FEBRUARY 2024

A THREAT LIKE NONE OTHER

The Development of Cybersecurity Policy and the Role of the Hewlett Foundation 1997-2023

BY GARRETT M. GRAFF [1]

[1] Journalist and historian Garrett M. Graff has covered and written about national security and cybersecurity for more than a decade, including as the editor of *POLITICO Magazine* and as a contributing editor at *WIRED Magazine*. He is the author, among other books, of *The Threat Matrix: The FBI at War*, and co-author of *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat.* Today, he serves as the director of cyber initiatives at The Aspen Institute, where he helped found the Aspen Cybersecurity Group, and helps organize the Verify Conference, among other projects.

AUTHOR'S NOTE

This paper attempts to trace the rise and major influences in cybersecurity policy during, arguably, the first quarter-century of the field — from roughly 1997 through to present day, 2023. Parts I through V explain narratively the major incidents, attacks, wake-up calls, and shifts in governmental and corporate policy, as well as the role and influence of the Hewlett Foundation's Cyber Initiative, which, from 2014 to 2023, was the lead philanthropic funder for cybersecurity policy. The final two sections of the paper, parts VI and VII, attempt to capture the major unanswered structural and philosophical questions that the field confronts today that future work will be needed to answer.

The William and Flora Hewlett Foundation invests in creative thinkers and problem solvers working to ensure that people, communities, and the planet can flourish. Our Cyber Initiative provides funding for the development of a cyber policy field that offers thoughtful, multidisciplinary solutions to complex cyber challenges for the benefit of societies around the world.

A THREAT LIKE NONE OTHER

PROLOGUE: EARLY WARNINGS (1990s-2000s)

Read a quarter-century later, few government reports have held up as well or read as presciently as that put together by chairman Robert "Tom" Marsh and the commissioners who made up Bill Clinton's 1996 President's Commission on Critical Infrastructure Protection. The commission had come together in the wake of two major terrorism incidents — one foreign, the 1993 World Trade Center bombing, and one domestic, the 1995 Oklahoma City bombing — to consider how the U.S. government should adjust to a new era of threats. The commission's final 190-page report, though, focused primarily on a subject that at the time almost no one was talking about: cyber.

At the time of the commission's work, the World Wide Web was just a few years old and most U.S. households were not yet online. Just 20 million Americans had access to the internet in 1996, most over dial-up modems, and those spent only about 30 minutes a month online.[2] Many of them were funneled online through America Online, which, with five million subscribers, was the nation's largest internet provider. ("We can be like Coca-Cola. We can become like Disney, like Nike, like an MTV," AOL co-founder Ted Leonsis promised the growing company's 1,500 employees during a rally at their Dulles, Virginia, headquarters in 1996.[3]) Yahoo!, the nascent internet's fourth most-popular page, relied on humans to taxonomize new sites as they came online, organizing the internet into clearly definable and hierarchal topic directories that users could browse to find what they needed. The first web-based email, Hotmail, launched the same month as the Marsh Commission, as it was known, began work in July 1996, and the 56K baud modem, a technological marvel, would arrive as the commission, headed by staff director Phillip E. Lacombe, readied its final report in 1997.

It was not at all clear to many people that this new online world had any meaningful vulnerability, some questioned whether these new threats were overhyped already. "If you shut off all the lights in Iowa for two hours, that's not going to bring the country to its knees," Martin C. Libicki, then at National Defense University, told CNN as the Marsh Commission started work. "If you stop Visa card purchases for an hour, that's going to inconvenience people, but it's not going to bring the country to its knees."[4] In his view, digital attacks — if and when they ever emerged — would be routine incidents, like natural disasters, that the country would weather in turn. "During the snowstorm in the Northeast, roughly a quarter of the country was out of work for half a week, and that did not bring the country to its knees. It is just one of those things, like earthquakes and hurricanes," Libicki said.

And yet a small corner of government officials were already imagining something worse. As Deputy Attorney General Jamie Gorelick warned in July 1996, "We will have a cyber equivalent of Pearl Harbor at some time, and we do not want to wait for that wake-up call."

[2] Farhad Manjoo, "Jurassic Web," Slate, February 24, 2009, https://slate.com/technology/2009/02/the-unrecognizable-internet-of-1996.html.

[3] David S. Hilzenrath, "AOL Fights to Retain Subscribers," Washington Post, September 16, 1996, https://www.washingtonpost.com/archive/politics/1996/09/16/aol-fights-to-retain-subscribers/55ed2d30-b8f3-41fd-b7e1-ac59965c0084/.

[4] Brian Barger, "U.S. to Prepare for Cyberterrorism Attacks, but Is it Necessary?" CNN, July 16, 1996, http://www.cnn.com/US/9607/16/cyber.terrorism/index.html.

The Marsh Commission pointed to emerging, new, and unique challenges in the online arena, and they labeled the new threats with the prefix "cyber," a term drawn from William Gibson's 1984 debut novel, Neuromancer. (One of the Justice Department lawyers assigned to the commission, Michael Vatis, who knew Gibson's work had urged the term upon the Marsh team.)

"A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend," the commission wrote in its introduction. The commission saw a world where more and more corners of the basic infrastructure of daily American life — electricity, telecommunications, and water systems; banks and finance institutions; 911 and emergency radio networks; and oil and gas pipelines and fuel pumps — the routine day-in, day-out systems that it said were "the foundation for creating the wealth of our nation and our quality of life as a people," were vulnerable to new attacks from new actors. Government services were beginning to amass "mega-databases of a highly confidential nature [that] contai[n] information on private citizens" that could be exploited by bad actors. And all of these shifts were happening at an accelerating pace — even in its earliest stages, the Information Age was already beginning to outstrip the capability of government to respond. Altogether, the modern moment, the commission said, was as profound a shift as the one that came after the bombings of Hiroshima and Nagasaki ushered the world into the atomic age.

"For most of our history, broad oceans, peaceable neighbors and our military power provided all the infrastructure protection we needed. But just as the terrible long-range weapons of the Nuclear Age made us think differently about security in the last half of the 20th century, the electronic technology of the Information Age challenges us to invent new ways of protecting ourselves now," the commission wrote in its final report, entitled "Critical Foundations." "We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power. National defense is no longer the exclusive preserve of government, and economic security is no longer just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between government and the private sector."[5]

Much of the nation's vulnerable critical infrastructure wasn't under government control — it was the responsibility of the private sector. And critical pieces of information to stop or prevent possible attacks was spread between the government and numerous different corners of the private sector. Information sharing in this new world, the commission concluded, would be key. "Our most important finding is the need to think differently about infrastructure protection," Tom Marsh, a retired air force general, told Congress in presenting the commission's findings. "Today's approach was designed to deal with the Industrial Revolution, then was adjusted to address the stabilization of America after the Civil War, the Depression, World War II, and finally the nuclear stand-off of the Cold War. None of those approaches is particularly applicable to the world as it looks through the lens of information technology in the third millennium."

One of the events that heavily influenced the Marsh Report was the Pentagon's experience in 1997, known as Joint Exercise Eligible Receiver 97. It pitted a Blue Team of defenders from the National Security Agency against an offensive team of NSA hackers, pretending to be attackers from North Korea, Iran, and Cuba. The Red Team targeted both U.S. critical infrastructure as well as military command-and-control capabilities using only then-publicly available computer tools. The military found itself off-kilter almost immediately, as the

[5] "Critical Foundations: Protecting America's Infrastructures," President's Commission on Critical Infrastructure Protection," October 1997, https://sgp.fas.org/library/pccip.pdf.

hackers succeeded beyond anyone's imagination. Even nearly 30 years later, many of the details of the exercise remain classified, but they were able to infiltrate networks at Pacific Command as well as power grids and 911 systems across at least nine major U.S. cities. "We had the Blue Team on the run by the third day," one of the Red Team targeting officers recalled later, adding, "It could have been a lot worse." Deputy Secretary of Defense John Hamre was shocked at the exposed vulnerabilities: "We do know that they were very successful in penetrating DOD computers. I mean, we physically got messages from the bad guys on our own computers."[6] As he said, "Eligible Receiver changed a lot of our consciousness about the vulnerability of cyberwarfare."

The exercise also warned early of some of the challenges that would bedevil the U.S. government in the years to come, particularly in terms of understanding where to draw lines between a military response and a law enforcement one. As one after-action report concluded, "It is not easy to judge the threshold between a criminal act (terrorist, hacker, etc.) or a series of criminal acts, and a concerted attack on the security of the United States. This is important in deciding whether jurisdiction belongs to law enforcement agencies or the DoD."[7]

The warnings of the Marsh Commission and Eligible Receiver, as well as startling computer intrusions of Pentagon networks — including especially two incidents, known as Solar Sunrise and Moonlight Maze — focused government and military attention on hacking and cyber threats for the first time.

It was, in many ways, already too late. While the networks that grew into the modern internet had originally been developed and funded with federal grants and Pentagon research efforts, the government had taken a largely hands-off approach to its development and accelerating spread and evolution in the 1980s and 1990s. In fact, the story of the internet in the years ahead would make clear that the network's original designers had systematically underestimated how it would and could be utilized by bad actors, from criminals to terrorists to hackactivists to adversary nation-states. This collective failure to recognize and address real safety and security vulnerabilities, the enormous failure of imagination to understand how a network built for a small group of trusted academic institutions and researchers who knew each other's first names would transform as it became the backbone of a wired society's daily life, would mean that the U.S. and Western governments, law enforcement, the Pentagon, private sector companies, and civil society would spend the next quarter century playing a desperate game of catch-up — a game of catch-up that still, today, is underway.

Indeed, the first warnings and subsequent follow-up actions like the Clinton administration's 2000 cyber-security strategy and the Bush administration's 2001 effort, known as the President's Critical Infrastructure Protection Board, barely penetrated the consciousness of the country in the years before 9/11, but in the wake of the September 11th attacks, the nation began to reimagine wholesale the security apparatus necessary for the 21st century.

In February 2002, less than two months after the fires stopped burning at ground zero in New York, some 50 scientists and engineers wrote to the White House and called for a Manhattan Project-style "Cyber-Warfare Defense Project" to secure the nation's new digital infrastructure, an investment they saw as topping $1 billion a year once it got running. "The goal of our proposed Manhattan-style undertaking would be to create a national-scale cyber-defense policy and capability to prevent, detect, and respond to cyber threats to our critical infrastructure. We mean Manhattan-style in several senses: national priority, inclusion of top scientists, focus, scope, investment, and urgency with which a national capability must be developed," they wrote, adding an ominous warning. "The clock is ticking."

[6] "Interview with John Hamre," Frontline, February 18, 2003, https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html.

[7] "Observation Reports Submitted by MajGen Byron, USMC," Joint Chiefs of Staff, June 1997, https://nsarchive.gwu.edu/document/16743-document-8-joint-chiefs-staff-observation.

While the desired urgency and scale of effort didn't emerge, the Bush administration did push forward a year later, in February 2003, with a 76-page "National Strategy to Secure Cyberspace," an effort built around three strategic objectives: "(1) Prevent cyberattacks against America's critical infrastructures; (2) reduce national vulnerability to cyberattacks; and (3) minimize damage and recovery time from cyberattacks that do occur."[8]

The goals seemed simple— and smart— enough, but how exactly the government would go about doing that would remain a challenge for years to come. In fact, even as the world economy and daily life digitized, and the information revolution accelerated beyond almost the wildest imaginations of those Cassandras of the 1990s, the fundamental goals and threats outlined in those earliest cyber reports and strategies would change little over the next two decades. The government, private sector, and civil society struggled to address the most basic questions that confronted those early warnings — debates, in fact, that continue to this very day.

[8] "The National Strategy to Secure Cyberspace," George W. Bush White House, February 2003, https://www.hsdl.org/c/tl/national-strategy-secure-cyberspace/.

I. NO ONE'S PROBLEM (2005-2010)

Those who invented the technologies and protocols that would grow into the internet in the latter half of the 20th century never realized the world that they were creating — a global system that would become the digital backbone of everything from banking and health care to government, telecommunications, and even, increasingly, the objects of our daily life, from refrigerators to automobiles. Instead, those early internet pioneers were primarily building tools for a small, trusted community composed of engineers and academics. Security was not just an afterthought but something to be actively mocked. As Janet Abbate, the author of "Inventing the Internet," said, "They thought they were building a classroom, and it turned into a bank."[9] At MIT in the early days, its network was password-free by design. David D. Clark, the internet's chief protocol architect from 1981 to 1989, recalled that of the seven key goals of the early network, security was not even mentioned.[10] For years, it wasn't even clear that the government had any meaningful role in policing these digital networks; in 1990, "Harper's Magazine" hosted an 11-day debate on the popular online bulletin board, the Well — the Whole Earth 'Lectronic Link — asking "Is Computer Hacking a Crime?"

By the early 2000s, though, the internet had established itself as a thriving center of commerce and communication, a vital tool for office workers in the private sector and government, as well as families, students, and nearly everyone in between. By then, it was becoming increasingly clear that, if anything, the Marsh Report had underplayed the challenge from bad actors. Criminals were beginning to carry out increasingly sophisticated financial frauds online, discovering that such digital crimes often came with both higher payoffs and lower risk than similar crimes offline. A digital bank robbery was more lucrative and less violent than holding up the neighborhood branch. So-called computer "worms" and "viruses" had wreaked havoc more than once on internet networks, drowning systems in traffic and forcing other users' connections to a crawl. Pioneering prosecutions of computer crimes by Justice Department prosecutors like Scott Charney and Kent Walker — two leaders who, in the decades ahead, would go to play huge corporate roles in the future of cyber policy — had begun to outline new rules of the road online, even though not all the cases went smoothly.

In April 2007, the modern cyber age began when Estonia chose to relocate a Soviet-era war memorial known as the Bronze Soldier of Tallinn. The Estonian government had decided that the statute, which was unveiled in 1947 and originally called the "Monument to the Liberators of Tallinn," should be relocated outside the capital city — a recognition that the half-century post-war occupation by the Soviet Army was viewed as its own dark chapter of history, rather than as a glorious moment of liberation from Nazism. The move inflamed the local Russian population and angered the neighboring government in Russia itself; street protests broke out in Tallinn and, then, on April 27th, government, financial, and media websites began to be knocked offline, as widespread so-called distributed denial-of-service (DDoS) attacks deluged the Estonian websites with fake traffic and swamped their servers. For some three weeks, Estonian websites struggled to keep even basic functions

[9] Craig Timberg, "Net of Insecurity: A Flaw in the Design," Washington Post, May 30, 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

[10] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," MIT Laboratory for Computer Science, March 14, 2013, https://web.mit.edu/6.033/www/papers/darpa.pdf.

online — a devastating and embarrassing moment for a country that had long touted its sophisticated internet capabilities and been branding itself as "e-Estonia" for its advanced online government systems and ease of use. The primary suspect in the DDoS attacks was instantly clear: Russia, or at least Russia-friendly hackers.[11]

For officials across the world, the incident was a wake-up call to the cyber threats long warned about in dry reports and computer circles. As Chris Inglis, then deputy director of the National Security Agency, recalls, "It's no longer theoretical, and it's no longer simply a criminal enterprise — this is now a tool of power being used by nation-states."

