HARVARD Kennedy School
BELFER CENTER

HOMELAND SECURITY POLICY PAPER #5

Closing Critical Gaps that Hinder Homeland Security Technology Innovation

Nate Bruggeman* and Ben Rohrbaugh†

Authors' Note

We drafted this paper before the full extent of the coronavirus/COVID-19 pandemic became clear. We have been deeply concerned about the homeland security enterprise's approach to technological innovation for over a decade. The pandemic has only served to confirm our concerns. COVID-19 has overwhelmed the response systems of the United States and clearly shown the scale of the federal government's underinvestment in public safety technology. From developing testing capacity to producing medical supplies to rapidly expanding treatment capacity to developing a vaccine, the federal government has been unable to lead. The country instead relies on a patchwork of federal, state, local, and private sector resources to respond to a widespread public health emergency.

Stories are emerging of potentially lifesaving research or developed technologies that are not in place because of shortsighted decisions or budget cuts. One illustrative example is the U.S Department of Health and Human Services' flirtation with and ultimate abandonment of an initiative to improve facemask readiness.[1] For its part, the Department of Homeland Security (DHS) has had a minimal public role in providing any kind of public safety technology in this crisis. The issues attendant to responding to the virus are only the most recent, dramatic example of the innovation challenges facing the DHS and the broader homeland security enterprise. We are hopeful that, when the pandemic subsides, policymakers will pay particular attention to the government's technology and innovation deficits.

* **Nate Bruggeman** held senior policy positions at the U.S. Department of Homeland Security and U.S. Customs and Border Protection addressing border security, law enforcement intelligence, and U.S-Mexico engagement. He has also had a distinguished legal career, most recently at the Colorado Department of Law and previously in private practice. Bruggeman is a Fellow at the Belfer Center's Homeland Security Project and the Executive Editor of its Homeland Security Policy Paper Series

† **Ben Rohrbaugh** has been at the forefront of border and supply chain security and advancing U.S.-Mexico relations for a decade. Rohrbaugh held senior policy positions at the U.S. Department of Homeland Security and U.S. Customs and Border Protection, and he was a Director on the White House's National Security Council where he developed policy on border and supply chain security issues. Rohrbaugh is currently a Fellow at the Strauss Center for International Security and Law at the University of Texas-Austin.

Rohrbaugh is also a founder of a startup company, Lantern UAS, which develops systems using aerial drones for screening cargo containers. Lantern UAS has worked through DHS-sponsored funding mechanisms to support its research.

Executive Summary

Rapid technological advances are making nonstate actors much more capable than they were even a decade ago. Malicious actors like terrorist groups, criminal organizations, and state proxies are increasingly able to threaten American civilians and their interests around the world. At the same time, we are increasingly vulnerable to the emergence of new disease and natural disasters, as vividly shown by the hurricanes of 2017 (Harvey, Irma, and Maria) and the COVID-19 pandemic.

Effectively countering these threats, including by developing and supporting private sector-generated new technological solutions, is a core government responsibility. DHS is the U.S. government's primary civilian public safety agency and the main source of government funding for nonmilitary development of public safety technologies. Unfortunately, DHS has a poor record of developing new technological solutions to advance its mission and address emerging threats. This article assesses the current situation, identifies lines of research that are urgently needed, and makes recommendations on how DHS can more effectively partner with industry and how new technologies can be quickly seeded.

Background

DHS has struggled with technology innovation since its formation. Although the problem is often framed as one of acquisition failures—highlighted periodically by examples like the failed virtual fence, SBInet—the fundamental problem extends beyond procurement and acquisition. DHS lacks an innovation pipeline with the private sector, that is, a repeatable set of processes situated in an established structure to fund and match private sector solutions and technological innovation against critical homeland security problems. DHS also lacks the ability to effectively identify and directly fund lines of research to address its operators' needs.

