Understanding and Disrupting Offensive Innovations

Jason Healey
Columbia University
@Jason_Healey

Dmitri Alperovitch
Silverado Policy Accelerator
@DAlperovitch

With **Mike Klipstein** (SIPA) and **Rob Sheldon** (CrowdStrike)

30 July 2020

Bad Guys Finish First

SIPA

"Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought."

Bad Guys Finish First

"Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought."

Lt Col Roger Schell (USAF) *in 1979*

Central Question

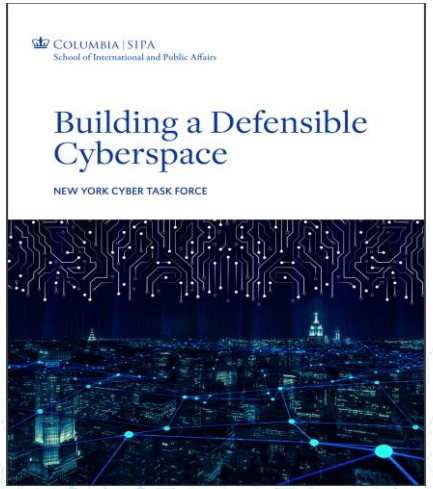
What cybersecurity innovations have given DEFENDERS the most advantage over ATTACKERS at greatest scale and least cost?

Key Questions for a Defensible Cyberspace

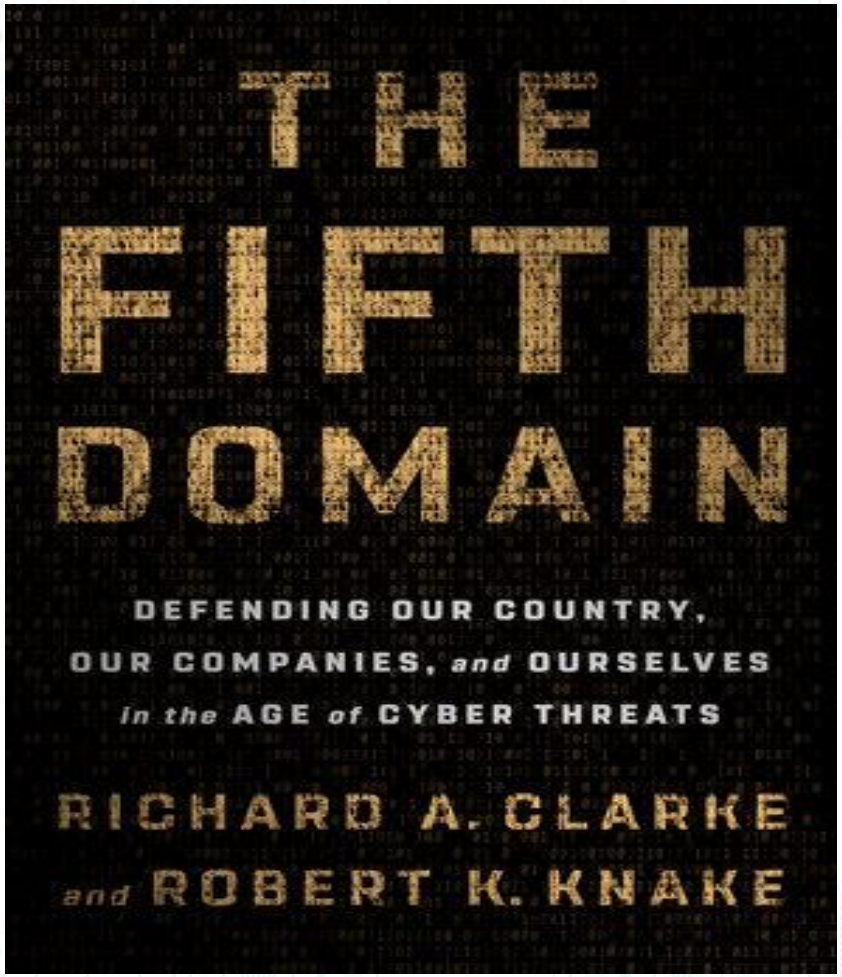
Results from NY Cyber Task Force

1. What is a defensible cyberspace and why hasn't it been defensible to date?
2. What past innovations have made the biggest difference? What made them so successful?
3. What innovations should we prioritize today?

