Minds & Machines
DOI 10.1007/s11023-017-9436-3

Cyber Conflicts and Political Power in Information Societies

Mariarosaria Taddeo[1,2]

Received: 17 May 2017 / Accepted: 18 May 2017

When asked what his goal was for the 1815 Waterloo Campaign, the Duke of Wellington answered "Why, to beat the French" (Gray 1984, 9).[1] By French he meant Napoleon, and by beating him he meant defeating him for good, so that Napoleon could not pose a threat to European states any longer. A conflict was the most effective means to achieve this goal. Fast-forward 200 years, now is China versus USA, the domain is cyberspace where China has been launching attacks against the USA for at least 4 years to acquire relevant information from USA companies and governmental offices. The USA would like to stop the cyber-attacks, to do so they do not engage in a cyber conflict and choose a political strategy: the American and Chinese presidents meet and define bilateral agreements to stop state-run cyber-attacks between their two countries. This conflict was not won by either of the two actors, but solved by both of them.

The Waterloo example highlights that there is a relation between political power and conflict waging (Freedman 1998). Historically, the capability of a state actor to win a conflict has often been equated with its ability to gain or maintain political power. This equation can be read minimally—the capability to win a conflict is a necessary condition to gain or maintain power—or maximally—the capability to win a conflict is a sufficient condition to gain or maintain power. When considering cyber conflicts and the dynamics of cyberspace, this equation, even the minimalist reading, no longer holds true. There is, indeed, a strong relation between cyber conflicts and political power, but it is different from the one linking kinetic conflicts and political power.

[1] Quoted in (Lonsdale 2017).

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

[1] Digital Ethics Lab, Oxford Internet Institute, University of Oxford, Oxford, UK

[2] Alan Turing Institute, London, UK

Published online: 23 May 2017

In cyberspace, a powerful political actor is the one able to *resolve*, more than win, conflicts, as the China versus USA example indicates. This is because of the nature of cyber conflicts and the power dynamics of the information age. Let us focus on the former first. Had he been preparing a cyber conflict, the Duke of Wellington may have given a different answer, as one may defend against a cyber opponent, or even dismount its attack, but very rarely it is possible to beat a cyber opponent in the way Napoleon was beaten at Waterloo. For one thing, the opponent may remain unknown. And even when attribution is not a problem, winning a cyber conflict may not mean crippling the opponent resources to make sure that it would not come back again. Paradoxically, when successful, the defending side of a cyber-attack may reveal too much about its cyber capabilities and skills. In doing so, it may expose itself to new, subsequent attacks.

Cyber conflicts are not won in the same way in which kinetic conflicts are. Victories in cyber conflicts are tactic. They are about blocking *this* attack or *that* threat, more than achieving long-term, strategic goals.[2] For this reason winning a cyber conflict does not gain political power to the winner, nor does losing a cyber conflict really compromises the authority of an already powerful actor in cyberspace.

This is not tantamount to saying that cyber conflicts do not pose any threat, quite the contrary. Indeed, cyber conflicts pose serious risks of escalation (Taddeo 2016), which may undermine national security and jeopardize international stability. These risks have been clearly stressed, for example, by NATO (Freedberg 2014), the UN Institute for Disarmament Research (UN Institute for Disarmament Research 2014), the UK Government (2014), and the US State Department (International Security Advisory Board 2014).

Escalation is already happening. In 2016, cyber-attacks increased from 480 million to 1.6 billion,[3] indicating a massive increasing of their frequency. It is reasonable to expect these numbers to continue to grow given the progressive weaponization and militarisation of cyberspace, as well as the reliance on malware for state-run cyber operations (like Titan Rain, Red October, and Stuxnet). It is not just about the frequency of cyber conflicts. The recent WannaCry[4] cyber-attack, the Mirai botnet DDOS attach,[5] the 2016 Russian cyber-attack against Ukraine power plant,[6] and the Russian infiltration in US Federal Offices[7] show that cyber conflicts have intensified their impact, as they now target and (can) cripple key infrastructures of our societies.

[2] This resonates with other fundamental differences between cyber and kinetic conflicts, which range from the domain in which they are waged; the nature of the involved actors and targets; and their level of violence. These differences are redefining our understanding of key concepts such as harm, violence, target, combatants, weapons, and attack, and pose serious challenges to any attempt to regulate conflicts in cyberspace (Dipert 2010; Floridi and Taddeo 2014; Taddeo 2012, 2014a, b).

[3] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/.

[4] https://en.wikipedia.org/wiki/WannaCry_cyber_attack.

