Defense at Hyperscale

Technologies and Policies for a Defensible Cyberspace

White Paper for Black Hat 2016

Jason Healey

Senior Research Scholar
Columbia University – School of International and Public Affairs

Why Hasn't Cyberspace Been Defensible?

Cyberspace must become easier to defend, or else it may simply cease to be the engine of innovation, commerce, culture, and expression it is today. Already, according to a survey by the US government, privacy and security concerns have stopped 45 percent of US online households "from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet."[1]

Whether curious or malicious hackers, organized criminals, or national spies or soldiers, for decades, those who want to use cyberspace to attack have held nearly all the cards. Cyber attack has been, for decades, far easier than cyber defense because of a wide range of reasons:

Internet architecture: "The Internet is not insecure because it is buggy, but because of specific design decisions" to make it more open and an easy platform on which to innovate without getting anyone's prior permission, as expressed by pioneer computer scientist, David Clark.[2]

Software weaknesses: Likewise, according to cryptographer and security expert Bruce Schneier "there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality."[3] Despite improvements by major vendors such as Apple and Microsoft since that was written in 2003, it is still largely true.

Attacker initiative: In 1991, one of the first US government reports to call attention to computer security issues, *Computers at Risk* highlighted the imbalance of the Internet where "[a]ttacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all," across an ever-widening attack surface as more devices become connected to the Internet.[4]

Incremental and poorly targeted solutions: The security industry has often provided, and security professionals demanded, IT security products. These incremental solutions solve a few related problem but at a relatively high cost yet not underlying more fundamental issues of the insecure IT products themselves and a flawed IT architecture.

Complexity and high cost of control: Most defensive solutions do not scale easily or understandably, resulting in "[p]rocesses that can be described, but not really understood ... often discovered through trial and error," in the words of Charles Perrow, who wrote on the perils of normal accidents in such complex systems.[5]

Troublesome humans: Even the best and most secure technological systems can be bypassed when its human users are lazy, confused or outright tricked.

Because of these dynamics, in cyberspace the advantage is to the attacker. More simply put, a dollar of attack buys more than a dollar of defense and an hour spent attacking yields far more advantage than an hour spent on defense.

The strategic goal of cyber defenders must be to change these underlying dynamics so cyberspace is no longer offense-advantaged. Innovative defensive solutions must chip away at these advantages while preserving the fundamental open nature of cyberspace.

A defensible cyberspace, where the defense has the advantage is not only an achievable goal but perhaps the only goal which can keep cyberspace as the engine of society, culture and the economy.

Without a more defensible cyberspace, we are only counting down until the next major attack which could strike again in New York or Washington DC or just as easily in Paris, London, or Beijing.

The New York Cyber Task Force

Much, but not all, of the material in this white paper is from the work of the New York Cyber Task Force.

The NY Cyber Task Force was formed in the fall of 2015 to bring together the unique perspective and talent of this city and state to the global discussion on cyber issues and bring a unique New York perspective on how to more decisively solve one of today's decisive challenges.

The NY Cyber Task Force has been working on three overlapping questions to help create a more **defensible cyberspace**, where the defense has more advantages than those attacking us:

1. What is a defensible cyberspace and why hasn't it been defensible to date?
2. What past interventions have made the biggest difference at the largest scale and least cost?
3. What interventions should we make today for the biggest differences at the largest scale and least cost?

The NY Cyber Task Force is co-chaired by Merit Janow (Dean of Columbia University's School of International and Public Affairs), Greg Rattray (Director of Global Cyber Partnerships and Government Strategy at JP Morgan Chase), and Phil Venables (Chief Information Risk Officer for Goldman Sachs). Jason Healey of SIPA is the executive director.

