COLUMBIA | SIPA
School of International and Public Affairs

Building a Defensible Cyberspace

NEW YORK CYBER TASK FORCE

Contents

A more defensible cyberspace is possible, but only through *leverage*: innovations that give defenders the most advantage at the greatest scale at least cost.

Foreword

Providing satisfactory security controls in a computer system is in itself a system design problem. A combination of hardware, software, communications, physical, personnel, and administrative-procedural safeguards is required for comprehensive security. In particular, software safeguards are not sufficient.

"Security Controls for Computer Systems: Report of the Defense Science Board on Computer Systems" *(aka, The Ware Report)*[1]

For decades, cybersecurity professionals have been treading water, putting in never-ending effort but rarely making progress. The quote above would not seem obsolete if it appeared today on a slide in a vendor presentation or at a computer security conference, *yet the report it was taken from was published in 1970*. Nearly five decades have passed, yet the problems remain the same. It is time for defenders to change their approach.

The New York Cyber Task Force was formed in the Fall of 2015 to try to break this stalemate. Our conclusion is that defense is possible, but only if we identify and prioritize the right innovations.

In keeping with the recommendations of the Ware Report, the task force was compromised of ~30 experts with varied backgrounds in cybersecurity, including many members from New York City, who contributed a distinct, practical, in the trenches perspective. As the nation's political capital, Washington, DC can sink into pessimism over cyber threats, the "new domain of warfare"; Silicon Valley, the global technological capital, sometimes falls victim to its own unbounded optimism.

For New Yorkers, balancing threats with opportunities is as natural as crossing the street. New York is one of the global cities; participants want the best for America but understand these interconnected and complex problems require global solutions.

During the course of dozens of meetings over 2 years, we carefully examined ways to make cyberspace more defensible, focusing on four core questions:

- Why hasn't cyberspace been defensible?
- What innovations in technology, operations, and policy have made the biggest difference on the largest scale and at the least cost?
- What common factors contributed to the success of these innovations?
- Based on these past successes, what new innovations deserve attention and investment?

This report presents our consensus on ways to make cyberspace more defensible without sacrificing what makes it essential to our national economies and personal lives. We coalesced around a concept that can be expressed in a single word: leverage.

The most successful innovations have been those that were leveraged, they operate on an internet-wide scale and impose the highest costs (roughly measured in both dollars and effort) on attackers with the least cost to defenders.

Leverage is not the same as increased cybersecurity return on investment, as understood by business executives; nor does it simply increase costs to attackers, a strategy commonly employed by military and law

enforcement. Rather, it facilitates broader thinking to maximize the impact of these and similar strategies, at Internet scale, for the least cost to the defender.

Some of our colleagues have given up on defense in favor of more counter-offensive attacks to disrupt the operations of our adversaries. Others place their faith in some kind of cyber deterrence. Such tactics have a role when they provide leverage, but they are only part of the solution. At the core of our recommendations are the many new innovations across technology, operations, and policy that will give defenders far more advantages than we have today.

Many in the field have called for a "moonshot" or even a "cyber Manhattan Project," a massive surge of effort to improve cybersecurity before it is too late. Perhaps that is indeed needed, but it should not detract from the incredible progress that can be made with the patient application of those innovations that provide the most leverage.

Our task force includes leading cybersecurity executives, world-recognized technologists, former White House and government officials, and renowned academics.

Some of our recommendations are directed at companies dependent on cyberspace. Others are aimed at policymakers, at technology executives developing the next generation of standards and IT tools, or at academics and think-tank experts. We believe that together, we can establish a more defensible cyberspace.

We give our thanks as co-chairs to the members of the task force, who gave their time and ideas, as well as many other practitioners and academics who provided valuable input. Our special thanks to Jason Healey, the author of this report, for playing a lead role in conceptualizing and organizing this effort.

Not all members fully concurred with every finding in this document, but a broad consensus emerged on the goal of making cyberspace more defensible, the importance of leveraging innovations to achieve that goal, and that "to do nothing" is not an option.

The views represented and attributed herein are those of the participants and do not represent the policies or opinions of the organizations to which they are currently, or were previously, affiliated.

Many others helped us along this journey, including our colleagues at Harvard University's Belfer Center for Science and International Affairs, Stanford University's Center for International Security and Cooperation, McKinsey and Company, PricewaterhouseCoopers, Barclays, Baker McKenzie, participants of the Black Hat and New York State Cyber Security Conferences, the Cyber Green Initiative, Spencer Francus of JP Morgan Chase for his assistance with graphic design, and several SIPA students, including Christian van de Werken, Joyce Dong, Alex James, Claudia Shrivastava, and Christine Taylor.

To these and others, we give our thanks and the reminder that defense is possible. We hope that our conclusions in this report contribute to the ongoing essential dialogue regarding how we further enhance the security of cyberspace, the world depends on it.

Merit E. Janow **Gregory Rattray** **Phil Venables**

Members of the New York Cyber Task Force

Dmitri Alperovitch, CrowdStrike

Angela McKay, Microsoft

Edward G. Amoroso, TAG Cyber

Jeff Moss, DEF CON and Black Hat

Steven M. Bellovin, Columbia University

Derek O'Halloran, World Economic Forum

John W. Carlson, FS-ISAC

Gary Owen, Time Warner

Gordon M. Goldstein, Silver Lake

Neal Pollard, PricewaterhouseCoopers

Royal Hansen, American Express

Gregory Rattray,† JPMorgan Chase

Jason Healey,* Columbia University

Katheryn E. Rosen, Atlantic Council

Melody Hildebrandt, 21st Century Fox

Marcus H. Sachs, NERC

Yurie Ito, Cyber Green Initiative

Karl Schimmeck, Morgan Stanley

Merit E. Janow,† Columbia University

Adam Segal, Council on Foreign Relations

James Kaplan, McKinsey

Timothy Strabbing, Viola Foundation

Elena Kvochko, Barclays

Phil Venables,† Goldman Sachs

Arthur M. Langer, Columbia University

Matthew Waxman, Columbia University

David C. Lashway, Baker McKenzie

John Yetter, NASDAQ

Aaron K. Martin, JPMorgan Chase

Larry Zelvin, Citigroup

* Task Force Executive Director † Task Force Co-Chairs

Executive Summary

In a little over 20 years, the percent of the global population with access to the Internet (and the larger *cyberspace* of connected devices and information, terms this report will use interchangeably) has gone from less than one to about 40, over 3.595 billion people.[2] In the United States alone, the Internet sector makes up an estimated six percent of GDP; the "mobile internet and app services" subsector alone has a "contribution to the US GDP [of] approximately 3.11%, putting it at approximately the same size as the Automotive industry."[3] Yet, as the reach and benefits of the Internet have increased, so too have the economic costs. A 2015 study indicated that cybersecurity costs were likely to rise above $1.2 trillion by 2030 costing a total of roughly $20 trillion over those 15 years.[4]

The costs are high because attackers in cyberspace have for decades held fundamental advantages over defenders. The Internet was designed to be flexible and open, not secure. For years, nearly every device and piece of code added to cyberspace has reiterated this pattern: "minimum viable products" are rushed to market with security slapped on afterward as a band-aid, rather than built in. All this complexity has multiplied the costs and challenges of mounting a successful defense.

Still, defense is possible. This report builds on an increasingly rich set of cybersecurity research on creating a "defense advantage" that raises costs to attackers and enables cost-effective risk management. Some of these ideas, such as to allow the least privileges or to failsafe in a secure manner, date back to the 1970s.[5] Other work, especially in the business community, has centered on the return on investment of defensive innovations. Inspired by military tactics, others have sought to raise costs to attackers by making their task harder or actively disrupting their operations. The NY Cyber Task Force, through the experience of our members and interviews with other experts, has tried to combine these three perspectives.

Our task force started by asking, "what technological, operational, and policy innovations have had the greatest impact in thwarting attackers?" We found that the highest-impact innovations shared two key traits:

- Defense advantage: Any innovation by defenders must impose far greater costs on attackers. A "dollar of defense" (or hour or other measure of input) should yield not merely a "dollar of attack," but should force attackers to spend considerably more to defeat it.
- Hyperscale: The innovation must easily, even automatically, work across enterprises or cyberspace as a whole.

The task force members and the colleagues we interviewed consistently agreed on the past innovations with the highest scale and leverage over attackers: strong encryption, software that updates automatically with little or no user intervention, and software that is secure because it was designed that way (rather than having security bolted on afterwards), among others.

Importantly, the most transformative innovations have come not only from technology. Some of the greatest advances in defense advantage and hyperscale arose from improvements in organization, such as the creation of the first Computer Emergency Response Teams in the 1980s, and governance, such as the development of C-suite cybersecurity experts (e.g., Chief Information Security Officers) in the 1990s. Other successes have come from process innovations, like the "cyber kill chain" and "intelligence-driven operations." And, better mapping and analysis of the way attackers intrude into systems has led to better strategies to keep them out.

Policy actions, such as issuing legal indictments and threatening governmental sanctions, seem to have fostered bilateral norms and reduced the volume of espionage operations, particularly from China. In 2013, the White House set a new policy instructing

the US government to tell companies if it detects data breaches in their systems.[6] Largely because of this policy (barely 200 words long), notification from law enforcement is now one of the most common ways companies learn of intruders. This public-private cooperation means faster responses, limiting the disruption attackers can cause.[7]

In each of these cases, the solution (while not necessarily cheap in hours or dollars invested) reaped benefits that significantly outweighed costs. This kind of leverage can make cyberspace more defensible for a company, a sector, a nation, and the world as a whole.

Having carefully assessed a variety of innovations, we have concluded that defenders should adopt innovations that have the highest return. This, of course, requires that we assess each innovation for its benefits and costs, an analysis that seems obvious, but is not commonly employed today.

The task force also identified several innovations with potentially large impact, such as reaching a consensus between policymakers and technology leaders to build a defensible cyberspace, promoting more secure cloud-based technologies, and improving authentication by finally dispensing with passwords.

Certain innovations we assessed were controversial among the members of the task force, such as imposing regulations on network service providers and holding software and hardware makers liable for products with known but unpatched vulnerabilities. These and other approaches might deliver significant leverage, but would certainly be met with fierce resistance and potentially impose significant hurdles to innovation.

Some solutions can be implemented easily; others will be more difficult because they create clear winners and losers. All members of the task force agree that the best solutions rely on leverage and are necessary now to avoid far more intrusive ones later. Text Box 1, below, summarizes the steps needed. Below we summarize certain of our key findings regarding steps needed. Taken together, these steps will help build a more defensible cyberspace.

Text Box 1: *Summary of Action Plan*

Recommendations for the US Government

1. Create a new cyber strategy based on leverage
2. Focus on transparency and risk-based governance, especially when they align market forces
3. Migrate to cloud and other new technologies that will deliver leverage
4. Use federal funding to support leverage in the private sector
5. Assess any potential innovation for benefits and costs

Recommendations for IT and Cybersecurity Companies

1. Never stop implementing the highest-leverage innovations
2. Don't just share, but collaborate, including with funding to nonprofits doing critical work
3. Assess any potential innovation for benefits and costs

Recommendations for Highly IT-Dependent Organizations

1. Start from the board down, not the technology up
2. Implement the highest-leverage innovations
3. Emphasize agility and resilience, two of the most general-purpose investments available
4. Assess any potential innovation for benefits and costs

Introduction: The Upside and Downside Risks of Cyberspace

Cyberspace—the Internet and billions of devices connected to it—must be made more defensible, at scale and at modest cost, or it will cease to drive economic, social, and cultural empowerment as it has over recent decades.

Columbia University's School of International and Public Affairs convened a New York Cyber Task Force to assess how we can achieve a more defensible cyberspace and to develop recommendations relating to technological, operational, and policy innovations necessary to achieve that end. Task force members discussed the most defensible past innovations, the keys to their success, and the innovations policymakers, technologists, and cyber defenders should pursue next. The way ahead is hard, but a defensible cyberspace is possible.

