

RSA®C Sandbox

RSA®Conference2020
Sandbox

HUMAN
ELEMENT

SESSION ID: SBX1-R11

Understanding and Disrupting Offensive Innovations



Jason Healey

Columbia University
@Jason_Healey

Dmitri Alperovitch

Stealth Policy Accelerator, Co-Founder CrowdStrike
@DAIperovitch

RSA®Conference2020
#RSAC

Bad Guys Finish First

“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*

To slash or to trim

Emission reductions by policies/actions, bn tonnes CO₂ equivalent

Policy/Action	Cumulative emissions	Period	Annual emissions*
Montreal protocol ¹	135.0bn	1989-2013	5.6bn
Hydropower worldwide ²	2.8bn	2010	2.8bn
Nuclear power worldwide ²	2.2bn	2010	2.2bn
China one-child policy ³	1.3bn	2005	1.3bn
Other renewables worldwide ²	600m	2010	600m
US vehicle emissions & fuel economy standards ^{†4}	6.0bn	2012-25	460m
Brazil forest preservation ⁵	3.2bn	2005-13	400m
India land-use change ⁶	177m	2007	177m
Clean Development Mechanism ⁷	1.5bn	2004-14	150m
US building & appliances codes ⁴	3.0bn	2008-30	136m
China SOE efficiency targets ⁸	1.9bn	2005-20	126m
Collapse of USSR ⁹	709m	1992-98	118m
Global Environment Facility ¹⁰	2.3bn	1991-2014	100m
EU energy efficiency ¹¹	230m	2008-12	58m
US vehicle emissions & fuel economy standards ^{†4}	270m	2014-18	54m
EU renewables ¹¹	117m	2008-12	29m
US building codes (2013) ¹²	230m	2014-30	10m
US appliances (2013) ¹²	158m	2014-30	10m
Clean technology fund ¹³	1.7bn	project lifetime	na
EU vehicle emission standards ¹⁴	140m	2020	na

CATEGORIES:

Energy production
Transport
Other regulations
Global treaties
Land & forests
Other

See following panel for sources and explanations

*Annual emissions are cumulative emissions divided by the relevant period. The estimate for the current emissions avoided under the Montreal protocol is eight billion tonnes of CO₂e. The annual figure for the collapse of the USSR refers to the years 1992-98. [†]Cars and light trucks [‡]Heavy trucks