The Estonian attacks didn't exactly come out of the blue — warnings had been plentiful ever since the Marsh Report a decade earlier — but in 2007 the U.S. government remained so blind to cyberattacks that online attacks were not even listed among the 2007 "Worldwide Threat Assessment," the high-profile annual list of geopolitical risks, problem areas, and threats compiled by U.S. intelligence agencies and presented in boldface-name briefings to leaders on Capitol Hill. Finally, as 2008 began, the military and NSA were beginning to think hard about how "cyber" should be considered its own domain for military operations.

Then came the Pentagon's own embarrassing wake-up call: In October 2008, NSA officials found intruders had somehow accessed a classified Defense Department network, known as the Secret Internet Protocol Router Network, that was supposed to be fully separate from the public internet. It was the most serious breach they'd ever discovered and launched an 14-month, round-the-clock, no-holds-barred effort by the Pentagon; the NSA; and the NSA's director, three-star Air Force General Keith Alexander, to rid the hackers from U.S. networks, a project known as Operation Buckshot Yankee. The cyber threat, though, reached far beyond the Pentagon: In the midst of that year's presidential election campaign, Chinese government hackers targeted the networks and emails of both major party nominees, John McCain and Barack Obama, hoping to learn about their policy preferences and inclinations.

The NSA had realized early on that perfect computer security was never going to be possible. Inglis, who started with the NSA's National Computer Security Center in January 1986, recalls how early efforts to secure digital systems proved instead how many possible problems there were, between math, algorithms, compilers, and the end users (i.e., people) actually making choices about how to use systems. "All the sudden we kind of threw up our hands and said — and this is my contemporary words now — but, 'Security is not the goal. Defensible systems is the goal,'" he recalls. "We didn't call it cyber or cybersecurity in the day, but that was for me, my earliest kind of 'aha moment.' It's as much about the assignment of expectations to technology and doctrine — the people skills — as it is about getting the technology itself right." Now Buckshot Yankee and the Estonian incident forced the Pentagon and the NSA to rethink that balance of people, technology, and doctrine.

"Admiral Mike Mullen [the chairman of the Joint Chiefs of Staff] got it immediately — cyber isn't just a commodity in the corner like the motor pool that we make use to extend or kind of improve our mission performance. It's existential to our mission. Command and control is the very central nervous system of our operations," Inglis recalls. "He drove the thinking that we need to get serious about this and consider the possibility of not just describing cyber as a domain, but taking the necessary efforts to organize for that."

In 2009, Alexander convened a small team of promising mid-career officers — including Army Col. Paul Nakasone and Lt. Col. Jen Easterly, Navy Capt. T.J. White, and Air Force Col. Stephen Davis — to think through how the military should reposition itself for cyberspace. The group, who together came to be known

[11] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Cooperative Cyber Defence Centre of Excellence, 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

as the Four Horsemen, outlined a new military doctrine and organizational structure that would grow into U.S. Cyber Command, a stand-alone entity dedicated to fighting the nation's enemies online. For months, the team designed a work plan, org charts, and mission structures, and then developed a series of storyboards that they could use to brief D.C. stakeholders at the White House, Pentagon, and on Capitol Hill. ("It ended up being essentially a top-secret cartoon," Davis once told me.) By 2010 — a remarkably agile turnaround for the Pentagon — U.S. Cyber Command started up. The new command would be headed by General Keith Alexander, who would now be, in government parlance, "dual-hatted," as both the NSA director and the four-star commander of Cyber Command. The goal, at the time, was to use NSA's established capabilities in signals intelligence, networks, and code-breaking to give Cyber Command a running start on its own cyber mission to project power online. As Easterly recalls, "Cyber was going to be fundamentally grounded in the power of the cryptologic enterprise."

Cyber Command became just one part of a wider, stumbling series of moves across Washington as the government tried to orient itself to the new online threats. Ever since its creation in 2003, the Department of Homeland Security had struggled to figure out how to position itself in cyberspace. Even as its primary initial focus had been on physical attacks and terrorism, the department had tried to embrace the recommendations of the Bush administration's early cyber strategy and bring together efforts to protect critical infrastructure both offline and online. DHS's first assistant secretary for infrastructure protection, Robert Liscouski — a onetime homicide detective who had moved into the private sector and headed up Coca-Cola's information security program before moving into government — created the National Cyber Security Division (NCSD), a component tasked with protecting the government's civilian computer networks through a network monitoring system known as Einstein. The NCSD director position, though, was never empowered and remained stretched thin resource-wise, and its first occupant, Amit Yoran, lasted just a year before he quit with a single day's notice in October 2004. NCSD never had a permanent leader again.

Finally, recognizing the position needed more authority and resources, DHS created what it called the National Protection and Programs Directorate (NPPD) in 2007 and declared it would be the government's primary organization focused on "detecting and eliminating threats to critical physical and cyber infrastructure." Suddenly, the cyber arena was getting crowded — and no one seemed to know where to draw the lines between DHS, NSA, and the law enforcement components like the FBI and the Justice Department. Who was responsible for what?

That question, of the right level and approach to the government's involvement in tech policy and cybersecurity, wasn't one just for the executive branch, and the uncertainty surrounding tech and cyber policy was hardly a one-way street. Congress, dominated by aging lawmakers generally removed from the information revolution that was sweeping the country (the Senate in 2007, during the 110th Congress was the oldest it had ever been, with an average age of 62, a record that has only continued to grow in years since), remained remarkably blind to the changes and challenges ahead. In 2006, Senator Ted Stevens, the top Republican on the Commerce Committee charged with regulating the internet — who once declared that someone had sent him "an internet" — infamously, during a debate on net neutrality, referred to the internet as "a series of tubes." And in November 2007, while campaigning for president, Senator John McCain said in a debate hosted by YouTube that he planned to "rely on a vice president" for guidance on less-important issues like "information technology, which is the future of this nation's economy." (This remarkable level of political naiveté about the internet was hardly a passing concern or phase: As late as 2018, during a Senate hearing with Facebook CEO Mark Zuckerberg, Utah Senator Orrin Hatch asked how the social network made money. "Senator, we run ads," Zuckerberg said simply.)

At the same time, the rising giants of Silicon Valley found themselves just as confused and confounded about how to navigate Washington. In the summer of 2006, as Congress took up the issue of net neutrality that led to Stevens' infamous comment, Google had just a four-person office in D.C. When its co-founder, Sergey Brin, journeyed to Washington to lobby Congress, the 31-year-old Brin — then the world's 16th-richest person —

found he couldn't land meetings with most of the key senators, including Stevens, because he hadn't realized how much lead time was necessary to schedule them. (The Washington Post mocked him as a "tourist."[12]) As he said at the time, "We are a seven-year-old company. Having policy that really significantly affects us is kind of new to us. We are doing the best we can."

In its final year in office, 2008, the Bush administration launched the Comprehensive National Cybersecurity Initiative (CNCI), a multibillion-dollar effort that was carefully organized through months of meetings by Melissa Hathaway, a respected cyber leader working as senior advisor to Director of National Intelligence Mike McConnell.

The effort was meant to boost investment in digital defense and offense across government. After years of emphasizing a bottoms-up cyber policy that relied on much-vaunted "public-private partnerships" and encouraged the private sector to develop "their own strategies to protect the parts of cyberspace on which they rely," the CNCI was the first time that the White House seemed to recognize that the U.S. government itself must play a leading role in securing cybersecurity.

Until then, much of the U.S. government's cyber posture seemed rooted in the nuclear age, imagining that bad actors could be deterred online in the same way that "mutually assured destruction" had kept the peace during the Cold War. (As the Bush administration's 2007 National Strategy for Homeland Security read, "Actors can be deterred and dissuaded from conducting attacks if they perceive that they are not likely to achieve their objectives or that the costs of their efforts are too high.") But it was increasingly clear that deterrence alone wasn't going to work — the government needed to be taking more active measures to stop bad actors in cyberspace.

As the Obama administration took office, a commission at the Center for Strategic and International Studies — co-chaired by Reps. James R. Langevin and Michael T. McCaul, as well as Scott Charney and Lt. General Harry Raduege, USAF (Ret) — urged the new president to consider that not only was cybersecurity "now a major national security problem for the United States," but that it was, in fact, "one of the most urgent national security problems facing the new administration."[13] In its 96-page report, the commission argued that cybersecurity should be modeled on how the government focused on nuclear nonproliferation: No one agency or institution was in charge of nonproliferation efforts, but instead key agencies played specific roles as delineated by executive orders and legislation, with everything coordinated through the White House. It urged the creation of a new National Office for Cyberspace at the White House, akin organizationally to the Office of Science and Technology Policy, and a new Cybersecurity Directorate at the National Security Council, overseen by an assistant to the president for cyberspace. Such an office, they argued, would help protect against the militarization of cyberspace by keeping cybersecurity inside an operational civilian team at the White House, rather than turning it over entirely to the Pentagon or NSA.

[12] Arshad Mohammed and Sara Kehaulani Goo, "Google Is a Tourist in D.C., Brin Finds," Washington Post, June 7, 2006, https://www.washingtonpost.com/archive/business/2006/06/07/google-is-a-tourist-in-dc-brin-finds/2ce2f66c-a394-4292-9222-e8a353b7a27a/.

[13] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, December 2008, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Despite the commission suggestions and numerous other such transition warnings on cybersecurity, the Obama White House was slow to act. Like too many such efforts before it, CNCI stalled as the administrations changed. Melissa Hathaway, now the Obama administration's senior cyber aide, quit in August 2009 after months of waiting for action on the cyber strategy. ("I wasn't willing to continue to wait any longer, because I'm not empowered right now to continue to drive the change," she told the Washington Post. "I've concluded that I can do more now from a different role."[14]) A Government Accountability Office study in 2010 emphasized the wildly ill-defined roles and responsibilities across the government agencies handling cybersecurity, as well as a lack of measures of effectiveness that would help the government understand whether cybersecurity was improving. The Obama administration seemed initially committed to the back-seat posture the government had long had in cyberspace. Rob Knake, part of the cybersecurity team on Obama's National Security Council, called it the "Home Depot model" of working with the private sector: "You can do it, we can help."

A unique cross-agency effort early in the administration, though, sought to bring better clarity and energy to the internal government efforts. Then-FBI Director Robert Mueller convened a meeting with DHS Secretary Janet Napolitano and the NSA's director, Gen. Keith Alexander, to hash out each other's lanes in cyberspace. Mueller, who had started as FBI director just a week before 9/11 and driven a giant shift in the bureau's focus toward terrorism thereafter, had watched the steady rise of cyber threats. It was an area that had long intrigued him: He had started the Justice Department's first computer crime unit in 1991, while serving as the assistant attorney general for the criminal division, after reading "Cuckoo's Egg." The seminal 1989 book on hacking, it traced how a computer manager at the Lawrence Berkeley National Laboratory had identified and traced an intrusion by a KGB-linked hacker.

There were too many players with too many hats across government and everyone needed to better understand their own lanes. Together, they drew what came to be known as "the bubble chart," which was ultimately revised 75 times before all three agreed on their respective roles. As John Carlin, a top Mueller aide, would later summarize the chart: "DHS would be responsible for fixing, mitigating, and preventing attacks through information sharing and also for aiding with remediation after an attack. The FBI and the Justice Department would be responsible for the investigation and prosecution of an attack, as well as for deterrence. The Pentagon and NSA would focus on overseas disruption." It was the start of a more unified governmental approach, even if a lot more progress needed to be made.

Yet even as the government struggled to position itself regarding these new cyber threats, the depth and breadth of the threat was becoming increasingly inescapable.

[14] Ellen Nakashima, "Cybersecurity Official Resigns Over Delays in Appointment," Washington Post, August 4, 2009, https://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080302697.html.

II. THE AWAKENING (EARLY 2010s)

As the Obama administration unfolded, there was a steady drumbeat of cyber warnings and attacks month by month — and sometimes even week by week. These ranged from annoyances from the anonymous hacker collection LulzSec, which shut down the CIA homepage and hacked the U.S. Senate in June 2011, to more serious hacks of the Energy Department in the summer of 2011 and the Commerce Department in February 2012, which forced those cabinet departments to disconnect their computers from the internet temporarily. That same February, the government publicly discussed how Chinese hackers had penetrated Pentagon systems and defense contractors to steal classified information about the development of the F-35, and the Department of Homeland Security saw its website knocked offline by the hacker collective Anonymous.[15]

The uncertainty of federal responsibility and resistance from the private sector to the government's involvement came to a head in 2012 in the debate over what would be Congress' first significant foray into cybersecurity legislation. The so-called Lieberman-Collins bill, named for its lead co-sponsors in the Senate, Maine Republican Susan Collins and Connecticut independent Joe Lieberman, would have required mandatory minimum cybersecurity standards for critical infrastructure.

The first version of Lieberman-Collins, "Protecting Cyberspace as a National Asset Act of 2010," had been introduced in June 2010, with Lieberman saying, "The internet may have started out as a communications oddity some 40 years ago but it is now a necessity of modern life and, sadly, one that is under constant attack. Today, Senators Collins, Carper, and I are introducing legislation which we believe would help secure the most critical cyber networks and therefore all Americans." But the legislative push seemingly stalled after the 2010 midterms, as Republicans originally sympathetic and supportive of the bill balked anew following the strong wave of anti-government Tea Party candidates that flowed into Congress in 2011.

Soon, Lieberman-Collins became one of a whole series of competing bills that appeared in both the House and Senate, addressing not just critical infrastructure, but other priorities like information sharing, cybercrime statistics and metrics, and more. "About the only certain thing is that the question of cybersecurity is likely to set a new world record for competing bills with bipartisan co-sponsors. Everyone agrees the problem is important – they just don't agree at all on what to do about it," legal scholar Paul Rosenzweig wrote in analyzing the state of the legislation in 2012.[16]

In the summer of 2012, Lieberman and Collins introduced a new, watered-down version of the legislation that Senate Majority Leader Harry Reid wanted to bring up for a vote. Along the way, proponents and opponents of the regulatory approach debated how and where to draw the lines and definitions of what infrastructure was

[15] Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government," Heritage Foundation, May 24, 2012, https://www.heritage.org/defense/report/the-alarming-trend-cyber-security-breaches-and-failures-the-us-government.

[16] Paul Rosenzweig, "Cybersecurity Legislation - Big Issues at the 10,000 Foot Level," Lawfare, January 31, 2012, https://www.lawfaremedia.org/article/cybersecurity-legislation-big-issues-10000-foot-level

truly "critical," a question that would continue to dog the field to the present day. Stewart Baker, a former NSA general counsel, pointed to the oddity of limiting the bill's targets to systems that would cause an "extraordinary fatalities" (what exactly was an "ordinary" number of fatalities in a cyberattack?), and the Center for Strategic and International Studies' James Lewis complained how creating a list of entities that would be well-protected was a "bit like writing a targeting list of our opponents" of which entities would likely be poorly protected.

Through the summer, a steady stream of administration leaders raised alarms about the cyber threat. Gen. Keith Alexander said, on a scale of one to 10, the nation's digital defenses were no more than a three, and four former Republican officials — former NSA and CIA Director Michael Hayden, former Homeland Security Secretary Michael Chertoff, former Director of National Intelligence Adm. Mike McConnell, and former Deputy Defense Secretary Paul Wolfowitz — lobbied hard for the legislation, saying it was critical to securing vulnerable nationally significant private infrastructure.