The Internet and connected devices started as a niche for technical academics and blossomed to become a core feature of our professional and personal lives, allowing us to pursue our interests, innovate faster, and build a better, stronger economy. The payoff has been as breathtaking as the pace of change.

In just over 20 years, the percent of the global population with Internet access has gone from less than one to about 40, over 3.5 billion people.[8] Much of this growth has occurred in developed countries. In the United States alone, the Internet sector makes up an estimated six percent of GDP.[9] According to the McKinsey Global Institute, in the countries studied, "the Internet accounted for 21 percent of GDP growth over the last five years" from 2011.[10] Importantly, the benefits were broadly spread, as "most of the economic value created by the Internet falls outside of the technology sector, with 75 percent of the benefits captured by companies in more traditional industries." The scale of these statistics may at first seem surprising, but consider the Internet's impact on almost every facet of commerce. It allows small- and medium-sized enterprises to enhance their global outreach, small-plot farmers to check weather and prices, and grocery stores to reduce food waste and, as a result, prices.

One of the coming breakthroughs is the Internet of Things (IoT), which is already connecting the devices we use in everyday life to networks and to each other. Some IoT projects aim for convenience; online door locks and cameras will allow Airbnb hosts to use their smart phone to welcome guests. But the IoT also includes critical infrastructure, such as the Smart Grid, which brings electrical generation and distribution systems online to increase efficiency and reduce environmental impact. Self-driving cars will depend on computers and networks to reduce traffic accidents, saving perhaps 30,000 lives a year (provided that people come to trust them).[11]

Internet technologies are transforming not just the economy, but culture and society as well. There are over 1.9 billion Facebook users, sharing life stories, recipes, news, and photos.[12] Cities like New York have historically facilitated interaction between people from different backgrounds and allowed those with eclectic (or even taboo) interests and ideas to find kindred spirits. Online interest groups, with members from anywhere in the world, now re-create this community.

Despite the copious grounds for pessimism, the members of the NY Cyber Task Force believe the way ahead is hard, but a defensible cyberspace is possible.

But this widespread usage has a dark side. As the National Academies of Science noted back in 1991 in a landmark report, *Computers at Risk*:

> As computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems. Without more responsible design and use, system disruptions will increase, with harmful consequences for society.[13]

When the NY Cyber Task Force began meeting in the fall of 2015, distributed denial of service attacks were already considered a major scourge, with the largest reaching 400 gigabits per second; in January 2016, the onslaught increased by around 50 percent with a 600 gigabits per second attack.[14] Later that year, much of the Internet on the East Coast of the United States was disrupted when the attack size doubled yet again to 1.2 terabits per second.[15] The massive WannaCry ransomware attacks of May 2017 affected hundreds of thousands of computers, including 47 separate organizations in the UK National Health System, delaying surgeries and otherwise disrupting patient care.[16] These attacks demonstrated that nearly any target—even a large portion of a technologically advanced country that has spent tens of billions of dollars on cyber defense—can be taken offline without much effort.

Such threats are already limiting how people use the Internet. Email, the Internet's initial "killer app," managed to survive the onslaught of spam; 99.99 percent of the 400 billion daily spam messages are now caught.[17] But the world may have hit "peak email" in the face of spearphishing attempts, such as the hack of the Democratic National Committee, that trick the unwary into revealing passwords and mass dump embarrassing and politically sensitive emails.

As already-creaky critical infrastructure is connected to cyberspace, the hackers, spies, and militaries that breach the email of national leaders can also attack a country's electrical power or manufacturing firms. Nearly every part of the deployed IoT—including the Ukrainian electrical grid, a German foundry, refrigerators, and baby monitors—has already been hacked. Few of these devices were designed to be connected. As bad as cybersecurity seems now, with global dependency on fundamentally insecure technologies increasing, the worst may be still to come.

Screen capture from the Wannacry ransomware attack which affected hundreds of thousands of computers in May 2017

A 2015 Atlantic Council study found that cybersecurity costs were just over one percent of global GDP and likely to rise above $1.2 trillion annually by 2030, costing a cumulative ~$20 trillion over those 15 years.[18] If attackers definitively gained the upper hand, the worst case modeled in the study, global GDP could decline by more than seven percent. Internet connectivity might cease to be seen as a human right but rather a luxury good.[19]

Even with annual cybersecurity spending already passing $75 billion, cybersecurity has done little more than slow this progressive onslaught.[20] As cybersecurity expert Dan Geer has put it,

> There are over 1,000 cyber security startups somewhere between kitchen table and IPO [and] technology patents are running at three million per year […] A shortage of invention is probably not our problem. CyberCom's budget is $500 million; JPMChase alone is spending $600 million. Whether that is surprising or simply as it should be, a shortage of money is probably not our problem, either.[21]

What, then, is our problem? Perhaps our efforts have lacked the right focus. So despite the copious grounds for pessimism, the members of the NY Cyber Task Force believe defense is essential, and requires that we pursue technological, operational, and policy innovations that provide for the most benefit.

Factors that have Undermined Cyber Defense

It is not news that cyberspace is insecure. Attackers have had the advantage over defenders for not just years, but decades. Quotes from the late 1970s make it clear that cyber defenders then faced the same challenges we do today (and with a similar lack of success).[23] Defenders have not gained any lasting advantage from four decades' worth of innovation, tens or hundreds of billions of dollars spent on security, or the tens of thousands of certified cyber defenders. Cyberspace remains "attacker advantage."

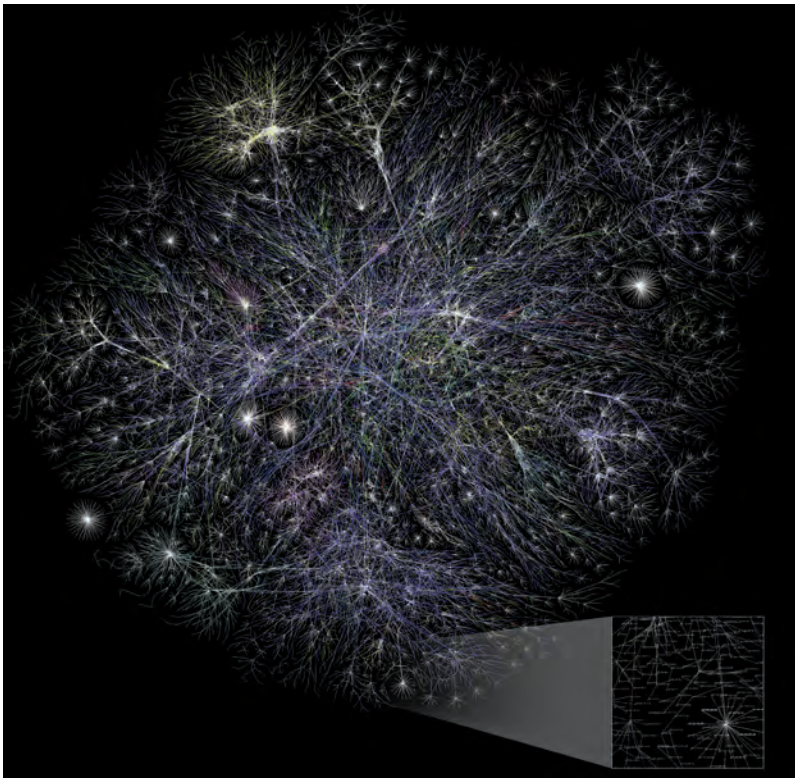
> "Offense has overwhelmed defense [leading] to a sense of helplessness . . . If we accept defense is futile because offense always wins, then we all stop trying as hard. We focus on cleanup instead of prevention."
>
> **Jeff Moss** (aka The Dark Tangent),
> *Founder of DEF CON and the Black Hat conferences*

Keeping cyber attackers from gaining a foothold in computers—and kicking them out once they do—remains easy to imagine but difficult to accomplish in practice. Why has this been so challenging? Every cyber defender has their own favorite reason. The NY Cyber Task Force identified the following as some of the most important:

- **Internet architecture:** "The Internet is not insecure because it is buggy, but because of specific design decisions" to make it more open, explains pioneer computer scientist David Clark.[24]
- **Software weaknesses:** Not only is it impossible to write bug-free code, but "[t]here are no real consequences for having bad security or having low-quality software … Even worse, the marketplace often rewards low quality," according to security expert Bruce Schneier.[25]
- **Attacker initiative:** An "[a]ttacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all," according to the 1991 report *Computers at Risk*.[26] Spending on defense is accordingly very diffuse.
- **Incremental solutions:** Fixes typically target symptoms rather than underlying problems. To paraphrase Phil Venables, NYCTF co-chair, the uninterrupted production of insecure IT products forces companies to buy ever more IT security products.[27]
- **Attacker incentives:** Cyber crimes, warfare, and espionage can seem risk free because of the often difficult process of attribution, ease of crossing borders to stymie law enforcement, sanctuary certain nations offer cyber criminals, and differing national laws.
- **Impact to convenience:** Improved security often imposes costs on ease of use. As a result, it is frequently bypassed, or never even implemented, by individual users and beleaguered IT staff.
- **Arcane security and opaque products:** "Most consumers have no real-world understanding of [cybersecurity] and cannot choose products wisely or make sound decisions about how to use them." This is as true today as when it was written in the 1991 *Computers at Risk* report. Cybersecurity has gotten so complex that even IT staff struggle to understand the products.[28]
- **Longevity of attack methods:**Attacker innovation in cyberspace is often unnecessary because older, simpler tools remain effective against most targets.
- **Troublesome humans:** People can be tricked or grow disgruntled and, in the words of one expert, "are always the weakest link … you can deploy all

the technology you want, but people simply cannot be programmed and can't be anticipated."[29]

- **Rapid pace of technological change:** The accelerating pace produces ever-larger potential attack surfaces and ever-more skills, education and certifications necessary for successful defense.
- **Complexity:** Defending this attack surface has required a profusion of new tools. "Increasing complexity increases cost" and "decreases the predictability of new costs."[30]
- **Sentient opponents:** According to expert Dan Geer, "the one thing that may make cybersecurity different … is that we have sentient opponents … [so that the] puzzles we have to solve are not drawn from some generally diminishing store of unsolved puzzles," as in physics or economics.[31] Those opponents fight for access to our systems in pursuit of profit, intelligence, military advantage or curiosity.
- **Lack of coherent strategy:** Few, if any, of the various reports or cyber strategies lay out an overall approach to bind the work or guide between competing priorities. They are instead lists of critical tasks with no underlying theory of how these tasks will lead to success.



The Internet (represented graphically here) is impossibly complex as is the software, hardware, and human interactions with all of it.

SOURCE: **Matt Britt** (https://commons.wikimedia.org/wiki/File:Internet_map_4096.png), "Internet map 4096," https://creativecommons.org/licenses/by/2.5/legalcode

A More Defensible Cyberspace

The NY Cyber Task Force believes that cyberspace can be made more defensible, perhaps even to the degree that defenders, not attackers, have the overall advantage. If so, then perhaps the IoT and other new technologies can be deployed safely, enabling further innovations for culture, society, and the global economy.

The NY Cyber Task Force has determined that to become more defensible, cyberspace must be:[22]

- Tolerant of flaws, strong and effective under adversity
- Capable of recovering readily with swift and well-coordinated responses
- Capable of agile decision making and crisis response
- Instrumented and measurable
- Well managed by multiple stakeholders
- Viable and valuable over the long term
- Capable of constraining negative externalities

These characteristics would not, however, make cyberspace a perfect utopia. Cyber criminals would still find sanctuaries and instigate security incidents (and even, occasionally, disasters). But cyberspace as a whole would be secure and resilient enough to give defenders the upper hand and keep incidents relatively insignificant. Analogously, pirates and other scourges still plague certain hot spots, yet the seas and oceans overall are safe for liners, container ships, and sailing boats, supporting global commerce, recreation, and culture.

