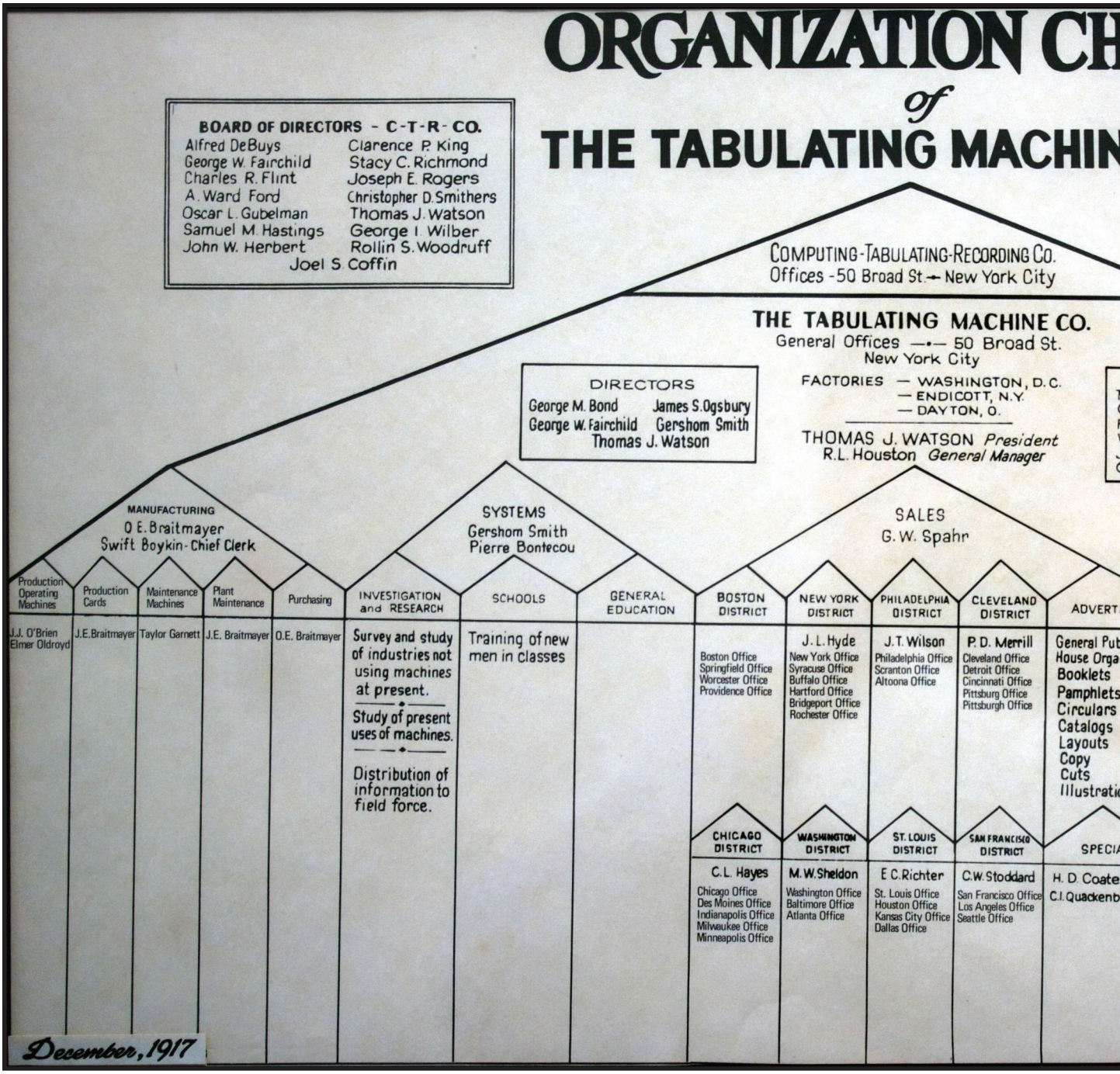
