power down

OMG! Hackers take down energy grid! **David Murakami Wood** and **Michael Carter** calmly explain the how and why (or why not) of infrastructure hacking today.

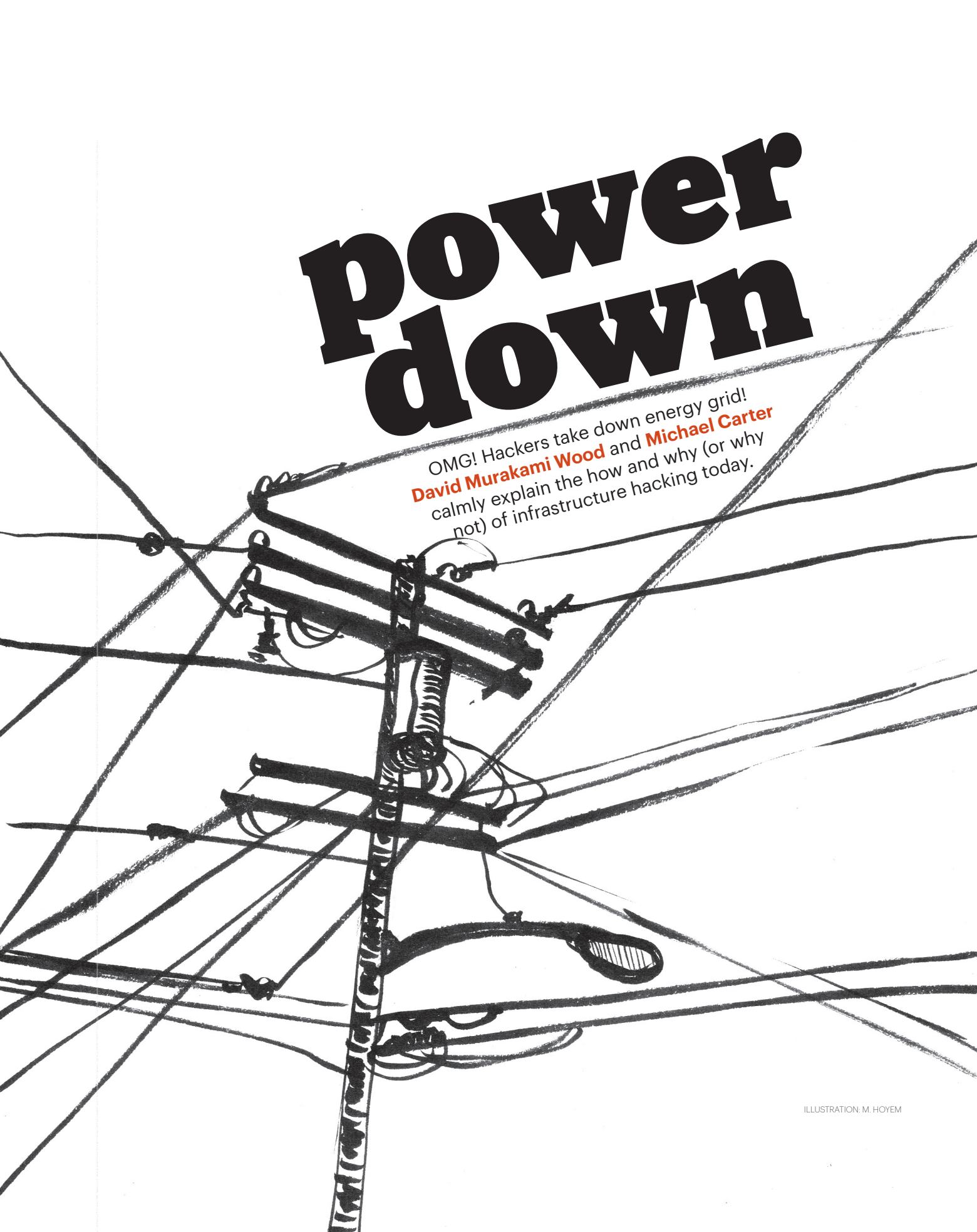


ILLUSTRATION: M. HOYEM

INTRODUCTION

The video game franchise, *Watch_Dogs* (Ubisoft 2014), offers a vision of infrastructure hacking as a smooth and seamless tool of hooded urban outsiders who, at the push of a button, can take out the traffic lights, hijack the closed-circuit television (CCTV) networks, or close down the power plants of major cities. Traffic and streets lights have not only become iconic in games, but also feature regularly in security threat scenarios for "smart city" projects. In early 2017, just days before the inauguration of President Trump, Washington, DC's downtown surveillance camera network was hacked and infected with ransomware that, city officials admitted two weeks later, prevented the city from digitally recording images from 80% of the cameras for three days (Williams 2017). The system was only brought back online two days before the inauguration.