Past Innovations to Make Cyberspace Defensible

In late 2014, *The Economist* published a policy briefing on climate change with two key findings relevant to cybersecurity.[32] First, the researchers seemed surprised that by far the most successful carbon-mitigation intervention was the Montreal Convention outlawing chlorofluorocarbons. That agreement of 119 nations and the European Union was as successful as nearly every other intervention combined. Scott Barrett of Columbia University called it "one of the greatest successes of international cooperation in human history."[33]

Second, as far as *The Economist* could determine, few had ever thought to ask the obvious public policy question, "What solutions have been most effective at least cost?" This crucial question should be applied to cybersecurity as well as the environment.

Accordingly, the NY Cyber Task Force has focused on the question, "Which innovations—across technology, operations, and policy—have made us the most secure at the least cost?" Rather than simply listing important next actions, cyber strategists should assess innovations and prioritize those that improve defense on the greatest scale and at the least cost, based on the precedent of successful past innovations.

Our preliminary assessment (see the main figure in the centerfold of this publication) is based on the views of the experts in the task force along with dozens of interviews and other research. Without these innovations, cyberspace would be far less defensible than it is today. Appendices will be posted online with more detail about each listed innovation.

Technological innovations, the leftmost column, are the most obvious solution to technological problems. These innovations started with passwords, firewalls, and other basic security tools that solved challenges within an organization's computing and network perimeter. Other technological solutions, such as automatic update programs, work across cyberspace as a whole. It was certainly not inexpensive for Microsoft to develop Windows Update, but it changed the security landscape by allowing all copies of Windows (even, eventually, illegal copies) to be patched to the most-secure configuration.

Unfortunately, too few technological solutions tackle the underlying problem of an insecure network and computing infrastructure. As Beau Woods of the Atlantic Council explains, in the early days of the Internet, it was easier and cheaper to apply after-market band-aids, like anti-virus software or intrusion detection systems, rather than solve those more fundamental issues.[34] As a result of quick fixes, the "economics have flipped." It is now band-aids all the way down, so much so that "buyers' remorse around purchased cybersecurity products" has now topped 50%.[35] Remedying underlying causes (especially, as we will see, with the possibilities offered by the cloud) has become comparatively easy and inexpensive.

Operational innovations, the center column, have picked up some of the slack. After the Morris Worm crashed around 10% of the early Internet in 1988, the Department of Defense created the Computer Emergency Response Team (CERT) to prepare for and respond to such events. Now, of course, CERTs are essential and ubiquitous. Likewise, the now common role of Chief Information Security Officer had to be invented, in this case by Citibank in 1995, after the cyber theft of $10 million.

C-suite officers who understand cybersecurity as a business or operational risk now work closely with CEOs and boards of directors, leading to better risk management, increased security resources, smarter investment of those resources, better integration of security requirements with business priorities, and top-level cover for hard decisions that are defensible to shareholders and customers. This board-level involvement (driven in part by regulations and reputation risk concerns) has helped align market forces for improved security.[36] CEOs and boards now ask better questions about their role in cybersecurity, driving smarter corporate behavior.

The DevOps movement is a relatively new set of *practices* bringing together software developers, system administrators, network engineers, and security experts for more effective and secure software. The innovation of the "cyber kill chain" helped change the way defenders detect and stop attackers not with a new IT widget but through a new *doctrine*.[37] Clearer thinking about the way attackers intrude into systems led to better strategies to keep them out.

The operational innovations with the most impact are perhaps the least known: the many formal, semi-formal and informal groups of non-state technical experts. Groups like the Cyber Threat Alliance, the North American Network Operators Group (NANOG), and the Industry Consortium for Advancement of Security on the Internet (ICASI) bring together the relevant professionals in purpose-built groups to combat threats and keep networks running smoothly.

Policy innovations, the rightmost column, have become more important as societies have become more technologically dependent (and certain technological fixes have failed to live up to their promises). In 2013, the White House instituted a new policy default position: if the US government obtains any information that a US company has been compromised, it should inform the company. Because of that 200-word policy, notification by law enforcement has become the top way that companies learn they've been breached. This notification allows responses to begin months or even years earlier, mitigating damage to the firms and the wider ecosystem.[38] Unfortunately, policy successes are not usually so obvious; they are often obscured by several factors, including a lack of metrics.

Because policy decisions made at the national level can change the direction of global technological innovation, the stakes are incredibly high. Such decisions can create winners and losers and can be in tension with other societal goods. The Federal Trade Commission, for example, may punish a company that suffers data breaches.[39] Is this a positive step towards holding a company responsible for data security, or an unfair outcome for a company that is the victim of a cyber crime?

Policy innovations are not only harder to measure, but confirmation bias and "ideological" differences can make it difficult to determine whether a solution is working at all, or whether a different solution would be more effective. Arguments over whether market forces or regulation would be more effective often lack direct evidence. Despite the factors, task force members were able to reach a near consensus on certain important policy innovations.

> "[P]olicy matters are now the most important matters . . . once a topic area, like cybersecurity, becomes interlaced with nearly every aspect of life for nearly everybody, the outcome differential between good policies and bad policies broadens, and the ease of finding answers falls."
>
> **Dan Geer,**
> *cybersecurity expert*

Offense innovations. The attackers have had their own innovations as well, which have generated offense-advantage and hyperscale. These are listed in the appropriate figure in the centerfold of this publication. Many of these technologies require little or no skill, allowing even newbies to point-and-click their way to hacking success. The attackers have also had operational and policy successes, such as establishing specialized markets for cyber crime as a service, including escrow accounts to build trust, and forming symbiotic relationships with corrupt governments to create sanctuaries for cyber crime.

Building a More Defensible Cyberspace

The Problem: Attackers in cyberspace have for decades held fundamental advantages, due to critical factors such as an Internet that was never designed for security and software weaknesses.

The Goal: Cyberspace must become more defensible.

- Tolerant of flaws, strong and effective under adversity
- Capable of agile decision making and crisis response
- Well managed by multiple stakeholders
- Capable of constraining negative externalities
- Capable of swift and well-coordinated responses
- Instrumented and measurable
- Viable and valuable over the long term

Our Strategy: To build leverage by enacting technological, operational and policy innovations with the following characteristics.

- **Defense advantage:** Any innovation by defenders must impose far greater costs on attackers. A "dollar of defense" (or hour or other measure of input) should yield not merely a "dollar of attack," but should force attackers to spend considerably more to defeat it.
- **Hyperscale:** The innovation must easily, even automatically, work across enterprises or cyberspace as a whole.

Leverage to Date: Cyberspace would be even less defensible today were it not for the last five decades of important technological, operational and policy innovations.

Lessons of Leverage: Analyzing these innovations provides critical lessons.

- Game-changing innovations share one key feature: scale massively aids the defense
- Game-changing innovations use the minimum necessary intervention
- Operational and policy innovations are powerful but overlooked and misunderstood

Leverage to Come: Cyberspace can be made defensible by applying innovations with leverage, including technological, operational and policy innovations.

- The biggest gains come from the innovations with the greatest defense advantage and with hyperscale, automatically working across cyberspace as a whole

Recommendations: Cyberspace can be made defensible by applying innovations with leverage, including technological, operational and policy innovations.

For the US Government

1. Create a new cyber strategy based on leverage
2. Focus on transparency and risk-based governance, especially where these align market forces
3. Migrate to cloud & other new technologies that will deliver leverage
4. Use federal funding to support leverage in the private sector

For IT and Security Companies

1. Never stop implementing the highest-leverage innovations
2. Don't just share, but collaborate, including with funding to non-profits doing critical work

For IT-Dependent Organizations

1. Start from the board down, not the technology up
2. Implement the highest-leverage innovations
3. Emphasize agility and resilience, two of the best general-purpose investments available

Leverage: The Key to Success

Not all defense innovations have been equally important. Those with the highest impact have created **leverage**. To make a real difference, an innovation should have two key traits:

- **Defense advantage**: Any innovation by defenders must impose far greater costs on attackers. A "dollar of defense" (or hour or other measure of input) should not yield just a "dollar of attack," but should force attackers to spend considerably more to defeat it.
- **Hyperscale**: The innovation must easily, even automatically, work across enterprises or cyberspace as a whole.

The innovations that generated the most leverage—including automatic software updates, firewalls, information sharing organizations, and cybersecurity laws—have been the hardest for attackers to adapt to and overcome. Encryption, an example provided by Herb Lin of Stanford University, is "a hyperscale solution—it's relatively inexpensive by itself, and yet it secures much larger value" and is relatively expensive to circumvent.[40] Defense would be far worse off were it not for past innovations that delivered leverage.

The idea of cybersecurity leverage is not entirely new. Practitioners and researchers have been exploring defense-advantage solutions, and businesses seek the best return on investment for their security dollars. The US military has been seeking a cost-imposition strategy to deter cyber adversaries.[41] Leverage builds on these foundations, deepening the idea of defense advantage to distinguish between enterprise and sector-wide innovations and broadening it to specifically include operational and policy innovations as well. Measuring ROI for security with any precision has been notoriously difficult. While cost imposition underlies many of the innovations in Figure 1, such as indictments and sanctions, it is only half the equation and ignores the need to reduce costs to defenders. The most germane work on this subject has been that of John Mallery of MIT, who has long argued that improved defense comes from raising the work factor of attackers and reducing that of defenders.[42]

Keeping the Internet at least as secure as it is today requires an understanding of what made the best past innovations successful: leverage. The next pages will explore the innovations with the most leverage, those that created the greatest defense advantage, at the largest scale, for the lowest cost.

But before discussing the hall of fame, it's worth mentioning the losers.

The most important technological, operational, and policy innovations have worked through specific mechanisms:

- *Hardening* of a network, program or device (e.g., firewalls, anti-malware)
- *General protection* from a wide range of attacks (international norms)
- Improved *situational awareness and coordination* (information sharing)
- More *effective response or improved resilience* to disruption (CERTs)
- Better *education, training and awareness* (exercises, certifications)
- Improved general *organizational and management capacity* (leadership and board attention)
- *Disrupting adversaries* or increasing their costs (arrests, botnet takedowns)

From Essential to Albatross

Even the best innovations have an expiration date. They roll through a cycle of four stages: promising, amazing, stale, and expired (see Figure 1 for a conceptual view). They fade as technologies change, adversaries adapt, and complexity increases.

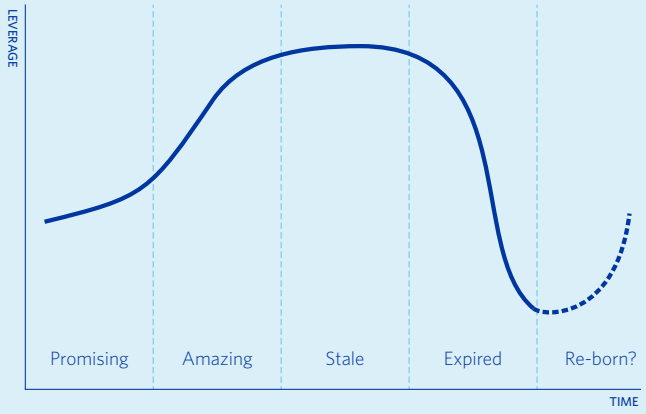


Figure 1: Cycle of Cybersecurity Innovations

Many other innovations, in the judgment of the task force and those interviewed, were bad ideas from the start. In the past few years, government arms control experts have introduced rules for applying the Wassenaar Arrangement on the export of dual-use technologies (those that have a peaceful purpose but could also serve as armaments) to offensive cyber technologies.[43] These rules generate "negative leverage," imposing high costs on defenders and placing only minor obstacles in the way of attackers. One cybersecurity company reported that it would have to request at least 1,000 export licenses to comply, instead of the ten it currently needs.[44]

Static and prescriptive "checking-the-box" cybersecurity typically also creates negative leverage (see text box 2). While perhaps satisfying regulators, these protections often force defenders to expend far more effort than it costs attackers to circumvent them. This was not always the case. Two decades ago, cybersecurity architectures were less complex and threats less varied, so defenses built on static checklists were more effective at keeping out adversaries.

