Editor: Virgilio A.F. Almeida • virgilio@dcc.ufmg.br

Cyberwarfare and Digital Governance

Virgilio A.F. Almeida • *Harvard University*

Danilo Doneda • *Rio de Janeiro State University*

Jacqueline de Souza Abreu • *University of São Paulo and InternetLab*

Dyn suffered multiple complex DDoS attacks in October 2016, constituting one of the largest cyberattacks of this nature ever documented. With this and other recent events in mind, the authors discuss conceptual and practical challenges around cyberwarfare and its impact on cyberspace governance.

Researchers have enunciated the capability to use cyberattacks to disrupt critical infrastructure sectors — including power, water, transportation, and communication systems — for years.[1] When these attacks take place, effects are felt not only in cyberspace, but also in the physical world, making them especially threatening.

A recent development revived these alerts. On 21 October 2016, the DNS provider Dyn suffered multiple and complex DDoS attacks, executed through the so-called Mirai botnet, making a wide-ranging variety of popular websites — such as Twitter and *The New York Times* — unavailable in extensive areas of the United States for about five hours. Experts consider this to have been one of the largest cyberattacks of this nature ever documented.

An ongoing investigation tries to unravel the mystery around the attacks' origin — most significantly to find out whether a nation-state mounted or participated in the attack. So far what's confirmed is that the botnet exploited vulnerabilities in thousands of Internet of Things (IoT) devices, which were converted into real cyber weapons that overloaded Dyn with traffic. Such attacks risk becoming even more frequent, as the future points to billions of devices connected to the Internet and to an increased "cyber dependence" — a state's economic, military, and governmental reliance on cyberspace.[2,3]

Many aspects of the Dyn attack can be mapped onto Internet governance issues, such as the role of intermediaries (including DNS providers), the participation of the government and private sector (for example, telco operators, content distribution networks, and government security agencies), and international relations (such as IoT equipment manufactured by different countries).

Thus, here we discuss the conceptual and practical challenges around cyberwarfare and its impact on cyberspace governance, as exposed by the Dyn incident and other recent events.

Cyberwarfare: Definitions and Categories

Malicious pieces of code (viruses, trojans, rootkits, worms, bots, and spyware) and weaponized zero days can be deployed not only to perpetrate common cybercrime but also to engage in cyberwarfare. Identity theft, online scams and fraud, and theft of intellectual property or classified information usually fall under the first category — that of "common cybercrimes." Other cyber activities, depending on their scale, effects, originators, and targets, are sometimes characterized as a "cyber act of war." The truth is, however, that there's no litmus test for the distinction between the two groups of malicious activities.

The problem rests largely in the lack of a consensus regarding what constitutes "cyberwarfare," which affects the legal treatment of cyber operations. For example, Richard Clarke and Robert Knake deem cyberwarfare as "actions by

 Published by the IEEE Computer Society 1089-7801/17/$33.00 © 2017 IEEE

a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[4] According to this definition, cyberwarfare necessarily involves two nation-states, one as a source, the other as target.

As such, these requirements can be rather restrictive, when it's not clear who the sources or targets of a cyber operation are — for instance, despite the speculations pointing to US and Israeli governments,[5] Stuxnet, a computer worm developed to sabotage Iran's nuclear facilities, remains an unattributed cyberattack. Accordingly, while the malware has been publicly taken as an act of cyberwarfare, it wouldn't fulfill the elements of the proposed definition. The case for the Dyn DDoS attacks is similar: so long as it isn't certain whether nation-states such as Russia or China were behind the attacks, they can't be brought to the realm of cyberwarfare and treated as acts of war, and thus it remains a common crime against Dyn. As a result, a cyber operation can end up being (sometimes inappropriately) addressed by criminal law as a "cybercrime" — or by war and international humanitarian law as an "act of war."

Given this and other definitional challenges, Daniel Hughes and Andrew Colarik put forth a treatment of the topic that focuses on critical features. These could be summarized in three points:

> *First, cyberwarfare involves actions that achieve political or military effect. Second, it involves the use of cyberspace to deliver direct or cascading kinetic effects that have comparable results to traditional military capabilities. Third, it creates results that either cause or are a crucial component of a serious threat to a nation's security or that are conducted in response to such a threat.*[2]

This open definition takes into consideration a central characteristic of cyberspace conflicts: the participation of state actors and non-state actors (for example, companies, hackers, individuals, and groups) on both sides of a conflict (that is, the offensive and defensive sides).