Yet even in its watered-down stage, the bill was still opposed vehemently by the U.S. Chamber of Commerce and other business groups, and Senate Republicans, led by Arizona's John McCain, moved successfully to kill the bill that summer; it failed in an August 2012 vote mostly along party lines. "Rarely have I been so disappointed in the Senate's failure to come to grips with a threat to our country," Collins said.

It was only weeks after the decisive senate vote that the country received a new wake-up call to the vulnerabilities and threats from the cyber realm. In September 2012, a mysterious group known as the Cyber Fighters of Izz Ad-Din Al Qassam announced it had launched a DDoS attack on Bank of America to punish the United States for a YouTube video known as "Innocence of Muslims." The initial DDoS attack came just days after global protests against the anti-Muslim video and a confusing deadly attack on the U.S. consulate in Benghazi, Libya, that killed the U.S. ambassador, but it quickly became clear that whoever was behind the digital assault wasn't who they said they were. In the days ahead, the DDoS attacks spread against some four dozen other U.S. financial firms, including JPMorgan Chase, PNC Bank, and Capital One.

That October, Defense Secretary Leon Panetta gave what would be the first major address on cybersecurity ever by a defense secretary. He echoed the words that Jamie Gorelick had used more than 15 years earlier as he warned of "a cyber Pearl Harbor" and the possibility of a cyber strike "as destructive as the terrorist attack of 9/11." Standing at the USS Intrepid in New York, Panetta said the nation was in a "pre-9/11 moment" in terms of cyber, and that he hoped the country would respond better to the growing warning signs. As he said, "Before September 11, 2001, the warning signs were there. We weren't organized. We weren't ready and we suffered terribly for that lack of attention. We cannot let that happen again."

The DDoS attacks continued through the fall and winter, and as they persisted, the U.S. government pointed the finger at Iran.

Iran had been actively escalating its online threat since 2007. The pro-democracy Green Movement in 2009 and the following year's Arab Spring had demonstrated to Iranian leaders how destabilizing the internet could be to authoritarian regimes, a warning that caused the regime to invest heavily in targeting internal dissidents online. Their growing efforts quickly attracted attention and alarm. In 2011, Iranian hackers managed to hack the Dutch firm DigiNotar, a provider of online security certificates, and spoofed hundreds of websites, from Gmail to the CIA.gov site. The next year, Iran launched one of the first-ever destructive cyberattacks, a carefully timed assault on the Saudi energy giant Aramco, using malware known as Shamoon to paralyze their computer networks. Tens of thousands of computers were destroyed and for months the company had to operate with typewriters, fax machines, and paper interoffice mail.

The DDoS attacks weren't anything close to the Shamoon attack; they were what Inglis calls the equivalent of "Nerf balls in cyberspace," an annoying and vexing problem with real opportunity costs that, by design, stopped well short of any permanent harm. Both the U.S. government and the targeted firms grew frustrated. U.S. government officials were puzzled by how unprepared even the nation's largest, best-funded financial

institutions seemed for such a routine online nuisance, and the private sector firms, in turn, were frustrated by the government's lack of help. "The government proved slow to take action and slow to help the victims," recalls John Carlin, then the chief of staff at the Justice Department's national security division. "We didn't have good vehicles, mechanisms, or relationships to convey information back to the private sector — either about what we were seeing across the spectrum or about what we knew about the defensive measures Wall Street firms could take to mitigate the attacks."

As Chris Inglis recalls, "The U.S. government made an intentional choice at that point to not stand in. It knew with great precision what they were doing and actually had the means to shut it down, but to intervene it would have to actually operate in, what it described at the time, as 'the sovereign space of the private sector,' and it chose not to do that." It was a signal moment in terms of where the U.S. government believed the lines existed online at the time — officials believed that they didn't have the right or responsibility to step in and defend private U.S. companies from foreign adversaries online. It was a decision that nearly everyone involved would soon come to understand was wrong.

For one thing, much to the horror of the U.S. government, several of the financial companies took it upon themselves to organize their own defense — targeting themselves the people they believed were causing them harm, launching so-called "hack back" attacks, sometimes at digital networks that turned out to have nothing to do with the Iranian infrastructure. It was an important wake-up call to the U.S. that the private sector didn't necessarily have the wherewithal to respond and defend themselves from nation-state actors. Moreover, the U.S. quickly realized that it didn't *want* U.S. companies going toe-to-toe with Tehran on their own. As Iran saw it, in fact, the DDoS attacks were really a response and retaliation for the U.S.' own covert cyberwar against its nuclear program. While the US officially continues to deny involvement, reporting by journalists like the New York Times' David Sanger have in the years since outlined an effort known as Operation Olympic Games, in which the U.S., apparently with the help of Israel, had launched malware against Iran's uranium enrichment program, targeting its centrifuges with a tool that caused them to malfunction. The attack — now widely understood to be the first destructive cyberattack, one launched by the U.S. itself — caused Iran to hit back with the DDoS attacks at the nation Iranian officials believed had attacked it. "The private sector found themselves caught up in something that really was a government-to-government, nation-to nation-issue, despite the fact that it happened to play out on the private sector's front lines," Inglis says. "That was a big lesson there for the United States — the doctrine began to decisively turn toward the U.S. government had a responsibility to defend the private sector, even in cyberspace."

The ongoing attacks also spurred the financial industry to commit greater resources to its own defenses through a cross-sector model that was to become increasingly popular, known as an ISAC (Information Sharing and Analysis Center), an independent, member-driven, nonprofit. In the years ahead, the financial sector ISAC (FS-ISAC), would work alongside another industry group created in the wake of the attacks, the Financial Systemic Analysis and Resilience Center (FSARC), and become the industry gold standard for a united, collaborative industry cyber defense operation.

NIST CYBERSECURITY FRAMEWORK

The Iran DDoS attacks drove high-level official interest in cybersecurity and critical infrastructure and the period of 2013-2014 would come to mark perhaps the most significant turning point in the U.S. government's focus and involvement in cybersecurity. In February 2013, even as the Iran attacks continued, the White House released Executive Order 13636, aimed at bolstering cybersecurity of critical infrastructure and achieving, through more voluntary procedures, much of the same impact as the failed Lieberman-Collins legislation. "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront," the order read. "It is the policy of the United States to

enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[17]

While parts of the executive order dealt with improving information sharing and protecting privacy and civil liberties online, its most lasting and transformative impact would come from its call for the secretary of commerce and director of the National Institute of Standards and Technology (NIST) to establish a Cybersecurity Framework for the private sector built around "voluntary consensus standards and industry best practices." In April that year, NIST, a nonregulatory agency, convened industry thinkers and corporate policy and technical experts for the first time, and outlined a six-month series of workshops that would collaboratively develop the framework. At first, industry, still wary of the Lieberman-Collins approach, was highly skeptical of the effort, assuming that it was a stalking horse for mandatory government regulations to come, but as the multiday workshops began, trust began to build.

"We treated it as an exercise to say, 'Okay, let's figure out what existing standards and guidelines and requirements are out there and let's try to coalesce around things that make sense for critical infrastructure to follow.' And then to the extent that there are gaps, we can identify those gaps and begin working towards them," recalls NIST's Adam Sedgewick, who helped lead the development of the framework. "The first couple of meetings are really contentious because industry thought it was kabuki theater, and we were just going to turn around and immediately turn it into regulation. We really had to work hard to generate trust and understanding that that was not the intent here."

Meeting by meeting, though, the industry representatives found that NIST was actually listening to them and that the draft pieces of the framework reflected an honest reckoning with the cyber challenge. "The physical change in the room as the private sector realized that this was going to be a genuine collaborative effort was remarkable. I physically watched people lean in over the course of the first few days after slouching in their chairs," recalls Jeff Greene, who participated in the workshops as Symantec's vice president for global government affairs and policy. "The body language changed when they saw the level of interaction that they were getting from government."

Multiday workshops unfolded throughout the year at Carnegie Mellon, the University of California, San Diego, the University of Texas at Dallas, and North Carolina State in Raleigh. "There was really, really positive energy near the end of the workshops," Sedgewick recalls, and participants even made up t-shirts mimicking a band's concert tour shirt, with a large eagle on the front and listing the draft framework's stops, coast to coast.

Version 1.0 of the NIST Cybersecurity Framework was released in February 2014 and it was designed to drive specific security outcomes through a five-stage function cycle: Identify, Protect, Detect, Respond, and Recover. "Functions organize basic cybersecurity activities at their highest level," the framework explained. "They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity."

[17] "Improving Critical Infrastructure Cybersecurity," Executive Order, Barack Obama White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Over the next year, Sedgewick was on a plane nearly every week presenting the framework at one industry conference or another — he took just a week off between February and October. The NIST Cybersecurity Framework would become one of the significant industry tools to organize, shape, and measure cyber investment and the maturation of security efforts. "We were seeing it in more and more places that you didn't necessarily expect, which is great, and people were using it and advancing in ways you hadn't really anticipated," he says.

In the years ahead, NIST, and its parent Commerce Department writ large, would continue to play a vital and central role in cybersecurity policy, including through leading the effort to develop standards around so-called "quantum-resistant cryptography," codes and encryption that would remain secure and withstand the future arrival of powerful quantum computers that would quickly decrypt and unravel the traditional encryption methods used across much of the 20th century. The following year, the National Science Foundation — which rightly and proudly points to its foundation funding help in the creation of the original internet — committed $74.5 million in new grants, as part of its $160 million in annual cybersecurity research funding, to support new multidisciplinary cybersecurity research. All told, it funded 257 projects, focused on everything from cryptocurrency to encryption to systems that could scan the internet for known vulnerabilities and patch them automatically.

TIME TO NAME AND SHAME

The first major change was to confront one of the most long-standing foreign challenges online: the extensive, ongoing, and rapacious campaign by the Chinese government to steal intellectual property from U.S. companies. Dozens, if not hundreds, of U.S. companies had suffered major thefts beginning in the 2000s and 2010s, as Chinese hackers, many linked to the military itself, stole industry secrets and used them to boost domestic Chinese industries and companies to compete with the west. Some companies had begun to complain both privately and more publicly.

In 2010, Google had been one of the first to publicly point the finger at China for a cyber intrusion. In a January 12, 2010, blog post, Google announced that it had been subject to a cyberattack that it traced to China. As more details emerged, it became clear that the Chinese hackers had targeted one of the most sensitive portions of Google's system — the Mountain View, California, tech giant's "legal discovery portal," which the company lawyers and security team used to monitor contact with law enforcement. (An alert security officer noticed the breach when he saw one of the portal's supposedly legitimate users querying a long list of Chinese names.) "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack," McAfee's then head of threat research, Dmitri Alperovitch, said afterward.[18]

Alperovitch named the incident Operation Aurora, a reference the Russian-born engineer pulled from his childhood history classes in the Soviet Union. The cruiser Aurora fired its cannon to signal the launch of the October Revolution by Lenin's Bolsheviks. "That shot changed the course of the 20th century, and indeed of world history, and I instantly felt back then that this hack marked another momentous and historic turning point," Alperovitch wrote later.

The intrusion at Google caused the company to reconsider its entire engagement with China. In the weeks ahead, it first announced it would stop, as requested by the government, censoring search results for users of google.cn inside China. Later, though, it went a step further and announced it was effectively exiting the Chinese market altogether — a major step given the giant potential size of the billion-consumer market.

[18] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired, January 14, 2010, https://www.wired.com/2010/01/operation-aurora/.

In the following months, McAfee's Alperovitch led the way in making public two more major Chinese campaigns: Operation Nightdragon in 2011, a large-scale Chinese effort targeting oil and gas companies, and, six months later, Operation Shady Rat, a coordinated espionage and intellectual property theft campaign against more than 70 organizations, ranging from U.S. defense contractors to the International Olympic Committee.

In 2013, the cybersecurity firm Mandiant dropped the next shoe, writing a groundbreaking 60-page report outlining the details behind APT1, a team of Chinese hackers it identified as belonging to the People's Liberation Army's (PLA) Unit 61398. An in-depth, front-page New York Times article in February 2013 built on the Mandiant report and even included a photo of the unit's headquarters off Datong Road outside Shanghai. It was the first time that such granular detail on specific units, and even individual hackers themselves, had become public, and pointed to how organized and sophisticated the state-sponsored attacks on U.S. industry were.

"Either they are coming from inside Unit 61398," said Kevin Mandia, the founder and chief executive of Mandiant told the Times reporters, "or the people who run the most-controlled, most-monitored internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood."[19]

Those headlines helped lay the groundwork for the U.S. government to take more official action too. In May 2014, the Justice Department announced indictments against five members of PLA Unit 61398, the first time criminal charges were filed against known nation-state actors for hacking.[20] "For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," FBI Director James B. Comey said. "The indictment announced today is an important step. But there are many more victims, and there is much more to be done."

The DOJ indictments marked a signal turning point — elevating cyber in the public consciousness and beginning to push it toward the front of geopolitical conversations. It was a change that couldn't come soon enough. Months later, that November, when North Korean hackers attacked Sony Pictures Entertainment, the U.S. government response was nearly 180 degrees different from its tepid, slow, and arms-length response to the Iranian DDoS attacks. The Obama administration forcefully stepped in to aid Sony Pictures, deploying U.S. teams to be on-site at the Hollywood giant, and taking retaliatory actions — still evidently classified — against the North Korean regime in response.

The U.S. was belatedly realizing that its declared posture of online restraint and deterrence, carryovers from the nuclear age doctrines, were, in fact, having the opposite intended effect on bad actors: They realized that they could escalate, attacking U.S. targets and pillaging U.S. intellectual property, with little worry of costly responses or retaliations by the U.S. government.

That realization was one that the private sector was coming to as well. Microsoft, in particular, was beginning to think through the role that industry could have in combating transnational cybercrime, and whether the private sector could step into some of the gap left as Western governments struggled to chase criminals overseas. After all, name-and-shame efforts like the indictments of Unit 61398 may have some geopolitical implications, but even across nearly a decade of such public indictments, only a handful of top cybercriminals have faced handcuffs and the inside of a courtroom.

[19] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," New York Times, February 18, 2013, https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[20] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

"What we recognized is that the thing that the private sector could do in the context of cybercrime is focus on disruption of the means of conducting cybercrime — targeting infrastructure that cybercriminals use both to conduct their crime and then the way in which they get paid, how the money they recover gets transferred and ultimately enriches the criminal," explains Tom Burt, a longtime Microsoft employee, who started with the company's digital trust group in the mid-2010s and whose role gradually expanded to his current position as corporate vice president for customer security and trust.

Microsoft recognized that private industry actually gathered a significant amount of information on cybercrimes and could trace much of how it unfolded through their networks, and then use that information to disrupt the underlying technical infrastructure, particularly in the case of botnets and other network-heavy criminal enterprises. Each month, its email program scanned around 200 billion emails for malware, it offered some 200 cloud services, and touched what it estimated were a billion end points across the internet — collectively a massive treasure trove of potential threat intelligence. To turn this data into action, the company began to build out a three-tiered internal operation that could harness the company's own data to identify, target, and disrupt criminal operations. It focused its resources around a Threat Intelligence Center, a Cyber Defense Operations Center, and a Digital Crimes Unit. It began to pursue court orders against online criminal infrastructure, like fake domain names set up as part of phishing campaigns, that allowed the company to take control of the domain and "sink hole" the malicious traffic.