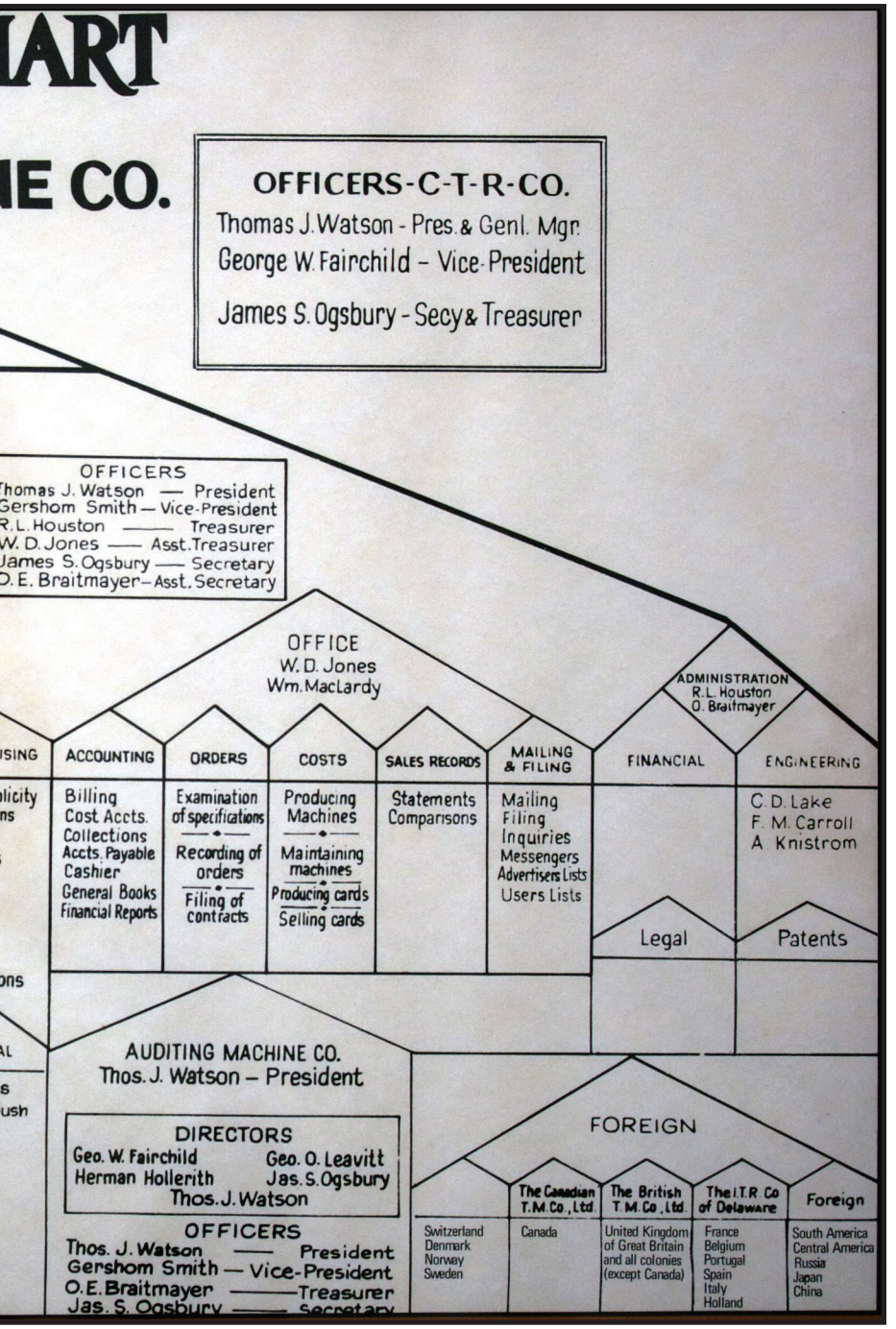