Check-the-box compliance has, in short, gone from essential to albatross. Once a game changer, it has over time become a drain on the resources of defenders.

The NY Cyber Task Force came across many such innovations that have persisted past their expiration date. Passwords, by far the most cited albatross, have long been an insufficient means of authentication when used on their own.

Firewalls, intrusion detection, and anti-malware may be approaching their expiration date. For the better part of two decades, they have been the basic building blocks of an effective defense. Now, however, they are growing increasingly stale, especially against sophisticated adversaries.

Data breach notification laws may soon reach their own limits. States enacted these laws to protect the privacy of citizens whose information might have been compromised and to incentivize companies to improve security and avoid the embarrassment of disclosure. But now data breaches are so commonplace, and the public so fatigued by endless notifications, disclosure is often seen as just another cost of business, with little to no leverage.

Expired innovations can create more pain for defenders than they cause for attackers. They should be retired, de-emphasized, or re-invented.

Most expired innovations should be retired, or at least de-emphasized. But some might gain a new lease on life if it is possible to drastically reduce their costs, use them in combination with other innovations to extend their life, or otherwise revamp them to regain leverage.

Passwords have regained leverage when combined with a second form of authentication, such as a text to a mobile phone. Even compliance can be reinvigorated when combined with risk-based frameworks. According to a PwC survey, organizations adopting structures like the National Institute of Standards and Technology (NIST) Cybersecurity Framework or ISO 27001 greatly improve their ability to identify and prioritize risks, detect and mitigate threats, and measure progress.[45]

Text Box 2: *Checklists and Leverage*

Innovations that are built around checklists initially spurred significant disagreement amongst the task force and the experts interviewed. Further conversations and reflection helped create a consensus.

Checklists and checklist-like documents can provide significant leverage, but only in circumstances when they can reduce complexity before a crisis hits.

- A checklist can show an administrator just how to most securely configure and connect a new device, simplifying what might otherwise seem insurmountable.
- Lists such as "The Top 20 Controls" by the Council on Cybersecurity serve a similar function, but for entire enterprises.
- Playbooks can guide operational response after an incident, preloading the tough decisions and keeping different response teams better coordinated.
- Auditors can glean important information about the security of an enterprise if checklist actions have been completed.

But checklists can be ruinous when used outside such tasks and depended upon for nearly the entirety of security, rather than as one method to achieve it. Checklist-driven security programs, especially when tied to compliance requirements rather than actual risk, often fail to keep pace with changing technologies. During an incident, checklists can guide decisions, but never substitute for them. Defenders relying on only checklist-driven protections cannot compete against sentient adversaries.

Further development of checklist-based innovations will be critical, since "under conditions of complexity, not only are checklists a help, they are required for success," according to Atul Gawande in *The Checklist Manifesto*. "There must always be room for judgment, but judgment aided—and even enhanced—by procedure."

But the NY Cyber Task Force found perhaps more disenchantment with static "check-the-box" cybersecurity than any other innovation. These kinds of checklists need to be either significantly reworked or discarded entirely.

NEW YORK CYBER TASK FORCE

Important Defensive Innovations of the Past 50 Years

- Hardening Assets
- Situational Awareness
- General Security
- Organizational & Management
- Education, Training, and Awareness
- Response & Resiliency
- Disrupting Adversaries

SIPA

Where is primary effect of the innovation? — *What kind of innovation is it?*

WITHIN ENTERPRISE

Changes implemented by centrally managed IT team

PAST

TECHNOLOGY

- Computer and network passwords (1960s–1980s)
- Intrusion detection (1990s)
- Mass vulnerability scanning (1990s)
- Encrypted data & comms (2000s)
- Intrusion prevention (2000s)
- Hardware-based security (e.g., TPM) (2000s)
- Cloud-based architectures (2010s)
- Multifactor authentication (2010s)
- Firewalls (1980s)
- Anti-virus/anti-malware (1990s+)
- Expedited deployment of patches (1990s+)
- Network segmentation (2000s)
- Malware sandboxing (2000s)
- Security analytics (2000s)
- User & entity behavioral analytics (2000s)
- DDoS protection (2010s)
- Tokenization (2010s)

OPERATIONS

- User education and awareness (1970s)
- Creation of CERTs (1980s)
- Creation of ISACs (1990s)
- Training & certifications (1990s)
- Asset inventories (2000s)
- Top 20 controls (2000s)
- Board involvement, liability (2010s)
- Presumption of breach (2010s)
- NIST cyber framework (2010s)
- Intel-driven operations (2010s)
- Creation of pentesting teams (1970s)
- Creation of CISO role (1990s)
- Capability Maturity Model (1990s)
- Response playbooks (1990s)
- Cyber exercises (2000s)
- Standard configurations (2000s)
- Cyber kill chain (2010s)
- Automated threat sharing (2010s)
- FBI sharing of IOCs (2010s)

POLICY

- Commission and task force reports (e.g., Ware Report, PCCIP) (1970s+)
- Cybersecurity laws (e.g., CFAA) (1980s)
- Single White House cyber official (2000s)
- State data breach laws (2000s)
- Recognition of cyber as operational/business risk (2000s)
- Board accountability including SEC guidance (2010s)
- USG disclosure to companies if they're breached (2010s)
- FTC enforcement actions (2010s)
- Enabling policies and laws (e.g., Info. sharing, CISA, Exec. Orders) (1990s)
- Leveraging existing regulations, as with finance sector (FFIEC IT Handbooks, GLBA)

POTENTIAL FUTURE INNOVATIONS

TECHNOLOGY

- Critical mass of cloud deployment
- Automated measurement of attack surface
- Computer-generated software diversity
- Widespread chip-and-pin deployment
- Scalable security automation
- Autonomic and autonomous defenses
- Strong bio-authentication
- Alternate computing and security architectures (e.g., islets)
- Instrumenting data with sensors
- Analog controls

OPERATIONS

- Security scorecards and ratings
- Active vendor management
- Insurance and other risk transfer
- Improved security metrics from cloud
- More holistic combination of risk, cybersecurity, physical security, business continuity, crisis management
- Software bill of materials

POLICY

- Safe harbor provisions for sharing
- National data breach notification law

ACROSS CYBERSPACE AS A WHOLE

1. Change at end points that "floats all boats"
2. Change to "key terrain" like ISPs

PAST

TECHNOLOGY

- Automated updates (1990s)
- Built-in NAT firewalls (1990s)
- Adding security to s/w development lifecycle (2000s)
- Dev environment security (2000s)
- Security added to IETF standards process (2000s)
- OS hardening (2010s)
- Ubiquitous, transparent encryption (2010s)
- Cloud-based security at platform companies (2010s)
- Ubiquitous, secure protocols (HTTPS, TLS/SSL) (2010s)
- Automated testing (2010s)

OPERATIONS

- Physical protection, personnel security and operational security (1960s)
- Creation of operators' groups (e.g., NANOG, RIPE) (1990s)
- Security certifications (1990s)
- Arresting malicious attackers (1990s)
- Volunteer groups for response (e.g., Conficker, NSP-SEC) (2000s)
- Volunteer groups for protection (e.g., I Am the Cavalry) (2000s)
- Rise of security industry and outsourced monitoring (2000s)
- Industry Associations (e.g., ICASI, Cyber Threat Alliance, M3AAWG) (2000s)
- Rise of DevOps (2000s)
- Institutionalized bug bounty programs (2010s)
- Attribution methodologies (2010s)
- Botnet Takedowns (2010s)

POLICY

- Education: Cybersecurity Core Curriculum, CAEs, NICE (1990s+)
- Budapest Convention (2000s)
- International capacity building (2000s)
- International coordination (e.g., UN GGE, London and EWI processes) (2010s)
- DMCA exemptions for security researchers (2010s)
- Law enforcement attachés (2010s)
- Vulnerabilities Equities Process (2010s)
- Indictments, sanctions (2010s)
- New USG orgs (e.g., CS&C, NCSC, CTIIC) (2010s)
- Scandinavian botnet policies and cleaning ecosystem (2010s)
- Australia ISP code of conduct (2010s)

POTENTIAL FUTURE INNOVATIONS

TECHNOLOGY

- Inexpensive formal methods, such as HACMS
- Formal methods applied to standards, like HTTPS
- Signed firmware
- Quantum encryption
- Blockchain

OPERATIONS

- Cyber Independent Testing Labs and other quantification and rating systems
- Continuous disruption of adversary operations
- Independent attribution organization
- Crowdsourcing IOCs for early detection

POLICY

- Norms: rules of the road for cyber conflict
- "Naming and shaming," especially when norms are violated
- FCC action
- Regulatory emphasis on response, rather than protection
- Global governance structure: G20+ICT20
- Shifts in liability, especially for software and IoT
- Federal insurance backstop
- Improved security metrics to drive better policy
- WTO and trade restrictions

The Lessons of Leverage

What factors distinguish those innovations that create leverage from those that do not?

Lesson #1:
Game-changing innovations share one key feature: scale massively aids the defense.

The massive scale of the Internet usually aids attackers. Ever more devices and increasingly complex software means more doors potentially left unlocked. The most successful cybersecurity innovations reverse this dynamic and employ scale to advantage the defense. They are far easier for defenders to deploy *en masse* than for attackers to circumvent.

This mechanism works in several ways. The most obvious hyperscale emerges when *vendors or service providers change the physics of defense*.[46] Because cyberspace was invented by humans and is constantly maintained, built, and adapted, humans can fundamentally change technologies, standards, and networks in ways they cannot change the air, land or sea.

Defenders need solutions that seize the benefits of Internet scale away from attackers by

- Changing the physics of cyber defense
- Making changes that help all users
- Taking the user out of the solution
- Improving security by reducing the cost of control
- Removing entire classes of attacks

These innovations also "*make a change that helps all their users*," in the words of task force member Jeff Moss.[47] Microsoft's creation of Windows Update (and especially the Critical Update Notification Tool) in the mid-1990s is widely regarded as one of the most game-changing innovations to date, improving security for hundreds of millions of devices.[48] Several years later, in response to customer complaints that Microsoft security hadn't gone far enough, CEO Bill Gates told his software developers that, "when we face a choice between adding features and resolving security issues, we need to choose security."[49] The improved resilience and security of the resulting code affected all of cyberspace.

Game changers also "*take the user out of the solution*," according to security expert Bruce Schneier.[50] Default end-to-end encryption, as implemented by Apple and others, requires no action from users, who may have no idea how to configure such protection themselves.

The best technological, operational and policy solutions "*improve security by reducing the cost of control*," in the words of NY Cyber Task Force co-chair Phil Venables.[51] Technologies like the cloud allow completely new architectures with scale that aids defenders more than attackers. "[T]he cloud provides several critical security advantages over perimeter-based models including greater automation, self-tailoring, and self-healing characteristics of virtualized security," according to NY Cyber Task Force member Ed Amoroso.[52] Playbooks can guide operational responses by essentially "preloading" tough decisions, facilitating swifter action in the critical first hours after an attack. Technologies like Trusted Platform Modules use dedicated hardware to generate and protect cryptographic keys, greatly increasing the effort attackers must expend.

Some game-changing technologies achieve hyperscale by *removing entire classes of attacks*. The most obvious is encryption. White-hat security researchers like Dan Kaminsky and NY Cyber Task Force member Jeff Moss recommend candidate solutions such as changes to random number generation or computer-processor timing, which can disarm many typical attacks. Windows 10 has been hardened with "exploit mitigation features" to make it resistant to zero-day attacks even before patches are available.[53]

Lesson #2:
Game-changing innovations use the minimum necessary intervention.

