Minds and Machines (2019) 29:349–354
https://doi.org/10.1007/s11023-019-09507-5

EDITORIAL

Is Cybersecurity a Public Good?

Mariarosaria Taddeo[1,2]

Published online: 5 October 2019

The World Economic Forum's Global Risks Report 2019 ranked cyber attacks among the top-ten most impactful global risks. A report published in 2019 by the Ponemon Institute shows that 90% of companies supporting national critical infrastructures—energy, health, industrial and manufacturing, and transport—experienced at least one cyber attacks between 2017 and 2019 that led to data breaches or significant disruption of operations (Ponemon Institute LLC 2019). These reports are two of a long series of studies conducted over the past decade on the status of cybersecurity. From year to year, data about cyber attacks and their impact continue to increase indicating that cyber attacks pose an ever-growing threat for information societies.

There are two lessons to be learned from these data. The first lesson is not controversial, digital infrastructures are *porous*. We should think of them as agile, flexible, but brittle systems. This brittleness, as I argued elsewhere (Taddeo 2016, 2017a), favours offence over defence, explaining in part the continue growth of cyber threats and the escalation of their impact. The more digital technologies become pervasive, the wider becomes the surface of attacks, and with it also number of successful attacks grows. Think for example about the distribution of Internet of Things (IoT). In 2018, a Symantec study reported an average of 5200 attacks per month on IoT devices, the figure almost double the 3650 attacks counted in 2016. The second lesson may be harder to learn, for it is about the inadequacy of the ways in which we have framed and governed cybersecurity. This is clear when considering that data on the escalation of number and impact of cyber attacks, despite the growing value of the cybersecurity market and the increasing efforts of companies and state actors to improve the security of information systems and infrastructures (Technavio 2018).

The lack of effective cybersecurity measures has a potential knock-on effect on the information revolution, and on the development of information societies around

An early version of this letter has been published here https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/

✉ Mariarosaria Taddeo
mariarosaria.taddeo@oii.ox.ac.uk

[1] Oxford Internet Institute, University of Oxford, Oxford, UK

[2] Alan Turing Institute, London, UK

the globe (Floridi 2016). Two aspects are relevant here: international stability and trust. Without proper security measures in place, cyber threats may undermine the stability of information societies (Taddeo and Floridi 2018a), making digital technologies a source of risks as well as a source of development. The series of cyber attacks that allegedly Russia and the US launched against each other's national critical infrastructures between 2018 and 2019[1] is indicative of how cyber attacks may pose a threat to national stability. At the same time, lack of security of digital technologies will erode the trust of users (Taddeo 2010, 2012, 2017b); this in turn will cripple adoption, and hinder innovation.

Learning the second lesson entails reconsidering the frameworks underpinning the governance of cybersecurity. In this respect, there is a mounting consensus on treating cybersecurity as a *public good* to be managed in the public interest (Mulligan and Schneider 2011; Schneider et al. 2016; Weber 2017). I agree with this view. 'Cyber' is a constitutive elements of information societies, it is interwoven with the physical, economic, social and political elements, and its security it is essential to foster societal development, technological progress (Floridi 2014), and also to harness the potential of digital technologies to deliver socially good outcomes (Taddeo and Floridi 2018b). Cybersecurity encompasses a wide set of practices, from risk assessment and penetration tests; disaster recovery; cryptography; access control and surveillance; architecture, software, and network security; to hack-back and security operations, and physical security. Framing cybersecurity as a public good without a careful distinction of between practices, scopes, and actors is conceptually unwarranted and problematic when considering the governance of cybersecurity.

At a high level of abstraction cybersecurity has three main domains—engineering systems that are *robust* and can withstand attacks; design methods and system for threat and anomaly detection to guarantee a system's *resilience*; define system *responses* to attacks. While I agree that system robustness qualifies as a public good, I argue that this is not the case for system's resilience and response.

Treating System Robustness as a Public Good

Robustness measures the divergence between the actual and the expected behaviour of a system when it is fed with erroneous inputs or when there are errors in the execution. A system is more or less robust depending on the size of divergence between the actual and the expected behaviour. Robustness is essential (though not sufficient) to mitigate the impact of attacks and ensure reliable systems. At the same time, improving system robustness is a costly process: it requires accurate design, as well as code verification and validation, testing and probing for vulnerabilities. This makes robustness a *club good*, in that it is not exhausted by its use (i.e. it is non-rivalrous), but its access is regulated by its cost (i.e. excludable).

The escalation of cyber threats indicates that this approach is ineffective, if not problematic. Market dynamics foster a non-collaborative approach, and costs lead

[1] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

to uneven distribution. Building robustness into digital end-point devices will have an impact on their cost, to the extent that producers may sacrifice robustness in search of commercial competitiveness. This is often the case, for example, with IoT technologies—which risks favouring a pervasive distribution, on a global scale, of devices whose robustness is ephemeral. The question then is how do we develop and regulate the design of robust systems in an effective way?