More broadly, though, even a decade into the rise of cyber threats, there was little coherence or organization to the wider policy field. Few outside of government and major private sector companies were thinking hard about the strategies, policies, and procedures that would help guide society in this new digital age. Conversations were still siloed within government and industry, public policy debates still fraught — as Lieberman-Collins demonstrated — and there was still too little trust between the private sector defenders and the government operators. Overall, in fact, there was little meaningful cross-pollination or communication between the government, civil society, and the private sector. Moreover, the number of people who worked on the policy-side questions around cyber issues across government and the private sector remained shockingly low. "The bench was very shallow," recalls Megan Stifel, who worked on cyber issues at the Justice Department and White House at the time.

THE HEWLETT EFFORT LAUNCHES

Just a month after the publication of the NIST Cybersecurity Framework, in March 2014, the William and Flora Hewlett Foundation officially launched its Cyber Initiative, aimed at investing in the cyber policy arena at a time when the "cyber field" remained ill-defined, starved for funding, and disaggregated across multiple topical areas, from encryption to the emerging Internet of Things. Still, nearly 20 years after the Marsh Report, many remained unconvinced that there was much to cyber threats at all. As the Hewlett Foundation wrote, "Outside the tech community, most people thought of it as an inconvenience at most — annoying spam and silly requests from 'Nigerian strangers' seeking help to acquire fortunes. We were almost alone in insisting that cyber threats posed a looming threat to our economy, society, and government, and that we needed to get ahead of the problem."[21]

By contrast, Hewlett looked at the entire ecosystem of philanthropic funders, research fellowships, think tanks, graduate programs, and career paths that had grown up around the field of nuclear strategy during the Cold War. Over the 75 years since the advent of the atomic age, a whole host of nuclear-focused think tanks and research

[21] "Cyber Initiative Grantmaking Strategy," William and Flora Hewlett Foundation, November 2017, https://hewlett.org/wp-content/uploads/2017/11/Cyber-Initiative-Grantmaking-Strategy-11.2017.pdf.

centers had emerged that worked on issues from security and strategy to disarmament — from the Bulletin for Atomic Scientists, famous for their Doomsday Clock, to the Nuclear Threat Initiative, the Physicists Coalition for Nuclear Threat Reduction, the Carnegie Endowment's Nuclear Policy Program, the Center for Arms Control and Non-Proliferation, the Council on Strategic Risks' Nolan Center, and the Ploughshares Fund, among others. Almost every major think tank hosted distinguished senior fellows who specialized in nuclear policy and nearly every public policy graduate program offered coursework in nuclear and strategic weapons and related subjects. Moreover, an entire network of graduate and research fellowships supported early-career thinkers: The Stanton Foundation, for instance, had funded nuclear security research fellowship programs at MIT, RAND Corporation, Stanford, and the Council on Foreign Relations. Stanford also, separately, offered the MacArthur Foundation Nuclear Security Fellowship, and the Federation of American Scientists offered a New Voices on Nuclear Weapons fellowship, among others. Beyond that, the government itself funded any number of centers of excellence and research facilities on nuclear issues at the national laboratories and key military bases and schools. Taken all together, the robust ecosystem around nuclear strategy had encouraged multiple generations of thinkers to imagine and pursue lifelong careers and provided a steady supply of seasoned, experienced thinkers for government roles at the Defense Department, Department of Energy, State Department, White House, and in private industry.

Cybersecurity, at the time, had almost none of that policy infrastructure. There were few schools thinking seriously about the policy side of technology and security issues, and only a handful of people inside government were working on the pressing questions around cyber policy.

The Hewlett Foundation's first effort to jump-start a more defined and coherent field began with major $15 million gifts, in November 2014, to the University of California, Berkeley, MIT, and Stanford to launch substantive cross-disciplinary cyber policy efforts. The foundation said it hoped to "generat[e] a robust 'marketplace of ideas' about how best to enhance the trustworthiness of computer systems and appropriately balance rights of privacy, the need for data security, innovation, and the broader public interest." The gifts were meant to play to each institution's strengths: At MIT, the grant created a new Cybersecurity and Internet Policy Initiative across the departments of engineering, social science, and management that focused on quantitative metrics and qualitative models that could help policymakers understand the cyber field; Stanford's new Cyber Initiative focused on trustworthiness and network governance; while UC Berkeley founded the Center for Long-Term Cybersecurity (CLTC), an interdisciplinary research and education effort aimed at studying the longer arc of technology and differing possible policy paths.

As Hewlett Foundation President Larry Kramer said in announcing the gifts, "Choices we are making today about internet governance and security have profound implications for the future. To make those choices well, it is imperative that they be made with some sense of what lies ahead and, still more important, of where we want to go. We view these grants as providing seed capital to begin generating thoughtful options."[22]

UC Berkeley's approach, in particular, was aimed at changing the nature of cyber policy — which was often still heavily reactive and tactical, responding to unfolding threats and problems in real-time — and focused instead on the opportunity for more big-picture strategic conversations. As CLTC's Steven Weber says, "So much of the cyber world was still operating like an emergency room, you patch someone up and then send them for long-term care and rehabilitation. But there wasn't anyone doing long-term care. We wanted to move the field toward foresight."

[22] "Hewlett Foundation Announces $45 Million in Grants to MIT, Stanford, UC Berkeley to Establish Major New Academic Centers for Cybersecurity Policy Research," William and Flora Hewlett Foundation, November 18, 2014, https://hewlett.org/newsroom/hewlett-foundation-announces-45-million-in-grants-to-mit-stanford-uc-berkeley-to-establish-major-new-academic-centers-for-cybersecurity-policy-research/.

The Hewlett Foundation initiative's first permanent program officer was Eli Sugarman, a one-time lawyer, State Department foreign service officer, and consultant, who had become interested in the intersection of technology and geopolitical risk while working in D.C. with Zalmay Khalilzad, the Bush administration's ambassador to, variously, Afghanistan, Iraq, and the United Nations. Sugarman, who arrived just after the initial $45 million in grants, immediately saw the impact the headline-grabbing grants had made in the field. In January 2016, the Harvard Kennedy School's Belfer Center received a $15 million grant to launch its own Cyber Security Project.[23] "We'd clearly set the buy-in at $15 million for a serious cyber project," Sugarman says.

As Sugarman settled into his new role — then funded for about $4 million a year in annual grantmaking — he began to build a landscape for the cyber policy field. He saw a need for the Cyber Initiative to focus on building a network and a sense of community among the different players in the cyber field, as well as to close the gap between the technical and nontechnical communities within it and improve the quality and relevance of research outputs to maximize their future policy impact. Sugarman recalls finding, in his early months of meetings and conversations, that the field was even more disjointed and splintered than he had imagined, sorely lacking in camaraderie, mutual understanding, respect, and ability to communicate among and across the broad array of positions and expertise that were lumped together under "cyber." As he recalls, "There wasn't necessarily a sense of 'Okay, we're all part of the same field.' It was much more like, 'Oh, we're the computer scientists who've been working on this for decades — and who are you, late-start policy people who don't know anything about the technology, to be making grand decisions we think are bad from the technical perspective?'" There was not a lot of connectivity, social capital, or trust between the nascent civil society folks, academic researchers, government policy leaders, and the policy shops of private sector companies.

What little trust, shared perspective, or willingness to cooperate may have ever existed had been sorely stretched or outright destroyed by the world-rending 2013 revelations of NSA whistleblower Edward Snowden. The one-time NSA contractor's leaks to major news outlets about the extent of the U.S. government's tech surveillance apparatus and the awesome breadth, depth, and scope of NSA's computing hacking abilities had badly jolted private sector engineers and civil society researchers who had long seen themselves as on the same side as the U.S. government, law enforcement, and national security apparatus. Now, suddenly, the exposure of individual surveillance programs like PRISM, as well as his broader revelations of the tremendous scale of the U.S.' $60 billion annual black budget had shaken both the U.S. tech community and chilled the willingness of foreign governments and companies to work with U.S. tech giants like Google, Microsoft, IBM, and Yahoo.[24] Microsoft deputy general counsel John E. Frank told the New York Times in 2014, "We're hearing from customers, especially global enterprise customers, that they care more than ever about where their content is stored and how it is used and secured." Any chance at a global conversation about cyber had splintered in the wake of the revelations, creating new divides and distrust both between U.S. companies and its government, as well as between Europeans and Americans more broadly.

Sugarman began his role by trying to learn where the bright spots for policy work existed, attending conferences, hosting lunches, and talking with leaders across the field. He saw his role — and the role of a successful funder — as less about trying to master the minutiae of each individual policy area and question it than about understanding the field's broad lay of the land and potential promise, learning which experts and institutions had built trust with government policymakers and corporate leaders. ("Frankly, it wasn't that hard to identify those folks because there weren't a whole lot of them," he recalls. "It wasn't like there were

[23] "Gift to Belfer Center to Launch Cyber Security Project," Harvard Gazette, January 19, 2016, https://news.harvard.edu/gazette/story/newsplus/gift-to-belfer-center-to-launch-cyber-security-project/.

[24] "Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," New York Times, March 21, 2014, https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

millions of organizations of people to choose from, it was actually a pretty small segment of the field.") But even among that small segment that was making an impact on cyber policy, there was little cross-conversation and pollination. There were distinct, identifiable, and independent clusters: those focused on the legal and ethical questions around privacy and civil liberties; those focused on international laws; those focused on white-hat hacking (i.e., ethical hacking); and then, in the private sector, a community largely populated by former Justice Department prosecutors or veterans of the intelligence community. He understood early on that his challenge would be to build the field's inclusiveness and connectivity. "It was really about running around the field and building trust," he says. "These clusters weren't reaching across to say, 'You actually have part of this puzzle, I have part of the puzzle, we can solve more of the puzzle together.' That was not happening at scale, and that really, really stood out."

Sugarman and Hewlett's hope was to use its funding and grants to nurture and grow dedicated centers of cyber policy excellence and invest in the professionalization of the field. "It was about making bets on people and on institutions that had a leadership commitment to growing cyber programs — not just places where cyber would number 83 on a list of 87 programs, but places that were focused on this as a real area of expertise and potential," Sugarman says. "It was about finding who was collaborative, has the relationships, and the ideas, and who understands the landscape well enough to bring those ideas into fruition. We were looking for people who didn't want to just stay in their silo. There weren't that many academics trying to do policy-relevant research. There weren't that many people trying to communicate and build a network, people trying to serve those strategic ends."

KEYS UNDER DOORMATS

One early — and important — right spot in the field that Hewlett identified was the possibility of shaping the post-Snowden debate around encryption. The debate had been rising in policy circles in Washington, particularly since a 2014 speech by FBI Director James Comey that laid out the "going dark" problem. After decades where the government could use court-authorized search warrants to listen in on phone conversations, inspect mail, and otherwise intercept communications among criminals, Comey argued that in the modern era criminals and terrorists were beginning to turn to devices and tools that circumvented those law enforcement tools. Comey's remarks came a month after the new iPhone 6 and its iOS 8 launched with encryption so robust that not even Apple could decode what was on the device; only the user entering the PIN would decrypt the device, so Apple had created a system where, by design, it couldn't comply with a court-authorized order to decrypt an iPhone.

"Technology has become the tool of choice for some very dangerous people," Comey told an audience at the Brookings Institution in October 2014. "Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'going dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism, even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."

As the FBI director saw it, his agents, and law enforcement more generally, increasingly confronted two challenges: the real-time court-authorized interception of "data in motion," like phone calls, email, or chat sessions, as well as the increasingly pernicious problem of "data at rest" that was being encrypted on devices and hard drives and thus thwarting agents' lawful court-ordered access to those email, text messages, photos, or videos.[25] To make

[25] James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" Federal Bureau of Investigation, Speech at Brookings Institution, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

his case, he pointed to a parade of horribles — sex predators preying on teens, parents accused of killing their two-year-old, and drug trafficking cartels — all of whom were convicted through evidence collected off their phones with lawful court authorizations.

To confront this new challenge, Comey and other U.S. officials were pushing for an update to the 20-year-old law known as the Communications Assistance for Law Enforcement Act (CALEA), passed "a lifetime [ago] in the internet age," Comey said. Updating the law would better balance civilian encryption with the government's need to access communications and devices with a lawful court order, forcing tech companies to build "lawful intercept capabilities for law enforcement." As Comey saw it, "I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me." His efforts were eventually followed-up internationally, too, as the U.K.'s Government Communications Headquarters Director Robert Hannigan and, later, U.K. Prime Minister David Cameron, both pushed the same subject and concern across the pond. As the threat of ISIS rose, Hannigan charged that the encrypted technologies of U.S. tech companies had become "the command and control networks of choice" for terrorists.[26]

Critics of the proposed move saw the effort as nothing less than undermining the fundamental promise of encryption. Any attempt to build a "back door" into encrypted communications would open up the possibility of exploitation by hackers, including the U.S. NSA or other foreign signals intelligence agencies.

The burgeoning debate led to a new policy effort at MIT, which grew out of the school's Cyber Security Initiative, and built on then-cutting-edge research done in the 1990s by Steven M. Bellovin, Whitfield Diffie, Bruce Schneier, Matt Blaze, and others, on fundamental building blocks of cryptography like key length and escrow. The research then argued against the introduction of the "Clipper chip," a special device for secure communications that could be intercepted by governments. They, along with a broader set of cryptology experts like Susan Landau, convened a series of meetings and conversations that led to the publication, in July 2015, of a groundbreaking 34-page report called "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications."[27]

"As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details," the paper began. In the following pages, it outlined the very real and complex technical challenges of any such effort to build "exceptional access" for law enforcement into software and devices, and the trade-offs, in terms of innovation, security, and the inadvertent introduction of new vulnerabilities. It explained how any such effort would create rich new targets for bad actors since the credentials to unencrypt communications would have to be held by the tech companies, law enforcement, or some other trusted third party.

[26] Ben Quinn, James Ball, and Dominic Rushe, "GCHQ Chief Accuses US Tech Giants of Becoming Terrorists' 'Networks of Choice'," Guardian, November 3, 2014, https://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.

[27] Harold Abelson, et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," MIT, July 6, 2015, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

"The need to grapple with these legal and policy concerns could move the internet overnight from its current open and entrepreneurial model to becoming a highly regulated industry," the group wrote, concluding "analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict. The costs to developed countries' soft power and to our moral authority would also be considerable. Policy-makers need to be clear-eyed in evaluating the likely costs and benefits."

The MIT report, and a following work by another Hewlett-funded team at Harvard's Berkman-Klein Center, entitled "Don't Panic: Making Progress on the Going Dark Debate," redefined the public debate over "going dark."[28] (It was downloaded more than 100,000 times from Harvard's website, a startlingly large number for a policy paper.) Other internet bodies, from the World Wide Web Consortium (W3C) Technical Architecture Group to the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), rallied to the cause too, endorsing the conclusions of the "Keys Under Doormats" policy.

