doi:10.1017/aju.2017.7

SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

BEYOND BUNKER AND VACCINE: THE DNC HACK AS A CONFLICT OF LAWS ISSUE

Fleur Johns and Annelise Riles*[†]

Who was responsible for the cyberincursions upon the Democratic National Committee (DNC) that took place during the U.S. presidential campaign? Russia's "senior most officials"?[1] A "a tattooed 26-year-old" running a server rental company in western Siberia?[2] U.S. political party leaders and other insiders disinclined to implement "best in class" cybersecurity measures?[3] Or does responsibility lie elsewhere?

And what should we make of these events? What might we learn, from the recent spate of cyberincidents with murky geopolitical overtones, about international order—legal and otherwise? What degree and kind of "security" might one expect to see wrapped around "cyber" on the global plane?

The hacking of the DNC presents a fascinating case for public international law (PIL). It is one that fits awkwardly, if at all, into the rubric of interstate conflict with which PIL has long grappled. Although the Obama administration formally accused Russia of orchestrating the attack,[4] and took retaliatory steps accordingly,[5] it acknowledged too that the attack involved "a variety of actors, both state and criminal."[6] Even the boundaries of the event itself remain murky: "Americans cannot know for certain that the hacking has ended."[7] Most of all, the attack suggested new prospects for weaponizing information on the global plane, albeit with roots in conventional warfare and with parallels to certain corporate competition and domestic political strategies.

In trying to understand what to make of the DNC hack, we propose that the dominant ways of thinking about cybersecurity, which partly derive from the law and tactics of war, might benefit from an overlay of a different conceptual framework, that of private international law (or conflict of laws). In thinking and acting in this context, we argue, conflict of laws offers an approach that holds considerable promise. In order to understand the value of a private international law approach we need to get some perspective on the dominant frameworks currently used to think about cybersecurity. Thinking around cybersecurity tends to proceed along one of two metaphoric routes, or via combinations of the two. One is the metaphor of the bunker. A second is the metaphor of the vaccine. Each of these serves certain purposes, but also has certain weaknesses.

* *Professor of Law and Associate Dean of Research at UNSW Sydney.*

[†] *Jack G. Clarke Professor of Far East Legal Studies, Cornell University.*

[1] David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. Times (Oct. 7, 2016).

[2] Andrew E. Kramer, *A Voice Cuts Through, and Adds to, the Intrigue of Russia's Cyberattacks*, N.Y. Times (Sept. 27, 2016).

[3] Nolan D. McCaskill, *DNC creates cybersecurity advisory board following hack*, Politico (Nov. 8, 2016, 5:29 PM).

[4] Sanger & Savage, *supra* note 1.

[5] David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. Times (Dec. 29, 2016).

[6] *White House will not comment on Democratic email hack probe*, Reuters (July 25, 2016, 1:39 PM).

[7] *Warning Russia on Hacking Isn't Enough*, N.Y. Times (Nov. 24, 2016).

In the Bunker

For some, the theft and leaking of DNC data was a quasi-military intervention against which the United States had to defend itself.[8] Those responsible "should be punished," insisted U.S. Senator Lindsey Graham.[9] The Obama administration publicly took a range of retaliatory responses.[10] The administration rallied allies, briefed NATO members, and sought multilateral consensus according to a standard playbook of response to military interventions.

These responses reflect what we will call the bunker mentality concerning cybersecurity—an approach that aims to create something analogous to a military dug-out or reinforced shelter to protect against attacks. Cybersecurity specialists think of this in terms of "perimeter defense." However, the approach entails more than the maintenance of technical and physical perimeters. It also entails gathering defensive resources, infrastructure, and knowledge superior to those of adversaries to insulate the homeland, and pursuing those responsible through targeted incursions outside the defended territory.

The infrastructure used to build this metaphoric bunker will typically be both material and ideational. For instance, it will be as important to assemble treaty alliances and soft law standards as to maintain certain physical and technical infrastructure, as normative like-mindedness is an important component of the defensive buffer. Strategic resources for building the bunker also include forensic knowledge about past attacks and intelligence about potential future attacks. Also significant to this approach is the prospect of amassing some means of retaliation. Regardless of their actual effectiveness in deterring attacks, prosecution and retaliation help to create a sense that something is being done and that those inside the bunker are safer as a result.

