RSAC Sandbox

RSAConference2020 RSAC 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
@DAlperovitch

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 CO_2 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 CO_2e. The annual figure for the collapse of the USSR refers to the years 1992-98. †Cars and light trucks ‡Heavy trucks

http://www.economist.com/news/briefing/21618680-our-guide-actions-have-done-most-slow-global-warming-deepest-cuts

Central Question

RSAC Sandbox

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

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

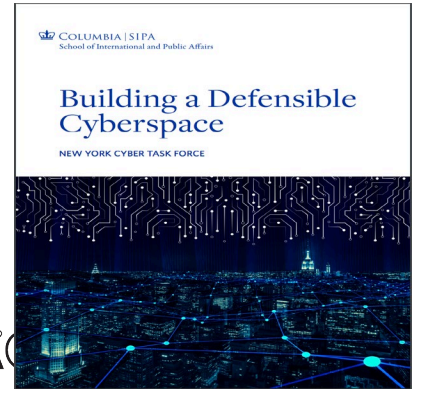
Key Questions for a Defensible Cyberspce

Results from NY Cyber Task Force

RSAC Sandbox

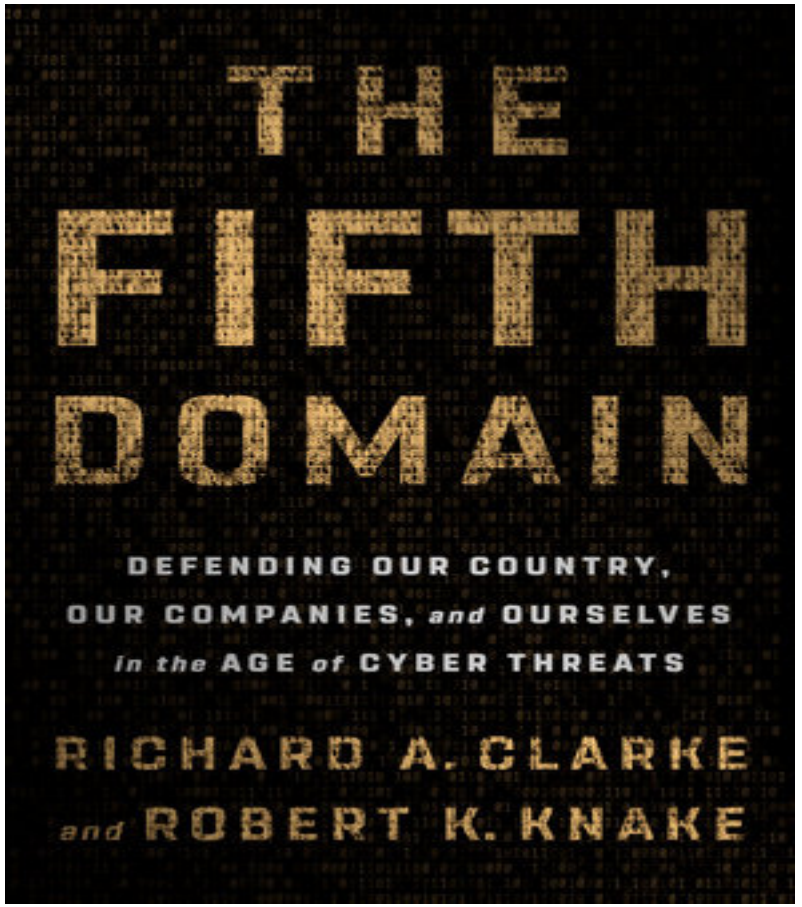
1. What is a defensible cyberspace and why hasn't it been defensible to date?
2. What past innovations have made the biggest difference? What made them so successful?
3. What innovations should we prioritize today?