CAN YOU SECURE



LEFT: A 1917 exemplar of bureaucracy—the Tabulating Machines Company (later IBM).

Are bureaucracies defensible? Nils Gilman, Jesse Goldhammer, and Steven Weber explore the Office of Personnel Management hack, and what it tells us about the inherent vulnerabilities of bureaucratic organizations in a digital age.

AN IRON CAGE?

OVER THE COURSE OF 2014 AND 2015, The U.S. Office of Personnel Management (OPM) slowly discovered—and even more slowly disclosed—that it had been the victim of one of the biggest and most significant to national security hacks of personally identifiable information in U.S. history. Eventually OPM would admit that more that 21 million individuals' records had been compromised, including the real identities and fingerprints of more than 5 million people both inside and outside the federal government: virtually everyone who at some point in the last 30 years had either sought or been required to obtain a security clearance.

OPM is a classic example of a bureaucracy, one of the defining inventions of the modern age: rational, rule based, and results oriented. When it works well, bureaucracy is a remarkable form of human organization that has enabled modern governments and corporations to provide previously unimaginable benefits to humans around the world. Before "scale" ever became a Silicon Valley slogan, it described a distinct post-18th-century organizational capacity to deliver goods and services to millions in a consistent, orderly, and equitable manner[1]

But as we know from Max Weber, bureaucracy has a dark side: many "customers" and "citizens" experience bureaucracy as inexplicable confusion, frustration, and alienation. It was the bureaucratic insiders whom Weber saw as most painfully struggling with dehumanizing "systems," processes, and rules. Weber worried about the impact of bureaucratic structure on individual freedom, an anxiety that gave rise to what is arguably his most famous metaphor: the "iron cage" (*stahlhartes Gehäuse*).

Weber's metaphor paid homage to the dominant form of production at the time: industrial machines. Weber imagined bureaucracies as the organizational analog to an efficient machine: "The fully developed bureaucratic apparatus," he observed in *Economy and Society*, "compares with other organizations exactly as does the machine with non-mechanical modes of production" (Weber 1978:973). But has modern bureaucracy finally met its match in the internet era? Put another way: In a networked digital age, does bureaucracy remain an efficient and effective apparatus for managing human affairs?

Important insights about this simultaneously theoretical and empirical question emerge from the now-infamous theft of data belonging to the federal government's OPM in 2014 and 2015. The OPM breach turns out to be a powerful illustration of how a Weberian bureaucracy struggles and fails to meet one of the most profound challenges facing organizations that operate internet-connected digital networks in the 21st century: the hack. How OPM lost this battle foreshadows a deeply troubled future for bureaucracies in the increasingly digital decades to come.

THE OPM HACK: A SLOW REVEAL

Established in 1979 as part of the Civil Service Reform Act, OPM is essentially a human resources agency charged with overseeing the civil service of the U.S. federal government. In addition to "recruiting, retaining and honoring a world-class force to serve the American people,"[2] it is also responsible for the management of security clearances, not only for federal employees but also for the millions of contractors who serve in security-sensitive capacities.

Until 1996, OPM itself conducted background investigations for security clearances. That year, as part of then-Vice President Al Gore's "Reinventing Government" initiative that aimed to shrink the size of the federal civil service, OPM outsourced its investigative branch to private sector consulting firms, many of which were run by former high-level OPM employees. Two of these companies, the United States Investigations Services (USIS) and KeyPoint Government Solutions, would come to dominate the federal market for investigation services, conducting millions of background investigations over the next two decades on behalf of their federal clients. With the exception of the Nuclear Regulatory Commission, which manages security related to the U.S. nuclear industry, the formerly separate security clearance programs of each executive department were gradually merged into a single, government-wide clearance system charged with investigating both federal workers and contractors seeking Secret and Top Secret clearances.

Had OPM and its investigative surrogates continued to operate with paper files—even millions of them—OPM's outsourcing almost certainly would not have posed the same risk as the pooling of digital files. But this combination of centralization of systems and outsourcing of functions established a risk-filled playing field through which the OPM hack would unfold over the course of 2014 and 2015 (Castelluccio 2015:79).

The public dimension of the OPM hack officially began on June 17, 2014, when USIS sent a memo notifying 15 federal agencies that it had uncovered a data breach that had taken place three months earlier, in March, with "all the markings of state-sponsored attack." The breach had resulted, USIS said, in the disclosure of about 25,000 federal employees' records.

One can only imagine the difficult conversations that must have ensued among OPM leaders when they

1 For two radically divergent recent histories of bureaucracy, see Fukuyama (2014) and Graeber (2015)

2 https://www.opm.gov/about-us/our-mission-role-history/

received this letter. As it turned out, OPM had itself also been the subject of an direct cyber attack by Chinese hackers back in March, one OPM had informed the White House about but had never disclosed publicly, because at the time OPM managers believed it had successfully thwarted the attack using an Intrusion Detection System, a computer network-monitoring appliance designed to spot malicious activity or policy violations (Smith 2015).