Engineering robust systems has direct and indirect implications on the public interest of information societies; for it enables critical national infrastructures and services to work, and allows citizens to perform their daily routines relying on secure technologies. For these reasons, robustness should not be framed and managed as a club good, it should be treated as a *public good*. That is, a non-rivalrous good that is also non-excludable.

Managing costs is a key aspect to develop system robustness as a public good. To be considered as a public good, system robustness need not to come free of charge for the end users, but it is essential that its costs do not become a discriminating factor, determining access it. The key point here is to ensure that all users have access to digital technologies whose robustness is adequate to the purpose and the context of deployment. Just like street-lights and national defence—both involve costs, while allowing all citizens of a state to access them and maintain them through their taxes—cybersecurity can function as a non-rivalrous, non-excludable good, if its costs are shared *equitably* among the relevant stakeholders. An implication of this approach is that the public sector will have to shoulder some of the costs of cybersecurity, which may include, for example, costs related to the establishing of standards and certification procedures, as well as costs associated with testing technologies, while also ensuring that digital devices available on the market meet the necessary level of robustness.

Three important advantages follow from managing cybersecurity as a public good: a systemic approach to security; shared responsibilities among different stakeholders; and facilitation of collaboration.

Systemic Approach. The management of a public good requires consideration of both direct and indirect externalities, as well as medium and long-term consequences. This favours approaches that focus on interdependences in the security of different, but connected, technologies, and their impact on the context of deployment, and on the relevant public interest at stake.

Shared Responsibilities. As a public good, its management requires collaboration between the private and the public sector to ensure high level of system robustness. It is up to the public sector to establish standards, certification and testing, oversight procedures, to ensure that a sufficient level of security is maintained to protect and foster the public interest and redressing and compensation measures are in place when responsibilities are not discharged properly. At the same time, the private sector bears the responsibility of designing robust systems, developing and improving methods to foster robustness of the services and product that they offer, and collaborating with the public sector for the controlling and testing mechanisms. Envisaging system robustness as a public good also places some responsibilities on the users with respect to their cyber hygiene.

The distribution of responsibilities among the different actors as well as the need to consider direct and indirect externalities is likely to **favour collaboration and information sharing**. Sharing of information about vulnerabilities of different systems involved in the same supply chain, for example, will become essential for the private sector to guarantee system robustness and learn from peers. At the same time, the public sector may support this practice by including information sharing and collaboration as part of capabilities building initiatives and procedures. These practices can facilitate patching procedures and may reduce the zero-day and exploits market. In turn, this could slow down the cyber arms-race and weaponization dynamics of cyberspace (Taddeo 2016; Taddeo and Floridi 2018a).

A clarification will help before moving to the analysis of systems' resilience and response. The concept of 'public good' is an economic, and not a normative, one. However, societies may decide to treat something as public good on a normative ground, for example, to support public interest. Traffic lights are a good example, as they have a great positive impact on road safety, we treat them as public good. It is the same for systems' robustness, it is not per se a public good, but because of its essential role for our societies, it should be treated as one. Thus, digital technologies should be designed and developed according to high standards for robustness and robust systems should available to users notwithstanding market dynamics. Things are different when considering the other two domains of cybersecurity: systems' resilience and systems' response.

When Cybersecurity is not a Public Good

Systems' resilience and response are the active side of cybersecurity. Over the past few years, as cyber attacks continue to grow, they have attracted increasing interests. In the UK for example, the National Cyber Security Centre (NCSC) launched an Active Cyber Defence Programme, which fosters forms of network monitoring to identify attacks and sources of attacks and enables some forms of threat response. From an economic point of view, we could start treating systems' resilience and systems' responses as public good, instead of considering them club good. But, in both cases, the normative analysis would not justify this move. Unlikely system robustness, system's resilience and response are not essential to the security of a system. With an analogy, if system's robustness allows us to build solid, reliable systems, resilience and response allows us to ring-fence them. But ring-fencing may come at some high costs for the public interest and mislead the governance of cybersecurity.

Systems' resilience improves the ability of a system to withstand attacks, by facilitating threat and anomaly detection. Resilient systems require some forms of monitoring to identification possible threats, this may include scanning files, emails, mobile and endpoint devices, or even traffic data on a network. Monitoring can also extends to users behaviour and biometric profiles, like for example, the unique way in which a user moves her mouse around (BehavioSec: Continuous Authentication Through Behavioral Biometrics 2019). An Israeli company, offering services to support systems' resilience, notes on its website that they

> "[monitor] sensor data and human-device interaction from your app/website. Every touch event, device motion, or mouse gesture is collected" (Unbotify 2019).