The Legal Treatment of Cyberwarfare

The time authors have on trying to define what cyberwarfare stands for isn't at all an academic or abstract problem, as it's also a reflection of the mutable — and often not easily envisioned — nature of forces and interests behind a cyberattack. While the fundamental importance of the characterization is clear, international law applied to warfare still hasn't (at least literally) directly solved this conceptual problem in treaties and conventions; but neither has it directly approached its peculiarities. At the same time, at least since the series of cyberattacks perpetrated against Estonia in 2007, the need to integrate the issue into classical international warfare rules has become evident and urgent.[6]

This approach to the integration of cyberwarfare matters in international law is due both to a yet-incipient definition of what cyberwarfare stands for as well as to the fact that traditional principles of international law on war can be worked out to fit and encompass cyberwarfare situations. As such, some of the main war-related fields that international law covers, such as the so-called *jus ad bellum* (in short, the considerations a nation "should" make before entering a war in order for it be deemed "just") or the *jus in bello* (which, to its turn, is the set of conducts that shall be deemed as "permitted" during wartime), are largely discussed in the context of cyberwarfare. In this sense and given the lack of direct sources of international law, the *Tallinn Manual* (*Tallinn Manual on the International Law Applicable to Cyber Warfare*), an academic book written by a group of scholars invited by the NATO Cooperative Cyber Defence Centre of Excellence, is a well-regarded reference on how international law can apply to existing cyberwarfare.[7] Illustratively of the persisting conceptual challenges around cyberwarfare, the *Tallin Manual* understands cyberwarfare as cyber operations that implicate the use of force, which brings up another disputed legal concept to the table and raises the discussion of what consists as use of force in cyberspace. On its turn, international humanitarian law has also recognized the threat posed by cyberwarfare — even if not by proposing direct changes to international humanitarian law statutes, by considering the application of existing ones to cyberwarfare situations.[8]

Cyberwar and Internet Governance

Episodes associated with the 2016 presidential election in the United States demonstrate that offensive operations based in cyberspace are expanding. They also show that the concepts of cyberattacks and cyberwar are changing. According to a recent article by David Sanger,[3] the attempt of a foreign power to disrupt the 2016 presidential election is a clear sign of cyberespionage and information-warfare actions, that have been viewed by some analysts as an act of war.[9] As a consequence, questions about cyberspace conflicts arise in different sectors of society, such as: How can a country defend its interests in cyberspace? How can Internet governance bodies participate in global efforts to minimize cyber conflicts?

Cyber initiatives to protect from attacks and hostile actions can be grouped into a few broad categories[10]: cyberdefense, cyberdeterrence, cyberpreemption, and cyber arms control. The implementation of these initiatives faces many challenges. Cyberdeterrence aims at dissuading adversaries. However, because of the

difficulties in attributing the source of a cyberattack and due to the many possible actors involved in the attack, cyberdeterrence hasn't been considered an effective strategy yet. Cyberpreemption refers to acts to reduce the capability of the potential forces of an adversary. As proposed in a recent *New York Times* editorial, the best way to reduce cyber risks is "to accelerate international efforts to negotiate limits on the cyberarms race, akin to the arms-control treaties of the Cold War."[11] Cyberspace governance bodies can play a role in constructing an international framework that minimizes global cyber threats.

The Role of National Cyberspace Governance Bodies

In his efforts to characterize cyberspace,[12] David Clark views cyberspace's architecture in four layers. From top to bottom the layers are as follows: first, the people who participate in cyberspace; second, the information that's stored, transmitted, and transformed in cyberspace; third, the logical building blocks that make up services and platforms; and fourth, the physical layer that supports the logical layer, such as devices and communication networks.

In all layers, society, government, and the private sector participate in different roles and levels of intensity. National governance bodies, composed of different stakeholders, can practically contribute to cyberdefense in the following ways:

- *Including cyberwarfare as a topic of the governance agenda.* The inclusion can contribute to increased awareness of the society and government about cyber threats and conflicts. It also can show the potential of considerable damage that can be caused by cyberwarfare.
- *Improving communication among state and non state actors.* Initiatives in this sense can be fruitful, such as fostering fora and councils where the most diversified and relevant actors in cyberwarfare and cybersecurity can gather together. Effective communication between government agencies and citizens is needed to increase awareness of the potential dangers, including the risk that information warfare can influence public opinion.
- *Promoting the discussion of cybernorms, that refer to shared expectations of appropriate behavior in cyberspace.* The G-20 endorsement of a prohibition on cyberespionage for commercial purposes is an example of a cybernorm.[13] Joseph Nye has discussed the challenges for adopting norms for cyberspace,[14] showing that breadth — that is, the number of state and nonstate actors that accept norms for warfare — is still low. Internet governance bodies can play a relevant role in the process through which new cybernorms can be developed and proposed for global cybersecurity and cyberwarfare.
- *Proposing cyber hygiene initiatives to protect against cyber threats.* Some cyberattacks against US targets — including political groups, government agencies, and news organizations — were perpetrated using simple methods, such as spear phishing schemes. Cyber hygiene initiatives aim at using cybersecurity best practices to appropriately protect and maintain systems and devices connected to the Internet.