OPM's official response to the June 2014 USIS letter was straight from the bureaucratic playbook: sever its contracts with USIS and admonish its employees to be more vigilant with respect to cybersecurity threats (*Washington Post* 2015). In fact, as yet unbeknownst to OPM, the attackers were already inside their systems, having succeeded in dropping a RAT (remote access trojan) on one of OPM's key Microsoft SQL servers. By June 23, 2014, the hackers had moved laterally through OPM's computer network and found their way into one of OPM's mainframe computers. A legacy system incapable of supporting modern encryption technologies, this mainframe was where OPM kept its hypersensitive data on background investigations.

By July, the FBI had launched a wide-ranging investigation. In September, this investigation detected a data breach affecting KeyPoint Government Solutions, the other major provider of investigations services for the U.S. government, primarily serving the Department of Homeland Security (DHS). This breach is believed to have compromised as many as 400,000 current and former DHS employees, contracts, and job applicants (Associated Press 2015). In December, yet another, separate breach was discovered at KeyPoint, leading OPM to notify more than 48,000 federal employees that their security credentials as well as other personally identifiable information had been compromised.

Though the U.S. government didn't realize it at the time, the aim of the hackers was not just to gain access to the data stored at USIS or KeyPoint, but even more to acquire virtual private network (VPN) credentials from these contractors that would enable the hackers to access data inside OPM itself. In April 2015, when OPM upgraded its internal security tools, it discovered that since the previous December it had been the victim of a months-long data breach.

Called to testify before Congress on the matter on April 22, 2015, OPM's Chief Information Officer Donna Seymour admitted not only that USIS and OPM had both been hacked near simultaneously back in March 2014, but also that the KeyPoint and OPM attacks were coincident in December 2014 (Sternstein 2015). It was now becoming clear that the contractors were serving as vectors for entering the U.S. government systems themselves.

It was only in June 2015, nearly a year after the original OPM breach, that the government began to realize (or admit) the breathtaking scope of the hack. The breach, including massive amounts of data from OPM's e-QIP System, which a year earlier the *Washington Post* had described as "including applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers" (Nakashima and Rein 2014). In addition to this data, the hackers would also have acquired information from "adjudication," or the supplemental information that investigators would have considered before granting a security clearance, including:

> ...information on "sexual behavior" that "reflects lack of discretion or judgment" to evidence of "foreign influence," including a broad definition of "risk of foreign exploitation" associated with mere "'contact with a foreign family member." For instance, the information collected to adjudicate a simple Top Secret single-scope background investigation includes a "Personal Subject Interview" and "interviews with neighbors, employers, educators, references and spouses/cohabitants." It also includes "record checks with local law enforcement where the individual lived, worked, or went to school in the past 10 years" (Adams 2016).

Finally, while it has been widely reported that the OPM hackers were able to obtain fingerprint data from 5.6 million individuals, it may also be the case that they obtained polygraph results from individuals who sought high-level security clearances, as this information would have been included in any typical adjudication process.

THE INHERENT CYBER VULNERABILITY OF WEBERIAN BUREAUCRACIES

The hackers who stole a treasure trove of data about U.S. citizens did not simply demonstrate the vulnerability of a particular government agency. Rather, they systematically exploited weaknesses that are endemic in bureaucracies and did so in a way that calls into question their *modus operandi*, which Max Weber articulated succinctly: the definition of bureaucratic administration is domination through knowledge and process (Weber 1978:225).

OPM's information networks mirrored the structure of the organization itself. When OPM outsourced functions like investigations to improve its efficiency, it necessarily created new network nodes, managed by private contractors, which increased complexity, vulnerability, and risk.

That changing network architecture configuration ultimately put OPM in a terrible bind. It was not enough just for OPM to build information technology (IT) systems that support its core mission, namely the management of human resource records; it would also need to develop a new and highly costly expertise that was far afield from the types of knowledge that OPM had managed since its inception. And, that

new knowledge—cybersecurity—would reside in and govern not only OPM itself, but also its symbiotically intertwined contractors. This put OPM in the position of requiring a wide range of technical standards, from authentication to encryption to threat mitigation, that OPM was itself unable to meet.