A Defensible Cyberspace

“Defensible” essentially just means a cyberspace where the defense, not the attackers, have the ultimate advantage. The NY Cyber Task Force has described several characteristics of a more defensible cyberspace:

1. Tolerant of flaws, strong and effective under adversity
2. Agile decision making and response to crisis
3. Multi-stakeholder and well-governed by active stewards
4. Negative externalities are hard to impose on others
5. Recovers readily with swift and well-coordinated responses
6. Instrumented and measurable
7. Indefinitely viable and valuable

In such a defensible cyberspace, there will still be sanctuaries of cyber criminals – bad neighborhoods – and many other security problems, but the system remains secure enough that attackers have difficulty operating.

Giving Defense the Advantage Over Attackers at Hyperscale

A “defensible cyberspace” is entirely feasible, if we pursue the right kinds of solutions.

The core of the initial work of the NY Cyber Task Force has been to identify the policy, operational, and technology innovations that been game changers, offering the highest payoff. “Game-changing” in this sense means those solutions that have both scale and advantage:

Scale: A dollar (or an hour) spent imposes costs far higher than a dollar on attackers

Advantage: A dollar spent does not just deliver a dollar or two in benefit but ten or a hundred or a million

Hyperscale solutions will have the highest payoff, having made the biggest difference at the largest scale and least cost. It is not an exaggeration to discuss innovations that deliver both scale and advantage in the ranges suggested here. In fact, it is perhaps only through such hyperscale of getting a million-fold return on our security investment that true success is possible. And if not, then a campaign of attacks of staggering consequences will someday catch up to us.

The perspective of hyperscale solutions can be applied to many existing solutions which sometimes have quite a low payoff. For example, the combination of scale and advantage has been applied to re-invigorate cyber awareness education, the often mundane set of tasks to get users to not click on links. A quarterly awareness video certainly doesn’t suffice, as there is probably less than a dollar of additional security for each dollar spent. Rather, many firms are now conducting their own phishing campaigns as an educational exercise and targeting those that click on suspicious links for specific follow-up training.

Hyperscale solutions are particularly compelling when they can work across the entire ecosystem of the environment. Past solutions have often only benefited a few well-funded enterprises, leading to what Internet pioneer David Clarke calls "Security NIMBY – kicking the security problem from your backyard to someone else's" so that it is their problem now.[6] Defense must be better than offense across an organization, an economic sector, a nation, and cyberspace as a whole.

How will we know if cyberspace is becoming more defensible?

Useful metrics and measurements remain scarce in cybersecurity, but there are some that may be proxies to determine if defenders are succeeding in making cyberspace more defensible.

The Index of Cybersecurity is perhaps the most suggestive. Though it the *rate* of increase has been decreasing over 2015, the overall growth of the index means that cybersecurity practitioners have grown more concerned every month since the inception of the index in 2011.

The annual Verizon Data Breach Investigations Report remains an excellent source for useful measurements, noting that "attackers are getting even quicker at compromising their victims" although there has been slight improvements in how quickly defenders detect compromises.

As mentioned at the beginning of this report, the US Department of Commerce has startling statistics from a survey showing 45 percent of US online households have stopped some sensitive online transactions, possibly heralding the worst cyber futures outline above.

Fortunately, other efforts such as CyberGreen, led by NY Cyber Task Force member Yurie Ito, are working to add 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."

Technology: Game-Changing & Incrementally Effective Solutions

Making cyberspace more defensible particularly requires game-changing technology solutions. The NY Cyber Task has identified a number of such innovations in three broad categories, which over the past two decades have been some of the most effective at giving an edge to the defender.

Solutions where scale aids the defender. Usually the massive scale of the Internet aids the attacker. As more computers are added to a company's IT network, there is a now a larger 'attack surface' for the attacker to find new vulnerabilities and gain illicit access. More connected devices just means more doors potentially left unlocked.

Better solutions "improve security by reducing the cost of control," in the words of NY Cyber Task Force member Phil Venables. New technologies like the cloud, for example, allow completely new architectures where scale aids the defender more than the attacker. With related technologies like virtualization and containterization, "the 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, former chief information security officer of AT&T.[7] Hyperscale solutions, especially those built on the cloud, will be key to a more defensible cyberspace.