That hackers can gain control of the systems that regulate physical infrastructures shows why government officials have pointed to hacking of control systems as an ever-growing and more ubiquitous threat. As technological infrastructures themselves have become something more expansive and pervasive, and as human societies and humans as individuals are being asked to depend more habitually on digitally connected systems, this threat has also acquired more serious consequences. The unauthorized destruction of or control over Supervisory Control And Data Acquisition (SCADA) systems, systems that manage other machines from factory robots to the aforementioned traffic light and surveillance camera networks, has become a particular concern, as the "move to open standards such as Ethernet, Transmission Control Protocol/Internet Protocol and Web technology is allowing hackers to take advantage of the control industry's unawareness" (Turk 2005: 5).

HISTORIES OF INFRASTRUCTURE HACKING

The standard history of SCADA hacking, and "infrastructure hacking" more broadly, is murky and mythologized. Interest is often dated back to the supposed Urengoy-Surgut-Chelyabinsk pipeline incident in the 1980s in which an 8-bit computer control system allegedly was infected remotely, triggering an explosion in a Soviet oil pipeline in Siberia. Yet as Thomas Rid (2013) and others have shown, there is no convincing evidence that this explosion ever happened, let alone that it was due to a hack. Indeed, Rid insists it was virtually impossible to "hide" any kind of Trojan on such a primitive control system.

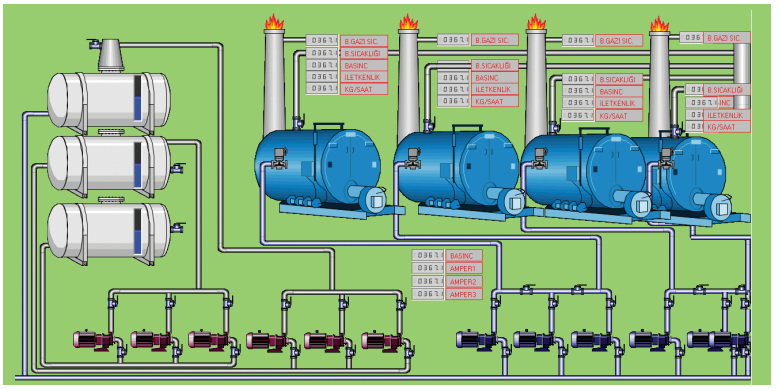
In fact, it remains difficult to find any actually confirmed incidents of significant infrastructure hacking. The Ukraine grid attacks of late 2015 were widely presented as "the first publicly acknowledged incidents to result in power outages" (Lee et al. 2016: 6), but

ABOVE: Hacking a pro-life lobbyist, tobacco exec in *Watchdogs,* 2014, Ubisoft.

is also mired in the propaganda war between Russia and Ukraine and its western allies. Much of the more immediate concern dates back to the 2003 electrical blackout across the northeastern United States and eastern Canada. However, this was not itself the result of a hack, but a combination of factors including old and buggy software, long-term policy and management failures, and a slow and inadequate response to the challenges of many simultaneous incidents of power lines being brought down by trees in a severe storm (U.S./Canada Power Outage Task Force 2004). It served to draw attention to the vulnerability of aging American electrical infrastructure and the relative complacency of power companies and governments in the face of multiple risks. The policy climate was already changing: "critical infrastructure protection" and "resilience" had become key concepts beyond simply emergency preparedness (Coaffee et al. 2009), and 9/11 not only accelerated those trends but reaffirmed and strengthened the place of security in the heart of state activity. This also hybridized with a longstanding obsession with "the enemy within," which has always formed one of the bases for policing, and which has surged visibly at particular historical junctures. The most recent surges took place first at the end of the Cold War as intelligence agencies sought to retain and even expand budgets in the face of a declining overt threat and looked to political activists as a new group of threats, and then again after 9/11, an event that persuaded politicians that certain groups of citizens might be potential saboteurs.