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

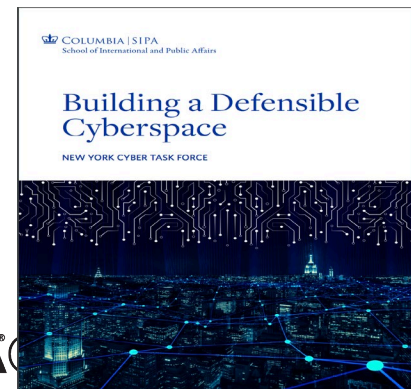
Matthew Waxman, Columbia University

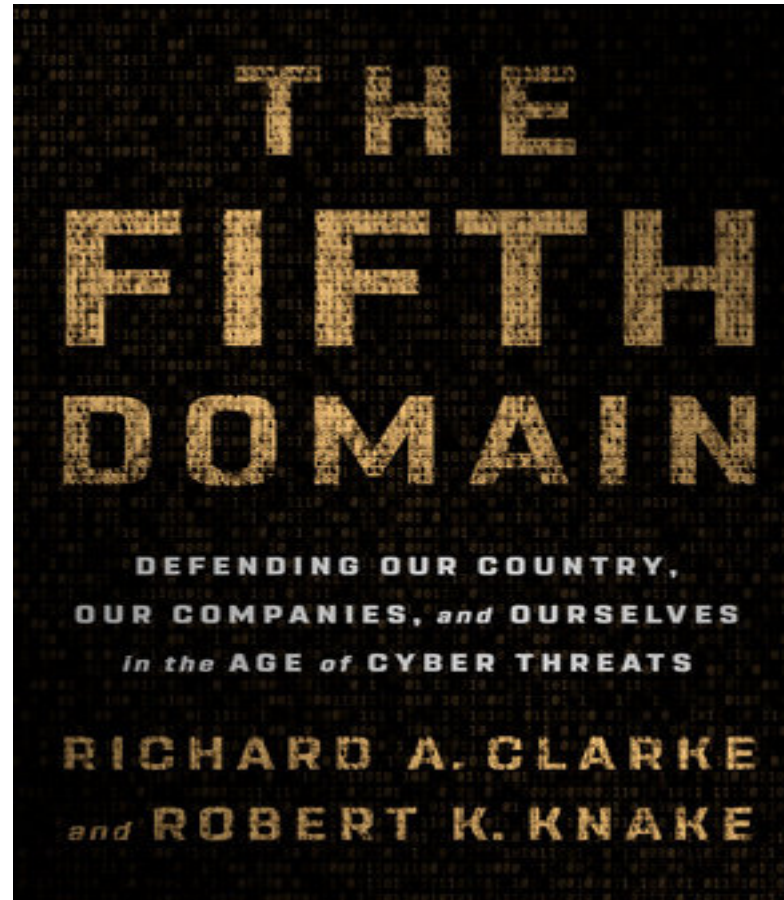
David C. Lashway, Baker McKenzie

John Yetter, NASDAQ

Aaron K. Martin, JPMorgan Chase

Larry Zelvin, Citigroup





Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

Where is primary effect of the innovation?

		TECHNOLOGY		What kind of innovation is it? OPERATIONS		POLICY	
WITHIN ENTERPRISE Changes implemented by centrally managed IT team	PAST	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Critical mass of cloud deploymentAutomated measurement of attack surfaceComputer-generated software diversityWidespread chip-and-pin deploymentScalable security automation	<ul style="list-style-type: none">Autonomic and autonomous defensesStrong bio-authenticationAlternate computing and security architectures (e.g., islets)Instrumenting data with sensorsAnalog controls	<ul style="list-style-type: none">Security scorecards and ratingsActive vendor managementInsurance and other risk transferImproved security metrics from cloudMore holistic combination of risk, cybersecurity, physical security, business continuity, crisis managementSoftware bill of materials		<ul style="list-style-type: none">Safe harbor provisions for sharingNational 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	<ul style="list-style-type: none">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)		<ul style="list-style-type: none">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)		<ul style="list-style-type: none">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	<ul style="list-style-type: none">Inexpensive formal methods, such as HACMSFormal methods applied to standards, like HTTPSSigned firmwareQuantum encryptionBlockchain		<ul style="list-style-type: none">Cyber Independent Testing Labs and other quantification and rating systemsContinuous disruption of adversary operationsIndependent attribution organizationCrowdsourcing IOCs for early detection		<ul style="list-style-type: none">Norms: rules of the road for cyber conflict"Naming and shaming," especially when norms are violatedFCC actionRegulatory emphasis on response, rather than protection <ul style="list-style-type: none">Global governance structure: G20+ICT20Shifts in liability, especially for software and IoTFederal insurance backstopImproved security metrics to drive better policyWTO and trade restrictions	

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

Where is primary effect of the innovation?

		TECHNOLOGY		OPERATIONS		POLICY
WITHIN ENTERPRISE	PAST	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Critical mass of cloud deploymentAutomated measurement of attack surfaceComputer-generated software diversityWidespread chip-and-pin deploymentScalable security automation	<ul style="list-style-type: none">Autonomic and autonomous defensesStrong bio-authenticationAlternate computing and security architectures (e.g., islets)Instrumenting data with sensorsAnalog controls	<ul style="list-style-type: none">Security scorecards and ratingsActive vendor managementInsurance and other risk transferImproved security metrics from cloudMore holistic combination of risk, cybersecurity, physical security, business continuity, crisis managementSoftware bill of materials	<ul style="list-style-type: none">Safe harbor provisions for sharingNational data breach notification law	
ACROSS CYBERSPACE AS A WHOLE	PAST	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">Detection, personnel security and operational security (1960s)Stakeholders' groups (e.g., NANOG, RIPE) (1990s)Security operations centers (1990s)Arresting attackers (1990s)Volunteer response (e.g., Conficker, NSP-SEC) (2000s)Volunteer groups for protectionRise of security industry and Industry Associations (e.g. (2000s)Rise of DevOps (2000s)Institutionalized bug bountyAttribution methodologiesBotnet Takedowns (2010s)	<ul style="list-style-type: none">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)		
	POTENTIAL FUTURE INNOVATIONS	<ul style="list-style-type: none">Inexpensive formal methods, such as HACMSFormal methods applied to standards, like HTTPSSigned firmwareQuantum encryptionBlockchain	<ul style="list-style-type: none">Cyber Independent Testing, rating systemsContinuous disruption of aIndependent attribution ofCrowdsourcing IOCs for e	<ul style="list-style-type: none">Global governance structure: G20+ICT20Shifts in liability, especially for software and IoTFederal insurance backstopImproved security metrics to drive better policyWTO and trade restrictions		