A variety of reasons exist for these deficiencies. DHS is primarily a law enforcement-centric enterprise. Historically, law enforcement has not driven technological innovation. Rather, law enforcement has been a people-centric endeavor—cops on the beat, investigators chasing leads, etc. Congress and the Executive Branch do not fully understand and/or merely pay lip service to the vital role technology plays in defending the homeland, and the fall back in practice is to rely on the politically expedient solution to hire more personnel. It is little surprise that human capital costs are the major component of the DHS annual budget and its principal financial focus.

DHS is also beset by structural problems both internally and with respect to Congress. The Department is unwieldy and still lacks a coherent management philosophy and structure.[2] On its organization chart, DHS has a central hub for technological innovation: Science and Technology Directorate (S&T). S&T, however, does not have the political and bureaucratic clout, resources, and access to drive major innovation initiatives.[3] While preparing this article,[‡] we talked with one former senior executive from the U.S. Border Patrol who told us the Border Patrol has numerous problems that would benefit from technology solutions. However, he could not remember ever attending a meeting with anyone from S&T while he served at the highest levels in Washington.[4] Put differently, S&T is peripheral to DHS' operational components, which are generally left on their own to find or try to develop new technologies.

‡ We interviewed numerous former DHS officials in preparing this article. All interviews were conducted on background so that the interviewees could speak candidly about their experiences.

A culture of technological innovation and an effective ecosystem for its development within DHS is, in short, conspicuous by its absence. What programs S&T does run to identify promising private sector technologies and directly fund new research are ineffective given program structures and/or the scope of the Department's needs.[§] S&T's Small Business Innovation Research (SBIR) program, for instance, puts out extremely detailed technical requirements rather than broader need descriptions that researchers could creatively address.[5] It also lacks operational champions from a component agency, and it almost never transitions to operators successfully. This is the same problem with S&T's Silicon Valley office[6]: it puts out very specific requests and does not have interest or the bandwidth to deal with ideas that come outside of their identified framework. And it is unclear whose priorities S&T is advancing. A former intelligence executive explained that, in three separate positions at DHS, S&T collected requirements from him to solve pressing intelligence capabilities needs; in each instance, he never heard back from S&T.[7]

The academic "centers of excellence" funded by DHS have not been able to fill the gap.[8] Funding through university research centers is slow moving and bureaucratic, and it emphasizes projects that align with academic interests rather than what the operators necessarily need. Combining academic bureaucracy and government bureaucracy renders it almost impossible for these centers to be nimble and innovative, even when they are staffed by talented people. It is also a very inefficient way to spend money, as universities essentially tax monies spent through these programs with indirect cost rates that can take up 60% or more of the funding for programs on overhead alone.

These circumstances leave DHS' operational agencies to figure out their technology needs largely on their own. As competent as these agencies are at their core missions, they are comparatively ill-equipped to be engines of technological innovation. They simply lack the expertise, resources, and time to invent new systems themselves or to find out about innovations in the private sector that might be relevant to their mission. There are, of course, exceptions (such as U.S. Customs and Border Protection's Air and Marine Operations Center), which self-initiate and find creative solutions. But the Department is not structured to support them, and, once the Department inserts itself in their efforts, it ends up compromising the effort through cumbersome processes, reviews, and red tape.[9] Rather than truly pursue an innovation mission, the agencies tend to fall back on known contractors to support their needs. Recycling through a handful of large companies may create some efficiencies, but it ultimately blinds DHS components to much of the breadth of private sector innovation and options.

Nor is DHS an environment conducive to the risk-taking necessary to identify and/or develop technology. Technological innovation is hard, and it takes an acceptance that a large number of projects will fail. A venture capital fund might invest in dozens of companies with the hope of finding a single winner.[10] Although no government agency, even the Department of Defense (DOD), takes project failure well, DHS is particularly risk averse. DHS has a high level of congressional oversight with over 110 committees and subcommittees watching it,[11] along with the usual departmental, agency, and Government Accountability Office inspectors. Under this scrutiny with the political blowback for a failed program, there are huge disincentives for S&T or any DHS agency to take chances or fund research that might fail. The result is an emphasis on grants and programs that "succeed," in that they achieve all of the detailed goals in their workplans and respond to detailed requirements, but which do not necessarily provide useful new technology to operators.