Consider, as an example of this approach to cybersecurity, the emphasis placed in the U.S. Comprehensive National Cybersecurity Initiative on intrusion detection and prevention systems and bolstering the impenetrability of classified networks.[11] This initiative is aimed at "building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities … and developing appropriate responses."

Such an approach is familiar from other military settings, and comforting for that reason. It corresponds to classic debates in the law of war about attributing responsibility and proportionate response. Yet the assurance of success that it carries may be unwarranted. As Fred Schneider reminds us in this symposium, the cost of securing information infrastructure is very high, both monetarily and in terms of inconvenience.[12] As a result, those in charge of procurement do not always prefer "best in class" security. Moreover, supply chains are increasingly interconnected digitally, and errors in software code are more or less ubiquitous, making walling off any one technology environment all but impossible. More generally, the bunker approach encourages an inward turn in the society: it represents a fantasy that a society or territory can close itself off from problems outside, and a presumption that "we" can be separated conceptually, politically, technologically from "them." As such it encourages an escalation of hostilities in tit-for-tat cycles.

Adaptive Immunity

A more recent approach to cybersecurity—also in evidence after the DNC attack—relies more on the metaphor of the vaccine than that of a bunker. In this mode, cybersecurity is premised less on differentiation from those

[8] Duncan Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, Opinio Juris (July 25, 2016, 3:02 PM).

[9] Matthew Rozsa, *Republican are now interested in looking into the hack against the DNC*, Salon (Nov. 16, 2016, 8:38 PM).

[10] Sanger, *supra* note 5.

[11] Comprehensive National Cybersecurity Initiative, White House President Barack Obama.

[12] Fred B. Schneider, *A Computer Scientist Musing about the DNC Hack*, 110 AJIL Unbound 343 (2017).

https://doi.org/10.1017/aju.2017.7 Published online by Cambridge University Press

domains to which cyberthreats may be traced, and more on enlightened mimicry of those domains. Vaccination entails the introduction of agents resembling disease-causing pathogens to provoke the development of immunity. Vaccination represents an effort to act proactively, rather than reactively, amidst uncertainty. Cybersecurity in this mode is a process of continuous innovation and adaption—often with the support of white and gray hat hackers.[13]

A classic example of the vaccine approach was the U.S. Department of Defense's open invitation to individual hackers to "Hack the Pentagon" and share with the Department information about its security vulnerabilities.[14] Views of the Australian government voiced in UN consultations were similarly indicative of this approach; Australia cast cybersecurity as a "global opportunity" for public and private investment.[15] In that spirit, the Obama administration appointed executives from Uber, Mastercard, and Microsoft to its Commission on Enhancing National Cybersecurity.[16]

In this mode, entrepreneurship, improvisation, and agility are synonymous with safety, and indeed survival. Vulnerabilities are countless and unavoidable, but there is a patch for anything with enough tech wizardry in the room. Pursuit of cybersecurity therefore requires stepping outside the government-to-government framework characteristic of PIL, either by involving private actors or by adopting their methodologies.

There is much to be said for collaborative "technology leadership" as a response to cybersecurity threats.[17] The difficulty with such an approach, however, is that it is premised on resource profusion and more or less equal interest in cybersecurity. In other words, it disregards inequality and dissensus. Exposure to cybersecurity risk is not equally distributed. Relatively few nations—and relatively few people within those nations—have the means to deploy tech wizardry effectively to cybersecurity ends. When basic public infrastructure fails, it is the marginal, highly leveraged, and welfare-dependent who often suffer most, as when Bangladesh's Ministry of Social Welfare was hacked in 2013[18] and its Central Bank targeted in 2016.[19] Low cost technologies widely used in developing countries are often those most vulnerable to cyberthreat because security measures may be too costly or otherwise inaccessible. As Nir Kshetri has pointed out, instructions for many software security products are available in the English language only.[20]

Nevertheless, the appeal of the vaccine approach from a PIL perspective is clear. PIL has continually strived to reach beyond the nation-state to engage a wider range of actors and to enroll the unconvinced in its normative projects. Cybersecurity in the vaccine mode seems to serve this goal. The vaccine mode also resonates with PIL's recent embrace of so-called "new governance techniques" that emphasize experimentation and collaboration as alternatives to state sanctions. As deployed in international organizations from the European Union to the Financial Stability Board, new governance aims to regulate by changing citizens' behaviour, and even by co-opting the enemies of global harmonization. Like the vaccine modality, new governance is imagined to outstrip the old PIL governance because it is more participatory, and because it repurposes tricks from the private sector to pursue PIL goals. Like the vaccine, new governance emphasizes *learning*—through experimentation and review, the regulatory system aims to improve itself and collaboratively generate new and better ideas, in real time, from the ground up.