One particularly low-intervention strategy is to increase transparency, enabling more informed risk management. The simplest transparency comes from media coverage. In a 2015 poll of CISOs, a majority "cited news coverage of large and harmful security breaches as the driver for increased budgets"; such coverage provides policymakers plenty of teachable moments to push important programs.[54]

Unfortunately, it is not always so easy. As Beau Woods of the Atlantic Council explains, most consumers cannot make rational choices when there is no obvious way to compare product security, no way to determine true risk-adjusted lifecycle costs, and no recourse in case of harm. To make this case, Woods keeps a package of Twinkies handy: it is easier to learn what goes into a snack cake—and whether or not it is healthy—than to learn anything about technology products, even the software or hardware controlling critical infrastructure.[55] Informing IT users of the basic ingredients and general security of products can align market forces, often with far less intervention than direct regulation.

One of the better examples of transparency relates not to technology, but to national policy. The best solutions are often based on the ways society and organizations have tackled similar problems. The US Securities and Exchange Commission has advised the boards of directors of publicly traded companies to disclose "material" cyber incidents to investors, as they would any other risk.[56] There is still far to go (such as deciding what constitutes materiality), but with just 2500 words piggybacked onto existing private-sector governance mechanisms, the SEC is encouraging boards to focus on cyber risk.

The SEC did not mandate security standards, but is instead *regulating for transparency* to make shareholders more aware of risk. As this report will discuss later, other transparency measures, such as independent testing labs, can improve security by aligning market mechanisms, such as improving insurance markets or encouraging consumers to make smarter security choices.

The rise of information-sharing organizations demonstrates that when incentives are aligned, policy creates the conditions for operational and technical success, which leads in turn to new policy options. In 1988, the Clinton Administration issued Presidential Decision Directive 63, which called for the voluntary creation of Information Sharing and Analysis Centers (ISAC) for "critical infrastructure" sectors.[57] The first sector to establish an ISAC was financial services. Today, the FS-ISAC has grown to about 7,000 financial institutions in 38 countries and includes banks, credit card and insurance companies, broker dealers, and credit unions.[58] Many other critical infrastructure sectors have established ISACs and also coordinate and share information through the National Council of ISACs.

To build on these new organizations, the Department of Homeland Security encouraged new tools for automated sharing of threat indicators. These indicators were immediately fed to detection and prevention systems, reducing response times from hours to seconds, a *technological* success. A later executive order by President Obama continued the cycle, expanding information-sharing mechanisms beyond critical infrastructure sectors to a wider set of companies and organizations.[59]

Often, the "least intervention" involves a simple removal of headwinds that are limiting progress. A joint statement from the Department of Justice and Federal Trade Commission dispelled corporate antitrust concerns over sharing security-related information with competitors.[60]

Lesson #3:
Operational and policy innovations are powerful but overlooked and misunderstood.

Cyberspace is a technical domain, and the vast majority of experts are techies: software or hardware developers, network engineers, or security researchers. A computer "expert is seldom an expert on consequences and policy implications," as one author put it in 1965.[61] Policymakers, with their nearly opposite skillset and body of knowledge, rarely understand the technology and can underestimate second- and third-order effects as well as the effort needed to successfully implement policies.

Still, some of the best security improvements of the last thirty years have emerged from process innovation rather than new technological devices. Though

Organizational Innovation in Cyber Security

Computer Emergency Response Teams (CERT), 1988
Driven by Cyber Incident, the Morris Worm

Chief Information Security Officers (CISO), 1994
Driven by Cyber Incident, Hacker Theft from Bank

Information Sharing and Analysis Centers (ISAC), 1998
Driven by National Policy, PDD-63

Information Sharing and Analysis Organizations (ISAO), 2015
Driven by successes and limitations of ISACs

What is the next major innovation in cybersecurity organizations?

widespread now, Computer Emergency Response Teams had to be *invented* to fill a gap. Few current practitioners view them as an innovation or consider how new organizations might contribute to the next generation of success. Similarly, the role of Chief Information Security Officer, now a must-have, was an innovation by Citibank after a massive intrusion in 1994. Cyber exercises, especially in the financial sector, have led to protection and response improvements, an increase in trust, and deep insight into vulnerabilities and interdependencies.[62]

Volunteer groups like I Am the Cavalry bring together researchers, vendors and even regulators for collective solutions that would be impossible when these groups are arrayed against one another. Since 1997, rather than ignoring or threatening researchers, software vendors have used "bug bounty programs" to reward those who disclose vulnerabilities.[63] In a recent "Hack the Pentagon" contest, 1410 hackers found 138 important bugs in DoD software for an outlay of just $75,000 in bounties.[64]

Operational and policy innovations are at their best when they align incentives, work through existing governance mechanisms, and can evolve over time. An often-mentioned example is the 2013 NIST Cybersecurity Framework. When the Obama administration called for a "baseline framework to reduce cyber risk," many experts feared a strong-arm regulatory structure.[65] But NIST instead convened industry and other non-state groups to develop a relatively flexible, risk-based document, which it continues to update based on community feedback.[66]

According to a recent RAND study, such operational innovations and other "tools which do not lend themselves to countermeasures (e.g. better configuration management) are likely to retain their usefulness in the long run."[67] Because attackers have a harder time working around them, these tools "resist obsolescence."

Regulation has an essential role but is best when risk based, flexible, and focused on transparency rather than solely security. The SEC guidance mentioned above meets these characteristics. Several members of the task force also mentioned the data security requirements of the Graham-Leach-Bliley Act, requiring "risk-based" response programs, and "supervisory guidance" of financial regulators.[68] Both certainly helped focus the attention of the executives and board directors of financial companies.

Regulations, and compliance in general, are *least* successful when they are rigid, overly focused on checklists, or unharmonized. In this regard, many task force members and other experts expressed dissatisfaction with the PCI standard for credit card payments.[69] Even the NIST Cybersecurity Framework has been implemented differently (or ignored) by different regulators, forcing some companies to meet divergent or conflicting standards.[70]

Curveballs

Not all coming innovation will provide leverage to defenders. Quantum computing, for example, will almost certainly provide more leverage to attackers by rendering most modern, non-quantum encryption worthless. Other coming innovations will help both defenders and attackers; it's still too soon to know who will gain the most.

Blockchain and other distributed ledgers have significantly helped attackers, who use hard-to-trace bitcoins as payment for cybercrime services or as part of a payment demand to unscramble data in ransomware attacks. Other security researchers are investigating how distributed ledger technologies might enable decentralized control of botnets; distributing the brains of malicious software could make it exceedingly resilient.[71] But distributed ledger technologies can also aid the defense by removing the need for central authorities. Identity and trust certificates and operations such as the Domain Name System currently require central authorities that could be disrupted in an attack or struggle to adapt to the growing complexity (and borders) of cyberspace.[72]

A collection of technologies related to **automation and autonomy** are among the greatest hopes for defensible breakthroughs. Artificial intelligence might soon be able to stop hackers faster than any human defender. IBM is starting beta testing for its Watson supercomputer to monitor technical security event logs, speeding incident detection.[73] DARPA went even further, funding a Cyber Grand Challenge in which seven teams programmed supercomputers to discover and patch their own software vulnerabilities, defending themselves with no human intervention in a capture-the-flag style hacking competition.[74]

The DARPA challenge, however, demonstrated that AI and supercomputers can also revolutionize attack. After finding vulnerabilities in their own software, the supercomputers weaponized those vulnerabilities to attack each other. It is entirely possible that by 2025 or 2030, a supercomputer-driven attack could overwhelm any traditional cyber defenses on the planet; only a supercomputer-driven defense could react in time. In such a situation, effective cybersecurity might only be possible for organizations large enough or rich enough to afford supercomputer-driven defenses or the services of a managed supercomputer security service provider (MSSSP). These conditions would call for centralized monitoring and response, handing more power to large corporations and governments: security for the 1%. Indeed, human cyber defenders could become as rare as stock market floor traders. Time will tell.

The Future of Cyber Conflict? Autonomous attack and defense by supercomputers at the DARPA Cyber Grand Challenge, August 2016

The last important curveball is **stronger Internet borders** as national governments demand more say over their citizens' data and what information can enter or leave sovereign borders. Borders could improve security if nations imposed restrictive standards and regulations and more tightly monitored and controlled cross-border Internet traffic. However, such actions could also undermine international trust and cooperation, casting the Internet as a source of national security threats and foreigners as potential adversaries rather than promising partners.[75]

Future Innovations to Make Cyberspace Defensible

Political, cybersecurity, and thought leaders must set a strategic goal of creating a defensible cyberspace, where the defense, not the attackers, have the advantage. A more defense-advantage Internet is possible.

Of course, a myriad of incremental solutions will always be required. In the early decades of computer security, such solutions were far cheaper than more fundamental fixes. The accumulated weight of layer after layer of incremental band-aid solutions has now become so significant (annual cybersecurity spending is projected to reach $170 billion by 2020) that more wide-scale fixes are needed.[76]

To achieve more significant results, defenders must recognize and emulate the innovations with the greatest leverage. See the main figure in the centerfold for a summary of the initial list, compiled by the NY Cyber Task Force, of innovations that may bring defense advantage and hyperscale. The following pages summarize these innovations. Text Boxes 3a, b and c provide a more structured action plan for governments, technology and security companies, and organizations dependent on technology. The action plan is written from a US perspective, but the specific recommendations apply to the European Union as well. These problems, and solutions, are necessarily global.

Somewhat Easier Choices

It is difficult to pick the true winners in advance, but several across technology, operations and policy stood out in our conversations within the task force and with other experts. There are still potentially large, relatively easy, leverage-creating gains to be had. Because of the sometimes tight linkage between the innovations of policy and of operations, these are categorized together.

Technology-Focused Innovations

There are major gains still to be made with cloud-based technologies. Cloud-based technologies offer the chance to build more secure architectures without pouring investment into an increasingly indefensible perimeter. With the cloud, defenders can use scale to reduce complexity to more tractable levels: if everything resides on cloud, then there is only one set to keep updated and secure rather than dozens, hundreds, or thousands.[77] Further, with sufficient data and computing power, the cloud enables revolutionary new ways of analysis, measuring, and monitoring.

Best of all, instead of band-aids on top of band-aids, the cloud allows solutions to be built on a more secure foundation. It has been, according to PwC, the "one unifying element ... to leverage and link cloud-based cybersecurity tools, Big Data analytics and advanced authentication."[78] The members of the NY Cyber Task Force see such developments as critical to overcoming many of the specific factors that have contributed to offense dominance and building a new, more secure foundation.

However, organizations cannot simply hand their data to cloud providers and assume everything will run smoothly, as security and resilience issues linger. By educating IT staff and smoothing the path to cloud adoption, programs such as the Cloud Security Alliance and the US Federal Risk and Authorization Management Program (FedRAMP) can substantially reduce such risks.[79] Within the US government, increased reliance on cloud and other shared services can help break down bureaucratic barriers, allowing improved monitoring, protection and response.

Additionally, mounting data nationalism has triggered skepticism around the world about trusting the clouds of American digital giants. Because these critical concerns could undermine the most important security innovation we identified, the NY Cyber Task Force recommends steps at the policy level to increase international confidence in the cloud.

Many technology companies and computer security researchers are already working to improve authentication by finally **migrating away from passwords**, either with new solutions or "by mixing together multiple weaker indicators into one solid piece of evidence that

you are who you say you are."[80] These efforts should be encouraged and accelerated.

Many future innovations will focus on drastically **reducing the cost and effort needed to develop secure code**. Already, new software tools (such as fortified source and stack guards) and operational innovations (like adding security to the software development lifecycle and, more recently, DevOps) have made it easier to develop code with security already baked in. These methods should be advanced, and further innovations should be developed.