§ S&T initially had a sub-component to emulate, at least in part, the Department of Defense's Defense Advanced Research Projects Agency (DARPA): the Homeland Security Advanced Research Projects Agency (HSARPA). From the outset, it suffered from a lack of a clear identity and mission, and it was neither structured nor supported to support robust research and development. *See* Dana A. Shea, *The DHS S&T Directorate: Selected Issues for Congress*, R43064 (Washington, DC: Congressional Research Service 2014): 17; Michael Myser, "Don't Call it DARPA," *WIRED*, January 1, 2004. HSARPA has been subsumed as part of an S&T reorganization. *See* U.S. Department of Homeland Security, *FY 2021 Budget in Brief*: 71.

There is significant reluctance throughout much of the private sector to working directly with the government, and this is particularly true for startup companies. A government contract might be a business changing opportunity, but more often than not vast cultural differences, bureaucratic inefficiencies, and regulatory compliance make such opportunities a bad return on time invested. As validated by one of the author's own experiences in a startup company, private investors want to know when government contracts could materialize and how much they will be worth. Short of this, they want to see clear partnership opportunities and pilot projects with government entities. Because the DHS-industry partnership processes are so unpredictable and constricted, it effectively closes off DHS business to all but the most heavily funded and connected new companies; no startup founder can expect investors to accept the kinds of year-long delays or sudden changes in priorities that are common in these processes. The DHS officials involved in these programs are often either unaware of or unconcerned with the impact of their actions on startups and small businesses.

Data collected by the National Institute of Standards and Technology (NIST) demonstrates the technology-innovation deficit at DHS as compared to other federal agencies (many of which would not themselves be considered innovation drivers). The most recent report, analyzing fiscal year 2016 data, shows DHS at the bottom as measured by budget committed to research:

Federal Obligations for R&D: By Agency FY2016 ($ million)[12]

All Agencies	$115,040
DOD	$44,749
DOE	$11,601
HHS	$32,216
NASA	$12,404
USDA	$2,358
DOC	$1,351
DOI	$857
VA	$695
DOT	$937
DHS	$532
EPA	$508

The chart below shows inventions and new technology disclosed by agencies to NIST from 2008 to 2015. DHS—the third largest department in the government—is consistently among the lowest producers.

Invention/Technology Disclosures by Federal Agency[13]

	FY08	FY09	FY10	FY11	FY012	FY13	FY14	FY15	FY16
USDA	133	154	164	152	160	191	117	222	244
DOC	40	41	34	26	60	41	47	61	64
DOD	1018	831	698	929	1078	1032	963	781	874
DOE	1460	1439	1616	1820	1661	1796	1588	1645	1760
HHS	447	389	363	402	352	320	351	321	320
DHS	10	32	7	38	40	20	36	15	17
DOI	7	4	5	5	10	9	6	7	8
DOT	3	3	1	2	2	13	3	0	0
VA	164	150	168	191	310	282	289	217	239
EPA	9	8	5	8	18	8	5	7	6
NASA	1324	1412	1735	1721	1656	1627	1701	1550	1554

Analysis

DHS' low innovation output is alarming because of the particularly urgent need for research into technologies to counter current threats to the homeland, asymmetric and otherwise. This includes nonstate actors like criminal organizations and terrorists, as well as proxies of malicious states who cannot compete militarily with the United States. Vulnerabilities are growing across numerous threat vectors. The following represent some of the most critical areas and those which lack an effective system to spur the needed research to counter them.[¶]