Systems' resilience hinges on a delicate trade-off between security and individual rights (Taddeo 2013, 2014). It poses serious risks of undermining and breaching users' privacy, users' exposure to extra risks, should data confidentiality be breached, and may have a mass-surveillance effect. Framing systems' resilience as public good used for the public interest may aggravate these risks by skewing public debate on this trade-off, misrepresent the level of security threats, the need for monitoring and surveillance, and the risks that these measures may pose to individual rights.

In the same vein, commercial products and services are available on the market to enable systems' response, for example by providing autonomous and semi-autonomous systems endowed with a playbook of pre-determined responses for a number of threats (DarkLight Offers First of Its Kind Artificial Intelligence to Enhance Cybersecurity Defenses 2017). This allows (non-state) users to investigate, isolate and disable malware, viruses, and botnets. Facilitating systems' responses may not improve security of cyberspace. Quite the contrary, it is likely to lead to intensification of cyber attacks, which, in turn, may lead to kinetic (physical) consequences and pose serious risks of escalation and physical security (Taddeo 2017a). In 2018 a number of US Senators proposed to allow companies to hack back—respond—to cyber attacks. The proposal has not been approved, but the path that it open is a dangerously slippery. Regulations may extenuate these risks, by identifying legitimate actors and targets, legitimate methods and proportionality criteria, as well as responsible behaviour. All this would be harder to achieve, if systems' abilities to respond to attacks are presented as a public good used in the public interest.

Considering some of digital technologies, or uses of uses of digital technologies, as public good will be a step in the right direction insofar as it done cautiously and to support policy and governance approaches that will foster tolerant, just, open, pluralistic, and stable information societies.

References

DarkLight Offers First of Its Kind Artificial Intelligence to Enhance Cybersecurity Defenses. (2017). 26 July 2017. https://www.businesswire.com/news/home/20170726005117/en/DarkLight-Offers-Kind-Artificial-Intelligence-Enhance-Cybersecurity.

Floridi, L. (2014). *The fourth revolution, how the infosphere is reshaping human reality*. Oxford: Oxford University Press.

Floridi, L. (2016). Mature information societies—a matter of expectations. *Philosophy & Technology, 29*(1), 1–4. https://doi.org/10.1007/s13347-016-0214-6.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus, 140*(4), 70–92.

Ponemon Institute LLC. (2019). 'CyberseCurity in OperatiOnal TeChnOlOgy: 7 Insights YOu Need tO KnOw, MarCh 2019'. Ponemon Institute LLC. blob:https://lookbook.tenable.com/ee2b2c72-e552-43f6-843e-3a63a29d895c.

Schneider, F. B., Elain, S. M., & Deirdre, M. K. (2016). *Public cybersecurity and rationalizing information sharing*. Lausanne: Opinion Piece for the International Risk Governance Center (IRGC). http://www.irgc.org.

Taddeo, M. (2010). Trust in technology: A distinctive and a problematic relation. *Knowledge, Technology & Policy, 23*(3–4), 283–286. https://doi.org/10.1007/s12130-010-9113-9.

Taddeo, M. (2012). An analysis for a just cyber warfare. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, pp 1–10.

Taddeo, M. (2013). Cyber security and individual rights, striking the right balance. *Philosophy & Technology, 26*(4), 353–356. https://doi.org/10.1007/s13347-013-0140-9.

Taddeo, M. (2014). The struggle between liberties and authorities in the information age. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-014-9586-0.

Taddeo, M. (2016). On the risks of relying on analogies to understand cyber conflicts. *Minds and Machines, 26*(4), 317–321. https://doi.org/10.1007/s11023-016-9408-z.

Taddeo, M. (2017a). The limits of deterrence theory in cyberspace. *Philosophy & Technology*. https://doi.org/10.1007/s13347-017-0290-2.

Taddeo, M. (2017b). Deterrence by norms to stop interstate cyber attacks. *Minds and Machines*. https://doi.org/10.1007/s11023-017-9446-1.

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature, 556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6.

Taddeo, M., & Luciano, F. (2018). How AI can be a force for good. *Science, 361*(6404), 751–752. https://doi.org/10.1126/science.aat5991.

Technavio. (2018). *Global artificial intelligence-based cybersecurity market 2018–2022*. Technavio. 2018. https://www.technavio.com/report/global-artificial-intelligence-based-cyber-security-market-analysis-share-2018.

Unbotify. (2019). *Unbotify Home*. Unbotify | Behavioral Biometric Bot Detection. 2019. http://www.unbotify.com/.

Weber, S. (2017). Coercion in cybersecurity: What public health models reveal. *Journal of Cybersecurity, 3*(3), 173–183. https://doi.org/10.1093/cybsec/tyx005.