Formal methods are an effective (and increasingly inexpensive) means of reducing software vulnerabilities to create "provably secure" systems. Costs have dropped by several orders of magnitude, allowing researchers to jump these methods out of musty computer science labs and into advanced experiments and the real world. DARPA has used formal methods to secure a test helicopter drone,[81] while Microsoft is using them to develop more secure versions of standards, such as HTTPS, for Internet-wide leverage.[82]

Encryption already delivers tremendous advantages to defenders; quantum encryption (or more precisely, quantum key distribution) might extend this lead. This will depend on whether with this method it is truly "not possible to intercept communications without the communicating parties knowing about it," as "the only way to break its security is to break the laws of physics."[83]

Operational- and Policy-Focused Innovations

Faster patching is one of the most critical ways enterprises can protect themselves. Software that automatically updates itself is of no use if the process is delayed by enterprise IT staff that needs to exhaustively test every new change. The WannaCry attack of May 2017 would have been stopped in its tracks if only enterprises had applied the existing Microsoft patch. Yet on average organizations take 12 weeks to patch, far longer than hackers need to turn vulnerabilities into exploits.[85] Much of that software remains unpatched because it is so out of date. There are still perhaps 140 million computers running Windows XP, even though it became officially obsolete and unsupported in 2014. Accordingly, **updating obsolete software** is a critical "innovation" that provides significant leverage.

Increased transparency for consumers, shareholders, and other concerned parties can further align incentives. Certain transparency-increasing solutions relate to technology, such as software bills of materials (or similar "nutrition labels") allowing consumers and enterprises to "identify all the software components very quickly, compare against a list of known vulnerabilities, and see where the software is affected and how."[86] If provided in a machine-readable format (as recommended by the top finance-sector cybersecurity group), then enterprises can more quickly learn of exposures to new vulnerabilities.[87]

Other transparency-related ideas should be encouraged, like the Cyber Independent Testing Labs (ITL) set up by Sarah and Peiter "Mudge" Zatko, as well as the inclusion of cybersecurity in reviews by Consumer Reports. The Cyber ITL is already assessing in an open and repeatable manner whether major browsers use best security practices like heap protection or stack guards.[88] Consumer Reports will assess "whether software is built using best security practices, studying how much information is collected about a consumer and checking whether companies delete all user data when an account is terminated."[89]

Other possible future innovations focused on better aligning incentives include **cyber insurance**. Though it has been promising for a decade, cyber insurance has not yet aligned market forces the way that, for example, fire insurance has done with building codes.[90] Robert Knake of the Council of Foreign Relations believes that to succeed, the market needs a federal insurance backstop, similar to the Terrorism Risk Insurance Act.[91] Whether or not that is the correct policy lever, a properly functioning insurance market could drive change at hyperscale.

Incentives might also be aligned through regulatory emphasis on corporations' ability to respond, contain, and recover, and on preventative controls. Corporations still invest in cybersecurity as a function of compliance as much as anything else. Even if investment in response and recovery, as well as prevention and controls, did not foil cyber attackers, it could potentially reduce the business impact and ultimate cost of successful attacks. Regulators can incentivize a more balanced corporate investment between prevention and response.

Text Box 3a: *Recommendations for the US Government*

1. **Create a new cyber strategy based on leverage:**
   a. The White House should issue a new national cyber strategy centered on the goal of a defensible cyberspace and encouraging leverage in technological, operational, and policy innovations.
   b. The White House should review whether major programs are achieving leverage and de-invest in those that are not to prioritize new work that is more likely to be successful at scale.
   c. The United States, European Union and others should continue to push norms for national conduct in cyberspace.
2. **Focus on transparency and risk-based governance, especially when they align market forces:**
   a. The White House and Congress should align FISMA and other laws away from compliance and towards cyber risk management—using frameworks such as that of NIST—as well as readiness to respond to, contain, and recover from cyber crises.
   b. The White House, Congress, and regulatory agencies must work to harmonize regulations around risk frameworks and cooperate with partners overseas on better regulatory convergence.
   c. The White House and DHS, working with Congress where necessary, should align market forces using a federal insurance backstop, transparency measures (such as mandatory software bills of materials), and behavioral "nudges."
   d. DHS should continue to push playbooks, exercises, and other low-cost operational innovations.
3. **Migrate to cloud and other new technologies that will deliver leverage:**
   a. The White House and Congress should push towards federal shared services and far heavier use of the cloud.
   b. Additional funding should be set aside for FedRAMP and other programs mitigating the risks of cloud use and educating employees on wise and secure usage.
4. **Use federal funding to support leverage in the private sector:**
   a. The Office of Science and Technology Policy, the National Academies of Science, DHS, and other agencies should continue funding technologies likely to provide the most leverage, such as formal methods, secure standards, and quantum key distribution.
   b. DHS should pursue grants for nonprofits involved in high-leverage work, such as operational response, information sharing, transparency, metrics, and security open-source software.

Text Box 3b: *Recommendations for IT and Cybersecurity Companies*

1. **Never stop implementing the highest-leverage innovations:**
   a. Continue to reduce the cost and effort of developing secure code. Push solutions that remove entire classes of attacks. Ensure systems are patchable, patched, and provided with a software bill of materials.
   b. Push solutions with security built in or automatic, so that the security of the system is not dependent on action (or inaction) by users.
   c. Implement a vulnerability disclosure program and work with security researchers to find and fix bugs.
2. **Don't just share, but collaborate, including with funding to nonprofits doing critical work:**
   a. Cooperate with and help fund nonprofits involved in high-leverage work, such as operational response, information sharing, transparency, metrics, and security open-source software.

Text Box 3c: *Recommendations for Highly IT-Dependent Organizations*

1. **Start from the board down, not the technology up:**
   a. Name tech-savvy board directors to help drive organizational change and encourage the move from compliance-based security to more risk-driven approaches.
   b. Build a governance structure around risk and the critical business processes of the organization, not around budgets and cybersecurity tools.
2. **Implement the highest-leverage innovations:**
   a. Embrace the cloud for more robust security, built from the foundation up.
   b. Push other mature high-leverage innovations, such as expedited patching, encryption, and two-factor authentication.
   c. Require software that is patchable, free of known defects, has its vulnerabilities patched regularly, and comes with a software bill of materials so that IT managers can understand the risk.
3. **Emphasize agility and resilience, two of the most general-purpose investments available:**
   a. Develop and exercise response playbooks at all levels of the organization. Spending time and money in agility and response is a general-purpose investment, applicable to a wide range of crises.

Text Box 4: *Measuring Whether Cyberspace is Becoming More Defensible*

Useful cybersecurity metrics and measurements remain scarce, but some may serve as proxies to evaluate whether cyberspace is becoming more defensible.

- The Index of Cybersecurity is perhaps the most suggestive. Though its rate of increase slowed over 2015, the overall growth of the index indicates that cybersecurity practitioners have become more concerned every month since its inception in 2011.
- The annual Verizon Data Breach Investigations Report remains an excellent source for useful measurements. The 2016 edition notes that "attackers are getting even quicker at compromising their victims," although there have been slight improvements in how quickly defenders detect compromises.
- A US Department of Commerce survey showed that a startling 45 percent of US households with internet have ceased conducting some sensitive transactions online.
- Efforts such as the Cyber Green Initiative, led by NY Cyber Task Force member Yurie Ito, are working to provide more useful statistics "to help understand where improvements can be made and how, together, we can achieve a more sustainable, secure, and resilient cyber ecosystem."

Many **public policy "nudges"** are built around transparency, to align incentives and help technologists, consumers, and organizations make better decisions. The success stories from behavioral scientists of "nudges" leading to better outcomes opens up a very promising new area for innovation. According to a UK team that applied these lessons to public policy, "If you want to encourage a behaviour, make it Easy, Attractive, Social and Timely."[92]

For example, home users are probably more likely to patch their systems if they know most others are doing so as well. Similar behavioral economic interventions can be devised for vendors and network service providers. Pressure could, for example, come from more transparency calling out the "dirtiest" network providers, those that do the least to inform customers or filter known attacks.

Improving operational coordination—through response playbooks, frequent exercises, and groups like Information Sharing and Analysis Organizations—can be an inexpensive way to build significant capability, especially as it aligns with incentives for many parts of the private sector, from cybersecurity companies to well-intentioned volunteers. "[O]ptimizing parts is not a good route to system excellence"; better to improve coordination and functioning of the system as a whole.[93]

This coordination should lead to more effective "**Internet clean up**—private sector and law enforcement working together continuously to shut down botnets and other malicious infrastructure."[94] Botnet takedowns, while effective, have taken significant investment of time and resources. A continuous process might bring scale and leverage. Disrupting non-technical operations at scale are possible as well: research has found that "95% of spam-advertised pharmaceutical, replica and software products are monetized using merchant services from just a handful of banks," suggesting a probable source of leverage.[95]

Policymakers and technology leaders must **prioritize building a defensible cyberspace** (and develop supporting metrics, see Text Box 4). To do so, they must recognize the principles of leverage underlying the most important past successes and use these principles to build solutions that scale at least cost for greater security across all of cyberspace.

An increasing number of software professionals demand that new products push the **software golden trio**: (1) be patchable (especially key for IoT devices), (2) have no known defects (new vulnerabilities are regularly patched), and (3) include a software bill of materials or nutrition label (as discussed above). Together, these three priorities would make software risk more manageable.[96]

Harmonization of cybersecurity regulations could reduce costs and make defense simpler and more effective. This is particularly true in the financial sector, where regulators from individual states, the federal government, and other countries can have different, even competing, rules and guidelines.

New organizational structures that can easily bridge national borders will be needed to deal with cybersecurity issues. Exactly which organizations are most needed is still in question, and often controversial, but the need for them is not. Microsoft has already proposed two: (i) an independent organization to investigate and attribute cyber attacks,[97] and (ii) "G20 plus ICT20," a new extension of the G20 group of countries that would include globally significant technology companies.[98]

Rules of the road for cyber conflict could significantly increase stability, especially if focused on restricting the targeting of critical infrastructure. The promulgation of recent agreements (2015 has been called "the Year of Global Cyber Norms") has led, as of early 2017, to only marginal actual restraint.[99]

Pursue **additional cross-border cooperation** by governments and key cyber-related companies, including improved response and information sharing. Although global responses like the takedown of massive botnets show that sharing and cooperation can make a tremendous difference, such collaborations are still extremely time and resource intensive.[100] Continued exercises, sharing, and common response mechanisms (such as the Asia-Pacific CERT) can provide additional leverage.

And Much Harder Ones

Given the many advantages offense has, these relatively easy gains may be insufficient to make cyberspace truly defensible. At some point, decision makers will have to face harder choices. Certain potentially

game-changing solutions require uncomfortable answers to the key question, "who pays?"[101] As such, the members of the task force did not reach a consensus on the following tactics.

More **extreme transparency measures**, like a "nutrition label" for software, could drive market decisions by providing consumers and IT managers more information about the components and security of competing products. Such a tactic would be difficult to implement. Software is complex, and many vendors would resist, potentially making government regulation, rather than pure market forces, necessary.

To better align market incentives at hyperscale, Congress could make it easier to hold software and **hardware companies liable** for products with known, unpatched vulnerabilities and no mature process to identify and fix them. Giving consumers who've been sold "faulty" software this recourse remains a controversial solution, yet one that could provide more leverage than almost any other. Companies with a robust process for discovering and fixing vulnerabilities could be protected from liability in the face of sophisticated attacks, such as from nation states, which reasonable defenses could not be expected to withstand.

President Obama's recent Commission on Enhancing National Cybersecurity specifically called out the need to address the liability implications of the Internet of Things.[102] This would be especially critical for automobiles, medical devices, and other safety technologies, particularly after the scare of WannaCry infecting hospitals. But such liability would almost certainly hinder innovation, with the highest price paid by small start-up companies lacking the capacity for bug-bounty programs and liability lawyers.