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



https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF


THE
FIFTH
DOMAIN
DEFENDING OUR COUNTRY,
OUR COMPANIES, and OURSELVES
in the AGE of CYBER THREATS
RICHARD A. CLARKE
and ROBERT K. KNAKE

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

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

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

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, [illegible] continuity, crisis management
- [illegible] 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 [illegible], personnel security and operational security (1960s)
- Creation of o[illegible]tors' [illegible]
- Security certifications [illegible]
- Arresting malicious att[illegible]
- Volunteer groups for re[illegible]
- Volunteer groups for p[illegible]
- Rise of security industr[illegible]
- Industry Associations [illegible] (2000s)
- Rise of DevOps (2000[illegible]
- Institutionalized bug b[illegible]
- Attribution methodolo[illegible]
- Botnet Takedowns (20[illegible]

POLICY

- Education: Cybersecurity Core Curriculum, CAEs, NICE (1990s+)
- [illegible]nvention (2000s)
- capacity building (2000s)
- coordination (e.g., UN GGE, London and EWI processes)
- [illegible]ptions for security researchers (2010s)
- [illegible]nent attachés (2010s)
- [illegible]s Equities Process (2010s)
- [illegible]sanctions (2010s)
- [illegible]gs (e.g., CS&C, NCSC, CTIIC) (2010s)
- [illegible] botnet policies and cleaning ecosystem (2010s)
- [illegible] 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

We tend to invest and measure HERE: technology inside the enterprise

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

SIPA

What kind of innovation is it?

Where is primary effect of the innovation?

		TECHNOLOGY	OPERATIONS	POLICY
WITHIN ENTERPRISE Changes implemented by centrally managed IT team	PAST	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)	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 (20 NIST cyber framework (20 Intel-driven operations (20 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)	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) ith finance sector
	POTENTIAL FUTURE INNOVATIONS	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	Security scorecards and ra Active vendor managemen Insurance and other risk tra Improved security metrics More holistic combination business continuity, crisis r Software bill of materi	
ACROSS CYBERSPACE AS A WHOLE 1. Change at end points that "floats all boats" 2. Change in "[illegible] terrain" like ISPs	PAST	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)	Physic sonnel security and operational security (1960s) Creat tors' groups (e.g., NANOG, RIPE) (1990s) Secur cations (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)	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	Inexpensive formal methods, such as HACMS Formal methods applied to standards, like HTTPS Signed firmware Quantum encryption Blockchain	Cyber Independent Testing Labs and other quantification and rating systems Continuous disruption of adversary operations Independent attribution organization Crowdsourcing IOCs for early detection	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

When far bigger gains are here: innovations with impact not in a single enterprise but across all of cyberspace

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

SIPA

What kind of innovation is it?

Where is primary effect of the innovation?

		TECHNOLOGY	OPERATIONS	POLICY
WITHIN ENTERPRISE Changes implemented by centrally managed IT team	PAST	Computer and network passwords (1960s–1980s) Intrusion detection (1990s) Mass vulnerability scanning (1990s) Firewalls (1980s) Anti-virus/anti-malware (1990s+) Expedited deployment of patches (1990s+)	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)	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		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	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	Ubiquitous, transparent encryption (2010s) Cloud-based security at platform companies (2010s) Ubiquitous, secure protocols (HTTPS, TLS/SSL) (2010s) Automated testing (2010s)	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)	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	Inexpensive formal methods, such as HACMS Formal methods applied to standards, like HTTPS Signed firmware Quantum encryption Blockchain	Cyber Independent Testing Labs and other quantification and rating systems Continuous disruption of adversary operations Independent attribution organization Crowdsourcing IOCs for early detection	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

And overlook gains from operational and process innovations:

- CISO
- ISACs
- Kill Chain and @TTACK
- SECDEVOPS

Central Question

What cybersecurity innovations have given DEFENDERS the most advantage over ATTACKERS at greatest scale and least cost?

Extremely successful!

But what if flip the perspective and not center on defensive innovations…

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF

Let's Flip That Central Question

What cybersecurity innovations have given ATTACKERS the most advantage over DEFENDERS at greatest scale and least cost?