We tend to invest and measure HERE:

technology inside the enterprise

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

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

Where is primary effect of the innovation?

		TECHNOLOGY	OPERATIONS	POLICY		
WITHIN ENTERPRISE Changes implemented by centrally managed IT team	PAST	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)
	POTENTIAL FUTURE INNOVATIONS	<ul style="list-style-type: none">Critical mass of cloud deploymentAutomated measurement of attack surfaceComputer-generated software diversityWidespread chip-and-pin deploymentScalable security automation	<ul style="list-style-type: none">Autonomic and autonomous defensesStrong bio-authenticationAlternate computing and security architectures (e.g., islets)Instrumenting data with sensorsAnalog controls	<ul style="list-style-type: none">Security scorecards and risk managementActive vulnerability managementInsurance and risk transferImproved metrics for securityIntegration of security with business operationsIntegration of security with legal and compliance		
ACROSS CYBERSPACE AS A WHOLE 1. Change at end points that "floats all boats" 2. Change to "key terrain" like ISPs	PAST	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">Physical protection, personnelCreation of operators' groupsSecurity 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)	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Inexpensive formal methods, such as HACMSFormal methods applied to standards, like HTTPSSigned firmwareQuantum encryptionBlockchain	<ul style="list-style-type: none">Cyber Independent Testing Labs and other quantification and rating systemsContinuous disruption of adversary operationsIndependent attribution organizationCrowdsourcing IOCs for early detection	<ul style="list-style-type: none">Norms: rules of the road for cyber conflict"Naming and shaming," especially when norms are violatedFCC actionRegulatory emphasis on response, rather than protection	<ul style="list-style-type: none">Global governance structure: G20+ICT20Shifts in liability, especially for software and IoTFederal insurance backstopImproved security metrics to drive better policyWTO and trade restrictions	

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

When the real 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

Where is primary effect of the innovation?

ACROSS CYBERSPACE AS A WHOLE		TECHNOLOGY		OPERATIONS		POLICY	
1. Change at end points that "floats all boats" 2. Change to "key terrain" like ISPs	PAST	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">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)	<ul style="list-style-type: none">Creation of pen testing 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)	<ul style="list-style-type: none">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			<ul style="list-style-type: none">Security scorecards and ratingsActive vendor managementInsurance and other risk transferImproved security metrics from cloudMore holistic combination of risk, cybersecurity, physical security, business continuity, crisis managementSoftware bill of materials		<ul style="list-style-type: none">Safe harbor provisions for sharingNational data breach notification law	
2. Change to "key terrain" like ISPs	PAST	<ul style="list-style-type: none">OS hardening (2010s)Ubiquitous, transparent encryption (2010s)Cloud-based security at platform companies (2010s)Ubiquitous, secure protocols (HTTPS, TLS/SSL) (2010s)Automated testing (2010s)		<ul style="list-style-type: none">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)		<ul style="list-style-type: none">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	<ul style="list-style-type: none">Inexpensive formal methods, such as HACMSFormal methods applied to standards, like HTTPSSigned firmwareQuantum encryptionBlockchain		<ul style="list-style-type: none">Cyber Independent Testing Labs and other quantification and rating systemsContinuous disruption of adversary operationsIndependent attribution organizationCrowdsourcing IOCs for early detection		<ul style="list-style-type: none">Norms: rules of the road for cyber conflict"Naming and shaming," especially when norms are violatedFCC actionRegulatory emphasis on response, rather than protection	<ul style="list-style-type: none">Global governance structure: G20+ICT20Shifts in liability, especially for software and IoTFederal insurance backstopImproved security metrics to drive better policyWTO and trade restrictions

And overlook gains from operational and process innovations:

- CISO
- ISACs
- Kill Chain and @TTACK

And overlook gains from operational and process innovations:

- CISO
- ISACs
- Kill Chain and @TTACK

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...