The Federal Communications Commission, alongside other global communications regulators, could **impose security regulations on network service providers**, limiting, for example, their "passing the trash" of obvious DDoS traffic or spread of malware. Variants of this idea are already in place in Australia, Scandinavia, Germany, and other jurisdictions, though service providers are justifiably cautious of potential slowdowns in network performance and the burden of monitoring customer traffic, especially if on behalf of governments.[103] If nudges, transparency, and voluntary norms are ineffective, governments could tax "emissions" above a certain level or implement a cap-and-trade regime.[104]

Launching far **more aggressive active defense** might directly increase adversaries' costs and disrupt their operations, especially if companies were able to do so on their own.[105] However, such counterattacks might cause more trouble than they solve, possibly cascading out of control or prompting adversaries to escalate against the companies involved or against US espionage operations. Some have called for perhaps the ultimate active defense, a **defensive worm**. The best-known example, the Welchia worm, was set loose to stop the Blaster worm in 2003. It infected computers, downloaded the patch to stop Blaster, and attempted to delete Blaster if it was already on the computer.[106] A defensive worm certainly provides leverage, spreading automatically across the entire Internet. It would also be illegal in most countries and might cause systems to crash, potentially causing more problems than it solved.

Creating a new Internet, although not a favorite option of the task force, not least because of the expense of developing more secure standards and deploying new equipment, is a serious idea with serious backing. Former NSA director General Michael Hayden proposes a more reasonable approach: a two-Internet future. In the first, based on today's network, security cannot be guaranteed, more is permitted, and anonymity is allowed (and even cherished). The second is far more secure and restrictive and requires disclosure of identity.[107] The former is for fun and free speech, the latter for business and, especially, critical infrastructure.

Determining whether and how to punish nations that are sponsors of or sanctuaries to destabilizing cyber attackers is among the most difficult policy challenges. In Washington, DC, this may seem relatively straightforward in conversations about deterring China, Russia, Iran, and North Korea. But it is not that easy, as the US Intelligence Community has also been active in finding dangerous vulnerabilities in software made by US vendors and using them against the systems of other nations. In many cases, those nations have reason to believe the United States threw the first punch, and deterrence works very differently when nations feel they are retaliating rather than striking first. A careful balance must be established between deterrence and restraint.

Future Research

We hope this report of the NY Cyber Task Force has helped advance the concept of leverage as a key starting point for establishing a more defensible cyberspace. We believe this insight should be at the core of future efforts, and this report takes steps to identify different dimensions where it may be put in play. Nevertheless, we leave our deliberations unsatisfied, as much research remains to be done.

Our work was based on the experience of the task force members and interviews with dozens of experts. It was not, however, rooted in hard numbers. Metrics on the impact of different innovations either did not exist or were too far outside the scope of our project to assemble, normalize, and analyze. We hope researchers will use the concepts in this report to develop additional metrics to measure leverage and better understand the benefits and limitations of both past innovations and those now being introduced.

Future research should also extend this work to encompass the viewpoint of attackers: where do they achieve the greatest leverage, and how can it best be disrupted? As task force member Dmitri Alperovitch explains, such work should include "forcing attackers to have a high-level expertise to execute their attacks, rendering the environment more unpredictable so they don't have a high degree of confidence if their attacks will be successful, and ensuring attribution" so they can be held accountable.

In addition, significant future work should explore how the approaches of behavioral science, of making solutions "easy, attractive, social and timely," can improve cybersecurity at scale. Lastly, we encourage future research on engaging the R&D and venture capital communities to fund innovations with leverage, as it seems too much investment currently goes to the continued development of tools with only marginal gain.

Conclusion

A more defensible Internet is within reach. New game-changing technologies, such as the secure architectures permitted by cloud technologies, can radically alter cyberspace with advantage and scale in favor of defenders. But so too can operational and policy innovations, which are often overlooked or discounted.

When presented with new proposals, decision makers should ask a few simple questions:

Does this new policy, process, or technology clearly bring leverage? If the mechanism for creating leverage is not clear, then the innovation is probably at best an incremental improvement. Incremental improvements, while useful, should be treated as temporary band-aids and cannot (as information sharing legislation demonstrates) be the last word.

For any given problem, where will leverage deliver the most impact? Leverage can be applied to many existing, low-payoff solutions. For example, leverage has been applied to reinvigorating cyber awareness education, the often mundane set of tasks that discourages users from clicking on links. A quarterly awareness video that provides less than one dollar of additional security for each dollar spent certainly doesn't suffice. Many firms now conduct their own phishing campaigns as an educational exercise, targeting those who click on suspicious links for follow-up online training.

This report has argued for a new approach to cyber defense, one that can break the stalemate of the past five decades, so that defenders finally have the high ground, to fight with the advantage. This approach does not have to be a highly complex, government-run "Moon Shot." It certainly should not be a "Cyber Manhattan Project;" the Internet is a boon to individuals and societies, not a weapon. If anything, the world needs a cyber equivalent of *Silent Spring* to reveal to us how precious the Internet is and how our actions are destroying it, and energize stakeholders to make some hard tradeoffs.

The NY Cyber Task Force has tried to bring new, pragmatic approaches to cybersecurity. Some of our solutions can be implemented with relative ease now that we've identified the lessons of success. Others will be far more difficult, as they create clear winners and losers. All task force members agree that smaller interventions are necessary now to avoid even harder decisions as the situation worsens. Defense is possible, but only through leverage, and the sooner the better.

End Notes

1. Defense Science Board, "Security Controls for Computer Systems: Report of the Defense Science Board on Computer Systems" (aka The Ware Report), 11 February 1970, page vi, http://csrc.nist.gov/publications/history/ware70.pdf.
2. Internet Live Stats, as of 24 March 2016, www.internetlivestats.com/internet-users/.
3. Christopher Hooton, "Refreshing Our Understanding of the Internet Economy," Internet Association, 12 January 2017, http://internetassn.wpengine.com/reports/refreshing-understanding-internet-economy-ia-report/.
4. Atlantic Council, "Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures," September 2015, http://publications.atlanticcouncil.org/cyberrisks/.
5. Jerome H. Saltzer and Michael D. Schroeder, "The Protection of Information in Computer Systems," Communications of the ACM 17:7, July 1974, www.cs.virginia.edu/~evans/cs551/saltzer/.
6. The White House, "Executive Order—Promoting Private Sector Cybersecurity Information Sharing," Sections 4a and 4b, 13 February 2015, www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
7. "Verizon's 2017 Data Breach Investigations Report," available at www.verizonenterprise.com/verizon-insights-lab/dbir/2017/. As will be covered in more detail, the Obama administration set the new policy in Executive Order 13636 in 2013.
8. Internet Live Stats, as of 24 March 2016, www.internetlivestats.com/internet-users/.
9. "Measuring the US Internet Sector," Internet Association, 10 December 2015, www.internetassociation.org/121015econreport/.
10. McKinsey Global Institute, "Internet Matters," May 2011, www.mckinsey.com/industries/high-tech/our-insights/internet-matters.
11. Adrienne LaFrance, "Self-Driving Cars Could Save 300,000 Lives Per Decade in America," The Atlantic, 29 September 2015, www.theatlantic.com/technology/archive/2015/09/self-driving-cars-could-save-300000-lives-per-decade-in-america/407956/.
12. Statista, "Number of Monthly Active Facebook Users Worldwide as of 1st Quarter 2017 (in Millions)," www.statista.com/statistics/ 264810/number-of-monthly-active-facebook-users-worldwide/.
13. National Research Council, "Computers at Risk: Safe Computing in the Information Age," 1991, p1.
14. For details, see Arbor Networks' excellent "Worldwide Infrastructure Security Report" (www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf) and Akamai's "State of the Internet/Security Report" series (www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp).
15. Nicky Woolf, "DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say," The Guardian, 26 October 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.
16. Denis Campbell and Haroon Siddique, "Operations Cancelled as Hunt Accused of Ignoring Cyber-Attack Warnings," The Guardian, 15 May 2017, www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity.
17. Jordan Robertson, "Email Spam Goes Artisinal," Bloomberg Technology, 19 January 2016, www.bloomberg.com/news/articles/2016-01-19/e-mail-spam-goes-artisanal.
18. Atlantic Council, "Overcome by cyber risks?"
19. Access to the Internet was officially recognized as a human right with its addition to Article 19 of the Universal Declaration on Human Rights. See Catherine Howell and Darrell M. West, "The Internet as a Human Right," Brookings, 7 November 2016, www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a- human-right/.
20. Steve Morgan, "Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020," Forbes, 9 March 2016, www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#12f26fd476f8.
21. Dan Geer, email to Jason Healey, 20 March 2017.
22. Since part of the message of the NY Cyber Task Force is that, in many ways, little has changed despite decades of progress, it is unsurprising that these recommendations are very similar to those of the 1970 Defense Science Board. It recognized "general characteristics [that are] desirable in a secure system:" flexible, responsive, auditable, reliable, manageable, adaptable, dependable, and must assure configuration integrity. See the Ware Report, page 11.
23. See the Ware Report quote at the beginning of this report. Another excellent example comes from Lt. Col. Roger Schell, who said in 1979, "Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought" (see www.armedforces journal.com/learn-cyber-conflict-history-or-doom-yourself-to-repeat-it/). A dedicated team of hackers could not be stopped; even then, attackers had the advantage.
24. David Clark, comments at SIPA workshop on cybersecurity, 22-24 June 2015.
25. Bruce Schneier, "Liability Changes Everything," Schneier on Security, November 2003, www.schneier. com/essay-025.html.
26. National Research Council, "Computers at Risk," p14.
27. Phil Venables in discussion of NY Cyber Task Force. See also, "On the Record: The Year in Security Quotes," TechTarget, 29 December 2004, http://searchenterprisedesktop.techtarget.com/news/1036885/On-the-record-The-year-in-security-quotes.

28. National Research Council, "Computers at Risk," pp2-3.

29. Rik Ferguson, quoted by Stu Sjouwerman, in "Humans: The Weakest Link in Cybersecurity," Security Awareness Training Blog, 25 October 2012, https://blog.knowbe4.com/bid/252406/Humans-The-Weakest-Link-In-Cyber-Security.

30. Frank Spinney, "Defense Facts of Life," Office of the Secretary of Defense unofficial staff report, 5 December 1980, Page 14, www.pogoarchives.org/labyrinth/defense-facts-of-life-1980.pdf.

31. Dan Geer, "The Science of Security, and the Future," keynote at RSA Conference USA, 23 April 2015, www.rsaconference.com/writable/presentations/file_upload/exp-r02_dan-geer-on-the-future-of-security.pdf.

32. *The Economist*, "The Deepest Cuts," 20 September 2014, www.economist.com/news/briefing/21618680-our-guide-actions-have-done-most-slow-global-warming-deepest-cuts.

33. Jorge Salazar, "Scott Barrett on Crafting a Successful Climate Agreement in Copenhagen," EarthSky, 30 November 2009, www.earthsky.org/earth/scott-barrett-on-crafting-a-successful-climate-agreement-at-copenhagen-climate-summit.

34. Beau Woods, interview with Jason Healey, December 2016.

35. Dan Geer, "Complexity Theory and Adapting to New Cyber Technologies," paper for the National Intelligence Council, 10 February 2017.

36. Neal Pollard, email to Jason Healey, 25 April 2017.

37. Lockheed Martin, "Cyber Kill Chain," http://cyber.lockheedmartin.com/solutions/cyber-kill-chain.

38. "Verizon's 2016 Data Breach Investigations Report." [Looks like FN7 was updated to 2017 report, should this be as well? If not, include "available at www.verizonenterprise.com/verizon-insights-lab/dbir/2016/."]

39. See Federal Trade Commission, "Enforcing Privacy Promises," www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

40. Herb Lin, email to Jason Healey, 20 August 2016.

41. White House cyber deterrence statement to Congress, December 2015, available at www.fedscoop.com/obama-cybersecurity-deterrence-strategy/.

42. See John Mallery, "A Strategy for Cyber Defense: Presentation at the 2010 Workshop on Cyber Security and Global Affairs & Security Confabulation IV, July 7-9, 2010," www.slideplayer.com/slide/8389708/.

43. Tom Reeve, "Wassenaar Arrangement 'Inhibits International Cybersecurity Efforts,'" SC Magazine, 21 July 2016, www.scmagazineuk.com/wassenaar-arrangement-inhibits-international-cyber-security-efforts/article/530845/.