Thanks to our collaborators on this!
- Mike Klipstein (SIPA)
- Rob Sheldon (CrowdStrike)

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF

OFFENSIVE INNOVATIONS

TWO KINDS: DRIVEN BY OFFENSE, DRIVE BY DEFENSE

Important Offensive Innovations of the Past 50 Years

New York Cyber Task Force

SIPA

Type of innovation

	Technology	Operations	Policy
Innovations Benefiting or Driven By Offense Innovation originated with hackers, security researchers or other non-defenders	• Whistle for 2600Hz tone (1960s) • Mass scanning, eg NMAP (1990s) • Password cracking tools: John the Ripper, Rainbow Tables, hydra (1990s) • Point-and-click worm and virus kits (1990s) • Interactive reversing tools: IDA Pro, Binary Ninja, Ghidra, etc (1990s) • Malware obfuscation (2000s) • Inexpensive rootkits, eg BO2K (2000s) • Metasploit (2000s) • Botnet and effective command & control (2000s) • Exploit writing aides: Pwntools, mona, ROP chain finders (i.e., Ropper, RopGadget), Cain & Abel • Fuzzers: Peach, BURP Suite, AFL, etc. • Shodan for IoT scanning (2010s) • Low-cost COTS offensive security capabilities: Pwnie Express, Wifi Pineapple, Rubber Duckie, ProxMark, etc. (2010s)	• Hacktivism organizations (1990s) • Information exchanges: Hacker conferences, YouTube videos, CTF competitions (1990s) • Carder markets (2000s) • 4chan instigation and organization of attacks operations (2000s) • Rent-a-DDoS or rent-a-botnet services (2000s) • Bulletproof hosting • Arrangements with banks for large-scale monetization • Cybercrime-as-a-service (2010s) • Bitcoin and other anonymized payment methods (2010s) • Snowden, Vault7, Shadow Broker leaks (2010s)	• National sanctuaries for cyber criminals if they don't attack host nation • States using proxy groups and ignoring criminal side jobs • Deliberately weak financial controls to abet corruption and criminal enterprises

- Many innovations helped defenders as well as attackers.
- Inclusion here doesn't imply they were mistakes or helped attackers more then defenders
- Dates are when innovations first started to gain mass. In many cases, they've continued to the present day

Important Offensive Innovations of the Past 50 Years

Technological Innovations

SIPA

Innovations Benefiting or Driven By Offense

Innovation originated with hackers, security researchers or other non-defenders

Technology

- Whistle for 2600Hz tone (1960s)
- Mass scanning, eg NMAP (1990s)
- Password cracking tools: John the Ripper, Rainbow Tables, hydra (1990s)
- Point-and-click worm and virus kits (1990s)
- Interactive reversing tools: IDA Pro, Binary Ninja, Ghidra, etc (1990s)
- Malware obfuscation (2000s)
- **Inexpensive rootkits, eg BO2K (2000s)**
- Metasploit (2000s)
- **Botnet and effective command & control (2000s)**
- Exploit writing aides: Pwntools, mona, ROP chain finders (i.e., Ropper, RopGadget), Cain & Abel
- Fuzzers: Peach, BURP Suite, AFL, etc.
- Shodan for IoT scanning (2010s)
- Low-cost COTS offensive security capabilities: Pwnie Express, Wifi Pineapple, Rubber Duckie, ProxMark, etc. (2010s)

- Inexpensive rootkits, eg BO2K (2000s)
- Botnet and effective command & control (2000s)

- Many innovations helped defenders as well as attackers.
- Inclusion here doesn't imply they were mistakes or helped attackers more then defenders
- Dates are when innovations first started to gain mass. In many cases, they've continued to the present day

Important Offensive Innovations of the Past 50 Years

Operational Innovations

Innovations Benefiting or Driven By Offense

Innovation originated with hackers, security researchers or other non-defenders

Operations

- Hacktivism organizations (1990s)
- Information exchanges: Hacker conferences, YouTube videos, CTF competitions (1990s)
- **Carder markets (2000s)**
- 4chan instigation and organization of attacks operations (2000s)
- Rent-a-DDoS or rent-a-botnet services (2000s)
- **Bulletproof hosting**
- Arrangements with banks for large-scale monetization
- Cybercrime-as-a-service (2010s)
- **Bitcoin and other anonymized payment methods (2010s)**
- Snowden, Vault7, Shadow Broker leaks (2010s)

- Carder markets (2000s)
- Bulletproof hosting
- Bitcoin and other anonymized payment methods

- Many innovations helped defenders as well as attackers.
- Inclusion here doesn't imply they were mistakes or helped attackers more then defenders
- Dates are when innovations first started to gain mass. In many cases, they've continued to the present day