By October 2015, the Obama administration backed down. It was a remarkable turn-about as Comey announced to a Senate Homeland Security and Governmental Affairs Committee meeting that the administration no longer intended to push for legislation that would compel such exceptional access. "As the president has said, the United States will work to ensure that malicious actors can be held to account, without weakening our commitment to strong encryption," National Security Council spokesman Mark Stroh told the New York Times. "As part of those efforts, we are actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time."[29]

And, for Sugarman and the Hewlett Foundation Cyber Initiative, the "Keys Under Doormats" report was a signal of how the cyber field could evolve by giving space to experts to set the terms of public policy debates. "Our grantees at MIT and Harvard played a crucial role by developing sophisticated arguments based on careful analysis of the evidence and policy tradeoffs. Their work helped put the debate on firmer ground, staving off a short-sighted and potentially dangerous policy decision that would undermine cybersecurity online," Hewlett championed at the time.

To Susan Landau, though, part of the shame of the "going dark" debate was that it was precisely the wrong conversation to have at the time, as new cyber threats were rising and swirling across the world — it was about unwinding security, rather than improving it. As she wrote in 2015, "Exceptional access is being pushed at a time when the real cybersecurity issue is securing our systems, all the time, everywhere."[30] The cybersecurity world needed to be united and focused outward, on developing systems and procedures to counter increasingly sophisticated adversaries, rather than on fighting against U.S. officials themselves.

And a specific new threat was just around the corner.

[28] Jonathan L. Zittrain, Matthew G. Olsen, David O'Brien, and Bruce Schneier, "Don't Panic: Making Progress on the 'Going Dark' Debate," Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[29] Nicole Perlroth and David E. Sanger, "Obama Won't Seek Access to Encrypted User Data," New York Times, October 10, 2015, https://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?mtrref=undefined.

[30] Susan Landau, "Keys Under Doormats: Mandating Insecurity," Lawfare, July 7, 2015, https://www.lawfare-media.org/article/keys-under-doormats-mandating-insecurity.

III. FIELD BUILDS (LATE 2010s)

The fallout from the 2016 presidential election shook the cybersecurity field, as a trickle of pre-election rumors and suspicions about Russia's online meddling in the election turned into years of news headlines, breaking news chyrons, federal indictments, and congressional investigations. By the end, it was clear that through social media trolls and hackers at its military intelligence unit, Russia had run a complex, multifaceted campaign to influence the outcome of the U.S. presidential election. It was, perhaps, the "cyber Pearl Harbor" that many had long warned about.

And if not that election attack, two other incidents in quick succession in 2017 delivered multibillion-dollar damages to Western companies. Two major international ransomware attacks — NotPetya and WannaCry — devastated major corporations and transformed and elevated the corporate board-level focus on cyber issues. The damage from NotPetya, launched by Russia and originally targeted against Ukraine before it went wild on networks much farther afield, stretched into the billions; FedEx reported some $300 million in damage and Merck saw about $310 million in damages, including having to replace more than 45,000 computers and 4,000 servers. The global shipping company Maersk was paralyzed for weeks.

This rising sense of threat drove yet more government reorganization. Even after settling the "bubble chart" debate, DHS had struggled to right-size its approach to cybersecurity. During the Obama administration, DHS's National Protection and Programs Directorate (NPPD), with the leadership of Undersecretary Suzanne Spaulding, had continued to elevate cyber threats and, in 2016, amid the rising fears of an attack on the election system, had stepped tentatively into providing cyber support to state and local election officials. It was a rough adjustment, as DHS was so new to that mission, and the initial foray left much to be desired and improved in future elections. One of the major cybersecurity successes of the Trump administration was the congressional approval to reorganize and rename NPPD into a stand-alone agency, the Cybersecurity and Infrastructure Security Agency (CISA), under the leadership of its founding director, Christopher Krebs, in 2018.

That reorganization, which clarified CISA's capabilities and mission and elevated its prominence as a partner for state, local, and tribal authorities, was just part of a major evolution across the government that tried to transform cybersecurity from an exotic subject into a routine one. The National Defense Act of 2019, for instance, stated for the first time that cyberattacks were to be considered a traditional instrument of power, as opposed to an extraordinary instrument of power. As Chris Inglis explains, "All of this led to the conclusion that cyber no longer needs to be leashed and constrained — it can be allocated for use within reasonable rules of engagement. We began to understand that cyber was not the only instrument of power that could be employed in cyberspace, but an instrument of power, to be used in conjunction with diplomacy, legal remedies, and public shaming."

THE START OF THE ASPEN INSTITUTE'S CYBER EFFORT

The Hewlett Foundation Cyber Initiative's overarching goal was straightforward: "To cultivate a field comprised of institutions with deep expertise to which decision makers can turn, and in which they and the public can place justified confidence, for solutions to pressing cyber policy challenges."[31] One small, early bet that Sugarman placed was to add the creation of a standing Cyber Strategy Group at the Aspen Institute. Aspen Institute CEO Walter Isaacson — long fascinated by technology and personally interested in the rising cyber threat — had first approached John Carlin, then the assistant attorney general for national security, at the Aspen Security Forum in 2015 about starting a cybersecurity program at the institute. Aspen had, for many years, hosted its famous Aspen Strategy Group, an ongoing group focused on discussing hard foreign policy questions, and more recently started a similar strategy group for homeland security to advise the secretary of the Department of Homeland Security. Isaacson saw a need for a similar cross-sector discussion forum around cybersecurity. Carlin, who had lived through the governmental policy debates around the Iranian DDoS attacks, Chinese intellectual property theft, among others, instantly understood the need.

"In other areas, there were standing groups where, as a government official tasked with responding to those threats, you could meet in a closed-door environment with people who were constantly thinking about the issue. It was an enormously useful check against groupthink inside government, as it brought perspectives from people in the private sector and civil society to think strategically and tactically. Nothing like that existed for cyber," Carlin recalls.

In the wake of 9/11 and after-action recommendations like the 9/11 Commission, the government had moved to create multiple new structures for information sharing inside and between government agencies, from the Office of the Director of National Intelligence to the National Counterterrorism Center. But there were still precious few such venues for solid information sharing and discussion around cybersecurity issues. As Carlin says, "That was a gap, particularly because so much of the responsibility for cybersecurity lies outside government. Over ninety percent of critical infrastructure was in private hands, and we had to get better at sharing information at speed and scale with the private sector."

When Carlin left government service at the end of the Obama administration, he launched the Aspen Institute's cybersecurity program. Its first project, along with his colleague Lisa Monaco, then the departing White House homeland security advisor, was to start the Aspen Cybersecurity Group.

In a remarkable moment of philanthropic kismet, Carlin had already begun to build the program in January 2017 when Sugarman sought him out to see if he was willing to start something similar. When he heard such an effort was already underway, Sugarman immediately offered to fund the first year of the program. That funding, Carlin says, was key to building the program's reputation and trust because it allowed the effort to start without relying on funding from any company that might have interests before the group.

Carlin and Monaco, though, wanted the Aspen Cybersecurity Group to do more than talk. They recruited Republican Rep. Will Hurd, then on the House Intelligence Committee, and the chairman, president, and CEO of IBM, Ginni Rometty, who both similarly recognized the rising threat, as co-chairs of the group. Together, they gathered some three dozen cyber leaders from civil society, academia, and private industry, as well as former government leaders, including two former NSA directors as the founding members of the Cybersecurity Group.

A key focus in building the group was Aspen's belief in mixing "tri-generational" leaders — ensuring that the group's membership represented "wise old owls" from industry and government, with decades of experience; "midcareer" professionals at the peak of their careers; and "rising stars," whose influence and responsibilities

[31] "Cyber Initiative Grantmaking Strategy," William and Flora Hewlett Foundation, November 2017, https://hewlett.org/wp-content/uploads/2017/11/Cyber-Initiative-Grantmaking-Strategy-11.2017.pdf.

would grow in the years ahead. (The Aspen Strategy Group, for instance, had long hosted voices like Ashton Carter and Condoleezza Rice, who, over the course of their careers, actually occupied all three roles in the group, beginning as young Ph.Ds and rotating in and out of the group as their government careers grew and thrived.)

In its inaugural meeting at IBM's headquarters in Armonk, New York, in January 2018, amid a giant snowstorm, the group settled on three initial priorities: workforce and talent pipeline development; improving operational collaboration; and developing security principles that should guide the development of Internet of Things (IoT) devices. In the months ahead, working groups pursued each project and developed their own consensus and recommendations. In particular, the workforce effort, led by Rometty and IBM, made a major impact in the industry. It developed a wide set of recommendations about how to improve cyber talent recruiting and retention, which included widening the aperture of potential candidates by rewriting job descriptions to be more inclusive, launching apprenticeship programs, and investing in cyber education at the elementary and secondary school levels. Rometty led an effort to ultimately get nearly 40 companies to sign on to the hiring reforms, from Apple and Bank of America to Johnson & Johnson and Northrop Grumman. The resulting actions demonstrably showed how minor tweaks could boost the diversity of applicants: At Johnson & Johnson, one formerly all-male security engineering team became 50/50 male/female within a year, as the rewritten job descriptions took effect.

Soon to enter its eighth year in existence, the Aspen Cybersecurity Group continues to meet in person regularly three times a year, with an ever-growing number of U.S. government representatives around the table, and, during its annual spring meeting in Washington, D.C., meets with Capitol Hill oversight staff to discuss pressing cyber topics. Recent reports have focused on the evolving role of the chief information security officer in corporate hierarchies, as well as guidance for organizations adopting generative AI.

THE CYBER ENFORCEMENT GAP

Also, in 2018, Mieke Eoyang, then at Third Way Institute, spotted an opportunity to bring a new perspective to the cyber debate. Eoyang, a former Capitol Hill national security staffer, had watched warily as cyber issues rose throughout her time on the Hill. She came, in particular, to discussions around government surveillance policy with a unique vantage point, having worked for California Rep. Ron Dellums. Dellums himself been targeted by the FBI's Cointelpro surveillance program in the '60s as part of its (illegal) efforts against domestic political dissidents, civil rights activists, and marginalized communities.

As Eoyang saw it, the government focused too much on "defense-only" policies, which would inevitably lead to evermore intrusive network surveillance tools. And yet there was still precious little attention paid to the fact that at the end of every cyber intrusion, crime, or attack, there was a human at the keyboard. The U.S., and allied governments across the world, needed also to focus on the people doing the crimes, and the gap between crimes and punishment was still too enormous. Third Way Institute estimated that barely 1% of cybercrimes ever faced punishment — compared to, for instance, one in five property crimes.

With funding from Hewlett, Eoyang launched a Cyber Enforcement Gap Initiative. As she announced the work, she wrote, "Here is the change we seek: The United States must institute a comprehensive cyber enforcement strategy that can sufficiently identify, stop, and punish global attackers. In order to develop this strategy we must (1) change the mindset that punishing the attackers is futile; (2) assess the current strengths and weaknesses of the current enforcement architecture; and (3) create a robust conversation around developing effective policy changes necessary to transform the government's response and rebalance it to one that prioritizes all tools in America's cybersecurity toolbox."[32]

[32] "Announcing the Third Way Cyber Enforcement Initiative," Third Way, October, 29, 2018, https://www.thirdway.org/memo/announcing-the-third-way-cyber-enforcement-initiative.

In tackling the questions about cyber enforcement, she hoped to avoid an over-militarized approach to cybersecurity defense, also centering and investing in responses by law enforcement. "When I first started doing that work, putting together groups of people to talk about it, and asking the question like, 'Why don't we do law enforcement?' The universal response was, 'That's too hard.' There was this mental block around doing that, and a whole bunch of assumptions against thinking about real solutions in cyber enforcement," Eoyang recalls. "We started the Cyber Enforcement Initiative specifically to say, 'There's not one big thing you can do here, but there's a whole bunch of little things that you could do here that actually make the problem better."

Through conversations with federal, state, and local law enforcement and intelligence community officials, she and a team of analysts, including Allison Peters, began to chip away at misguided assumptions and develop metrics and data that could inform the conversation. "We had to change the 'blame the victim' attitude," she says. "We worked really hard to show that, 'this thing is pervasive, it's happening to lots of people, and we can do something about it.'" Startlingly, through public policy polling, Third Way Institute determined that one in four people reported being victim of a cybercrime — a number that indicated the sheer scale of the societal problem. The total number of cyber enforcement efforts, by contrast, was vanishingly small.

The work culminated in two reports in 2020, one of which, "To Catch a Hacker," focused on 10 specific, actionable steps government could take to close the cyber enforcement — from improving data collection to investing in building capacity with foreign partners — as well as an action plan and transition guide for the incoming presidential administration in that year's election. The Third Way Institute's work would prove an important foundation for what would turn out to be the national breakout conversation around cybersecurity in 2021: the rise of ransomware.

DIGITAL DIPLOMACY

The steadily expanding cyber threats and the rising geopolitical significance of the major tech companies led, in the late 2010s, to the recognition that they would stand alongside traditional nation-states in terms of influence and power. Tech giants like Google, Facebook, Microsoft, and Apple, as well as smaller companies that oversaw critical network infrastructure, like Cloudflare, found themselves working across national borders. This, effectively, forced them to develop foreign policy operations that rivaled a small nation-state, with their CEOs treated almost like heads of state during foreign travel. Companies like Twitter and Facebook operated in dozens of languages, and their security teams regularly targeted content take-downs apparently backed by nation-state intelligence agencies. It was a scale of geopolitical complexity and economic centrality that few companies in history have achieved — and certainly few since the colonial days of global giants like the Dutch East India Company, Hudson's Bay Company, or the British East India Company.

In 2017, Microsoft Vice Chair and President Brad Smith used a keynote at the large industry cybersecurity gathering known as the RSA Conference to call for what he dubbed a "digital Geneva Convention," modeled on the treaty signed in Switzerland in 1949 that laid out the modern rules of warfare. "Let's face it, cyberspace is the new battlefield," he told the RSA audience. "But cyberspace is us. … Cyberspace is owned and operated by the private sector. It is private property, whether it's submarine cables or data centers or servers or laptops or smartphones. It is a different kind of battlefield than the world has seen before." The new agreement, he argued, needed to acknowledge the shared ownership and prerogatives in this new battle space of both nation-state governments and the private sector itself.

In laying out the need for such an updated international agreement, Smith pointed to recent deals at the United Nations and between the U.S. and China that laid out basic international cyber "norms." As Smith argued, "We need a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of the electrical

or the economic or the political variety. We need governments to pledge that, instead, they will work with the private sector to respond to vulnerabilities, that they will not stockpile vulnerabilities, and they will take additional measures."

As Smith saw it, the tech sector needed to be the 21st-century equivalent of a "digital Switzerland," neutral and trusted by all, offering what he called "100% defense and 0% offense." "We will assist and protect customers everywhere. We will not aid in attacking customers anywhere. We need to retain the world's trust. And every government, regardless of its policies or politics, needs a national *and* global IT infrastructure that it can trust."[33]

The next year, after working with Smith and his team, French President Emmanuel Macron picked up the challenge, using a speech at the annual UNESCO Internet Governance Forum in Paris, on November 12, 2018, to announce an initiative known as the Paris Call for Trust and Security in Cyberspace, aimed at formalizing international cyber norms. The effort's nine principles ranged from commitments that nation-states wouldn't digitally interfere in foreign electoral processes to a prohibition against private sector companies "hacking-back" on those who attacked them. The Paris Call was endorsed by a wide spectrum of countries, nonprofits, and private sector companies, including Microsoft, Facebook, Google, and IBM. Notably, though, neither the U.S. or Australia, two of the so-called Five Eyes intelligence partner countries, supported it, and neither did Israel, which has long had one of the most robust cyber intelligence and offense operations. It also wasn't endorsed by four of the West's primary adversary nations: China, Russia, Iran, and North Korea. (Within a year, the number of signatories would triple to 74 nations, 350 civil society organizations and NGOs, and more than 600 private sector companies, but the U.S. wouldn't join until 2021.[34])

These moves — mixing traditional nation-state government with private sector partners on international accords — were a clear statement that in the early years of the 21st century, a tier of private sector tech companies had arisen that could rival and shape nation-states themselves.