1. Biological weapon and pandemic disease response. The threat landscape around disease continues to become more concerning, and all the more so now given the COVID-19 pandemic. The threat includes both naturally occurring disease and manmade, biological weapons. The technological advances in biological laboratories have been so great that small laboratories can now do things that a few decades ago required the resources of a nation-state.[14] As a result, nonstate actors may now be able to develop infectious biological weapons that could quickly cause mass panic and overwhelm medical response capabilities. Relatedly, naturally occurring / evolving disease continues to present a critical danger across the globe. As COVID-19 has demonstrated, advances in the efficiency and throughput of commerce and travel will accelerate the spread of disease and exacerbate an outbreak with the possibility of mass casualty / mortality rates. Although detection and response has been improved, significant gaps remain in treating and stopping the spread of novel diseases.[15]

   New technological solutions are urgently needed to counter these threats. This would include rapidly developing and distributing testing, developing new vaccines more quickly, solutions to deploy vaccines and other medicine

¶ We recognize that DHS is not the lead agency for each of these issues. Our focus is on homeland security threats and not the specific roles and responsibilities of different agencies.

at scale and around the country in a crisis situation, technological solutions to the challenges of contact tracing and monitoring potentially exposed people, dual use facilities that can quickly produce medical supplies, and ways to monitor and respond to the release of detailed information about dangerous diseases (such as when Canadian researchers published a paper providing a detailed description of how to make a smallpox variant[16]).

2. Radiation detection in cargo and conveyances. Although often viewed as a doomsday-type scenario, the developed world must directly and aggressively confront the possibility that a nonstate actor, such as a terrorist group, obtains a radiological dispersal device ("dirty bomb") or nuclear weapon. These scenarios are very different, but they share common threads. Most importantly, they can and must be actively planned against, unlike a nuclear missile attack from a state which would be so devastating that it can only be prevented by the deterrent of a massive response.[17] Radiation detection systems throughout travel networks and supply chains are still limited. For example, cargo containers are only checked after arrival at a U.S. port,** and many small aircraft or boats are not checked at all. In the case of either type of attack by a nonstate actor, there would be a need for field hospitals and medicine to treat the injured on a likely mass scale; transportation and housing for thousands, if not millions, of displaced people; complex and expensive clean up requirements (if remediation is even possible); and an overwhelming need for improved detection systems to ensure that another device was not allowed to enter the country (of course, the detection requirement applied before the first device arrived).

3. Transnational organized crime and nonstate proxy organizations. Organized crime has globalized and become much more decentralized, better resourced, and dangerous for civilians.[18] As the rewards for criminal activity increase—exemplified by the tens of billions of dollars made by Mexican cartels supplying narcotics to the American market—the reach of and damage caused by these groups will continue to escalate. The potential for mass harm is amply demonstrated by the fentanyl crisis: the federal government still lacks the technology to reliably detect fentanyl in the cross-border movement of goods and people.[19] Preparing for the continuing growth of transnational crime and mitigating its impact on civilians will be enormously important. This could include countering money laundering, identifying perpetrators and victims of human trafficking, gathering intelligence about members of these organizations from publicly available sources, new technologies and approaches to detect narcotics and other contraband within supply chains, and sophisticated systems to allow government and companies to detect and stop internal corruption.[20]

4. Critical infrastructure and systems. The digital revolution has introduced heretofore unimagined fragility and vulnerabilities into essential systems through the explosion of digital networks and the replacement of engineering processes with software. The tragic debacle of Boeing's 737 MAX demonstrates the change: in the past, the plane would have been tested to no-fail engineering standards rather than relying on software fixes to design problems. The vulnerabilities attendant to the increased reliance on software is a problem when it causes disasters directly, but it is even more concerning when you imagine a hostile actor exploiting the software that now operates cars, airplanes, power plants, water treatment facilities, pharmaceutical manufacturing, food supply chains, and nearly everything else that modern life involves. Russian attempts to infiltrate the electric grid and other utilities are one example of the vulnerability.[21] These types of risks—i.e. risks inherent to the change to "software" based systems—are not what most private cybersecurity companies work on. The cyber security community focuses on monitoring networks to identify

** This is the type of threat for which Mr. Rohrbaugh's startup company, Lantern UAS, seeks to provide a solution.

and stop intrusions and "active defense" (where cyber-attacks are disrupted by penetrating the networks of cyber criminals and stopping them before they begin), and not increasing the resiliency of the systems themselves.