Important Offensive Innovations of the Past 50 Years

Policy Innovations

Policy

Innovations Benefiting or Driven By Offense

Innovation originated with hackers, security researchers or other non-defenders

- **National sanctuaries for cyber criminals if they don't attack host nation** (2000s)
- **States using proxy groups and ignoring criminal side jobs** (2010s)
- Deliberately weak financial controls to abet corruption and criminal enterprises (1500s)

- National sanctuaries for cyber criminals
- States using proxy groups and ignoring criminal side jobs

- Many innovations helped defenders as well as attackers.
- Inclusion here doesn't imply they were mistakes or helped attackers more then defenders
- Dates are when innovations first started to gain mass. In many cases, they've continued to the present day

Important Offensive Innovations of the Past 50 Years

Sometimes We Do It to Ourselves

What kind of innovation is it?

"Mistakes" Driven by Defenders

Innovation resulted from actions taken by defenders, consumers or other non-attackers

Technology

- Insecure fundamental protocols: BGP, TCP/UDP, DNS, IP v4/v6
- Insecure wireless protocols: BlueTooth, WiFi, Zigbee, etc
- Use of weak, hard-coded, or default passwords
- Hyper vulnerable, interactive web languages and client-side applications: Java Script, nodeJS, ActiveX, PHP, VBScript
- Deployment of insecure software
- Market incentives which reward rushing insecure software to market
- Mass deployment of insecure IoT
- Untrackable shadow IT
- Ubiquitous encryption across the boundary (e.g. SSL) obfuscating exfiltration of info

Operations

- Limited trust, reluctant information sharing, poor corporate governance
- Patch diffing for vulnerabilities

Policy

- Decreasing global trust and governance
- New top-level domains
- Weak cybersecurity laws
- Few, weak global cyber norms
- Lack of deterrent for 'grey area' operations
- Liability concerns driving secrecy
- Lack of sensible regulations that can drive accountability

Important Offensive Innovations of the Past 50 Years

Sometimes We Do It to Ourselves

"Mistakes" Driven by Defenders

Innovation resulted from actions taken by defenders, consumers or other non-attackers

What kind of innovation is it?

Technology

- Insecure fundamental protocols: BGP, TCP/UDP, DNS, IP v4/v6
- Market incentives which reward rushing insecure software to market
- Mass deployment of insecure IoT

Operations

- Patch diffing for vulnerabilities

Policy

- Few, weak global cyber norms
- Lack of deterrent for 'grey area' operations

LESSONS AND RECOMMENDATIONS

Commonalities and Differences

- Hard to argue that the ecosystem overall is improving despite individual successes
- Limited attacker innovation
- Many offensive innovations are ‘self-inflicted’

About Offensive Security

- OFFSEC does of course aid both attackers and defenders
- On balance, have tools advantaged attackers over defenders:
  - Far less – less - about equal - more - far more?
  - Needs analysis based on measurements not anecdotes or inertia
- **Critical questions:**
  - Which characteristics of OFFSEC tools preferentially helps malicious use over defensive use? Under which circumstances?
  - How can we shift the balance to maximize defensive advantage while minimizing malicious?

Potential Areas for Disruption

- Tech may only offer a few options for disruption at scale
  - Botnet disruption has not scaled
  - New US strategy of persistent engagement based on imposing friction. Success may hinge on whether defensive disruptive operations can cheaply scale
- Possibly higher chances in operations and policy
  - Botnet disruption has not scaled
  - Indictments have mixed results: more impact on Chinese actors than Iranians and Russians
  - Disrupt adversary *trust* networks (USCYBER versus IRA)
  - Promise for disruption of payment systems for monetization

Disrupting Offensive Innovations at Scale

Example: Disrupting Cashing Out

Click Trajectories: End-to-End Analysis of the Spam Value Chain

Kirill Levchenko* Andreas Pitsillidis* Neha Chachra* Brandon Enright* Márk Félegyházi‡ Chris Grier†
Tristan Halvorson* Chris Kanich* Christian Kreibich†◇ He Liu* Damon McCoy*
Nicholas Weaver†◇ Vern Paxson†◇ Geoffrey M. Voelker* Stefan Savage*

*Department of Computer Science and Engineering
University of California, San Diego

