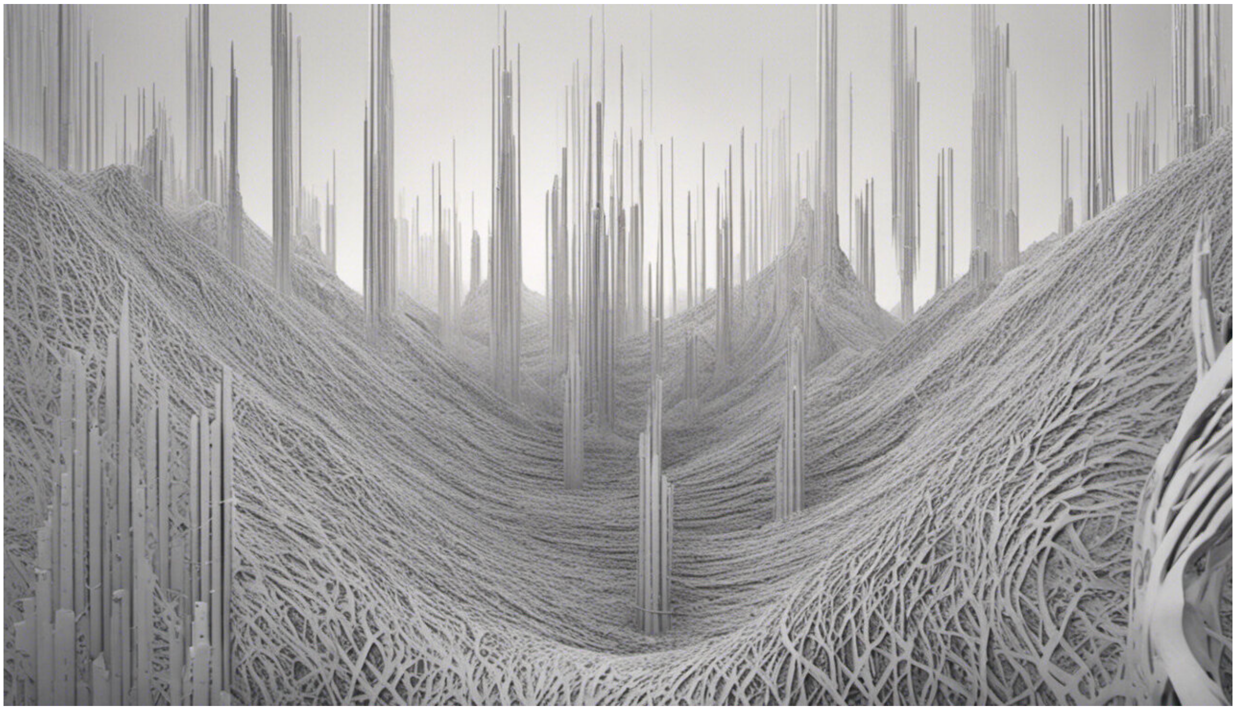
Why we need philosophy and ethics of cyber warfare

June 16 2022, by Mariarosaria Taddeo



Credit: AI-generated image (disclaimer)

Cyber-attacks are rarely out of the headlines. We know state actors, terrorists, and criminals can leverage cyber-means to target the digital infrastructures of our societies. We have also learned that, insofar as our societies grow dependent on digital technologies, they become more vulnerable to cyber-attacks.

There is no shortage of examples, ranging from the 2007 attacks against Estonia digital services and 2008 cyber-attack against a nuclear power plant in Georgia to WannaCry and NotPetya, two ransomware attacks that encrypted data and demanded ransom payments, and the ransomware cyber-attack on the US Colonial Pipeline, a U.S. oil pipeline system that provides fuel to South-eastern States.

When analyzing cyber-attacks' ethical and legal implications, it is crucial to distinguish the actors involved, since the permissibility of certain actions depends also on the actors involved.

My work focuses mostly on state vs state cyber-attacks. One of the most recent examples of this type of attack were those launched against Ukraine's military forces and attributed to the UNC1151, a Belarus military unit, ahead of the Russian invasion of Ukraine.

Observers looked at the Russian invasion and expected cyber to be a key element. Many feared a "cyber-Pearl Harbor," i.e., a massive cyber-attack which would have disproportionate destructive outcome and would lead to an escalation of the conflict.