In 2019, in part as a recognition of this new era, where the user base of a company like Facebook would rank alongside the population of the world's largest country, the Hewlett Foundation came together with Mastercard, Microsoft, and the Ford Foundation to provide the seed funding for the CyberPeace Institute. A nongovernmental organization (NGO) based in Geneva, CyberPeace would attempt to promote peace and justice online — operating as something like a Red Cross in cyberspace. Stéphane Duguin, a former Europol executive, served as the CEO, and Marietje Schaake, a respected former member of European Parliament, headed the new organization's advisory board. In the years ahead, the CyberPeace Institute would provide cyber training and awareness to NGOs, work to monitor cyberattacks, and protect the health care sector, among other efforts to safeguard vulnerable communities.

The creation of the CyberPeace Institute was just one of several new transnational NGOs aimed at bridging the divide between nation-states and their citizens and tech companies and their users. That same year, a horrific anti-Muslim mass shooting in Christchurch, New Zealand, was streamed live online by its perpetrator. The March 2019 incident, which saw 51 killed and more than 50 injured, was captured online and tech platforms struggled to stop it from being shared widely. Two months later, New Zealand Prime Minister Jacinda Ardern convened, along with Macron, a high-profile summit to target online hate and extremism.

The summit resulted in what would be known as the Christchurch Call, where companies and countries together pledged to "eliminate terrorist and violent extremist content online." (The U.S. again, initially, declined to join the nonbinding agreement.) As part of that effort, an online counterterrorism forum, the

[33] Brad Smith, "The Need for a Digital Geneva Convention," Microsoft on the Issues (blog), February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[34] John Frank, "Paris Call: Growing Consensus on Cyberspace," Microsoft on the Issues (blog), November 12, 2019, https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

Global Internet Forum to Counter Terrorism (GIFCT) — originally founded by Microsoft, Facebook, Twitter, and Google's YouTube — was reconstituted as an independent organization, with a dedicated staff. The Christchurch signatories outlined a new crisis response protocol to prevent future live-streamed attacks. "I don't want any other country to be placed in the situation New Zealand was in the minutes, hours, and days after the attack in Christchurch, when we were left scrambling to respond to and remove live-streamed hate," Ardern said.

IV. CYBER AS A KITCHEN TABLE ISSUE (2020s)

PROBLEMS OF TRUST AND TRUTH

Summits and international agreements like the Paris Call and Christchurch Call underscored the geopolitical transformation that the internet had wrought. The companies that provide the underlying basic infrastructure of the network, from cloud storage to social media to search to web hosting, now had to be at the table alongside nation-states for any online policy agreement to count. The livestreaming of the Christchurch massacre was only one of numerous incidents where private sector policy leaders found themselves adjudicating difficult questions surrounding the newsworthiness of global events, extremism, hate, terrorism, and the limits of free speech.

In 2020, Facebook even went so far as to create in an independent Oversight Board, funded through an irrevocable $130 million trust, that CEO Mark Zuckerberg described as the company's "Supreme Court." Through an organized appeals and complaint process, the review board could analyze the company's policies, as well as material and content that had been taken down, and decide particularly difficult cases — it even, Zuckerberg said, had the power to override the company's internal moderation decisions.

The co-founder of Cloudflare, Matthew Prince, meanwhile, highlighted in media interviews the immense power granted to those companies that make up the basic infrastructure of the internet. Cloudflare, largely anonymous to the browsing public at large, hosted and provided DDoS protection to millions of websites around the world — so many, in fact, that one in 10 internet requests flow through its servers. It faced multiple rounds of controversy in 2017 and subsequent years over websites it provided hosting and DDoS protection to, including the neo-Nazi site the Daily Stormer. Cloudflare had long been uniquely permissive and content agnostic in its hosting — some of its first customers were Turkish escorts. But as white supremacists asserted themselves in the early years of the Trump administration, and the wake of the ugly August 2017 torch-bearing march in Charlottesville, where a neo-Nazi had driven his car into a crowd of peaceful counterprotesters and killed one, Prince found himself reconsidering the power and protection his company provided. When the domain registrar GoDaddy canceled the Daily Stormer domain, Prince found Cloudflare as effectively the last line of defense in keeping the hate-filled website online. He had long been a strong proponent of liberal free speech principles — comparing his service, in a way, to a telephone company that shouldn't be policing what's said on its phone lines — but found his position increasingly untenable and uncomfortable. He pulled the protection for Daily Stormer and then wrote a public blog post explaining why it was such a dangerous precedent. In a separate internal memo to staff, he wrote more bluntly, "Literally, I woke up in a bad mood and decided someone shouldn't be allowed on the internet. No one should have that power."

Beyond the comparatively simple questions of online hate, though, lay more gray territory online when companies and governments confronted questions of misinformation, disinformation, and even active information operations by nation-state intelligence services. The revelations throughout 2018 and 2019 about the scope of Russia's attack on the 2016 presidential election, and the rising fears about floods of misinformation and disinformation heading into the 2020 election led to an important broadening and redefinition of the cyber challenge. Whereas "cybersecurity" had been largely defined, until then, as technical problems and challenges

— ransomware, DDoS, phishing, malware, kinetic destructive attacks, and similar incidents — practitioners in the field began to recognize that information operations were an equally important and pernicious challenge and threat as well.

One of the most significant new efforts in that vein was the June 2019 launch of the Stanford Internet Observatory (SIO), headed by Alex Stamos, one-time chief security officer at Facebook, and researcher Renée DiResta. The program included both new university courses, including Trust & Safety Engineering, as well as a major effort to study, record, and catalogue social media in a depth never yet attempted. The Internet Observatory pitched itself as a "laboratory for the study of abuse in current information technologies, with a focus on the misuse of social media," and drew on the astronomical reference in its name. "The term 'observatory' was not an accident: for centuries, physicists and astronomers have coordinated resources to build the massive technological infrastructure necessary to research the universe. The internet is similarly an ecosystem constantly in flux as new apps, emerging technologies, and new communities of users transform the space; researchers need innovative capabilities to research this new information frontier."

"We are developing a novel curriculum on trust and safety that is a first in computer science education, and our research discoveries will lead to trainings and policy innovations to serve the public good," said Alex Stamos at the time. He explained, "this gift from Craig Newmark will help make this curriculum a reality by allowing us to bring in diverse and innovative talent."

The launch of the Stanford Internet Observatory came, in part, thanks to a $5 million gift from Craig Newmark Philanthropies (CNP), heralding the arrival of a major new funder in the cybersecurity space. In fact, one of the biggest impacts on the cyber field in the wake of Russia's attack on the 2016 election was how it, and the ongoing battles over mis- and disinformation online, spurred craigslist Founder Craig Newmark and his philanthropic vehicle, Craig Newmark Philanthropies, to commit to the cyber field as a core giving priority. Newmark, who had long supported areas like veterans' issues and women in technology, saw the need to invest in what he called the "arsenals of democracy," funding cybersecurity efforts as well as efforts to counter mis- and disinformation. In the years ahead, Newmark would first pledge $50 million and then, later, a second $50 million to cybersecurity funding — making him the second-largest funder in the space after the Hewlett Foundation's Cyber Initiative, albeit with CNP's monies being handed out on a more rapid timeframe than the $150 million that the Hewlett Foundation initiative ultimately totaled.

The Stanford Internet Observatory — as well as a number of other academic and civil society efforts focused on mis- and disinformation, like the work of Dr. Kate Starbird at the University of Washington and Dr. Joan Donovan's work at the Shorenstein Center at the Harvard Kennedy School — moved into high gear in 2020, amid the dual information vortices of the election and the pandemic. As SIO expanded, it launched the "Journal of Online Trust and Safety" and an annual Trust and Safety Research Conference to promote and highlight new research from academia, civil society, and industry, and hosted nearly a 100 student researchers and graduate assistants.

The following year, the Aspen Institute launched a nine-month research effort, known as the Commission on Information Disorder, which brought together nearly 20 experts under co-chairs former CISA Director Christopher Krebs, news anchor Katie Couric, and Rashad Robinson, the president of Color of Change. They heard from dozens of experts and hosted 21 Disinfo Discussions — videotaped interviews and discussions with leading thinkers from across the political spectrum, all of which were posted online for public viewing. Their final 80-page report included specific, actionable recommendations on improving trust and transparency online, ranging from more public accounting of viral social media posts to advertising disclosures to new norms around accountability and investment in local media.

One of the major challenges everyone working in the field is confronting in the 2020s is how a threat that had started overseas, primarily with Russia, has quickly morphed into a domestic threat as well, as bad-faith actors, partisan media outlets, political organizations, and even elected officials themselves embraced disinformation

tactics, trying to shape political debates with malign efforts protected by the First Amendment. Those moves undermined many of the governmental efforts and complicated corporate strategies to combat such tactics. As Suzanne Spaulding says, "We certainly did not fully appreciate what might happen domestically — how the techniques of 2016 would be picked up and carried forward and the blurring of the lines between domestic and foreign. I'm very worried that we've actually lost ground there."

Unfortunately, in the years that followed, the public debate and discussion around combatting mis- and disinformation deteriorated amid partisan scuffles and political polarization. The very real fight against harmful information online — from the efficacy of COVID-19 vaccines to political disinformation — would become chilled as bad-faith actors seized upon such efforts as censorship.

THE RISE OF RANSOMWARE

For years, ransomware had been rising as a threat in the background of cybersecurity conversations. In two particularly high-profile incidents, the city of Baltimore's operations were hit by a major attack that paralyzed city services in 2018, and, the following year, Atlanta suffered similar outages, costing millions of dollars in damages.

The rise of ransomware seemed to provide a unique opportunity for a broader civil society engagement. Philip Reiner, the CEO of the Institute for Security and Technology, began recruiting, in December 2020, a team to examine possible solutions and strategies to combat ransomware. In the end, Reiner's eight-member team included representatives from the private sector — like Kemba Walden from Microsoft, Jen Ellis from Rapid7, and John Davis from Palo Alto Networks — as well as former government thinkers, including Michael Daniel from the Cyber Threat Alliance, Megan Stifel from the Global Cyber Alliance, and Chris Painter, the former cyber ambassador for State Department. As Stifel recalls, "We decided that we're going to look at 'prepare and respond,' but we're also going to think about 'deter and disrupt.'" Over the months to come, the task force's working groups met weekly, identified different stakeholders, and met and heard from more than 60 people as they sorted through possible paths forward on the issue over just four months of work. The high volume of conversations, intense pace, and relative distance from government allowed the task force to bring forward ideas and proposals that transcended many of the normal organizational fights inside bureaucracies. "There wasn't as much parochialism as there might have been," Stifel recalls. "We didn't have to negotiate with the Department of Justice or the Department of State to give up their piece of the issue so that we can all come to a consensus on this document, which gave us the ability to move more quickly.

The sheer scale and immediacy of the problem was evident in the numbers the task force gathered: The average business hit by ransomware saw an average of 21 days of downtime and took more than nine months to fully recover; the average ransomware paid in 2021 was some $312,000, a number that translated to about $350 million flowing into the coffers of the transnational organized criminal groups and nation-states that sponsored ransomware.[35]

The final 81-page report, in April 2021, presented a suite of actions totaling 48 specific recommendations that "government and industry leaders can pursue to significantly disrupt the ransomware business model and mitigate the impact of these attacks in the immediate and longer terms." As it argued, "Ransomware is not just financial extortion; it is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the health care industry during the COVID pandemic, and has shut down

[35] Ransomware Task Force, "Combating Ransomware," Institute for Security and Technology, April 2021, https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

schools, hospitals, police stations, city governments, and U.S. military facilities. It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction."

The work turned out to be amazingly well timed. Just days later, the gas pipeline company Colonial Pipeline was hit by ransomware. That incident, which paralyzed the pipeline itself and cut off gasoline flows to the East Coast of the United States, delivered cybersecurity to the front page of major news outlets and top-level briefings inside the White House, as gas stations ran low on fuel and long lines formed of impatient and concerned drivers. Suddenly — and finally — cybersecurity had arrived as a kitchen table topic in America. The year ahead, which saw multiple major ransomware variants paralyze hospitals, local police departments, school systems, and other local and state-level targets brought the subject to too many organizations at a personal, visceral level.

CYBER SOLARIUM COMMISSION

As the questions and challenges around ransomware pulsed across the United States, a bipartisan, congressionally mandated intergovernmental body was studying how to better align the government to address cyber threats. The Cyberspace Solarium Commission was modeled on an Eisenhower-era effort that focused on aligning the government to the Cold War and potential for nuclear war. It mixed a unique stew of congressional leaders, including co-chairs Senator Angus King and Representative Mike Gallagher; with independent commissioners, including Chris Inglis, Suzanne Spaulding, and utility executive Tom Fanning; with representatives from the Pentagon, DHS, ODNI, and FBI. Much of the group's conversations focused on deterrence and how to better impose consequences on bad actors.

As Spaulding recalls, the commission's work also came to embrace resilience as a core tenet of effective cybersecurity, "The more we heard from private sector folks and understood the challenges and the issues, the more everybody came around to the importance of resilience."

The commission focused heavily on the question of deterrence and how to achieve it through creating a resilient economy, reforming government, and building a more agile and united response system through public-private partnerships. Their final report, in March 2020, was specifically and narrowly tailored to possible legislative reforms and included 83 actionable recommendations. The most notable was the establishment of a White House Office of National Cyber Director, to serve as the president's top cyber advisor and as a coordinator of cyber efforts across the U.S. government — a measure that passed, with remarkable speed, into law, as did many others. ("I would never have anticipated the success that the commission had in terms of implementation of its recommendations," Spaulding says.)

In the Biden administration, Inglis was nominated and confirmed as the founding National Cyber director and wrote the office's first strategy. He notes that the Solarium Commission's most startling finding was how often the U.S. itself was being deterred in its goals in cyberspace. "It was a wake-up call for most of the folks who participated, and those who gave the final report a close and careful read, that the U.S. was actually falling behind in cyber," he says. "We needed to get back up on the horse and figure out how do we change the decision calculus of those who would use it for malign or malignant purposes?"

The U.S., the commission declared, needed to be doing more to shape adversary behavior online by denying the benefits of cyberattacks and imposing greater costs. "This posture signals to adversaries that the U.S. government will respond to cyberattacks, even those below the level of armed conflict that do not cause physical destruction or death, with all the tools at its disposal and consistent with international law," the report read.

HEWLETT SUCCESSES

One notable pivot in the Cyber Initiative was to invest in international grantmaking as well. India, in particular, was singled out for its influential role in the middle of so many internet debates — a massive developing consumer market in a fragile democracy that boasts the largest user population that most Western companies have left to reach, given that most of them don't operate in China. "I think India is arguably still to this day the fulcrum state when it comes to all internet policy issues," Sugarman says. "The example that India sets on how it educates people and the policies it implements will be copied and followed by many countries around the world." Beyond India, the Cyber Initiative made major investments in the cyber policy field in France and Germany, two nations that played critical and distinct roles in the evolving EU and continental debates over privacy, data, and regulation, and funded more modest efforts in Israel, Estonia, and Canada, among other countries. "We tried to fund a mix of university programs, think tanks, and civil society groups who could bring different perspectives to bear and thoughtful, empirically sound research to the policy debate there," Sugarman says.