National multistakeholder models for cyberspace governance can contribute to building bridges between the military, the intelligence community, and society to minimize the risks of cyber conflict, warfare, and information war. Governance models that include representatives from civil society organizations, business, technology, and academia might help to increase awareness about cyber threats and about prevention, detection, and response to cyber incidents. It isn't an easy undertaking to have representatives of the civil society participating in national security initiatives. But considering the transformative nature of cyberspace, it's worth trying.

Cyberwarfare isn't only about the public fears that have been discussed for years, such as attacks to electrical grids, transportation systems, or airline and financial networks. It's also a conflict over information that can create social and material disruption. Cyberspace conflicts may take different forms in the future and can even reach a certain threshold of confrontation that would characterize a full war.

In this scenario, conceptual ambiguities that now surround national and international law applicable to cyberwarfare bring uncertainty to the legal treatment of cyberattacks and, therefore, call for close attention. At the same time, there's an important role to be played by national cyberspace governance bodies leveraging on their longstanding experience in cybersecurity issues and strengthening the cooperation between multiple stakeholders.

References

1. R. Knake, "Internet Governance in an Age of Cyber Insecurity," special report no. 56, Council on Foreign Relations, Sept. 2010, p. 10; www.cfr.org/internet-policy/internet-governance-age-cyber-insecurity/p22832.
2. D. Hughes and A. Colarik, "Predicting the Proliferation of Cyber Weapons in Small States," *Joint Force Quarterly*, vol. 83, 4th quarter, 2016, pp. 19–26.
3. D.E. Sanger, "Under the Din of the Presidential Race Lies a Once and Future Threat: Cyberwarfare," *The New York Times*, 6 Nov. 2016; www.nytimes.com/2016/11/07/us/

politics/under-the-din-of-the-presidential-race-lies-a-once-and-future-threat-cyber-warfare.html?_r=0.
4. R. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, Ecco, 2010, p. 6.
5. M.J. Gross, "A Declaration of Cyber-War," *Vanity Fair*, Apr. 2011; www.vanityfair.com/news/2011/03/stuxnet-201104.
6. M.N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Rev.*, vol. 25, pp. 269–300; https://journals.law.stanford.edu/sites/default/files/stanford-law-policy-review/print/2014/06/schmitt_25_stan._l._poly_rev._269_final.pdf.
7. M.N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge Univ. Press, 2013; www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.
8. N. Melzer, "Cyberwarfare and International Law," *UNIDIR Resources*, 2011; http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
9. A. Zegart, "Vladimir Putin Is Trying to Hack the Election. What Should US Do?" *CNN.com*, 24 Oct. 2016; www.cnn.com/2016/10/23/opinions/elections-hacks-russia-warning-zegart/.
10. *Cybersecurity Dilemmas: Technology, Policy, and Incentives – Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.–U.K. Scientific Forum*, tech. report, Nat'l Academies Press, 2015; doi:10.17226/21833.
11. The Editorial Board, "Arms Control for a Cyberage," *The New York Times*, 26 Feb. 2015; www.nytimes.com/2015/02/26/opinion/arms-control-for-a-cyberage.html.
12. D. Clark, "Characterizing Cyberspace: Past, Present, and Future," working paper, Explorations in Cyber Int'l Relations (ECIR), Mar. 2010; http://ecir.mit.edu/index.php/research/working-papers/112-characterizing-cyberspace-past-present-and-future.
13. M. Finnemore and D. Hollis, "Constructing Norms for Global Cybersecurity," *110 Am. J. Int'l Law*, 2016, to be published; https://ssrn.com/abstract=2843913.
14. J.S. Nye, The Regime Complex for Managing Global Cyber Activities, paper series no. 1, Global Commission on Internet Governance, Nov. 2014; www.belfercenter.org/sites/default/files/legacy/files/global-cyber-final-web.pdf.

Virgilio A.F. Almeida is a professor in the Computer Science Department at the Federal University of Minas Gerais (UFMG), Brazil, and currently a visiting professor at Harvard University and a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University. His research interests include large-scale distributed systems, the Internet, social computing, and cyber policies. Almeida has a PhD in computer science from Vanderbilt University. Contact him at virgilio@dcc.ufmg.br or valmeida@cyber.law.harvard.edu.

Danilo Doneda is a professor of civil law at the Law School of the Rio de Janeiro State University (UERJ). His research interests include private law and regulation, privacy, and data protection. Doneda has a PhD in civil law from UERJ. Contact him at danilo@doneda.net.

Jacqueline de Souza Abreu is a PhD student at the University of São Paulo and researcher at InternetLab, Brazil. Her research interests include privacy law, cyber law and policy, constitutional law, and legal theory. Abreu has LLM degrees from the University of Munich and from the University of California at Berkeley. Contact her at jacqueline.abreu@usp.br.