The innovation gap facing the homeland security community is daunting, but the current dysfunctional state of affairs is not preordained. Other government agencies, in particular DOD and the Intelligence Community, have confronted similar challenges and found ways to mitigate them. Even if imperfect, their experiences show that the government can build relatively robust technology pipelines. Two of the more well-known examples are DOD's Defense Advanced Research Projects Agency (DARPA)[22] and In-Q-Tel[23], which supports the national security community. National security departments also have a more established track-record of effective university partnerships, including with flagship research institutions. A now underappreciated example of a truly effective public-private innovation partnership was AT&T's Bell Laboratories. Bell Labs made critical contributions to the country's security through invention and innovation, and much of its work ultimately had important dual use applications for the civilian sector.[24]

Of course, DHS is not and will never be funded like DOD. But with the proper focus and structure, substantial improvements can be made with relatively modest investments. Because DHS cannot throw money at problems the way DOD does, it is even more urgent for the Department to deploy a thoughtful innovative approach that effectively taps into the innovation and technology development boom in the private sector.

Recommendations

Recommendation 1: DHS needs to break its overreliance on well-known, legacy government contractors so it can effectively partner with a broader cross-section of the private sector.

DHS should overhaul its private sector engagement to create understandable and efficient way to do business that make it accessible to nontraditional contracting partners. DHS should focus on encouraging and leveraging dual use technology and opportunities to modify technology that has been established in other contexts for its missions. Rather than recreate the wheel by building something itself, DHS should buy existing technology. DHS has made some recent progress in this area (for instance, leveraging Section 880 authority granted to DHS under the National Defense Authorization Act of 2017[25]), but much more needs to be done. This change in approach requires the following shifts:

1. Encouraging explicitly the development of dual use technologies and approaches that could lead to technologies that are commercially viable in the private sector as well as government.

2. Establishing clear preferences for modifying existing technologies that are proven in other areas for DHS purposes, rather than building systems from the ground up.

3. Establishing new programs that allow companies with promising technologies to demonstrate them outside of the incredibly complex world of prime contractors and contract vehicles.

4. Changing how the Department solicits the private sector away from prescribing a solution through detailed requirements to describing problems for which industry can propose solutions.

5. Consolidating departmental management of technology responsibilities to encourage cross-component efficiencies and ensure that contractors are not simply engaged in an end-run with individual agencies.

Recommendation 2: Congress needs to give homeland security research and development the attention and financial support it deserves.

Congress must fund research and development that supports the homeland security enterprise at a level commensurate to its importance. For example, in 1991, Congress passed the Cooperative Threat Reduction program, better known as the Nunn-Lugar Act, which provided funds to secure nuclear materials in the former Soviet Union and naturalize Soviet nuclear scientists. In 2014, DOD, DHS, and DOE spent $1.6 billion on non-proliferation programs.[26] This seems like a major investment, but given the impacts to the United States should a nuclear attack occur, the investment should be much higher. Also, most of these funds were not spent on what is arguably the most urgent part of the problem: establishing an effective screening regime that would reliably prevent a device from being smuggled into the United States. By way of comparison, the U.S. government spends almost $90 billion on missile defense programs,[27] and the wars in Afghanistan and Iraq since 2001 have cost $5.9 trillion.[28] Other examples of insufficient financial commitments abound: pandemic preparedness and response, cyber resiliency, election security, and countering narcotics smuggling and transnational criminal organizations, among many others.

Recommendation 3: Policymakers need to encourage a culture that understands and supports smart risk taking.