The Cyber Initiative's work also unfolded as the long-time dream of a united global internet fractured. Rather than a single international network beyond the reach of any one government, today there are three distinct governmental spheres of influence online: a U.S.-centric internet largely built on surveillance capitalism with broad free speech protections; a much more heavily regulated and privacy-centric European model; and a third locked-down internet in repressive, authoritarian regimes, like China and Russia, where content is heavily policed and conversations chilled.

Another key focus of the Hewlett Cyber Initiative came in building what it called the "translation architecture" for cybersecurity. These included efforts to educate journalists around cyber issues, investments in media training for people working in cyber policy, and even an effort to generate and create better imagery that could accompany articles on cybersecurity.

In 2018, the Cyber Initiative founded the Verify Conference, an effort to bring together journalists and policymakers for two days of annual discussion, just outside San Francisco. Through a mix of high-profile on-the-record keynotes, small-group off-the-record discussions, and hands-on exercises, journalists learned about pressing cyber topics, emerging technologies, and the nuances of current policy debates. "Through efforts like this, the field overall has really matured," Sugarman says. "It is much more robust and better able to serve people's interests more concretely. I think you see a whole generation of reporters who are super deep and thoughtful on these issues, and who, in turn, are educating their readers and government policymakers."

Beyond the Verify Conference, Hewlett helped support and drive smarter and more inclusive coverage of cybersecurity issues, including through its support of Lawfare, a website founded at the Brookings Institution by journalist Benjamin Wittes, former Justice Department leader and professor Jack Goldsmith, and law professor Robert Chesney. Lawfare aimed to host debates, scholarship, and articles examining what they called "hard national security choices." As cyber questions moved to the fore in Washington, Lawfare's reporting and analysis on proposed legislation and policies became required reading for people both in Washington and out. (The originally niche legal site would become a key destination for the broader public during the Trump administration, as its writers sifted through the controversial questions around the 2016 Russian election interference and other White House policy efforts.)

In a related 2018 effort, frustrated and tired of the seemingly endless stock photos of shadowy hackers wearing hoodies, Hewlett also hosted and ran a contest to address what it saw as the "abysmal" state of imagery that news organizations and website traditionally used to accompany articles on cybersecurity. "We wanted to get away from the hackers in dark hoodies and ominous fingers-on-the-keyboard imagery that had long dogged stories about cybersecurity," explains Heath Wickline, the foundation's communications officer for the Cyber Initiative. Twenty-three semifinalists in the Cyber Visuals contest received $500 and five winners received the top prize of $7,000, and all the resulting images were released free of charge under a Creative Commons license.

Another "translation infrastructure" investment provided the startup funding for what came to be known as the Aspen Tech Policy Hub, a project of the Aspen Institute that was started by Betsy Cooper, the former director of UC Berkeley's Center for Long-Term Cybersecurity. Cooper's Tech Policy Hub brought in classes of technologist fellows for rigorous training in the policy realm, teaching everything from effective op-ed writing to policy briefs to how to have impact with legislators, regulators, and the executive branch. Over its four years of existence, the Tech Policy Hub has trained thousands of technologists and its alumni have gone into roles across federal and state governments.

A more recent pivot in the Cyber Initiative, driven by the national reckoning on race following the murder of George Floyd in 2020, was to invest in cybersecurity education targeted at historically underrepresented communities. While gender diversity had long been a topic of focus and conversation in cybersecurity, until 2020 the broader challenge of racial and ethnic diversity amid a field historically heavily white and male had generally not been addressed. ("I think the Cyber Initiative evolved as society did," Sugarman says.)

In 2021, Kelly Born took over as the Cyber Initiative program director, after Sugarman departed to work for Facebook's Oversight Board. She led a major effort to invest in education efforts targeted at diverse communities, which resulted, in 2023, with grants totaling $20 million to support new cyber policy programs at Tallahassee's Florida A&M University and Spelman College in Atlanta, two historically Black institutions; Florida International University in Miami, a Hispanic-serving institution; and Turtle Mountain Community College, a tribal college in Belcourt, North Dakota. As Dr. Raquel Hill, professor and chair of the Computer and Information Sciences Department at Spelman, said at the time, "This grant will enable Spelman to expand its traditional computer science and political science degree program offerings to include an interdisciplinary program in cybersecurity policy that explores and creates an understanding of cyber technology, its impact on society, the challenges of securing such systems, and how evolving technologies shape policies, as well as the impact of policy on cyber."

Those grants from Hewlett were part of a broader investment in cybersecurity research and policy as the field matured. In 2021, the co-founder of the cybersecurity firm CrowdStrike, Dmitri Alperovitch, and his wife, Maureen Hinman (who together founded the Silverado Policy Accelerator after Alperovitch left CrowdStrike) announced a large gift to create the Alperovitch Institute for Cybersecurity Studies at Johns Hopkins University's School of Advanced International Studies in Washington, D.C. The new institute, led by respected cyber leader Dr. Thomas Rid, would include both research work, as well as Ph.D fellowships for cyber studies. In an elaborate launch event that included DHS Secretary Alejandro Mayorkas and made clear just how deeply cyber issues had penetrated the U.S. government, Alperovitch explained how important cross-disciplinary lenses were to the issue.

"Our nation's cyber problems at their core are geopolitical ones," he said. "The major adversaries we face — Russia, China, Iran, and North Korea — present global challenges across the entire spectrum of threats: diplomatic, economic, kinetic, and cyber. Better defenses are not sufficient to defeat cyber threats, and tackling today's toughest cybersecurity challenges requires effective statecraft, driven by new skills and updated tradecraft. The creation of this institute is an acknowledgement that we can't address any of these challenges in isolation. Successfully countering these threats requires us going beyond the technical aspects of cyber, and mandates that we study our adversaries' unique motivations, capabilities, and histories."

Taken together, these investments — some made by Hewlett, some spurred by Hewlett, some entirely independently — have transformed the cyber policy field over the last decade and laid the foundation for an important policy community.

There are meaningful and important successes across the field, many of them, unfortunately, driven by the costly, high-profile cyberattacks and incidents that have belatedly spurred more serious attention to the issue. Cyber is now a top-tier policy issue; it has, in the wake of Colonial Pipeline and other incidents, arrived as a kitchen table topic. It has been institutionalized across government structures — including at the State

Department, which, in April 2022, established a stand-alone Bureau of Cyberspace and Digital Policy and an ambassador-rank position for cyber issues. (Other governments around the world have adopted similar models.) And it is now a major field of effort in education, academia, and civil society — from civil society groups and think tank like the Aspen Institute and Carnegie Endowment to schools like Stanford to UT Austin.

But perhaps more than anything, it has been Hewlett's investments in people that have paid off. As the Biden administration arrived in Washington in 2021 and as Chris Inglis set up new Office of the National Cyber Director later that year, the success and reach of the Hewlett Foundation's efforts to build a cybersecurity policy field became clear. Nearly a third of the Aspen Cyber Group members moved into new roles in government, including co-chair Lisa Monaco, as deputy attorney general, and Inglis himself. Mieke Eoyang, who had headed the Third Way Institute cyber enforcement gap work, became the deputy assistant secretary of defense for cyber policy, overseeing the nation's military approach to both cyber defense and offense. And Inglis hired and populated his new White House office with many cyber leaders who had participated in Hewlett-related efforts, including his deputy, Kemba Walden, who had been a member of the ransomware task force, and former NSC staffer and Council on Foreign Relations cyber expert Rob Knake, as the principal deputy national cyber director.

V. CONCLUSION: THE SEED IS PLANTED

The Biden administration's rough wake-up call to cyber issues — the hack of SolarWinds, followed spring of 2021 by the Colonial Pipeline incident — helped drive a major new effort inside the National Security Council for a new cyber-focused executive order. The resulting order, issued on May 12, 2021, was one of the most significant and meaty federal policy statements in years on cybersecurity. "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life," it read.

Some of the furthest-reaching impact came in the EO's fourth section, which focused on software supply chain security and mandated that the government buy secure software — a move that the White House, rightly, believed would alter and drive private sector software to strengthen security top to bottom and deliver better products to consumers as well. After all, it didn't really make sense for companies to offer two different versions of the same software: secure and insecure. Instead, by utilizing the carrot and stick of the government's purchasing power, the White House saw the opportunity to drive smarter software development in the private sector.

The Biden EO was part of what has become a sustained, consistent, government-wide engagement on cyber and tech issues, a cross-government, cross-sector approach highlighted in the passage in 2023 of the CHIPs and Science Act — an enormous moonshot-scale effort that includes about $280 billion in funding to both bolster U.S. semiconductor manufacturing, as well as help decouple the U.S. economically and technologically from China. The bill and related spending marked one of the most significant legislative economic development and technical investment effort in decades.

The private sector also, increasingly, is taking steps to tackle complex policy issues across and among companies. A group known as the Technology Coalition, which began in 2006, has grown into a partnership among nearly two dozen companies, including giants like Amazon, Facebook, Apple, Microsoft, Twitter, and Google, as well as smaller companies like Discord, Bumble, and Patreon. It has focused on combating child sexual abuse online and, in 2020, launched Project Protect, later adding a multimillion-dollar innovation and research fund.

Microsoft has also continued its international engagement and leadership on legal cybersecurity questions. In May 2020, it helped launch the Oxford Process on International Law Protections in Cyberspace, at the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) within its Blavatnik School of Government. After years of questions and debates about what holes regarding cyberspace may exist in international law, the Oxford Process brought together respected experts for an intense study and examination of how current structures may also apply online. It resulted in five different legal papers that outlined existing norms and protections in international law and how they apply to cyberspace — from electoral interference to the targeting to the health care sector. "Their conclusion largely was that international law did apply for the most part to cyberspace, and there weren't as many gaps in the law applicable to cyberspace as many feared," Microsoft's Tom Burt says.

In August 2021, Google's president of global affairs, Kent Walker, announced the company's $10 billion commitment over five years to advance cybersecurity, an effort that included a pledge to train 100,000 Americans through its career certificates. Follow-on commitments by Google included a new Hacking Policy

Council, launched with firms like HackerOne and Bugcrowd, that would press for best practices around vulnerability management and disclosure, and a legal defense fund that would help protect good-faith industry researchers, the so-called white-hat researchers.

There remain challenges in bridging divides between nation-state government and private sector companies. — for instance, including private sector voices in formal happenings at the United Nations — but the global engagement of tech giants like Microsoft and Google have established their voices at the international table on key policy questions.

In fact, in almost every realm, the cyber policy field has experienced meaningful progress in building cross-sector relationships and trust, even if the threats seem worse than ever. Perhaps the surest sign of that maturation and evolution of the cyber policy landscape came in 2023 as NIST embarked on revamping its established Cybersecurity Framework. The NIST framework was always meant to remain a living document — NIST released a version 1.1 in April 2018 — and, in 2022, NIST embarked on a full-scale effort to develop a 2.0 framework, which was published in late 2023. Notably, by then, the cybersecurity field had matured to the point where the main industry-driven desires to be included in the revised framework were *precisely* the two issues considered too controversial for the first framework: privacy standards and supply chain risk management.

Just how far the U.S. government had come, internally, in prioritizing and elevating cybersecurity became clear when the State Department — long seen as one of the worst corners in the government digital security-wise — was the first department to detect a wide-ranging foreign effort to hack top U.S. officials, targeting both Commerce Secretary Gina Raimondo and the U.S. ambassador to China, Nicholas Burns. At the same time, the case was almost a reminder of how little, in some respects, the cyber landscape has changed: The culprit was, again, China.

China, for its part, denied responsibility.

VI. CURRENT FIELD CHALLENGES

Even some two decades into the rise of cyber threats and the development of the cyber policy field, it has to face some fundamental — even existential — challenges. These include five major open questions:

1 HOW DOES CYBER SCALE?

A major issue remains that cybercrime, in particular, far outstrips the resources allocated to it by governments at all levels. Even as digital clues have become a part of nearly every criminal investigation, few local and state-level law enforcement agencies have the skills, capabilities, funding, or interest to pursue the vast majority of cybercrimes. Federal law enforcement resources, similarly, have actually scaled back; the Secret Service, which for most of the 1990s and 2000s was the nation's leading cyber investigator, has all-but given up on such investigation as its resources have been stretched thin in recent years by its protective mission. The FBI, which long saw its cyber talent clustered in a small handful of offices — primarily in New York, Pittsburgh, Atlanta, Anchorage, and San Francisco — is now investing in new cyber squads across the country, attempting, as part of a new cyber strategy, to build a basic operating capability in every one of its 56 field offices. However, its scale of investment and resources are still dwarfed by those surged toward counterterrorism cases in the wake of 9/11.

Today, cybercrime receives nowhere near the level of focus or attention that counterterrorism had after 9/11 — and that means it's not clear what types of crimes do or do not get investigative resources. As former FBI general counsel Jim Baker points out, in the wake of 9/11, every counterterrorism *tip* was tracked and investigated. Today, meanwhile, completed crimes totaling six- or even seven-figures in victim damages and losses still go uninvestigated. "We still don't have a sense of what's the threshold below which or above which law enforcement's definitely going to get involved," Mieke Eoyang says.

Bright spots in the "scale" question are programs at UT Austin, led by Bobby Chesney, and at UC Berkeley, led by Ann Cleaveland, that aim to offer "cyber clinics" for organizations who exist below what the industry the "security poverty line," much like law schools offer clinics for clients who can't afford full legal representation. Berkeley's Citizen Clinics offer tools and training to under-resourced civil society organizations to protect themselves from cyber threats. UT Austin's efforts, run out of its Strauss Center, similarly offer pro bono student-led cyber defenses to Texas small businesses, nonprofits, and public sector organizations. Efforts like these have earned the support of Google.org, which, in 2023, pledged $20 million to the Consortium of Cybersecurity Clinics to expand its work across 20 new higher education institutions in the U.S., promising that it would offer scholarships so that participating students at those clinics could earn, for free, Google's professional cybersecurity certificate. In October 2023, Google vice president for privacy, safety, and security engineering Royal Hansen announced the first 10 schools that would receive clinic funding: the University of Alabama; University of Georgia, Athens; Indiana University; MIT; University of Nevada, Las Vegas; Rochester Institute of Technology (RIT); Stillman College; UT Austin; UT San Antonio; and UC Berkeley.

Similarly, the Cybercrime Support Network (fightcybercrime.org) provides resources for people affected by cybercrime, since the vast majority of victims, despite facing real harms and damages, are too small to receive support from the government or law enforcement.