†Computer Science Division
University of California, Berkeley

◇International Computer Science Institute
Berkeley, CA

‡Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics

***Abstract*—Spam-based advertising is a business. While it has engendered both widespread antipathy and a multi-billion dollar anti-spam industry, it continues to exist because it fuels a profitable enterprise. We lack, however, a solid understanding of this enterprise's full structure, and thus most anti-spam interventions focus on only one facet of the overall spam value chain (e.g., spam filtering, URL blacklisting, site takedown). In this paper we present a holistic analysis that quantifies the full set of resources employed to monetize spam email—including naming, hosting, payment and fulfillment—using extensive measurements of three months of diverse spam data, broad crawling of naming and hosting infrastructures, and over 100 purchases from spam-advertised sites. We relate these resources to the organizations who administer them and then use this data to characterize the relative prospects for defensive interventions at each link in the spam value chain. In particular, we provide the first strong evidence of payment bottlenecks in the spam value chain; 95% of spam-advertised pharmaceutical, replica and software products are monetized using merchant services from just a handful of banks.**

it is these very relationships that capture the structural dependencies—and hence the potential *weaknesses*—within the spam ecosystem's business processes. Indeed, each distinct *path* through this chain—registrar, name server, hosting, affiliate program, payment processing, fulfillment—directly reflects an "entrepreneurial activity" by which the perpetrators muster capital investments and business relationships to create value. Today we lack insight into even the most basic characteristics of this activity. How many organizations are complicit in the spam ecosystem? Which points in their value chains do they share and which operate independently? How "wide" is the bottleneck at each stage of the value chain—do miscreants find alternatives plentiful and cheap, or scarce, requiring careful husbanding?

The desire to address these kinds of questions empirically—and thus guide decisions about the most effective mechanisms for addressing the spam problem—forms the core motivation of our work. In this paper we develop

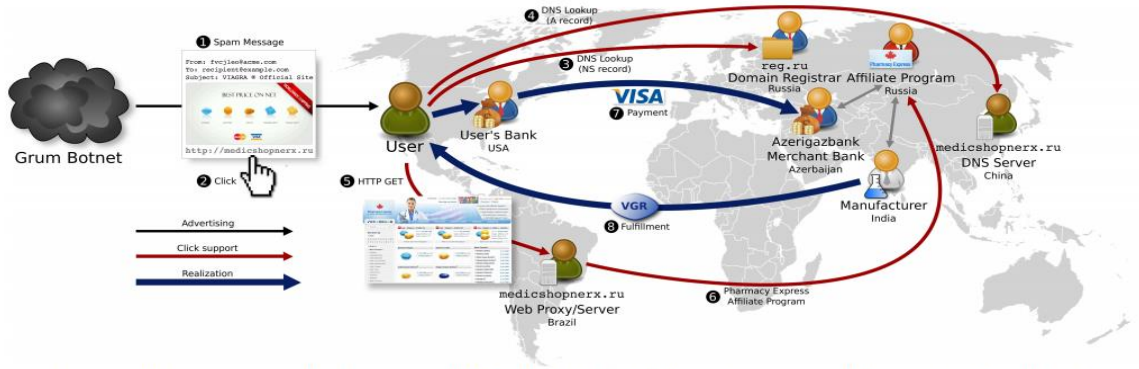
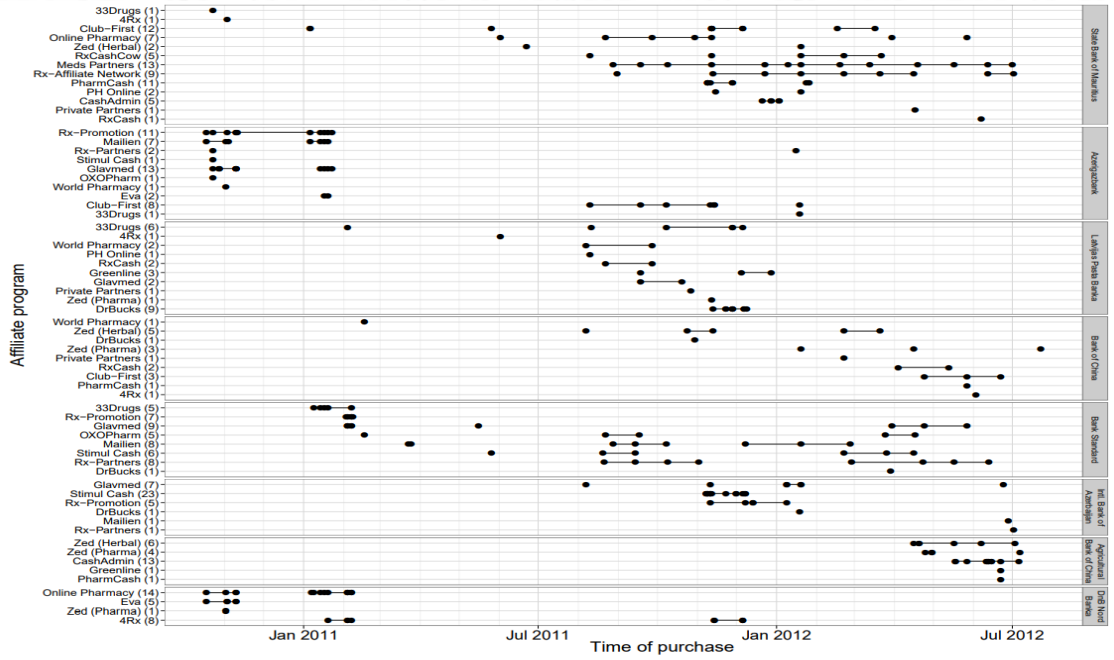