Gabriella Coleman (2014) shows that this continues to be a major concern in her book on *Anonymous*, in which she recounts being quizzed by CSIS (the Canadian equivalent of the CIA) on whether the hacking collective could take down the electricity grid, despite the fact that they had given no indication of interest in doing such a thing. In other words, the argument was, if this can happen by accident, how much worse could it be if a determined effort was made to

1 Security experts have questioned the conditions of the experiment in many ways, and raised doubts as to whether it demonstrated anything that would be practically possible.



ABOVE: One of many SCADA control system diagrams; this one for controlling boilers.

deliberately disrupt electrical grids by internal or external adversaries?

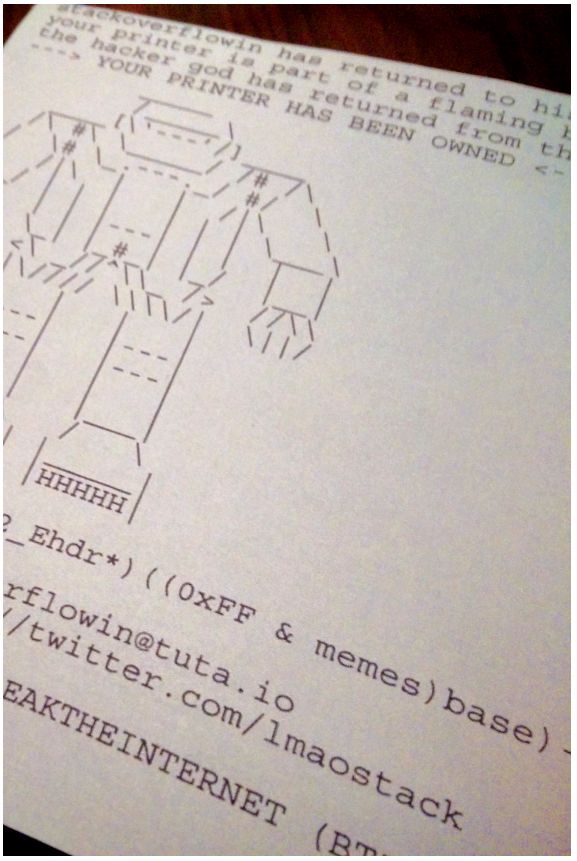
The pressure was therefore increased to develop "self-healing grids" (Amin 2004) based on the model of the original ARPAnet that became the Internet, intended as a military computer communications system that would be distributed and contain multiple redundancies to route around damage to any part. The U.S. government established a "Smart Grid Committee' in 2007 to facilitate movement toward such smart grids. But "smartness" itself was leading to new fears of vulnerabilities, as was shown by the Aurora grid hacking demonstration in that same year. This experiment, conducted in Idaho, demonstrated that in the experimental set-up, at least, a targeted systems intrusion could cause mechanical generators to operate slightly out of synchronization with the rest of the grid, creating a malfunction leading to explosion and fire.[1]

The concern with infrastructural vulnerability has also grown because the very organizations tasked to prevent such attacks by western nation-states, largely intelligence agencies, know of the real possibilities of SCADA system hacking largely through their own use of such tactics against other states. The intelligence services' concerns about Anonymous, for example, are derived not just from Aurora but also from their own use of worms as a form of cyberattack, in particular Stuxnet, which marked a new phase in state involvement in hacking occupying a blurred space between espionage "black ops", and overt warfare (Zetter 2015). Stuxnet is almost certainly a weapon devised through U.S.-Israeli cooperation specifically to attack Microsoft Windows-based Siemens SCADA systems. In the original release, the worm was aimed at the control systems for centrifuges in Iranian factories suspected of producing nuclear materials; however, it did so with unprecedented precision and complexity, exploiting not just one or two vulnerabilities, but four "zero-day" (previously unidentified) vulnerabilities in different points in the system.