2 WHERE DOES SUSTAINABLE, LONG-TERM FUNDING FOR CYBER POLICY COME FROM?

Over the last decade, nearly all of the cyber policy field has been reliant on just two funders, the Hewlett Foundation and Craig Newmark Philanthropies. Beyond that, there has been some industry funding, particularly from Google and Microsoft, and while some new funders have entered the space — including, notably, Omidyar Networks, Ron Gula, and the Verstandig family — the field remains a long way from the sustainable endowments and long-term funding support that has grown up around, for instance, the nuclear strategy and policy field. Philanthropic funding for cybersecurity has never taken off in the way that it has for other tech topics, like AI, or for other security topics, like counterterrorism or extremism. Cyber simply never became the shiny philanthropic object and broadening the funding field remains a major challenge, particularly as the Hewlett Cyber Initiative winds down and exits the field. Part of the issue seems to be a deep-seated reluctance to engage on cyber because it's too "technical," when in reality many, if not most, people who work in cyber policy are not technically minded. Beyond that, Camber Collective's study of the cyber funding landscape shows that, while many philanthropies do makes grants around cybersecurity, it's often through other programs targeted at other adjacent topics — like journalism, AI, or broader tech policy concerns.

Relatedly, how does cybersecurity transition toward a less bubble-gum-and-shoe-string existence? Too often, cybersecurity feels like it is reliant on Band-Aids when it needs advanced medical care. Across the internet, too many critical systems and websites are run as essentially volunteer projects, lurching from funding crisis to funding crisis, and reliant on the goodwill of a small number of dedicated engineers or technologists. There remains little focus, planning, support, or attention on where to find the hundreds of millions of dollars necessary to ensure an internet that's safe, secure, resilient, and reliable, and how to find support for all the tiny critical pieces and protocols that fall just outside the lines of a single company, and yet don't rise to the level of a government responsibility. This is the critical infrastructure upon which modern society runs, and it needs to be recognized, resourced, and treated appropriately.

3 HOW DOES THE FIELD GROW AND IMPROVE PUBLIC ATTENTION AND AWARENESS AROUND CYBERSECURITY?

Even after years of warnings, too much of cybersecurity remains basic blocking-and-tackling, e.g., encouraging public awareness and adoption of secure passwords and multi-factor authentication, and basic education about computer literacy, phishing attacks, and other threats. Initiatives like Craig Newmark Philanthropies' "Cyber Civil Defense" and CISA's "Shields Up" are working to address these basics and build foundational public awareness around cyber protections, but—much like past public health campaigns around smoking and seat belts—there remains a long way to go before widespread adoption of these lowest-hanging-fruit cyber tools and defenses will start to make the job of attackers more difficult.

4 HOW SHOULD GOVERNMENT, ACADEMIA, AND THE PRIVATE SECTOR BETTER EXPAND, ENRICH, AND PRIORITIZE THE TALENT PIPELINE?

The cybersecurity industry has come a long way from its early days, even if some reforms have come slowly — it took years of rising controversy for major industry conferences, like RSA, to ban so-called "booth babes," scantily clad women that vendors used to promote products and attract attention in exhibit halls. Still today, too many companies and organizations primarily center and promote white, male voices in their events — "manels" (all-male panels) remain shockingly common at industry events. There's much work to be done to bring many, distinct under-represented communities into the fold, from women to communities of color. Too often, diversity efforts remain siloed projects or initiatives, rather than being incorporated into the heart of organizations, programs, and companies. The field, overall, is not doing a great job diversifying.

Moreover, many key institutions, from Congress to the FBI, still don't clearly prioritize or honor cyber expertise. Too many Capitol Hill policymakers, from members of Congress down to committee staff and aides, still don't have appropriate working knowledge of cyber policy issues and broader tech policy concerns We're less removed, insight-wise, from Stevens' "series of tubes" than we should be. Similarly, within government, like at the FBI, cyber expertise is not clearly and widely valued. After 9/11, it was quickly evident that advancing in the FBI leadership ranks required tours on counterterrorism investigations and international operations; today, there are not such clear signals that cyber knowledge and leadership is critical to career advancement. While it has made broad gains in advancing minimum "cyber operating capacity" in each field office — the recent complex Hive ransomware case was run by a new cyber squad out of the Orlando FBI resident agency — such stories remain the exception rather than the norm.

The cyber workforce pipeline, though, is one area where government funding has had a meaningful impact. Among other efforts, the National Science Foundation's 20-year-old CyberCorps® Scholarship for Service program has delivered tens of millions of dollars to nearly 100 academic institutions, across 39 states and Puerto Rico, to build next-generation cyber talent.

5 CAN "TRUST & SAFETY" SURVIVE THE CULTURE WARS?

Notably, major tech companies like Apple, Google, Microsoft, and Amazon have moved, over the last 10-12 years, to invest seriously in cybersecurity, both technically and on the policy side. There is little doubt industry-wise that they, and many other tech companies, are committed to making their users' experience secure and see their investments in information security as important parts of their product experience. Such investments, projects, and policies are hardly perfect, but companies now understand, for instance, that combating data breaches is a core part of their work.

By contrast, social media companies like Facebook and Twitter (now X), have appeared to move in the other direction: After years of investing in robust "trust & safety" teams and meaningful, albeit imperfect, efforts at content moderation, they're reversing course. They seem to be moving away from these commitments as issues of disinformation, misinformation, free speech, and election integrity are increasingly presented by bad actors as being part of brewing political culture wars. Content moderation teams have been gutted at Twitter and at Facebook, news has been deprioritized in algorithmic feeds. Such moves come at a real cost to communities and individuals who face harassment, bullying, self-harm, and hate speech online, and chill conversation across platforms.

6 HOW DOES THE CYBER FIELD GO GLOBAL?

Cybersecurity remains, often, a parochial conversation. While there are meaningful efforts, including the CyberPeace Institute and the Aspen Institute's Global Cyber Group, that aim to build cross-border, multicontinent consensus around key issues, the internet today is splintering faster than ever. Too often, the cybersecurity debate doesn't include the voices and needs of developing societies, including, broadly, the Global South, and remains focused on the perspectives inside just three locales: Silicon Valley, Washington, D.C., and Brussels. The field needs to build, support, and grow voices who represent all global users of these technologies who deserve to be safe and secure — and it needs to better recognize the complexity of these conversations outside of Western-style democracies.

Beyond including more voices more robustly, the splintering of the global internet is opening up opportunities for less-free governments to take more steps to fracture the internet further. There's increasing pressure, even among certain backsliding democracies, to limit free expression and debate online, and seemingly a growing global consensus around each country or region carving out their own regulatory regimes, rather than uniting around globally accepted standards and practices.

7 HOW DO WE BETTER DETER NATION-STATES FROM DESTRUCTIVE ATTACKS?

The need, grasped in the Cyberspace Solarium Commission report, to build better strategies for deterrence has been clear in the wake of Russia's 2021 attack on Ukraine and the following years of conflict, which have included numerous important lessons in the effectiveness of both cyber defense and offense. Companies like Viasat found themselves under direct attack from Russia, Starlink became a critical lifeline for the country, and Microsoft ended up fighting, effectively, on the front lines as it helped the Ukraine government rapidly move its ministries to cloud computing networks after Russia targeted Ukrainian data centers. As U.S. after-action reports came out and the Pentagon advanced its new national cyber strategy, a key tenet was that war wasn't going to be something that governments could conduct on their own anymore. "It was a recognition that the private sector had a tremendous role in shaping what was happening on the battlefield," Eoyang says.

In subsequent years, though, destructive cyberattacks have actually spread, as countries like Russia and Iran use cyber tools to try to shape and grow their influence overseas and as the "hybrid warfare" in Ukraine has continued with new wiper attacks. "Where we need to make progress — and we're losing ground, not gaining ground — is the use by nation-states of destructive cyber tools to expand their influence outside their borders," Microsoft's Tom Burt says. "It isn't getting the kind of international opprobrium that I think would be appropriate if we're going to confine such attacks." Albania, for instance, faced devastating and coordinated cyberattacks and information operations in 2022 from Iran-backed hackers after Iran objected to the Balkan country hosting an Iranian dissident group known as Mojahedin-e-Khalq (MEK). The operations included ransomware attacks, deleting government data, and exposing the identities of Albanian intelligence officers. And, worryingly, they arguably succeeded: Albania cracked down on dissident group leaders in 2023 and MEK leaders have been exploring relocating to another country, perhaps Canada. The primary incident came and went with little public attention. "Where was the international governmental outcry against Iran extending its foreign influence outside its geographic borders to another country in a way that caused that country to change its policies?" Burt asks. The attacks continued for the better part of a year—including as recently as a December 2023 attack where hackers claimed to delete two petabytes of data.

VII: PHILOSOPHICAL BALANCING ACTS STILL TO SOLVE

Beyond questions about the future of the policy field itself, there are still major philosophical questions around the practice, adoption, and future of cybersecurity itself. These include:

1 HOW DO WE REGULATE CYBERSECURITY?

Arguably, more aggressive government regulation became inevitable as our tech-enabled society evolved into one where connected devices could kill and injure people. That level of societal threat and disruption from connected devices — and the accompanying potential for loss of life and property and economic damage — has made cybersecurity impossible for the government to ignore. How exactly, though, those regulations unfold, and the ongoing balance between voluntary and mandatory compliance, remain very much open questions. How do we introduce cybersecurity regulations that are smart and produce better cybersecurity, yet don't stifle innovation? What level of policing is done by regulators vs. legislation? State vs. federal? Regardless of the specific answers, it's clear that one of, if not *the*, biggest unsettled policy questions around cyber issues is: How is regulation done right?

Relatedly, critical lessons are being learned right now in Ukraine about the importance of system resilience. How do we, through some combination of security, innovation, and regulation, better emphasize and incorporate resiliency into our society and remove single points of failure?

2 WHERE SHOULD THE BURDEN OF CYBERSECURITY LIE?

For a variety of reasons, from market pressures and priorities to technological tradition, the responsibility for cybersecurity has generally been pushed all the way out to the edge, to the end user. Even years after the benefits of multifactor authentication and similar "secure-by-design" steps, most programs and websites require users to opt-in to stronger security measures, and many devices, including in the IoT space, ship with obvious vulnerabilities, like hard-coded passwords, and without meaningful security systems. Making cybersecurity the responsibility of the end user has contributed to a long-standing "blame the victim" mentality and results in easily exploitable systems. As the societal risks of hackable systems become increasingly clear and present, how do we start to realign this equation and rebalance where the responsibility for these security measures lies? Relatedly, what are we going to give those who take up the cybersecurity burden? It seems untenable, for instance, to mandate that security be the sole responsibility of telecommunication carriers or ISPs, but are there incentives — legal or software liability protections, for instance — that would make companies more interested in assuming the burden themselves?

3 HOW DO WE GET CLOSER TO THE PLATONIC IDEAL OF CYBERSECURITY, WHERE A VULNERABILITY OR ATTACK VECTOR IS ONLY ABLE TO BE USED ONCE BY AN ADVERSARY?

Too many attacks rely on asymmetric information advantages — hackers continuing to use already-patched exploits on victims whose systems haven't been updated or, alternatively, using the same exploit against multiple victims/sectors because of poor information sharing, siloed intrusion responses, or companies that hush up and fail to communicate intrusions to law enforcement. As Chris Inglis says, "We're still not as coherent as we should be in saying that if the government knows something, then all of the government knows something and, if the government knows something that is of interest to the private sector, than everyone in government will make sure that the private sector knows that." Advancing toward that goal will introduce additional friction for attacks and raise the cost of such efforts. Too often, attackers succeed and thrive because the costs today are too low, both technological and consequences-wise, in terms of criminal charges, sanctions, or other government efforts.

4 HOW DO WE INSTILL A SENSE OF CIVIC RESPONSIBILITY INTO TECH?

It's become increasingly clear that one of the biggest challenges facing cybersecurity is how we encourage technologists, entrepreneurs, and innovators to think more thoughtfully and deeply about the societal risks and challenges of the tools and websites that they're building. The last quarter century has seen repeated instances of companies rolling out new capabilities and tools without considering the civic costs and challenges associated with the advancing technology. As Suzanne Spaulding says, "It's also increasingly apparent that the folks who work in our tech sector and our innovators could benefit from an injection of these basic concepts around civic responsibility." Many people in the tech field have not internalized that they have a responsibility that goes beyond themselves — a responsibility to society, the nation, and their fellow citizens — to design safe and secure systems where all users are welcome and feel safe to participate.

5 SHOULD RANSOMWARE AND ONLINE EXTORTION PAYMENTS BE BANNED OR, ALTERNATIVELY, SHOULD PAYMENT REPORTING BE MADE MANDATORY?

The strong majority of ransomware payments continue to happen in the shadows, without necessarily being reported to regulators or law enforcement. Those payments continue to fuel a thriving ecosystem that allows bad actors to invest in even better tools to become better threat actors or criminal groups. What, if any, steps should governments take to either block or force greater transparency around these payments?

6 HOW DO WE GOVERN PRIVACY — AND WHO GETS TO GOVERN IT?

More than a decade into the era of big data breaches, the United States still doesn't have a uniform regulatory approach to privacy and security incidents. Instead, a patchwork of state-by-state laws and rules from separate regulators, often contradictory, have evolved. The result benefits no one. The EU, meanwhile, has evolved in totally different directions, forcing companies to navigate unsteadily through a mess of rules. No one thinks the current system works and is a rational solution, and unfortunately it results in a global system where neither carrots nor sticks end up being particularly effective in driving smarter security, privacy, or regulation. Now, as new technologies like AI come

into widespread use, we risk a similarly embarrassing and ineffectual patchwork policy response. Nationally and globally, governments need to work to standardize, as much as possible, the regulatory regime around technology, security, and privacy.

Relatedly, we are seeing global pushes for data localization. What's the right model? As more data moves into cloud providers, the EU, China, and the U.S., as well as many other countries in between, are all having fierce political debates around where and how data should be stored.

7 CAN WE STANDARDIZE ATTRIBUTION?

Two of the biggest myths broken in recent years is how cyberattackers are often unknown or mysterious and that crypto payments are untraceable. In fact, governments, and even private companies, have become remarkably adept at tracing bad actors and tracking crypto payments. In multiple high-profile cyber incidents in recent years, Western governments have individually or jointly issued statements attributing attacks to specific nation-states and even, in some cases, indicting specific individual actors. More work, though, needs to be done to develop a coalition of like-minded countries and agree on attribution standards that make it possible to hold rogue parties accountable.

8 HOW DOES CYBERSECURITY FACTOR INTO, APPROACH, CONFRONT, AND RESPONSE TO NEW, EMERGING TECHNOLOGIES?

While the rise of AI and large language models are top of mind in the current conversations around technologies — and will, almost certainly, lead to major change in work and daily life in the years ahead — they are just part of a suite of interconnected transformations that will unfold over the next decade or two. These advances include the rise of quantum computers (and the associated need to develop and deploy quantum-resistant cryptography), as well as the rise of all-new biosecurity challenges, including at-home gene splicing technologies. One of the major challenges of the last quarter-century of cybersecurity is how we moved our information online, onto inherently vulnerable and insecure systems never built to protect the secrets they now carry. "We realized, at the end of the day, that cybersecurity was essential to our existence, and with a lot of pain and suffering, brought it back in and welded it to the frame," Inglis says.

How do we learn the lessons of that last quarter-century and move toward thinking through systems that are secure by design? How do we create spaces where humans are comfortable and safe? How do we be intentional about security and safety, while balancing the need to preserve innovation and experimentation? How do we understand the risks better upfront and make more conscious choices about security? We're still catching up to yesterday's threats — can we do more to prevent or mitigate the threats of tomorrow?