Building a Defensible Cyberspace

FINDINGS FROM THE NEW YORK CYBER TASK FORCE

For decades, cybersecurity professionals have been treading water, putting in never-ending effort but rarely making progress. The New York Cyber Task Force was formed to break this stalemate. The group, co-chaired by Phil Venables (Goldman Sachs), Greg Rattray (JPMorgan Chase), and Merit Janow (Columbia University SIPA) concluded that defense is possible, but only if defenders focus on the right kinds of solutions, those which provide leverage.

This booklet summarizes the findings of the NY Cyber Task Force's efforts and we believe it brings a fresh perspective. Washington, DC can sink into pessimism over cyber threats while Silicon Valley 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; NY Cyber Task Force's participants want the best for America but understand these interconnected and complex problems require global solutions

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

The Goal: Cyberspace must become more *defensible*, meaning it must have several key features:

- Tolerant of flaws and effective under adversity
- Capable of agile decision making and response
- Well managed by multiple stakeholders
- Capable of constraining negative externalities

Our Strategy, Leverage: To make a defensible cyberspace requires leverage, which requires technology, operational and policy innovations with the following characteristics:

- **Defense advantage:** Any innovation by defenders must impose far greater costs on attackers. Roughly put, 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 all cyberspace. The larger the scale, the more leverage it can deliver.

Leverage to Date: Cyberspace would be even less defensible to date were it not for the last five decades of important technology, operational and policy innovations. These are listed in the center pages of this booklet. based on research, interviews, and the experience of the NY Cyber Task Force members.

Lessons from Past Innovations: Analyzing these innovations provides critical lessons:

1. Game-changing innovations share one key feature: scale massively aids the defense. This can happen in several ways, such as taking the user out of the solution, taking away entire classes of attacks, or when a vendor or provider makes a change that benefits all their customers.
2. Use the minimum necessary intervention. For example, increased transparency, such as security rankings to drive consumer choice or insurance, can be a low-cost way to align market incentives. If regulation is necessary, regulate first for transparency, rather than security.
3. Operational and policy innovations are powerful but overlooked and misunderstood. Some of the best security improvements of the last thirty years have emerged from process or organizational innovations rather than new technological devices. In past decades we created the Computer Emergency Response Team (1988), Chief Information Security Officer (1995), Information Sharing and Analysis Center (1998), and NIST Cybersecurity Framework (2014). What will be the next major innovation?

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

What kind of innovation is it?

Where is primary effect of the innovation?

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

Leverage to Come: Cyberspace can be made defensible by applying innovations with leverage, including the technology, operational and policy innovations listed in this booklet. It is difficult to pick the true winners in advance, but several across technology, operations and policy stood out and the task force believes there are still potentially large, relatively easy gains to be had. Some of these include:

- Cloud-based technologies still have more to offer, in particular the chance to build more secure architectures without pouring investment into an increasingly indefensible perimeter.
- Many future innovations, such as formal methods, will focus on drastically reducing the cost and effort needed to develop secure code.
- Increased transparency for consumers, shareholders, and other concerned parties can further align incentives, especially for insurance.
- 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.
- Harmonization of cybersecurity regulations could reduce costs and simplify defenses.
- Policymakers and technology leaders must prioritize building a defensible cyberspace and include it as central to new corporate, sector-wide, and national cyber strategies.

Other innovations promise massive gains, but also create winners and losers and their knock-on effects are still poorly understood. Accordingly, the NY Cyber Task Force only recognizes, but does not endorse, innovations like liability for software manufacturers, stricter regulations on network service providers, or more aggressive active defenses against attackers.

Recommendations: In addition to these promising innovations, we had specific recommendations:

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 techs which 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. Leverage the most high-leverage innovations
3. Emphasize agility and resilience, two of the most general-purpose investments available

The NY Cyber Task Force has tried to bring new, pragmatic approaches to cybersecurity. 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. Defense is possible, but only through leverage, and the sooner the better.