Take away entire classes of attacks. Other game-changing technologies give advantages to the defender not through scale itself, but by relatively simple changes which remove vulnerabilities entirely. The most obvious is encryption, which is certainly not invulnerable but according to cryptographer and NY Cyber Task Force member Steve Bellovin, is one of the only places where the defender has all the advantages against the attacker. White-hat security researchers like Dan Kaminsky and Jeff Moss (also a NY Cyber Task Force member) recommend several candidate solutions such as changes to random number generation or computer-processor timing, which disarm many of the typical tricks used by attackers.

Take user out of the solution and **"those responsible make a change that helps all their users"** These related ideas, provided to the NY Cyber Task Force respectively from Bruce Schneier and Jeff Moss, cover a range of technology solutions, best represented by software vendors providing automated updates to their software. "Once Microsoft got vested in security they were in the best position to do something about it," according to Moss, and their Windows Update solution in 1998 is widely seen as one of the innovations that has been one of the most game-changing technologies to date. This fits a key demand of Phil Venables, that "we need more secure IT products, not more IT security products."

Solutions like Windows Update are particularly effective because they do not just work at scale but also because they remove the user from the critical path. Default end-to-end encryption, as implemented by Apple and others, takes place without any actions needed by users, who often have no idea how to configure such protection themselves.

All of these easily succeed at being ‘game-changers’ as, even though they can be expensive, they are far cheaper for defenders to implement than for attackers to defeat. Also, they give far higher benefits than their costs would suggest. Just to focus on one, it was certainly not inexpensive for Microsoft to institute Windows Update in 1998 but once they had, they were able to better protection millions or even billions of computers.

By comparison over those nearly 20 years, other solutions -- such as firewalls, anti-virus and intrusion detection systems, and secure software development -- have been undeniably important to defenders. According to Mike Aiello of Goldman Sachs basics such as anti-virus and a good password manager give the best “bang for the buck” especially for people or organizations that cannot afford big security teams and sophisticated security and risk procedures.

But the success of many of these technologies has been rather incremental. Effective when used in combination with other defenses, firewalls, intrusion detection and similar technologies have protected defenders but often impose significantly increased complexity which is far outside the capability of many defenders.

The consensus of the NY Cyber Task Force and was that the lowest payoff generally came from compliance-related solutions. Security solutions that depend on “checking-the-box” for compliance usually seemed to impose far higher costs on the defender than it imposed on any attackers.

Operations: Game-Changing & Incrementally Effective Solutions

While the game-changing technology innovations are often obvious, the NY Cyber Task Force found it far harder to determine what operational measures have been most successful. The impact of these changes to processes and cooperation is harder to measure, being farther from the technology plane. Indeed, operational measures are often not even considered as a category of actions separate from either technology or policy. These innovations seem commonplace now, but had first to be invented and such operational and process innovation is too overlooked in the quest for new technologies.

Still, several operational measures seem destined for the hall of fame, bringing both scale and advantage.