OPM's centralizing and outsourcing of its investigative services reflected what seemed at the time a rational choice for a federal human resources bureaucracy charged with the mandate to operate more cost-effectively. What Daniel Yergin once termed the Reagan bureaucratic "revolution" (Yergin and Stanislaw 1998) was in fact less of a revolution than an evolutionary move to redirect bureaucratic functions from the public to the private sector (Gualmini 2008). The goal of this move was to drive efficiency. Whereas public sector bureaucracies are typically governed by process norms (are they operating according to the appropriate laws, regulations, rules, and norms?), private sector bureaucracies in for-profit businesses are supposed to be governed more powerfully by efficiency objectives: How much does it cost to get the job done? The private incentives are to maximize productivity and minimize wasteful processes.

But private sector bureaucracies are still bureaucracies: hierarchical, rule-driven, complex, and when they operate at scale, anti-entrepreneurial. The ideology behind outsourcing was rooted not in a critique of bureaucracy per se, but in a belief in the disciplining force of the profit motive and a concomitant anti-statist disposition against *government* bureaucracies (Considine and Lewis 1999).

The efficiency argument turned out to have less weight than its proponents had hoped. This is because, as Paul Dimaggio and Walter Powell observed in their classic 1983 paper "The Iron Cage Revisited," organizations that interact intensely and largely exclusively start to converge in structure and processes so that their interactions can themselves become efficient. In other words, the larger and more intimately connected to the public sector a "private" bureaucracy is, the more it looks and operates like (becomes isomorphic with) the public sector agencies it serves. Because the contractors serving OPM had to interact intensively with government agencies, they inevitably began to mirror OPM's operational habits and organizational structures. Going private didn't offer an escape from the iron cage of bureaucratic inefficiency; it just shifted the bars on the windows (Dimaggio and Powell 1983).

This convergence might have been merely a disappointment to efficiency mavens. But 1996 was also the year that the World Wide Web came into widespread use, signaling a new era in organizations' dependence on digital networks. The U.S. government bureaucracy and its stable of contractors found itself unprepared for a set of threats that were unforeseen at the time: cyber attacks from networked adversaries. The greater complexity of the outsourcing system may have increased its vulnerability to adversaries who were aware of that complexity and prepared to exploit it ruthlessly for criminal gain.

Bureaucracies have been historically successful when they are able to master knowledge complexity through the develOPMent of expertise, role differentiation, and process innovation. Contemporary information networks profoundly challenge this supremacy. The digital world operates with infinitely greater speed than the old paper-based models that bureaucracies were invented to manage. Digital networks encompass stores of information that far exceed the carrying capacity of a traditional bureaucracy. Digital machines execute actions on the basis of highly complex data analyses that exceed human cognitive abilities. The problem is simple: bureaucracies are designed to seek control through mastery of detail and predictable processes. Large-scale information networks have too many details—that is, they are too complex—to master in this way. Indeed, they are hackable precisely because specialization and division of labor do not actually facilitate the understanding, let alone management, of hardware and software vulnerabilities, especially given the fact that increasing technological sophistication also inadvertently multiplies complexity and vulnerability.

Bureaucracies have to operate according to codified rules and procedures. This can be effective for parrying *known* risks and threats, but can be worse than useless when defenders don't know the nature or source of the dangers in question. This dynamic is multiplied in the software environment. Frederick Brooks's classic study of software engineering is titled "The Mythical Man Month" (1975) for a reason: in the tar-pit that is software code, bureaucratic processes (like adding more workers to a project that has fallen behind schedule) often have perverse and literally counterproductive effects. "Brooks's Law" puts it this way: adding manpower to a late software project makes it even more late. Software engineers have developed alternative approaches to organizing that seek to compensate for Brooks's Law (such as Agile Programming), but such approaches to fostering innovation are at odds with bureaucratic demands for things like documentation and metrics of productivity and performance.[3] Outsourcing work to private sector bureaucracies that serve the government bureaucracy changes nothing in this regard.

The offense-defense balance around bureaucracy is almost precisely reversed in the digital era from what it was during the industrial era. Now, bureaucracies are easier to attack than they are to defend, easier to undermine than they are to stabilize. And this calls the sustainability of the bureaucratic form into real

3 This point was recognized half a century ago in Thompson (1965).

question.[4]

We can bemoan the fact that OPM did not upgrade its information technologies and did not implement common-sense cybersecurity protocols, such as data encryption, in an effort to protect highly sensitive data about millions of Americans. But that lamentation rests on the assumption that bureaucracies can build and sustain information networks able to serve their core missions without dramatically increasing risks that can also be managed through a mastery of cybersecurity expertise.