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!

- Rob Sheldon
- Mike Klipstein



OFFENSIVE INNOVATIONS

Important Offensive Innovations of the Past 50 Years

New York Cyber Task Force

Type of innovation.

	Technology	Operations	Policy
<p>Driven by Attackers</p> <p>Innovation originated with hackers, security researchers or other non-defenders</p>	<ul style="list-style-type: none"> • 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) • 	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • National sanctuaries for cyber criminals if they don't attack host nation • States using proxy groups and ignoring criminal side jobs • Lack of deterrent for 'grey area' operations • 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 than 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

New York Cyber Task Force

What kind of innovation is it?			
Driven by Defenders	Technology	Operations	Policy
	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Limited trust, reluctant information sharing, poor corporate governance	<ul style="list-style-type: none">• Decreasing global trust and governance• New top-level domains• Weak cybersecurity laws• Few, weak global cyber norms• Liability concerns driving secrecy• Lack of sensible regulations that can drive accountability



LESSONS AND RECOMMENDATIONS

Commonalities and Differences

- Limited attacker innovation
- Many offensive innovations are ‘self-inflicted’
- In many cases though, defensive benefits outweigh the offensive gains
- More debate is needed on costs vs benefits or how to limit criminal use
- Hard to argue that the ecosystem overall is improving despite individual successes

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 Félégyházi[‡] Chris Grier[‡]
Tristan Halvorsen^{*} 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 dependencies—and hence the potential *weak* the spam ecosystem's business processes: distinct *path* through this chain—registrars, hosting, affiliate program, payment processing directly reflects an “entrepreneurial activity” perpetrators muster capital investments and tionships to create value. Today we lack in the most basic characteristics of this activity: organizations are complicit in the spam ecosystem in their value chains do they share and independently? How “wide” is the bottleneck of the value chain—do miscreants find alter and cheap, or scarce, requiring careful husbandry? The desire to address these kinds empirically—and thus guide decisions about tative mechanisms for addressing the spam problem is the core motivation of our work. In this paper

