedom to choose experts, and autonomy. However, if this solution is to be applicable to more of the present and future cyborg technologies, it would require more and quicker minds and hands, at least for some time into the future. For this I have proposed how we could implement data exchange layer technologies that could bring together various public and private institutions, communities, and information to secure the future with cyborg technologies.

Acknowledgment:
I would like to thank Oliver Laas for providing valuable feedback on the early draft of this paper.

REFERENCES

Barfield, Woodrow; Williams, Alexander (2017). "Law, Cyborgs, and Technologically Enhanced Brains." *Philosophies* 2 (1): 6. https://doi.org/10.3390/philosophies 2010006.

Chopra, Samir; Dexter, Scott D. (2008). *Decoding Liberation: The Promise of Free and Open Source Software*. Routledge Studies in New Media and Cyberculture 4. New York London: Routledge, Taylor & Francis Group.

———. (2007). "Free Software and the Political Philosophy of the Cyborg World." *ACM SIGCAS Computers and Society* 37 (2): 41–52. https://doi.org/10.1145/1327325. 1327328.

Clynes, Manfred E.; Kline, Nathan S. (1960). "Cyborgs and Space." *Astronautice* 14 (9): 26–27, 74–76.

Coeckelbergh, Mark (2011). "Vulnerable Cyborgs: Learning to Live with Our Dragons." *Journal of Evolution and Technology* 22 (1): 1–9.

———. (2013). *Human Being @ Risk*. Philosophy of Engineering and Technology. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-6025-7.

Cooper, Robert; Foster, Michael (1971). "Sociotechnical Systems." *American Psychologist* 26 (5): 467–74. https://doi.org/10.1037/h0031539.

De Maria, Carmelo; Di Pietro, Licia; Díaz Lantada, Andrés; Madete, June; Makobore, Philippa Ngaju; Mridha, Mannan; Ravizza, Alice; Torop, Janno; Ahluwalia, Arti (2018). "Safe Innovation: On Medical Device Legislation in Europe and Africa." *Health Policy and Technology* 7 (2): 156–65. https://doi.org/10.1016/j.hlpt.2018.01.012.

De Maria, Carmelo; Di Pietro, Licia; Ravizza, Alice; Díaz Lantada, Andrés; Ahluwalia, Arti Devi (2020). "Chapter 2 – Open-Source Medical Devices: Healthcare Solutions for Low-, Middle-, and High-Resource Settings." In *Clinical Engineering Handbook (Second Edition)*, edited by Ernesto Iadanza, 7–14. Academic Press. https://doi.org/10.1016/B978-0-12-813467-2.00002-X.

Debian Project (2004). "Debian Social Contract." https://www.debian.org/social_contract #guidelines.

Denning, Tamara; Kramer, Daniel B.; Friedman, Batya; Reynolds, Matthew R.; Gill, Brian; Kohno; Tadayoshi (2014). "CPS: Beyond Usability: Applying Value Sensitive Design Based Methods to Investigate Domain Characteristics for Security for Implantable Cardiac Devices." In *Proceedings of the 30th Annual Computer Security Applications Conference*, 426–35. New Orleans Louisiana USA: ACM. https://doi.org/10.1145/2664243.2664289.

Estonian Information System Authority (2022). "X-Road® Data Exchange Layer." X-Road® Data Exchange Layer. 2022. https://x-road.global/xroad-introduction.

Evans, Nicholas G.; Selgelid, Michael J. (2015). "Biosecurity and Open-Source Biology: The Promise and Peril of Distributed Synthetic Biological Technologies." *Science and Engineering Ethics* 21 (4): 1065–83. https://doi.org/10.1007/s11948-014-9591-3.

Featherstone, Mike, Burrows, Roger (eds.) (1995). *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment*. Theory, Culture & Society. London: Sage.

Fogel, Karl (2005). *Producing Open Source Software: How to Run a Successful Free Software Project*. 1st ed. Beijing; Sebastopol, CA: O'Reilly.

Franssen, Maarten; Kroes, Peter (2009). "Sociotechnical Systems." In *A Companion to the Philosophy of Technology*, edited by Jan Kyrre Berg Olsen Friis, Stig Andur Pedersen, and Vincent F. Hendricks, 223–26. Blackwell Companions to Philosophy 43. Chichester, UK ; Malden, MA: Wiley-Blackwell.

Gray, Chris Hables (2000). *Cyborg Citizen: Politics in the Posthuman Age*. New York: Routledge.

Greguric, Ivana (2014). "Ethical Issues of Human Enhancement Technologies: Cyborg Technology as the Extension of Human Biology." *Journal of Information, Communication and Ethics in Society* 12 (2): 133–48. https://doi.org/10.1108/JICES-10-2013-0040.

———. (2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics:* Advances in Human and Social Aspects of Technology. IGI Global. https://doi.org/10.4018/978-1-7998-9231-1.

Halperin, Daniel; Heydt-Benjamin, Thomas S.; Fu, Kevin; Kohno, Tadayoshi; Maisel, William H. (2008). "Security and Privacy for Implantable Medical Devices." *IEEE Pervasive Computing* 7 (1): 30–39. https://doi.org/10.1109/MPRV.2008.16.