Because Iran knew hacking attacks were targeting such secret nuclear work, Iranian managers made sure that the control systems themselves were not online or connected to any outside network, a practice known as "air-gapping." The Stuxnet program was therefore much more than just conventional hacking; it also involved old-fashioned subversion and the recruitment or insertion of human intelligence assets, or moles, inside the factory who could transport and insert the worm into the SCADA systems with a USB stick. Stuxnet was by all accounts "successful," and yet this highly dangerous weapon has also been discovered in numerous networked systems in countries as far afield as India and Indonesia (Falliere et al. 2011), so it must have been used on more than just those air-gapped factory machines. Stuxnet was programmed to self-destruct after around two years, but this was not, as one industry speaker at the Computers, Privacy and Data Protection 2017 conference asserted, an example of "ethics" in cybersecurity. Rather, it was a form of prevention to keep the worm from turning and becoming a danger to factory SCADA systems in "friendly" countries, and also to prevent it from being repurposed by unfriendly ones.

Stuxnet took years to plan, millions of dollars in development, and careful cultivation of human plants inside targeted organizations who had to breech "air gaps" and carefully separated systems. This seems a long way from Anonymous's "for the lulz" mode of ad-hoc and freewheeling political activism. However, both the fact of the leakage of Stuxnet "into the wild" and the increase in connected "things" of all kinds provides the rationale for the concern over the possibility of Anons taking down the electrical grid. The new wave of infrastructure hacking relies less on discovering and taking down the single "control" behind a particular system, and more on exploiting generalized connection of systems and objects, most obviously in the Internet of Things (IoT). Driven by the search for new profits within a saturated, globalized economy, entrepreneurial technological capitalism has discovered these potential profits in the surplus value of intimate and previously inaccessible intimate data generated by bodies and in the home, and the marketing of mass-customized services built on such data. The profit imperative demands that these sources of data must be connected, and connected quickly with minimal interest in the security of devices, networks, and people.

While the vulnerability of IoT devices is now well known, it is not just cheap consumer equipment that lacks sensible protocols or whose existing security capabilities remain undeployed by—or inaccessible to—their users. In one 2009 incident very important in thinking about such IoT-enabled hacking, Shi'ite



LEFT: Hacker "stackoverflowin" owned 150,000 thermal printers in February 2017.

insurgent forces in Iraq hacked U.S. military surveillance drones, allowing them to watch the watchers, track what the U.S. surveillance military system was seeing, and adjust their positions and movements accordingly (Shachtman 2009). This was as far from the operational scale or investment involved in Stuxnet as one could imagine. Deploying a tactic not far removed from urban WiFi sniffing, the insurgents used a $26 off-the-shelf Russian Skygrabber software more commonly used to download satellite television programs. There are crucial differences between this attack and Stuxnet. The Skygrabber hack is a cheap, flexible attack that exploits both the technological sophistication and the distribution and generalized nature of the system being hacked, whereas the Stuxnet attack was a major state-backed investment that engineered vulnerability in a highly secure system probably less technologically sophisticated than the attack itself. The key point here is that despite the turn to resilience and security, "infrastructure," whether military or civil, is increasingly generalized, connected, and distributed, and less likely to be air gapped and secured in the manner of Iranian nuclear component factories.

This new shifting, flexible, and contingent form of operation can be seen in the exploitation of the fact that manufacturers and suppliers appear broadly unconcerned with the vulnerability of the systems they make and sell. Whereas people would like technology to work (and that includes being secure), the tech world seems to believe that users should do the work themselves to make technology secure. This has resulted in several new threats both in practice and experiment. In the first category, alarm has increased about the hijacking of insecure IoT devices from toasters to smart home alarm systems and their integration into remotely controlled botnets used in distributed denial of service (DDoS) attacks. The attempted takedown of the Krebs on Security site created what was then the largest ever such botnet (Krebs 2016a) by the so-called "Mirai" malware, which looked for IoT devices still using insecure factory defaults (Krebs 2016b). In 2017, a similar hack took place that mobilized 150,000 printers, this time specifically to demonstrate the threat posed by unsecure connected devices (Moyer 2017). In this case, the printers were made to print out ASCII pictures of robots and were not actually part of a botnet, but the point was made: they could so easily have been.