[5] https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

[6] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[7] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

Escalation is, therefore, the main challenge for political actors, and in particular for state actors as supreme providers of national and international security. Ultimately, to meet this challenge, coercive (military and non-military) means, technical solution, alongside to diplomatic inducements need to be put in place to resolve the underlying frictions and define new equilibriums that can guarantee international stability and avert the risks of more dramatic conflicts (Taddeo 2014a). Powerful political actors in information societies will be those able to define such strategies and to impose them to the other actors in the international arena. As Weber put it, power is "the ability of an individual or group to achieve their own goals or aims when others are trying to prevent them from realising them" (Weber 1947, 152). Strategies to avert cyber conflicts and develop a stable cyberspace are one of the key goals for political actors in mature information societies (Freedberg 2014; UN Institute for Disarmament Research 2014; International Security Advisory Board 2014; UK Government 2014; Floridi 2016; Taddeo 2016).

The shift from winning to resolving conflicts as a sign of political power is consistent with the power dynamics of our societies. In pre-information societies, political power was *transferred* from A to B, and conflicts often facilitated this transfer, as in the case of the Waterloo Campaign. This is not the case in information age. Power is now *diffused*, and not transferred, among state and non-state actors (Nye 2004, 2010). On the one hand, the diffusion of power contributes to the erosion of the Westphalian model of nation-state, as Eriksson and Giacomiello note:

> Though a single transnational actor is seldom able to challenge the political, military, or economic power of a state, the increasingly complex and globally penetrating web of transnational relations perforates sovereign states (Eriksson and Giacomello 2006, 230).

On the other hand, the diffusion of power does not mean that state and non-state actors enjoy the same type, or even amount, of power; nor does this mean that state actors have become powerless or irrelevant in the national or international arena. States are still the most powerful actors, but they share the international arena with an increasing number of non-state actors, as Nye suggests:

> States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control (Nye 2010, 1).

In this context, cyber conflicts will continue to be waged, because, if kept below the kinetic threshold, they cost little in terms of resources and risks to the attackers, while having high chances to be successful and achieve tactic goals. For this reason, the ability to *win* a cyber conflict speaks very little of the political power of both the defended and attacker. It is the ability to shape the international arena by creating a political agenda, *super partes* institutions, and treaties that would make engaging in cyber conflicts more hazardous in political, economic, and strategic terms that will distinguish powerful political actors from the other actors in information societies.

Acknowledgements I am grateful to Professor Luciano Floridi and Professor Massimo Durante for our insightful discussions on the topic of this letter and to Dr Jennifer Doubt for her comments on an early draft.

References

Dipert, R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics, 9*(4), 384–410.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review, 27*(3), 221–244. doi:10.1177/0192512106064462.

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

Floridi, L., & Taddeo, M. (Eds.). (2014). *The ethics of information warfare*. New York: Springer.

Freedberg, S. (2014). NATO hews to strategic ambiguity on cyber deterrence. http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.

Freedman, L. (1998). Military power and political influence. *International Affairs, 74*(4), 763–780. doi:10.1111/1468-2346.00044.

Gray, C. S. (1984). War-fighting for deterrence. *Journal of Strategic Studies, 7*(1), 5–28. doi:10.1080/01402398408437174.

International Security Advisory Board. (2014). *A framework for international cyber stability*. United States Department of State. http://goo.gl/azdM0B.

Lonsdale, D. J. (2017). Warfighting for cyber deterrence: A strategic and moral imperative. *Philosophy & Technology*. doi:10.1007/s13347-017-0252-8.

Nye, J. S. (2004). *Soft power: The means to success in world politics* (1st ed.). New York: Public Affairs.

Nye, J. (2010). *Cyber power*. Boston, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs. http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy and Technology, 25*(1), 105–120.

Taddeo, M. (2014a). Just information warfare. *Topoi*. doi:10.1007/s11245-014-9245-8.

Taddeo, M. (2014b). The struggle between liberties and authorities in the information age. *Science and Engineering Ethics*. doi: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. doi:10.1007/s11023-016-9408-z.

UK Government. (2014). Deterrence in the twenty-first century: Government response to the committee's eleventh report. http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/525/52504.htm.

UN Institute for Disarmament Research. (2014). Cyber stability seminar 2014: Preventing cyber conflict. http://link.law.upenn.edu/portal/UNIDIR-cyber-stability-seminar-2014–preventing/FegECNo01q0/.

Weber, M. (1947). In A. M. Henderson, & T. Parsons (Eds.), *The theory of social and economic organization*. New York: Oxford University Press.