This letter appeared in *Minds & Machines*

DOI: https://doi.org/10.1007/s11023-019-09507-5

When Is Cybersecurity a Public Good?

Mariarosaria Taddeo[1, 2]

[1] Oxford Internet Institute, University of Oxford, UK
[2] Alan Turing Institute, London, UK
mariarosaria.taddeo@oii.ox.ac.uk

The lack of effective cybersecurity measures has a potential knock-off effect on the development of information societies around the globe (Floridi 2016). Two aspects are relevant here: 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 more than a source of development. At the same time, lack of security of digital technologies will erode the trust of users (Taddeo 2010; 2017); this in turn will cripple adoption, and hinder innovation (Floridi and Taddeo 2016). Cybersecurity is a crucial resource of information societies ad improving it is essential to foster societal development, technological progress, and also harness the potential of digital technologies to deliver socially good outcomes (Taddeo and Floridi 2018b; Cowls et al. Forthcoming). Appropriate governance of cybersecurity practices is vital to this end. This, in turn, will be defined by the way we conceptualise cybersecurity in information societies.

There is a growing consensus that for societies depending extensively on digital technologies to function, cybersecurity is a public good (cit). I agree with this view. However, framing cybersecurity as a public good without a careful distinction of between practices, scopes, and actors is conceptually problematic and misleading when focusing on the governance of cybersecurity. Cybersecurity encompasses a wide set of practices, from risk assessment and penetration tests; disaster recovery; cryptography; access control; architecture, software, and network security; to security operations, and physical security. Is cybersecurity public good in all these cases?

Which Cybersecurity?

Cybersecurity has multiple areas, it ranges from engineering systems that are *robust* and can withstand attacks, to design of methods and system for threat and anomaly detection (TAD) to guarantee systems' *resilience*, and to define system *responses* to attacks. Systems' resilience and response are features that may or may not be present during the deployment of a system. One can think of them as *add-on* to a specific system. Whereas, robustness is a feature engrained in the design and development of cyber system. 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 how small is the divergence between the actual and the expected behaviour.

Robustness is a necessary element (albeit not sufficient) toward the security of digital technologies. It is crucial to mitigate the impact of attacks and ensure reliable systems. In societies depending on digital infrastructures to function, system robustness is an essential requirement for digital technologies. 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 cybersecurity a *club good*. This is a good that is not exhausted by its use (non-rivalrous), but whose access is regulated by its cost. The escalation of cyber threats indicates that this approach is ineffective, if not problematic.

Market dynamics fosters a non-collaborative approach and cost lead to uneven distribution. The robustness of digital end-point devices will have an impact on their costs, to the extent that, producers may sacrifice robustness to retain commercial competitiveness. This is often the case, for example, with IoT technologies, which risks favouring a pervasive distribution, on a global scale, of weak devices whose security is ephemeral. In 2018, a Symantec study reported an average of 5200 attacks per month on IoT devices. As IoT starts to become pervasive in private and public environments, its security vulnerabilities pose severe security and safety threats. The question then is how do we develop and regulate the design of robust systems in an effective way?

Clearly, engineering robust systems has direct and indirect externalities on the public interest of information societies. For it enables critical national infrastructures and services to work, allows citizens to perform their daily routines, and at time favours socially good outcomes of digital technologies. For these reasons, cybersecurity 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.

Make Cybersecurity a Public Good

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. The point can be clarified with two analogies. Streetlights are a notorious public good, so is national defence, both come at some cost. Nonetheless, all citizens of a state access them independently on these costs, and contribute through their taxes to maintaining them. In the same way, 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, this may include, for example, costs related to the establishing of standards and certification procedures, as well as cost associated to testing technologies.

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

Systemic approach. The management of a public good requires considering direct and indirect externalities, as well as medium and long-term consequences. This favours approaches to cybersecurity that focus on interdependences among 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 that system robustness is used to meet public interest. It is up to the public sector to set up standards, certification and testing procedures, able to ensure that sufficient level of security is maintained to protect and foster the public interest. At the same time, the private sector bears the responsibility to design robust systems, develop and improve new cybersecurity methods for the services and product that they offer, and collaborate 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 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 have a snowball effect on zero-day and exploits market. In turn, this could contribute to slow cyber arm-race and weaponisation dynamics of cyberspace.

However, framing cybersecurity as a public good without a careful distinction of between practices, scopes, and actors is conceptually problematic and misleading when focusing on the governance of cybersecurity. Cybersecurity encompasses a wide set of domains, from risk assessment and penetration tests, disaster recovery, and cryptography, and access control, architecture, software, and network security, to security operations, and physical security. Is cybersecurity public good in all these cases?

Consider the following cases. An Israeli company, Unbotify, 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). A handful of private companies offer more offensive options to threat response, usually for government customers, although with some commercial availability. On the more benign end of the spectrum, autonomous and semi-autonomous cybersecurity systems may be given a "playbook" of pre-determined responses to an activity, constraining the agent to known actions ('DarkLight Offers First of Its Kind Artificial Intelligence to Enhance Cybersecurity Defenses' 2017). Due to national legal boundaries around compromising computer systems, commercial clients may only have the option to investigate, isolate and disable malware, viruses, and botnets, without the ability to force access or disable an adversary's network. Autonomous systems also have the ability to learn adversarial behaviour and generate decoys and honeypots, thus actively luring threat actors ('Acalvio Autonomous Deception' 2019). AI for software testing is a new area of research and development. It is defined as 'emerging field aimed at the development of AI systems to

test software, methods to test AI systems, and ultimately designing software that is capable of self-testing and self-healing".[1] AI can help with verification and validation of software, liberating human experts from tedious jobs, and offering a faster and more accurate testing of a given system. In this sense, AI can take software testing to a new level, making systems more robust.

References

'Acalvio Autonomous Deception'. 2019. Acalvio. 2019. https://www.acalvio.com/.

Cowls, Josh, Thomas C. King, Mariarosaria Taddeo, and Luciano Floridi. Forthcoming. 'How to Design AI for Social Good: Seven Essential Factors'.

'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, Luciano. 2016. 'Mature Information Societies—a Matter of Expectations'. *Philosophy & Technology* 29 (1): 1–4. https://doi.org/10.1007/s13347-016-0214-6.

Floridi, Luciano, and Mariarosaria Taddeo. 2016. 'What Is Data Ethics?' *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083): 20160360. https://doi.org/10.1098/rsta.2016.0360.

Taddeo, Mariarosaria. 2010. 'Trust in Technology: A Distinctive and a Problematic Relation'. *Knowledge, Technology & Policy* 23 (3–4): 283–86. https://doi.org/10.1007/s12130-010-9113-9.

———. 2017. 'Trusting Digital Technologies Correctly'. *Minds and Machines* 27 (4): 565–68. https://doi.org/10.1007/s11023-017-9450-5.

———. 2019. 'Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity'. *Minds and Machines* 29 (2): 187–91. https://doi.org/10.1007/s11023-019-09504-8.

Taddeo, Mariarosaria, and Luciano Floridi. 2018a. 'Regulate Artificial Intelligence to Avert Cyber Arms Race'. *Nature* 556 (7701): 296–98. https://doi.org/10.1038/d41586-018-04602-6.

———. 2018b. 'How AI Can Be a Force for Good': *Science* 361 (6404): 751–52. https://doi.org/10.1126/science.aat5991.

Unbotify. 2019. 'Unbotify Home'. Unbotify | Behavioral Biometric Bot Detection. 2019. http://www.unbotify.com/.

[1] www.aitesting.org