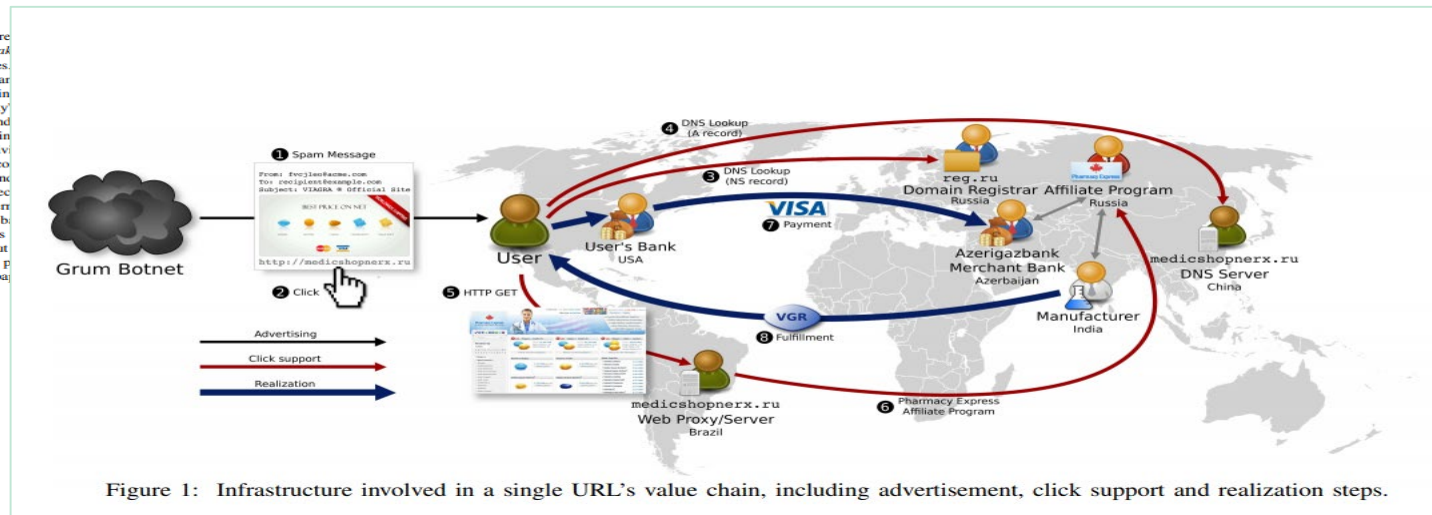
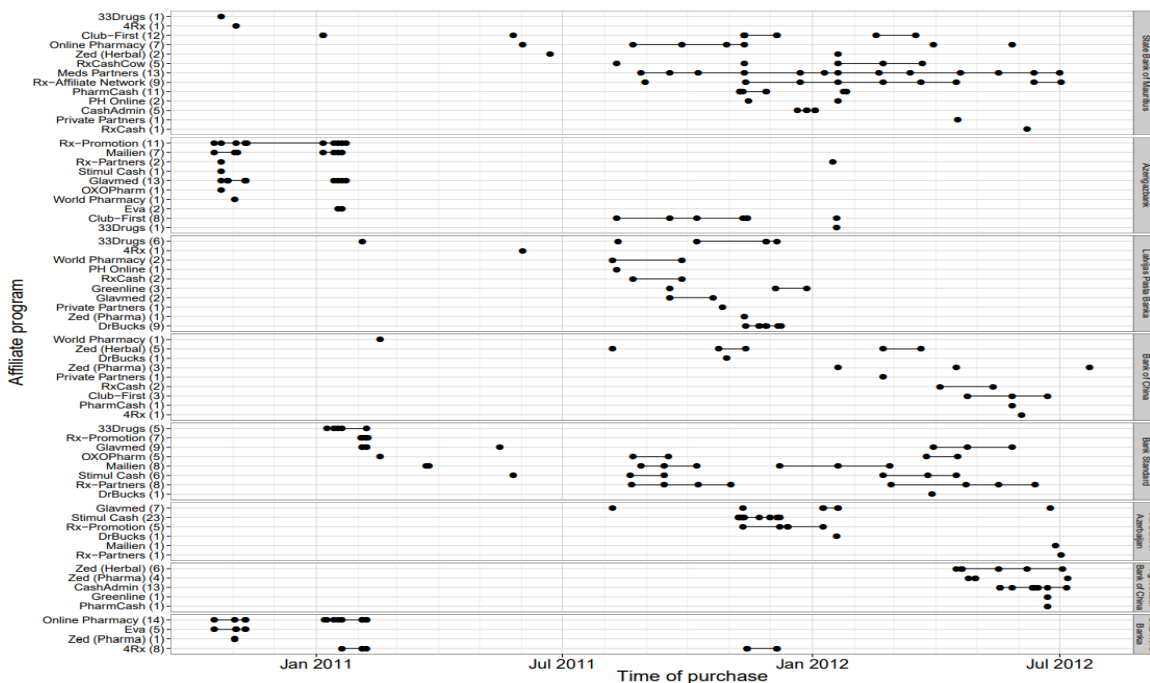


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

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

RSA[®]C
Sandbox



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 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 role of payment networks in the abusive ecosystem, how they infiltrate program ecosystem and characterize the dynamics of these relationships over two years within the counterfeit pharmaceutical and software sectors. By opportunistically combining data from payment networks with data from other sources, our 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 react to them 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 actors are profit-seeking and only participate in the activity 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 fraudulent scams such as fake advance fee [15]). We used a random sample of 1000 credit card statements from 155 users, and 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 would have a significant effect on the volume of spam advertising. However, at the time we lacked the data to evaluate this "payment intervention" theory; to the best of our knowledge, few such consumer actions were even being attempted. Over the last year, however, we have been able to obtain the data we needed.

- 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.**

About Offensive Security

- OFFSEC does of course aid defenders
- Critical question:
 - Which aspects most help defenders more than attackers?
 - Needs analysis based on measurements not anecdotes or inertia



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

THANK YOU

@Jason_Healey
@DAIperovitch

“Apply” Slide

- Bullet point here (see slides 5 – 8 for instructions)
- Bullet point here
- Bullet point here