We would have to believe that organizations like OPM can either administer their own robust cybersecurity protocols or outsource them to other parts of the government and/or the private sector without at the same time increasing the risk that such complexity will actually make OPM more vulnerable, not less. Indeed, even if OPM had done everything right—whatever that might mean—we would also still need to believe that a determined and sophisticated nation-state actor intent on stealing OPM's data possibly could have been thwarted. In short, OPM was a sitting duck.

"A LINKEDIN FOR SPIES"

In July 2015, the news got even worse for Washington. United Airlines revealed that it too had been hacked, using the same exploits and techniques that had been used to penetrate USIS, Keypoint, and OPM. The data stolen from United consisted primarily of flight manifests, including information on flights' passengers, origins, and destinations (Riley and Robertson 2015). And, as it turned out, the same signatures, according to various experts, marked the hack of the enormous American health care insurer Anthem, which had revealed in February 2015 that it had had 79 million records stolen from across its various brands, including Blue Cross and Blue Shield, Amerigroup, Caremore, and Unicare (Menn 2015).

The specter that this hacking triple-play raised for the U.S. government was a fundamental compromising of the U.S. intelligence community, perhaps for a generation. As *Ars Technica* put it, "When pulled together into an analytical database, the information could essentially become a LinkedIn for spies, providing a foreign intelligence organization with a way to find individuals with the right job titles, the right connections, and traits that might make them more susceptible to recruitment or compromise" (Gallangher 2015).

Ars Technica's catchy "LinkedIn for spies" metaphor is just one installment among the dozens of imaginative and speculative thought pieces about how an adversary might take advantage of all of these data. Unfortunately, what we think we know about the consequences of the OPM, United, and Anthem hacks is belied by a stubborn reality. Did these hacks provide China with a geostrategic advantage?[5] We don't know. Did they compromise our intelligence professionals? We don't know. Did they harm anyone concretely or cause a human toll of any sort? So far, the answer appears to be a tentative "no," but this might be an artifact of government secrecy. Did these hacks usher in radical transparency with visible consequences? Answer: probably not, or at least not yet.

The thing bureaucracies hate more than anything else is uncertainty. And yet the only certain impact of the OPM and associated hacks was to embarrass the U.S. government. Even former CIA Director Michael Hayden described the Chinese hacking of government records as "honorable espionage work" of a "legitimate intelligence target." "This is a tremendously big deal," he said. "My deepest emotion is embarrassment" (*American Interest* 2015).

In response to this embarrassment, OPM did what bureaucracies know how to do: it promised to adopt new policies, processes, and procedures. Despite its lack of native cybersecurity competence, OPM pledged to implement two-factor authentication, continuous diagnostics, and data encryption, though OPM noted, plaintively, that some of its systems are so old that they cannot be encrypted (Medici 2015). OPM also explained that it would hire a cybersecurity expert from "outside government" who would report directly to the OPM director. Finally, OPM asked Congress for additional resources to modernize its IT systems and ensure appropriate oversight of it agency and contractors.

POST-WEBERIAN POSSIBILITIES

It wasn't so long ago that OPM managed investigations using paper, making it all but impossible to steal 21 million records. Now OPM and bureaucratic organizations like it are actively digitizing their core missions in the name of efficiency, and in so doing piling risks and vulnerabilities on top of each other as they venture beyond what humans and human processes are able to manage. While perfectly rational and appropriate in the Weberian model, these remedies are ineffective for addressing the fundamental weakness of traditional bureaucratic organizations that use modern information networks to prosecute their missions. In their current forms, such organizations simply cannot master the knowledge that is stored, transported, and analyzed on their networks. Instead, they will engage in flailing, piecemeal technical reforms to mitigate known risks, such as closing the ports from which their data have usually already escaped.

Worse, by extending the logic of Weberian bureaucracy, organizations like OPM are creating new classes of risks that they are also ill equipped to manage. For instance, they will embrace algorithmic policy decisions and enforcement, a digitization of their core functions, which may increase the efficiency with which they operate, but will also bury them in millions of lines of code

4 The idea that the cyber domain is an "offense dominant" one (in Robert Jervis's terminology) is explored in Sergei A. Medvedev (2015).