In the second category are attacks that allow hackers to take over networked control systems. Many of these are ransomware attacks, in which relatively easy ways into systems are used to lock their legitimate users out of them. The users are then asked to pay to have their access restored, usually in bitcoin or some other hard-to-trace blockchain-based electronic currency. Security researcher Cesar Cerrudo found in 2014 that many smart urban traffic control systems had vulnerabilities, and that these would "allow anyone to take complete control of the devices and send fake data to traffic control systems. Basically, anyone could cause a traffic mess by launching an attack with a simple exploit programmed on cheap hardware" (Cerrudo 2014). Cerrudo's findings are also relevant to the kinds of political decisions that might be made in response to such threats. He argues, "if a vulnerable device is compromised, it's really, really difficult and really, really costly to detect it" (Cerrudo 2014). This means that there could "already be compromised devices out there that no one knows about or could know about" (Cerrudo 2014). A serious implication here is whether the pressure to find cheap, "smart" urban fixes in an age of austerity will actually make hacking attacks more prevalent, even normal, and this might put urban authorities lacking both financial and technical security resources at a permanent disadvantage, having to choose between smart and secure rather than having both.

REGAINING CONTROL?

Several of these examples make *Watch_Dogs* seem less simplistic in its portrayal of the ease of infrastructure hacking. Cerrudo's insights are meant to provoke or force national governments to get more involved in assessing technologies. There is a more general issue here than simply hacking: in many jurisdictions, there is often barely any scrutiny of procurement by local government and other subnational agencies and

authorities for any reason, let alone a detailed technical or security assessment. This is compounded by the fact that states and large corporations have ported their response to hacking infrastructure directly from the predominant official vision of hacking as cybercrime or, increasingly, cyberwar, concentrating on attacks on "critical infrastructure" and nationally significant computing systems rather than considering the security of people, groups, and smaller, local governments as priorities or even as a matter for government at all.

The focus on this top-level aspect, the view from a rather traditional, "realist" national threat model, makes cybersecurity sound exceptional. But there is nothing truly exceptional about cybersecurity that makes it an extraordinary threat. Infrastructure hacking attacks are technical in their means, but their solutions are frequently human and behavioral. The first biggest threat to security of control systems are degradation, failure, and accident; second, human users; and finally—and least likely and damaging of all—intrusion or "attack." And many attacks are really exploiting human beings as much as the technical systems themselves; this is true even in the case of sophisticated worms such as Stuxnet, and all SCADA systems that are air gapped for security.

The question of air gapping should tell us something else: that the simplest form of security for infrastructure systems is disconnection. This is an important point to bear in mind when there is a mania for connecting everything, not just what one would formerly called computers or information systems, via the Internet of Things. Connection always means more openness and vulnerability, and every security action taken after connection is inevitably a (more expensive) mitigation of risk that also involves more intensive surveillance and compromises to privacy and other freedoms. We shouldn't forget that if it serves no necessary purpose to connect, it shouldn't be done. This lesson, however, goes against the powerful commercial imperatives that are driving the move towards the IoT, not only in terms of the sales of devices but the indirect exploitation of human users for yet more data, the direct sources having already been exhausted.

In the case of users, and that includes even relatively "expert" users such as police or security personnel, it is also ineffective and even counterproductive to blame individuals and demand that people conform to the systems or norms of highly expert producers within the developer community, especially because the commercial drivers assume and encourage such weakened privacy and security. Control also has an analogical meaning here in terms of measures, whether voluntarily by producers or mandated by stronger consumer protection laws that enable people and institutions that use connected devices to more easily control the security functions of devices and systems and understand the consequences. Again, this goes against certain technological trajectories, most notably the "infrastructurization" of certain systems, or the vanishing of such systems from the sight of users who depend upon them (Murakami Wood 2015). Although infrastructure is precisely designed to work unobtrusively and support other activities, and SCADA systems are the most invisible of all, this very invisibility can lead to inaccessibility to productive and useful alteration, as is already the case with many open source software design or mapping projects (Dodge and Kitchin 2013), but going further with crowdsourcing design or maintenance of civil infrastructure to provide greater real-world resilience and ownership, for example in helping to provide clean water in marginalized communities (von Heland et al. 2015). Far from all infrastructure hacking is offensive and destructive: as the growth of smart city hackathons, participatory programming, and the use of open data and open source is showing, many urban infrastructures can be more open and adjustable yet still be secure.