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

"95% of spam-advertised pharmaceutical, replica and software products are monetized using merchant services from just a handful of banks"

Disrupting Offensive Innovations at Scale



Transactions

Priceless: The Role of Payments in Abuse-advertised Goods

Damon McCoy, Hitesh Dharmdasani
George Mason University

Christian Kreibich
University of California, San Diego and International Computer Science Institute

Geoffrey M. Voelker and Stefan Savage
University of California, San Diego

ABSTRACT

Large-scale abusive advertising is a profit-driven endeavor. Without consumers purchasing spam-advertised Viagra, search-advertised counterfeit software or malware-advertised fake anti-virus, these campaigns could not be economically justified. Thus, in addition to the numerous efforts focused on identifying and blocking individual abusive advertising mechanisms, a parallel research direction has emerged focused on undermining the associated means of monetization: *payment networks*. In this paper we explain the complex role of payment processing in monetizing the modern affiliate program ecosystem and characterize the dynamics of these banking relationships over two years within the counterfeit pharmaceutical and software sectors. By opportunistically combining our own active purchasing data with contemporary disruption efforts by brand-holders and payment card networks, we gather the first empirical dataset concerning this approach. We discuss how well such payment interventions work, how abusive merchants respond in kind and the role that the payments ecosystem is likely to play in the future.

individual mechanisms directly, an alternative research agenda revolves around undermining the economics of the activity itself. In particular, as with all advertisers, the actors employing these abusive techniques are profit-seeking and only participate due to the promise of compensation (e.g., a typical pharmaceutical spammer is paid a 40% commission on the gross revenue of each sale they bring in). Thus, if these payments dried up, so too might the incentive to continue advertising.

In this paper we examine this question by focusing particularly on abusive advertising that is directly capitalized through consumer credit card payments (e.g., counterfeit goods such as pharmaceuticals [11] and some fraud scams such as fake anti-virus [15]). We are motivated in part by our previous work documenting that a small number of banks are implicated in handling credit card payments for the vast majority of spam-advertised goods [10]. In that paper, we hypothesized that interrupting those banking relationships might be an effective intervention for undermining such activity. However, at the time we lacked the data to evaluate this "payment intervention" theory; to the best of our knowledge, few such concerted actions were even being attempted. Over the last year, however, there has been significant adoption of this approach and we

- For the few tens of dollars for a modest online purchase, our data shows that it is possible to identify a portion of the underlying payment infrastructure and, within weeks, cause it to be terminated.
- This termination cost is inevitably far higher— in fines, in lost holdback, in time and in opportunity cost—than the cost of the intervention itself.
- **Relatively concentrated actions with key financial institutions can have outsized impacts**.

Parallel and Future Research

- **Other efforts**
  - NYCTF2 on operational collaboration at scale
  - Framework for defensive operational disruption and dataset
  - SIPA student capstone on effects of operational disruption
- **Possible Future efforts**
  - Collaborate with those engaged in research & active disruption ops
  - Expand out charts of innovations
  - Structured analysis of which offensive innovations may be most vulnerable to disruption

THANK YOU

@Jason_Healey

@DAlperovitch