There will always be a need to identify waste, fraud, and abuse, but congressional and Executive Branch overseers need to shift their focus away from demanding reporting and finding and punishing failed entrepreneurial effort to making sure DHS is effectively seeding innovation and opening opportunities up to companies outside of the circle of established contractors. So long as a "gotcha" culture predominates in oversight, DHS will never be able to effectively drive and create openings for innovative technological approaches to the Department's most pressing priorities.

Recommendation 4: Congress needs to reallocate resources for cybersecurity to DHS.

Unless the responsibility for security of civilian networks is going to be moved to somewhere else in government (e.g. DOD), DHS needs to be given resources necessary to execute its responsibilities. The center of gravity in U.S. cybersecurity continues to be NSA/Cyber Command because they have received the vast majority of resources and have the greatest capabilities.[29] They are legally prohibited, however, from operating on domestic systems to close vulnerabilities, and they are strategically focused on challenges from foreign states. This means that the organizations who receive nearly all of the cyber resources cannot address what is perhaps our most urgent cyber challenge. Civilian cybersecurity is an escalating and dire problem, and DHS's lack of capabilities to address a challenge on this scale is an argument for much greater investment, not less. Dismissing DHS as technologically incapable and incompetent at a mission for which it has never been given adequate resources is, on its face, unwarranted. Agencies taking on major new responsibilities always struggle and have failures, and Congress' responsibility is to make sure they are managing the process as effectively as possible, not to revert to strategies that are structurally incapable of addressing core problems.

Recommendation 5: DHS should have a dedicated, external partner that focuses on incubating technology from the private sector to support the homeland security enterprise.

DHS needs an effective interlocutor with the private sector. We understand the restrictions under which S&T operates, and it is precisely because of those constraints that we believe an innovation incubator should exist outside of the government as is the case with In-Q-Tel. The homeland security enterprise needs an accelerator that moves at the speed of the private sector and has the flexibility and nimbleness to adjust to rapid advances. Such an entity will require an initial infusion of resources, but the amount of money required would be relatively minimal (so-called budget dust). Over time, through fees, intellectual property licenses, and investment returns, the entity can grow and become self-sustaining.

This entity could seed the private development of these technologies in several ways:

1. Providing funding directly to companies. Funding could be structured in a number of different ways, potentially making venture investments or through convertible loans. This would make it possible for the entity to be self-sustaining if some of the investments succeeded. Alternatively, it could provide grants or other direct assistance, and then retain partial ownership or an exclusive license for intellectual property generated by the initiative.

2. Giving companies credibility and a stamp of approval from relevant experts, with both technological expertise and experience in government.

3. Connecting startups with different government entities and helping them understand requirements and opportunities. The entity would need to establish extensive connections to public safety officials at the state and federal level and obtain commitments from officials to allow the technologies it develops to be showcased to operators.

4. Working actively with established companies with significant research and development programs in the defense and intelligence space to identify potential dual use technologies, i.e. technology with a DHS/homeland security application

It is almost impossible to create an entity that can do this effectively within DHS; the level of oversight and bureaucracy involved would be suffocating. In particular, this entity would need freedom to fail at certain projects: by definition it would need to be able to provide financial support for technologies that may not ultimately succeed. Ambitious and cutting-edge research will always be unpredictable and result in more failures than successes. It also should not be based at a university because of the indirect costs, the inherent slowness and bureaucracy, and the difficulty of matching the interests and priorities of academic researchers with homeland security operators.

This could be a public / private partnership. There are a number of industries in which companies fund research and development that is relevant to homeland security challenges, and which could have an interest in the kinds of dual use technologies that would be developed. Our current problems, in short, are not insurmountable.

Endnotes

1 Jon Swaine, "Federal government spent millions to ramp up mask readiness, but that isn't helping now," *The Washington Post*, April 3, 2020.

2 Nate Bruggeman, "Congress needs bipartisan commission to fix Homeland Security," The Hill, Feb. 2, 2020.

3 David Inserra, *Congress Must Re-Set Department of Homeland Security Priorities: American Lives Depend on It* (Washington, DC: Heritage Foundation, Jan. 2017): 48-49.