It might well be that although allowing generalized access to the "guts" of systems might not in practice provide for outcomes that are in the general good, providing greater access to the outputs might allow for both new uses and useful feedback. As in the case of the Iraqi insurgent hacking of U.S. drones, it is clear that this undermines military advantage; there is no such rationale in the case of urban CCTV. There is no fundamental reason why all citizens should not have access to public video surveillance feeds rather than their being purely an instrument of state authority. And what both cases share is that "control" over the system itself does not have to be compromised to allow the products of a technical system to be more widely available.

Although the security of control systems that allow infrastructures to function need defensive measures, perhaps a greater emphasis on designing the wider systems to be open to hacking would be both more cost-effective and more democratic, and lead to less paranoia and unnecessary closure. However, there are some very important cautions to overenthusiasm about participatory hacking. As Keller Easterling (2014) has argued, infrastructures are instruments of what she calls "extrastatecraft," and in an age in which we are offered the false choice of neoliberalism and fascism, these can serve ends both exploitative and authoritarian. Despite the ongoing work of open source movements and the rise of Anonymous and the Pirate Party and other hackers with ethico-political motivations, both infrastructures and the tools of infiltration and control of those infrastructures remain predominantly in the hands of massively resourced state cybersecurity and cyberwar agencies or in the corporate campuses of Silicon Valley. There is no coherent current or foreseeable politics of hacking able to articulate a widely shared vision that is independent of either state or private sector. ■

DAVID MURAKAMI WOOD *is Canada Research Chair (Tier II) in Surveillance Studies at Queen's University, Ontario.* **MICHAEL CARTER** *is a doctoral research student in the Department of Geography, also at Queen's University.*

REFERENCES

Amin, Massoud. 2004. "Balancing Market Priorities with Security Issues." *IEEE Power and Energy Magazine* 2(4):30–38.

Cerrudo, Cesar. 2014. "Hacking US (and UK, Australia, France, etc.) Traffic Control Systems." *Ioactive*, April 30. https://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

Coaffee, Jon, David Murakami Wood, and Peter Rogers. 2009. *The Everyday Resilience of the City*. Basingstoke, UK: PalgraveMacmillan.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso.

Dodge, Martin, and Rob Kitchin. 2013. "Crowdsourced Cartography: Mapping Experience and Knowledge." *Environment and Planning A* 45(1):19–36.

Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. New York: Verso.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. W32.Stuxnet Dossier Version 1.4 (February). Cupertino CA: Symantec Corporation.

Krebs, Brian. 2016a. "KrebsOnSecurity Hit With Record DDoS." *KrebsOnSecurity*, September 16. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

———. 2016b. "Source Code for IoT Botnet 'Mirai' Released." *KrebsOnSecurity*, October 16. https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, DC: SANS Industrial Control Systems/NERC.

Moyer, Christopher. 2017. "This Teen Hacked 150,000 Printers to Show How the Internet of Things Is Shit." *Vice Motherboard*, February 8. https://motherboard.vice.com/en_us/article/this-teen-hacked-150000-printers-to-show-how-the-internet-of-things-is-shit

Murakami Wood, David. 2011. "Vanishing Surveillance: Why Seeing What Is Watching Us Matters." Insights on Privacy discussion paper. Ottawa, Canada: Office of the Privacy Commissioner (OPC). https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/wood_201107/

Rid, Thomas. 2013. *Cyberwar Will Not Take Place*. Oxford, UK: Oxford University Press.

Shachtman, Noah. 2009. "Insurgents Intercept Drone Video in King-Size Security Breach." *Wired*, December 17. https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/

Turk, Robert J. 2005. *Cyber Incidents Involving Control Systems*. Idaho Falls: Idaho National Engineering and Environmental Laboratory.

U.S./Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington DC: Office of Electricity Delivery & Energy Reliability.

von Heland, P. F., M. Nyberg, A. Bondesson, and P. Westerberg. 2015 "The Citizen Field Engineer: Crowdsourced Maintenance of Connected Water Infrastructure." Paper presented at the *Third International Conference on ICT for Sustainability (ICT4S 2015)*, Atlantis Press.

Williams, Clarence. 2017. "Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose. *Washington Post*, January 26. https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html

Zetter, Kim. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books.