- Creation of the first Computer Emergency Response Teams (or CERTs) in the late 1980s. CERTs, also called CSIRTs or similar terms, protect organizations by looking for new vulnerabilities, prepare for eventual incidents and led the response once incidents do occur. Though widespread now, they had to be invented, a creation of the Department of Defense after the Morris Worm took down 10% of the early Internet in 1988.
- Creation of the first Chief Information Security Officer position in the mid-1990s. As with CERTs, a CISO is considered a must-have for any significant organization as they streamline control, budget and reporting to the board of directors (or other stakeholders). But the role was an innovation, created by Citibank after a massive intrusion in 1994.
- Automated sharing of threat intelligence. For example, the Finance Sector Information Sharing and Analysis Center used to take no less than 10 minutes to share threat data and sometimes up to 11 hours, with another 45 needed to act on the intelligence. With their automated Soltra solution, over 2,000 financial institutions can now get the information in one second and act on it within 30 seconds, according to John Carlson, an NY Cyber Task Force member.
- Volunteer groups and industry alliances. Not all such groups have been game-changers, but some like the Conficker Working Group, NSP-SEC, ICASI and the Cyber Threat Alliance bring together like-minded technical experts with agility and subject matter expertise.
- Institutionalized "bug bounty programs" where vendors reward security researchers who find vulnerabilities, rather than ignore or even threaten them. 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.
- The doctrinal innovation of the "cyber kill chain."[8] By better conceptualizing the process of how attackers conduct reconnaissance, break into organizations, and then steal data, this idea from the cyber defense team at Lockheed Martin has helped revolutionize thinking about ways to detect and stop the attackers.

Other operational innovations, such as botnet takedowns and trust-based sharing networks, have also been extremely successful but so far are not as game-changing as they are often very resource intensive.

Policy: Game-Changing & Incrementally Effective Solutions

Even though policy innovations have received attention from heads of state, legislatures, and corporate board of directors, to date there has been little analysis on the kinds of policy interventions and their relative success. The NY Cyber Task Force accordingly started by categorizing cyber policy across five overlapping areas, including

1. **High government**, such as norms or the Budapest Convention on cyber crime;
2. **Governance**, especially but not only the Internet Corporation for Assigned Names and Numbers;
3. **Domestic policy**, including the Australian Voluntary Code of Conduct for Internet Service Providers and the NIST Cybersecurity Framework in the United States;
4. **Regulation**, such as that in the United States by the Security and Exchange Commission, Federal Trade Commission, or Federal Reserve Board; and
5. **Corporate initiatives**, such as board involvement and training.

Because nearly every policy initiative creates both winners and losers, it is especially difficult to determine the true game-changers, those with the highest payoff in improved defenses at the least cost. It is likely, even so, that the international cooperation created and encouraged by **Budapest Convention** on cyber crime qualifies, as surely has corporate initiatives to ensure boards of directors understand cyber risks and their mitigation. The **NIST Cybersecurity Framework**, a private-sector led initiative for a common structure for repeatable cyber risk-management, also may be considered a game changer.

Just in the past year, national diplomats and world leaders have made incredible progress on what **international norms** to try to reduce the violence and frequency of nation-state attacks on the Internet. It is still too early to know if this will lead to any real payoff, but given that the costs are so minimal, any significant gains could be game-changing. For example, if the agreement by President Obama of the United States and President Xi of China leads to even just a 5% reduction in commercial cyber espionage, it would likely be the most successful defense mechanism ever.

One of the policies with the most negative payoff is the Wassenaar Arrangement on the 'export' of cyber technology might have imposed extremely high costs on defenders in exchange for only mild obstacles in the way of attackers.

Implications for Getting This Right or Wrong

New York is a leading center of the world for finance and commerce, business and innovation, science and technology, arts and culture. All of this is at risk – not just in New York but in all cities everywhere – to future attacks and disruptions unless we make cyberspace more defensible.

According to a recent study by the Atlantic Council and Zurich Insurance Group, authored by NY Cyber Task Force executive director Jason Healey, a more defensible cyberspace could mean up to *$30 trillion* in additional global GDP over the assumed base case through 2030.[9] In this future, "secure and reliable access to the global network is a fundamental human right" because innovations in the defenders' policy, operations and technology has outpaced those of the attackers.

If attackers continue to gain, however, they may not just have the advantage as today but true supremacy, where "secure and reliable access to the global network is no longer a global right but a luxury good" and "digital identities and assets huddle behind high walls." In this future, the overall economic impact of widespread cyber attacks, cascading failures, and loss of trust could amount to a drop in global GDP of *$90 trillion* through 2030. That number would be even worse, except there was an assumption of "saturation of catastrophe" where cyberspace was so untrustworthy that it could hardly get any worse.