Thus far, the invasion of Ukraine has proved highly destructive and disproportionate, but cyber has played little, if no role at all, in the delivery of these outcomes. Does this mean a cyber-Pearl Harbor will never happen? More importantly, does this mean cyber-attacks are a secondary capability in war, and we can continue to leave their use under-regulated?

The short answer to both questions is no, but there are nuances. So far, cyber-attacks have not been used to cause massive destruction; a cyber-Pearl Harbor, as some commentators argued in early 2000. The lack of the cyber element in Ukraine is not a surprise, given how violent and destructive the Russian invasion has been. Cyber-attacks are disruptive more than destructive. They are not worth launching when actors are aiming at massive kinetic damage. Such destruction is achieved more effectively with conventional means.

However, cyber-attacks are neither victimless nor harmless and can lead to unwanted, disproportionate damage which can have serious negative consequences for individuals and for our societies at large. For this reason, we need adequate regulations to inform state use of these attacks.

For many years, the international debate on this topic has been led by a myopic approach. The rationale was to regulate interstate cyber-attacks insofar as they have similar outcomes to an armed (conventional) attack. As a result, the majority of inter-state cyber-attacks has been left unregulated.

This is the failure of what I dubbed the "analogy-approach" to the regulation of cyber warfare, which aims to regulate such warfare only to the extent it resembles kinetic warfare, i.e. if it leads to destruction, bloodshed, and casualties. In effect, it fails to capture the novelty of cyber-attack, which is disruptive more than destructive, and the severity of the threats that they pose to a digital society. Underpinning this approach is the failure to recognize the ethical, cultural, economic, infrastructural value digital assets have for our—digital—societies.

It is reassuring that, after the 2017 failure, in 2021, the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security group could agree that interstate cyber-attacks should be regulated in agreement with the principles of International Humanitarian Law (IHL).

Although this in the right direction, it is only a first, and overdue, step. Indeed, the principles of IHL, and the ethical principles of Just War Theory, are still valid when considering cyberwarfare. We need interstate cyber-attacks to be proportionate, necessary, and to distinguish combatants from non-combatants. However, the implementation of such principles is problematic in the context of cyber—for example, we lack a clear threshold for proportionate and disproportionate attacks, and criteria to assess damage to immaterial assets. We also lack rules to consider issues related to sovereignty and due diligence.

Philosophical and ethical analyses are needed to overcome this gap and understand the nature of a warfare which decouples aggression from violence, which targets non-physical objects and yet can cripple our societies. At the same time, we need to make sure that, as more defense institutions see digital technologies as a decisive asset to maintain superiority against the opponents, they invest in, develop and use these capabilities in line with the values underpinning democratic societies and to maintain international stability.

As digital technology continues to be integrated in the defense capabilities, see for example artificial intelligence (AI), more conceptual and ethical questions emerge concerning their governance. To this end, it is important that defense institutions identify and address the ethical risks and opportunities that these technologies bring about and work to mitigate the former and leverage the latter.

Yesterday, the Ministry of Defense in the U.K. issued a policy paper: Ambitious, safe, responsible: our response to the delivery of AI-enabled capability in Defense, containing an appendix giving Ethical Principles for use of AI in defense. It is a step in the right direction. The principles are broad, and more work needs to be done to implement them in specific defense contexts. However, they set an important milestone, as they show the commitment of the MoD to focus on the ethical implications of using AI and to address them coherently with the values of democratic societies.

These principles arrive two years after those published by the U.S. Defense Innovation Board. Between the two sets of principles, there is some converges which may hint at the emergence of a shared view among allies as to how use AI, and, more broadly, digital capabilities for defense. My hope is that these principles may be the seeds to develop a shared framework for the ethical governance of the use of digital technologies for defense purposes.

More information: Floridi, L., & Taddeo, M. (Eds.), The ethics of information warfare. (2014). Springer publications

Mariarosaria Taddeo, Just Information Warfare, *Topoi* (2014). DOI: 10.1007/s11245-014-9245-8

Mariarosaria Taddeo et al, Regulate artificial intelligence to avert cyber arms race, *Nature* (2018). DOI: 10.1038/d41586-018-04602-6

Mariarosaria Taddeo et al, Ethical Principles for Artificial Intelligence in National Defence, *Philosophy & Technology* (2021). DOI: 10.1007/s13347-021-00482-3

Provided by University of Oxford

Citation: Why we need philosophy and ethics of cyber warfare (2022, June 16) retrieved 25 April 2024 from https://techxplore.com/news/2022-06-philosophy-ethics-cyber-warfare.html