[13] Kim Zetter, *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?*, Wired (Apr. 13, 2016, 5:03 PM).

[14] *Hack the Pentagon*, Hacker One.

[15] UN Secretary-General, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/71/172 (July 19, 2016).

[16] Nick Statt, *Obama appoints execs from MasterCard, Uber, and Microsoft to cybersecurity panel*, The Verge (Apr. 13, 2016, 8:00 PM).

[17] Rajiv Gupta, *What the DNC Hack Says About the U.S. Government's Cybersecurity Strategy*, Fortune (July 28, 2016).

[18] Waqas Amir, *Bangladesh Ministry of Social Welfare website hacked by Abu Halil501*, Hack Read (June 27, 2013, 12:18 AM).

[19] Arafat Kabir, *After Hackers Steal $81 Million, What Now For Bangladesh Central Bank?*, Forbes (Mar. 16, 2016, 6:27 AM).

[20] Nir Kshetri, *Diffusion and Effects of Cyber-Crime in Developing Economies*, 31 Third World Q. 1057 (2010).

https://doi.org/10.1017/aju.2017.7 Published online by Cambridge University Press

Yet in recent years the limitations of these methods have become apparent and these are suggestive also of possible limits of cybersecurity in the vaccine mode. First, it turns out to be harder to co-opt one's enemies and enroll citizens in the agenda of international harmonization than was first imagined. Private parties maintain their own multiple and contradictory agendas, often producing stalemate and chaos. Second, new governance techniques often are far less successful in engaging the private sector than their designers hoped; those left outside may become distrustful and disillusioned.

Most importantly, the lesson for cybersecurity is that old methods die hard: although the aim of the vaccine is to overcome the bunker's limitations, vaccines often slide back into bunkers. Projects that begin with a commitment to supporting open borders, moral agnosticism, and experimentation often lapse into projects for building better ways of keeping the "bad guys" out. Likewise, practices adopted to encourage adaptation often become deployed as techniques for control, as "learning" slides into surveillance.

Beyond Bunker and Vaccine—Conflicts Technique

Private international law, or conflict of laws, is the body of law that governs transnational disputes between private parties. As its name suggests, it offers a way of taking cybersecurity out of the punitive registers of the law of war or criminal law, and turning it into an issue of the allocation of private rights and responsibilities across borders, without regard to moral fault. Its metaphoric register is one of a networked and morally diverse world in which the most local of issues can have contacts and implications in far flung places. In the conflicts sensibility, harmonization with a view to the kind of security pursued through the bunker and vaccine mentalities, is always something of a pipe dream; in the interstices all we have is technical *coordination*.

Private international law emphasizes horizontal relationships among private or hybrid parties rather than vertical relations of either cyberattack victims or perpetrators to particular nation-states. For example, in the DNC hacking, a private citizen, John Podesta, was personally targeted, allegedly to influence the U.S. election. In addition to the harm to the United States qua state, Podesta suffered harms to his personal reputation and interests. These harms, moreover, were caused by an individual or individuals hacking into his email account. They may have acted at state actors' direction, but they also acted in their capacity as private parties.

Private international law gives us a conceptual framework for meeting the harm where it occurs by starting with the private party that is harmed, as such, rather than seeing the private party as simply a stand-in for the state. Private international law permits the same in relation to perpetrators. It allows for the pursuit of different types of claims, and allegations of different types of responsibility, throughout complex networks of legal and natural persons.