Haraway, Donna Jeanne (1991). *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Hessel, Andrew (2006). "Open Source Biology." In *Open Sources 2.0: The Continuing Evolution*, edited by Chris DiBona, Danese Cooper, and Mark Stone, 1st ed, 281–96. Beijing; Sebastopol, CA: O'Reilly.

Hope, Janet (2008). *Biobazaar: The Open Source Revolution and Biotechnology*. Cambridge, Mass: Harvard University Press.

Irwin, Alan (1995). *Citizen science: a study of people, expertise, and sustainable development*. 1. publ. Environment and society. London: Routledge.

Kurzweil, Ray (2005). *The Singularity Is Near: When Humans Transcend Biology*. New York: Viking.

McLaughlin, James Alastair; Myers, Chris J.; Zundel, Zach; Mısırlı, Göksel; Zhang, Michael; Ofiteru, Irina Dana; Goñi-Moreno, Angel; Wipat, Anil (2018). "SynBioHub: A Standards-Enabled Design Repository for Synthetic Biology." *ACS Synthetic Biology* 7 (2): 682–88. https://doi.org/10.1021/acssynbio.7b00403.

Open Source Hardware Association (2022). "Open Source Hardware Definition." Open Source Hardware Association. 2022. https://www.oshwa.org/definition/.

Open Source Initiative (2007). "The Open Source Definition." 2007. https://opensource.org/osd.

Oudshoorn, Nelly (2015). "Sustaining Cyborgs: Sensing and Tuning Agencies of Pacemakers and Implantable Cardioverter Defibrillators." *Social Studies of Science* 45 (1): 56–76. https://doi.org/10.1177/0306312714557377.

———. (2016). "The Vulnerability of Cyborgs: The Case of ICD Shocks." *Science, Technology, & Human Values* 41 (5): 767–92. https://doi.org/10.1177/0162243916633755.

Paide, Karoline; Pappel, Ingrid; Vainsalu, Heiko; Draheim, Dirk (2018). "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships." In *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, 34–41. Galway Ireland: ACM. https://doi.org/10.1145/3209415.3209441.

Payne, Christian (2002). "On the Security of Open Source Software." *Information Systems Journal* 12 (1): 61–78. https://doi.org/10.1046/j.1365-2575.2002.00118.x.

Pycroft, Laurie; Aziz, Tipu Z. (2018). "Security of Implantable Medical Devices with Wireless Connections: The Dangers of Cyber-Attacks." *Expert Review of Medical Devices* 15 (6): 403–6. https://doi.org/10.1080/17434440.2018.1483235.

Rayes, Ammar; Salam, Samer (2022). *Internet of Things from Hype to Reality: The Road to Digitization*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-90158-5.

Raymond, Eric Steven (2001). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Rev. ed. Beijing ; Cambridge, Mass: O'Reilly.

———. (2020). "How To Become A Hacker." Thyrsus Enterprises. 2020. http://catb.org/~esr/faqs/hacker-howto.html.

Rodriguez-Blanco, Yiliam F.; Souki, Fouad; Tamayo, Evelyn; Candiotti, Keith (2013). "Magnets and Implantable Cardioverter Defibrillators: What's the Problem?" *Annals of Cardiac Anaesthesia* 16 (1): 54. https://doi.org/10.4103/0971-9784.105372.

Sandler, Karen; Moe, Marie (2021). "'Don't Mess With My Heart Device, I'll Do It Myself.' In Which Karen and Marie Interview Each Other." In *Modified: Living as a Cyborg*, edited by Chris Hables Gray, Heidi Figueroa-Sarriera, and Steven Mentor, First, 101–7. New York, NY: Routledge.

Sandler, Karen; Ohrstrom, Lysandra; Moy, Laura; McVay, Robert (2010). "Killed by Code: Software Transparency in Implantable Medical Devices." *Software Freedom Law Center*, 12.

Schryen, Guido; Kadura, Rouven (2009). "Open Source Vs. Closed Source Software: Towards Measuring Security." In *Proceedings of the 2009 ACM Symposium on Applied Computing*, 2016–23. SAC '09. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1529282.1529731.

Sorgner, Stefan Lorenz (2017). "Genetic Privacy, Big Gene Data, and the Internet Panopticon." *Journal of Posthuman Studies* 1 (1): 87. https://doi.org/10.5325/jpoststud.1.1.0087.

Sorgner, Stefan Lorenz (2021). *We Have Always Been Cyborgs: Digital Data, Gene Technologies, and an Ethics of Transhumanism*. Bristol: Bristol University Press.

Strickland, Eliza; Harris, Mark (2022). "Their Bionic Eyes Are Now Obsolete and Unsupported." *IEEE Spectrum*. February 15, 2022. https://spectrum.ieee.org/bionic-eye-obsolete.

Swan, Melanie (2015). "Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation [Commentary]." *IEEE Technology and Society Magazine* 34 (4): 41–52. https://doi.org/10.1109/MTS.2015.2494358.

———. (2019). "Transhuman Crypto Cloudminds." In *The Transhumanism Handbook*, edited by Newton Lee, 513–28. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-16920-6.

Tuomi, Ilkka (2002). *Networks of Innovation: Change and Meaning in the Age of the Internet*. Oxford; New York: Oxford University Press.

Weber, Steve (2004). *The Success of Open Source*. Cambridge, MA: Harvard University Press.