There are perhaps few other areas of technology or public policy where we can impact a staggering $120 trillion in global GDP over the next 15 years. We must build a more defensible cyberspace.

Summary and Initial Recommendations

This is only the first, summary report from the New York Cyber Task Force and the recommendations will therefore be more cursory than those in the following publications. The work to date, however, certainly implies a number of critical recommendations.

National leaders, cybersecurity innovators, and thought leaders need to set ourselves the strategic goal of a defensible cyberspace, where the defense not the attackers, have the advantage. Of course, we must continue to engage in the incremental must-do solutions, such as compliance, but to achieve more significant results we must recognize what innovations have had the highest payoff and repeat those kinds of successes. The most important past innovations have been those that offer both advantage and scale:

- Advantage: A dollar spent on them imposes costs far higher than a dollar on attackers.
- Scale: A dollar spent on them does not just deliver a dollar or two in benefit but ten or a hundred or a million.

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

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

- **Does this new policy, process or technology clearly bring both scale and advantage?** If the mechanism for doing so is not clear, then keep in mind it is probably at best an incremental improvement. There is nothing wrong, of course, with incremental improvements other than that they are often (such as with information sharing legislation) treated as if they will be the last word.
- **For any given problem, where can we apply the principles of advantage and scale to most effect?** Usually, these opportunities are not in government. As demonstrated by the 2002 letter from Bill Gates pushing Microsoft employees to improve security, vendors do respond to market signals to improve software security.[10] ISPs offer another area to achieve both scale and advantage, though not at the expense of privacy. Volunteer groups, such as the open source community, are frequently overlooked, yet are often best placed to fix a wide range of problems. Well-placed grants to expand their capabilities could boost capabilities far, far more than the same amount of money used to hire more bureaucrats.

References

[1] “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities,” Department of Commerce, NTIA, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[2] David Clarke, comments at SIPA workshop on cybersecurity, 22-24 June 2015.

[3] Bruce Schneier, "Liability Changes Everything," https://www.schneier.com/essay-025.html, November 2003.

[4] National Research Council, *Computers at Risk*, p14.

[5] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, 1984 and Updated Version, 1999, Princeton University Press, p85

[6] Clarke, ibid.

[7] Ed Amoroso, “The New Security Architecture,” Dark Reading, 20 November 2013, http://www.darkreading.com/compliance/the-new-security-architecture-/d/d-id/899845

[8] “Cyber Kill Chain,” Lockheed Martin, http://cyber.lockheedmartin.com/solutions/cyber-kill-chain.

[9] “Overcome by cyber risks? Economic benefits and costs of alternate cyber futures,” Atlantic Council, September 2015, http://publications.atlanticcouncil.org/cyberrisks//.

[10] Bill Gates’ letter to Microsoft employees, 15 January 2002, http://www.wired.com/2002/01/bill-gates-trustworthy-computing/.

For more than 60 years, Columbia University’s School of International and Public Affairs has been educating professionals who work in public, private and nonprofit organizations to make a difference in the world. Through rigorous social science research and hands-on practice, SIPA’s graduates and faculty strive to improve social services, advocate for human rights, strengthen markets, protect the environment, and secure peace, in their home communities and around the world.

The curricula of SIPA’s seven degree programs all combine training in analytical methods and practical management skills to ensure that graduates are prepared to understand problems and implement solutions. Students combine these core skills with a focus on a policy area of their choice, and they typically engage in a practice-oriented capstone or workshop experience toward the end of their studies. The School draws its strengths from the resources of New York City and Columbia University, and yet has a global reach, with a student body that is 50 percent international; 17,000 graduates in more than 150 countries; and educational partners in global cities such as London, Paris, Berlin, Singapore, Beijing, Mexico City, and São Paulo.