4 Interview with authors, Jan. 24, 2020.

5 See, e.g., DHS Science and Technology (S&T) Directorate, "Department of Homeland Security (DHS) Small Business Innovation Research (SBIR) FY 20 Solicitation," Solicitation # 70RSAT20R00000008, Dec. 18, 2019.

6 DHS Science and Technology (S&T) Directorate, "Silicon Valley Innovation Program," last visited Apr. 4, 2010, https://www.dhs.gov/science-and-technology/svip.

7 Interview with authors, Jan. 24, 2020.

8 DHS Science and Technology (S&T) Directorate, "Welcome to the Centers of Excellence," last visited Apr. 4, 2020, https://www.dhs.gov/science-and-technology/centers-excellence.

9 Interview with author, Jan. 27, 2020.

10 See, e.g., Corporate Finance Institute, "How VC's Look at Startups and Founders," last visited Apr. 4, 2020, https://corporatefinanceinstitute.com/resources/knowledge/other/how-vcs-look-at-startups-and-founders/.

11 Paul Rosenzweig, "Streamlining Congressional Oversight of DHS," *Lawfare*, Apr. 2, 2018.

12 National Institute of Standards and Technology, *Federal Laboratory Technology Transfer Fiscal Year 2016: Summary Report to the President and the Congress* (Washington, DC: U.S. Department of Commerce, Sept. 2019): 3.

13 Data gathered from annual NIST reports, which may be found at https://www.nist.gov/tpo/reports-and-publications/annual-reports.

14 Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-first Century* (New York, NY: Knopf, 2008): 9, 232.

15 Sigal Samuel, "The next global pandemic could kill millions of us. Experts say we're really not prepared," *Vox*, Sept. 19, 2019.

16 Kai Kupferschmidt, "A paper showing how to make a smallpox cousin just got published. Critics wonder why," *Science*, Jan. 19, 2018.

17 Bobbitt, *Terror and Consent*: 127, 146.

18 Alan Bersin and J. Chappell Lawson, "Homeland Security and Transnational Crime," in *Beyond 9/11: Homeland Security for the 21st Century*, Chappell Lawson, Alan D. Bersin, and Juliette Kayyem, eds. (Cambridge, MA: MIT Press, 2020).

19 Office of the Inspector General, U.S. Department of Homeland Security, "Limitations of CBP OFO's Screening Device Used to Identify Fentanyl and Other Narcotics," OIG-19-67, Sept. 30, 2019; Scott Higham and Sari Horwitz, "The flow of fentanyl: In the mail, over the border," *The Washington Post*, Aug. 23, 2019.

20 Bersin and Lawson, "Homeland Security and Transnational Crime."

21 Kelsey Atherton, "It's not just elections: Russia hacked the US electric grid," *Vox*, Mar. 28, 2018.

22 Duncan Graham-Rowe, "Fifty years of DARPA: A surprising history," *New Scientist*, May 15, 2008.

23 Dan Verton, "Study: CIA's In-Q-Tel 'worth the risk'," *Computerworld,* Aug. 7, 2001.

24 Jon Gertner, "True Innovation," *The New York Times*, Feb. 25, 2012.

25 Office of the Chief Procurement Officer, U.S. Department of Homeland Security, "Commercial Solutions Opening Pilot Program Guide," June 15, 2018.

26 Mary Beth D. Nikitin and Amy F. Woolf, "The Evolution of Cooperative Threat Reduction: Issues for Congress," R43143 (Washington, DC: Congressional Research Service, June 13, 2014), 10.

27 David Ruppe, "Missile Defense Cost Rises by $21 Billion," Nuclear Threat Initiative, Apr. 15, 2005.

28 Amanda Macias, "America has spent $5.9 trillion on wars in the Middle East and Asia since 2001, a new study says," CNBC.com, Nov. 15, 2018.

29 Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York, NY: Simon & Schuster, 2016): 186-89.