44. Cybersecurity executive in off-the-record conversation on Wassenaar, held at the Atlantic Council, 21 October 2015.

45. PwC, "Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016," page 4, www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf.

46. See e.g., John Lambert, "Changing the Physics of Defense," YouTube, 25 February 2016, www.youtube.com/watch?v=Ig2bbfSzBCM.

47. Jeff Moss, email to Jason Healey, 14 December 2014.

48. There were perhaps 57 million computers running Windows in 1998 when Windows Update and the Critical Update Notification Tool came into effect (http://money.cnn.com/1998/06/25/technology/win98_pkg/). Around 400 million devices run Microsoft 10 today (see Microsoft by the Numbers, https://news.microsoft.com/bythenumbers/windows-ten). Given turnover, the cumulative number of computers protected by Windows Update is likely in the billions.

49. Bill Gates, email to Microsoft employees, 15 January 2002, www.wired.com/2002/01/bill-gates-trustworthy-computing/.

50. Bruce Schneier, conversation with Jason Healey, 11 April 2016.

51. Phil Venables, conversations with Jason Healey, 2002.

52. Ed Amoroso, "The New Security Architecture," Dark Reading, 20 November 2013, www.darkreading.com/compliance/the-new-security-architecture-/d/d-id/899845.

53. Liam Tung, "Windows 10 Security: 'So Good, it Can Block Zero-Days Without Being Patched,'" ZDNet, 16 January 2017, www.zdnet.com/article/windows-10-security-so-good-it-can-block-zero-days-without-being-patched/.

54. Kim Cobb, "Survey Finds Executive Cybersecurity Decisions are Evolving from Compliance to Proactive Cyber-Risk Management," Phys.org, 15 October 2015, www.phys.org/news/2015-10-survey-cybersecurity-decisions-evolving-compliance.html.

55. Beau Woods, conversation with Jason Healey, December 2016.

56. US Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2, Cybersecurity," 13 October 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

57. The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," Federation of American Scientists, 22 May 1998, www.fas.org/irp/offdocs/pdd/pdd-63.htm.

58. "Overview of the Financial Services Information Sharing and Analysis Center (FS-ISAC)," March 2017, provided by John Carlson of FS-ISAC to NYCTF.

59. The White House, "Executive Order—Promoting Private Sector Cybersecurity."

60. Department of Justice and Federal Trade Commission, "Antitrust Policy Statement on Sharing of Cybersecurity Information," 10 April 2014, www.ftc.gov/public-statements/2014/04/department-justice-federal-trade-commission-antitrust-policy-statement.

61. Herbert Simon, *The Shape of Automation for Men and Management*, New York: Harper and Row, 1965, p. xiii.

62. "Overview of the FS-ISAC."

63. "Netscape Announces 'Netscape Bugs Bounty' With Release of Netscape Navigator 2.0 Beta," Netscape Communications, 10 October 1997, https://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html.

64. "Hack the Pentagon," HackerOne, www.hackerone.com/resources/hack-the-pentagon.

65. The White House, "Executive Order—Improving Critical Infrastructure Cybersecurity," 12 February 2013, www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

66. NIST, "Cybersecurity Framework," www.nist.gov/cyberframework.

67. Martin C. Libicki, Lillian Ablon, and Tim Webb, "The Defender's Dilemma: Charting a Course Towards Cybersecurity," RAND, page xx, 2015, www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf.

68. Financial Services Sector Coordinating Council (FSSCC), Letter to Senators Warren and Cummings, 9 December 2014.

69. Joseph Weiss, "The NERC CIP's are not Making the Grid More Secure or Reliable," Control, 19 January 2015, www.controlglobal.com/blogs/unfettered/the-nerc-cips-are-not-making-the-grid-more-secure-or-reliable/.

70. FSSCC, "Financial Services Sector Cybersecurity Recommendations," 18 January 2017, www.fsscc.org/files/galleries/FSSCC_Cybersecurity_ Recommendations_for_Administration _and_Congress_2017.pdf.

71. See e.g., Syed Taha Ali et al., "ZombieCoin: Powering Next-Generation Botnets with Bitcoin," International Conference on Financial Cryptography and Data Security, 5 September 2015, https://link.springer.com/chapter/10.1007/978-3-662-48051-9_3.

72. See Patricio Robles, "Can the Blockchain Replace SSL?" ProgrammableWeb, 17 March 2015, www.programmableweb.com/news/can-blockchain-replace-ssl/analysis/2015/03/17; Mike Ward, "Change is Coming: How the Blockchain will Transform the Domain Name Business," Cointelegraph, 23 April 2015, www.cointelegraph.com/news/change-is-coming-how-the-blockchain-will-transform-the-domain-name-business.

73. Brian Barrett, "IBM's Watson Now Fights Cybercrime in the Real World," Wired, 6 December 2016, www.wired.com/2016/12/ibm-watson-for-cybersecurity-beta/.

74. Kelsey Atherton, "DARPA's Cyber Grand Challenge Ends in Triumph," Popular Science, 5 August 2016, www.popsci.com/machines-win-darpas-cyber-grand-challenge.

75. World Economic Forum, "Digital Disintegration," Global Risks Report, 2014, http://reports.weforum.org/global-risks-2014/part-2-risks-in-focus/2-4-digital-disintegration/.

76. Morgan, "Worldwide Cybersecurity Spending."

77. Christian van de Werken, email with Jason Healey, 24 January 2017.

78. PwC, "Turnaround and Transformation, page 3.

79. See FedRAMP, "Program Overview," www.fedramp.gov/about-us/about/; Cloud Security Alliance, "About," www.cloudsecurityalliance.org/about/.

80. Alex Hern, "Google Aims to Kill Passwords by the End of this Year," The Guardian, 24 May 2016, www.theguardian.com/technology/2016/may/24/google-passwords-android.

81. Kelsey Atherton, "How DARPA is Prepping for the Next Cyberwar," Popular Science, 11 February 2016, www.popsci.com/darpa-is-building-tools-for-next-cyberwar. See also, DARPA, "High Assurance Cyber Military Systems," www.darpa.mil/program/high-assurance-cyber-military-systems.

82. Jeanette Wing, Microsoft Research, discussion at Columbia University Data Science Institute, 10 May 2016. See also, Kevin Hartnett, "Computer Scientists Close in on Perfect, Hack-Proof Code," Wired, 23 September 2016, www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

83. Niel Van Der Walt, "The Current State of Quantum Cryptography, QKD, and the Future of Information Security," MWR InfoSecurity, 20 June 2016, https://labs.mwrinfosecurity.com/blog/the-current-state-of-quantum-cryptography-qkd-and-the-future-of-information-security/.

84. "Verizon's 2017 Data Breach Investigations Report."

85. Jeff Parsons, "This is How Many Computers are Still Running Windows XP," The Mirror, 15 May 2017, www.mirror.co.uk/tech/how-many-computers-still-running-10425650.

86. Beau Woods, email to Jason Healey, 12 March 2017.

87. FSSCC, "Purchasers' Guide to Cyber Insurance Products," 2016, Appendix B, Section 4F, "Bill of Materials," www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.

88. Kim Zetter, "A Famed Hacker is Grading Thousands of Programs—and May Revolutionize Software in the Process," The Intercept, 29 July 2016, www.theintercept.com/2016/07/29/a-famed-hacker-is-grading-thousands-of-programs-and-may-revolutionize-software-in-the-process/.

89. Jim Finkle, "Consumer Reports to Consider Cybersecurity in Product Reviews," Reuters, 6 March 2017, www.reuters.com/article/us-cyber-consumerreports-idUSKBN16D0DN.

90. Though efforts like the FSSCC Cyber Insurance Purchasers Guide have helped: www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.

91. Robert Knake, "Creating a Federally Sponsored Cyber Insurance Program," Council on Foreign Relations Cyber Brief, November 2016, www.cfr.org/cybersecurity/creating-federally-sponsored-cyber-insurance-program/p38517.

92. UK Behavioural Insights Team, "EAST: Four Simple Ways to Apply Behavioural Insights," 2015, http://38r8om2xjhhl25mw24492dir.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/BIT-Publication-EAST_FA_WEB.pdf.

93. Atul Gawande, *The Checklist Manifesto: How to Get Things Right*. New York: Picador, 2010, p. 185.

94. Dmitri Alperovitch, email to Jason Healey, 28 April 2017.

95. Kirill Levchenko, et al, "Click Trajectories: End-to-End Analysis of the Spam Value Chain," Proceedings of the 2011 IEEE Symposium on Security and Privacy, 2011, p431-446. Available at https://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf.

96. See e.g., the Royce Bill (HR 5793), the FSSCC "Purchasers' Guide to Cyber Insurance Products," and the Mayo Clinic's new cyber supply chain guidelines.

97. See Brad Smith, "The need for a Digital Geneva Convention," Microsoft, 14 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

98. See Microsoft, "International Cybersecurity Norms: Reducing conflict in an Internet Dependent World," December 2014, available at http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

99. Jason Healey and Tim Maurer, "What it'll Take to Forge Peace in Cyberspace," New Dimensions in Cybersecurity, 20 March 2017, www.medium.com/new-dimensions-in-cybersecurity/what-itll-take-to-forge-peace-in-cyberspace-aff915f7c804#.bvpu1cdqg.

100. See e.g., Garrett M. Graff, "Inside the Hunt for Russia's Most Notorious Hacker," Wired, 21 March 2017, www.wired.com/2017/03/russian-hacker-spy-botnet. For another excellent example, see Mark Bowden's description of the response to Conficker in *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

101. With appreciation to Michael Sulmeyer of Harvard University's Belfer Center for Science and International Affairs for highlighting this, 2 February 2017.

102. The White House, "Commission on Enhancing National Cybersecurity: Report on Security and Growing the Digital Economy," 1 December 2016, www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

103. Melissa Hathaway, "Creating the Demand Curve for Cybersecurity," Georgetown Journal of International Affairs, 2011, www.belfercenter.org/sites/default/files/files/publication/hathaway-creating-demand-curve-gt-%202011.pdf. See also, Hathaway and John Savage, "Stewardship of Cyberspace: Duties for Internet Service Providers," CyberDialogue2012, March 2012, www.belfercenter.org/sites/default/files/legacy/files/cyberdialogue2012_hathaway-savage.pdf.

104. See Jason Healey and Hannah Pitts, "Applying International Environmental Legal Norms to Cyber Statecraft," I/S: A Journal of Law and Policy for the Information Society, Vol. 8:2 2012, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/6.Healey.Pitts_.pdf. See also, Healey, "Understanding Approaches for Addressing Cyber Conflict," in James Mulvenon and Gregory Rattray (Eds.), *Addressing Cyber Instability*. Cyber Conflict Studies Association, 2012.

105. See the final report of the Active Defense Task Force (which had several members in common with the NY Cyber Task Force), "Into the Grey Zone: The Private Sector and Defense Against Cyber Threats," The George Washington University Center for Cyber & Homeland Security, 2016, at https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf. See also, Irving Lachow, "Active Cyber Defense: A Framework for Policymakers," Center for a New American Security, 2013, www.cnas.org/publications/reports/active-cyber-defense-a-framework- for-policymakers.

106. W32.Welchia.Worm, Symantec, 13 February 2007, www.symantec.com/security_response/writeup.jsp?docid=2003-081815-2308-99. More recently, the Linux.Wifatch worm secured home routers and other devices. See Jai Vijayan, "And Now a Malware Tool that has your Back," Dark Reading, 1 October 2015, www.darkreading.com/vulnerabilities---threats/and-now-a-malware-tool-that-has-your-back/d/d-id/1322451.

107. See e.g., Aliya Sternstein, "Former CIA Director: Build a New Internet to Improve Cybersecurity," NextGov, 6 July 2011, www.nextgov.com/cybersecurity/2011/07/former-cia-director-build-a-new-internet-to-improve-cybersecurity/49354/.

Produced by the Columbia School of International and Public Affairs

WHERE THE
WORLD CONNECTS

Cyber@SIPA
SIPA.COLUMBIA.EDU