At the same time, however, Podesta is no ordinary private party, and those responsible appear not to have been garden variety hackers. Podesta was targeted precisely because of the implications of his private activities for the security of the nation-state. And the nature of that hack suggests high level state involvement. This slippery boundary between private and public is precisely what makes cyberattacks so challenging from a PIL point of view. Yet this slipperiness may be easier to countenance from a private international law perspective. Private international law has a series of techniques for making sense of private subjects as always already constituted by their relationship to one or more nation-states. The doctrine of state or governmental interests—at the core of American conflicts doctrines—is one classic example. Private international law gives us a metaphor of a world in which the state is still very much present, but often disintegrated into or refracted through private interests.

To some, the very idea of thinking about cyberattacks such as the DNC hacking in a private international law mode, rather than through PIL, may sound jarring given the involvement of state actors as both perpetrators and victims. Yet from a practical point of view, private international law remedies one central complaint on the part of target states about existing frameworks—that they have no way of controlling the behaviour of hackers located

https://doi.org/10.1017/aju.2017.7 Published online by Cambridge University Press

outside their jurisdiction. Where PIL largely assumes a territorialized world in which states only have access, for enforcement purposes, to perpetrators physically located in their jurisdiction (absent extradition), private international law presumes a more nuanced and pluralistic entanglement of legal systems. For example, private international law allows for the prospect that action outside U.S. territory taken with the specific purpose of having effects within U.S. territory could in proper circumstances be subject to U.S. law. It also contemplates civil judgments obtained in non-U.S. courts (whether or not under U.S. law) being enforced against assets located within U.S. territory.

To enter, for a moment, into a private international law mode of thinking about cybersecurity—and the DNC hack in particular—imagine a lawsuit by Podesta against Russia based on *in rem* jurisdiction over Russian assets in the United States.[21] Let's assume that the hacking was legal where it occurred—although that may not be the case. One determinant of whether Podesta could claim compensation would be whether U.S. law would apply to a lawsuit to recover damages for injury to his reputation: a classic private international law question. There are strong reasons to think that it would, and if so, that Podesta should be able to recover against any assets the defendants have in the United States.

Private international law thinking leads us to ask: are there other responses to cyberthreats than state-based retaliation? The vaccine metaphor already suggests that there must be—that private innovation on the defensive side, through technologies such as encryption, is one important response. But what about other proactive steps? We can view a private lawsuit as one action a private party might take in this vein, in collaboration with the state through its judicial institutions. But it is only one among others. For example, Podesta could also join with other nonstate parties, such as corporations and civil society groups, to boycott perpetrators of cyberattacks or sellers of substandard technology vulnerable to such attacks, as a private complement to state mandated sanctions. These private actions deserve theorization alongside more public ones.

If private parties are to play a role in responding to cyberattacks, they, like states, need criteria to decide what kind of action is appropriate, and when "our" ethical choices should trump others' choices, given that the same conduct may look reprehensible to some and justifiable to others. The same can be said of state actors: what kind of retaliation for cyberattacks is appropriate and against whom?[22] Here lies the greatest value of a conflict of laws approach: although we do not have space to go into detail here, its complex techniques for evaluating questions of responsibility, across the chasms of cultural and political differences, offer a nuanced set of tools for thinking through these moral and tactical choices. Conflicts offers a road map that is not based in substantive ethical criteria held in common, but rather in technical doctrinal questions such as "contacts" with relevant jurisdictions and "interests" of relevant jurisdictions. Analogizing the substantive question of whether retaliation is appropriate to the technical question of whether U.S. law should apply to the harm, where that question is seen through a conflict of laws lens, for example, yields a subtle, context-attentive view of when harms are appropriately submitted to domestic normative standards and when they are best deferred to the standards of others.

In sum, private international law offers an addition to treaty alliances and normative consensus (the bunker) based in coordination rather than substantive harmonization. It acknowledges that there are different, conflicting value systems at work in an interconnected world that can't be reconciled. At the same time, it offers a way to think about the intermingling of private and public interests and parties in cyberwarfare that goes beyond simply harnessing the know-how of the private sector for state purposes and trying to recruit all the "good guys" onto the winning team (the vaccine). Perhaps the addition of a new legal technology to the mix may give us new ways of thinking about how we think about cybersecurity.

[21] Legal Information Institute, Wex: *In Rem*, Cornell University Law School.

[22] Cory Bennett & Bryan Bender, *Retaliating for DNC hack poses political minefield*, Politico (July 25, 2016, 06:09 PM).

https://doi.org/10.1017/aju.2017.7 Published online by Cambridge University Press