5 China is widely believed to be the nation-state behind these hacks, even if no conclusive evidence has been proffered publicly.

and exacerbate the impact of mistakes. In response to current threats, IT and cybersecurity functions will expand into every corner of these organizations, but the irony is that this expansion will merely create a wealth of new opportunities for hackers. Finally, to meet oversight requirements, these bureaucracies will come under increasing pressure to develop highly sophisticated compliance software that tracks every bit of data: where it's stored, who accessed it and when, why they accessed it, how it was combined with other types of data and, finally, when and how it was deleted. These highly complex compliance systems will provide a panoramic view into complex information networks, but they too will be vulnerable and hackable.

As we watch the struggles of the U.S. federal bureaucracy to adapt in the face of these novel threats, we are left with a fundamental question about the future of an organizational form. Is the digital revolution also the death throes of the traditional bureaucracy, presaging a future of declining governmental effectiveness punctuated by occasional catastrophe? What seems certain is that government bureaucracies face a radical reset of stakeholder performance and risk expectations, that is, with the citizens they are supposed to serve. ■

NILS GILMAN *Nils Gilman is an historian and the Vice President of Programs at the Berggruen Institute.* **JESSE GOLDHAMMER** *is a political scientist and the Associate Dean at the UC Berkeley School of Information.* **STEVEN WEBER** *is Professor at the School of Information and Department of Political Science, UC Berkeley.*

BIBLIOGRAPHY

Adams, Michael. 2016. "Why the OPM Hack Is Far Worse Than You Imagine." *Lawfare*, March 11. Available at link.

American Interest. 2015. "Former CIA Head: OPM Hack was 'Honorable Espionage Work.'" *The American Interest*, June 16. Available at link

Associated Press. 2015. "Hack May Have Exposed Info on 390,000 People Tied to Homeland Security." June 15. Available at link.

Brooks, Frederick P. 1975. *The Mythical Man Month: Essays on Software Engineering*. Boston, MA: Addison Wesley Professional.

Castelluccio, Michael. 2015. "The Biggest Government Hack Yet." *Strategic Finance* 97(2):79.

Considine, Mark, and Jenny M. Lewis. 1999. "Governance at Ground Level: The Frontline Bureaucrat in the Age of Markets and Networks." *Public Administration Review* 59(6):467–480.

Dimaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2):147–160.

Fukuyama, Francis. 2014. *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy*. New York: Macmillan.

Gallangher, Sean. 2015. "'EPIC' fail—how OPM hackers tapped the mother lode of espionage data." *Ars Technica*, June 21. Available at link.

Graeber, David. 2015. *The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy*. New York: Melville House.

Gualmini, Elisabetta. 2008. "Restructuring Weberian Bureaucracy: Comparing Managerial Reforms in Europe and the United States." *Public Administration* 86(1):75–94.

Medici, Andy. 2015. "OPM fires back at hack criticism, vows further reform." *Federal Times*, June 24. Available at link.

Medvedev, Sergei A. 2015. *Offense-defense theory analysis of Russian cyber capability* [dissertation]. Naval Postgraduate School. Monterey, CA.

Menn, Joseph. 2015. "U.S. employee data breach tied to Chinese intelligence." *Reuters*, June 19. Available at link.

Nakashima, Ellen, and Lisa Rein. 2014. "Chinese Hackers Go after U.S. Workers' Personal Data." *The Washington Post*, July 10. Available at link.

Riley, Michael, and Jordan Robertson. 2015. "China-Tied Hackers That Hit U.S. Said to Breach United Airlines." *Bloomberg.com*, July 29. Available at link.

Smith, Ian. 2015. "OPM Data Breach: What You Need to Know," June 8. Available at link.

Sternstein, Aliya. 2015. "Here's What OPM Told Congress the Last Time Hackers Breached Its Networks." NextGov.com, June 15. Available at link.

Thompson, V. A. 1965. "Bureaucracy and Innovation." *Administrative Science Quarterly* 10:1–20.

Washington Post. 2014. "E-mail to OPM staff on security breach." July 10. Available at link.

Weber, Max. 1978. *Economy and Society*. Berkeley: University of California Press.

Yergin, Daniel, and Joseph Stanislaw. 1998. "The Real Revolution." *Forbes*, May 4, 85–91.