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



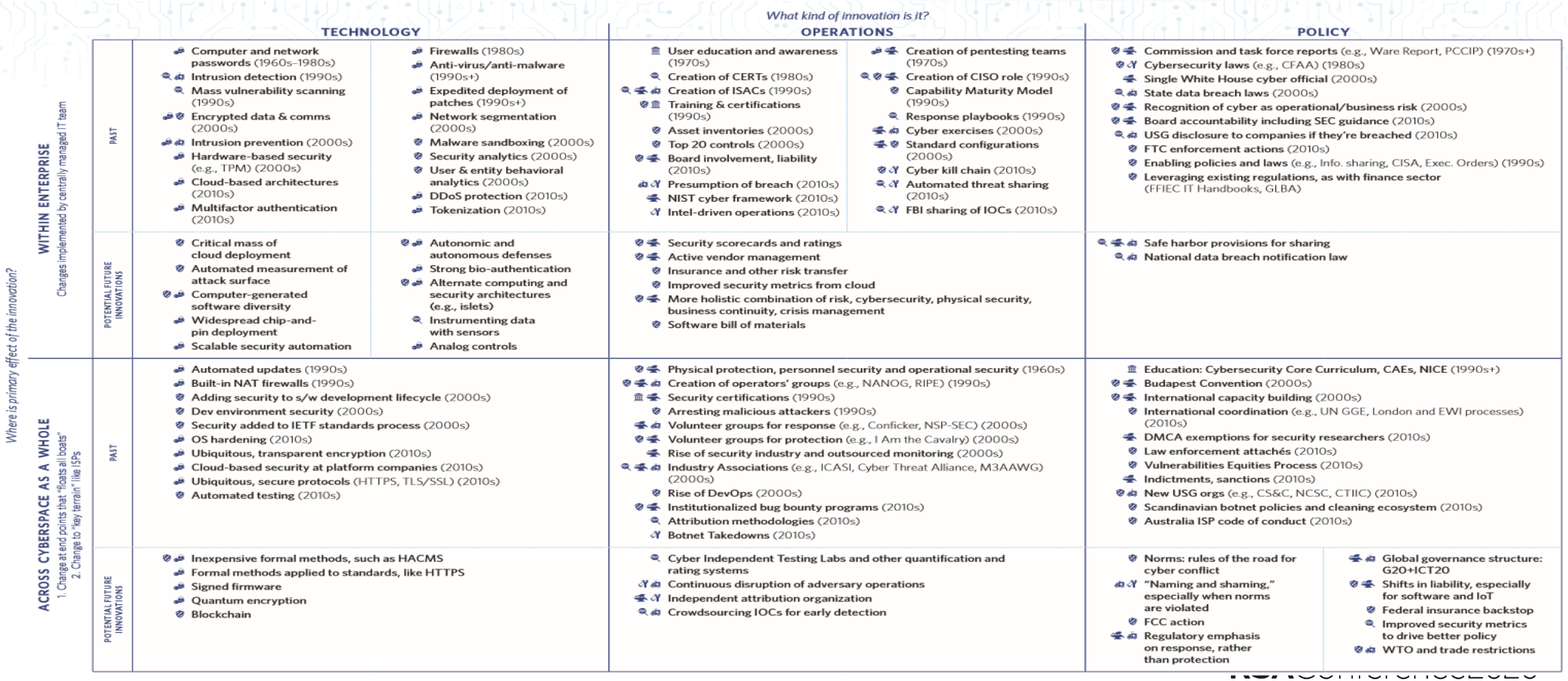
https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF

RSAC


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

RSAC Sandbox



Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

RSAC Sandbox

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

Important Defensive Innovations of the Past 50 Years

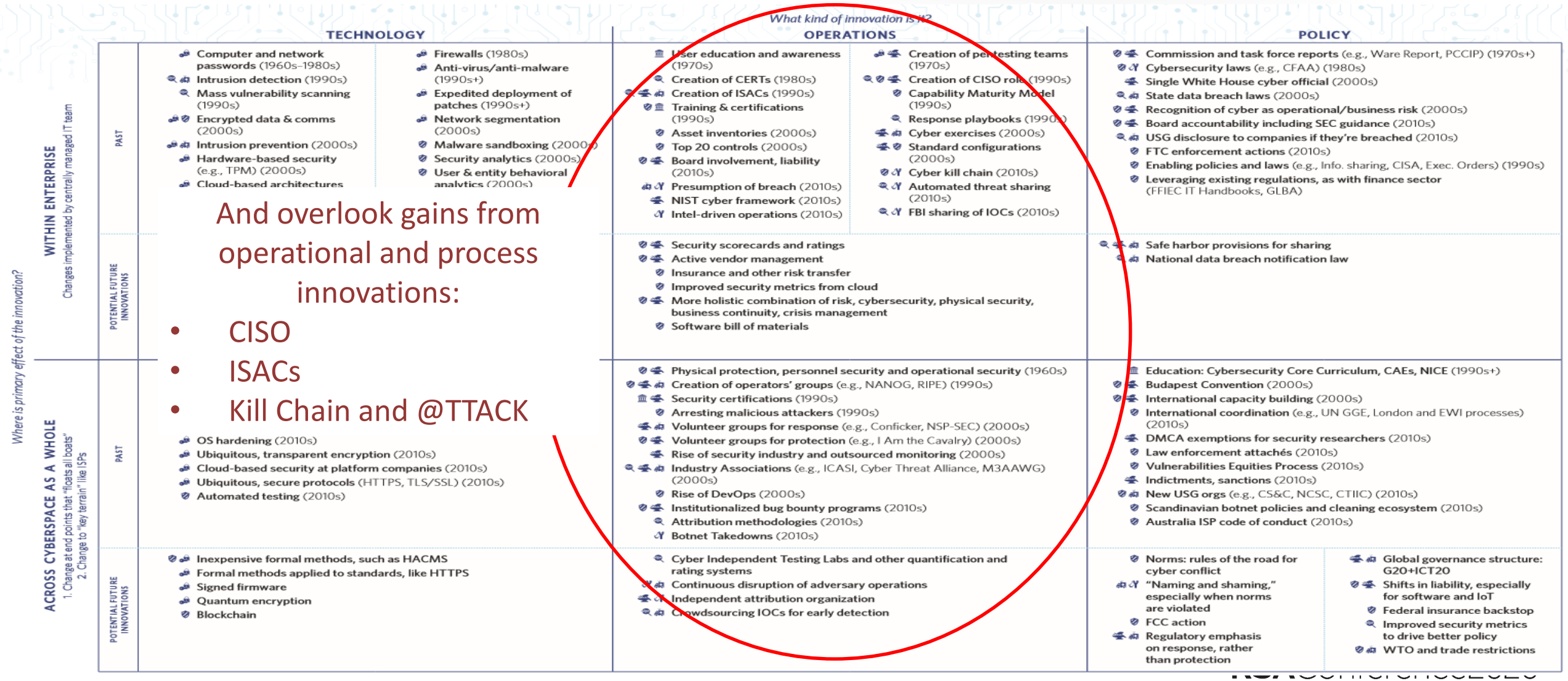
New York Cyber Task Force

RSAC Sandbox

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

RSAC Sandbox



And overlook gains from operational and process innovations:

- CISO
- ISACs
- Kill Chain and @TTACK

Central Question

RSAC Sandbox

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

RSAC Sandbox

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

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

OFFENSIVE INNOVATIONS

Important Offensive Innovations of the Past 50 Years

New York Cyber Task Force

RSAC Sandbox

Type of innovation.

	Technology	Operations	Policy
Driven by Attackers 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 • 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 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

New York Cyber Task Force

RSAC Sandbox

What kind of innovation is it?

	Technology	Operations	Policy
Driven by Defenders Innovation resulted from actions taken by defenders, consumers or other non-attackers	• 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	• Limited trust, reluctant information sharing, poor corporate governance	• 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

RSAC Sandbox

- 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

RSAC Sandbox

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
dependencies—and hence the potential *weak*
the spam ecosystem's business processes.
distinct *path* through this chain—registrar
hosting, affiliate program, payment processin
directly reflects an "entrepreneurial activity"
perpetrators muster capital investments and
tionships to create value. Today we lack in
the most basic characteristics of this activi
organizations are complicit in the spam eco
points in their value chains do they share an
independently? How "wide" is the bottlenec
of the value chain—do miscreants find altern
and cheap, or scarce, requiring careful husb
The desire to address these kinds
empirically—and thus guide decisions about
tive mechanisms for addressing the spam p
the core motivation of our work. In this pa

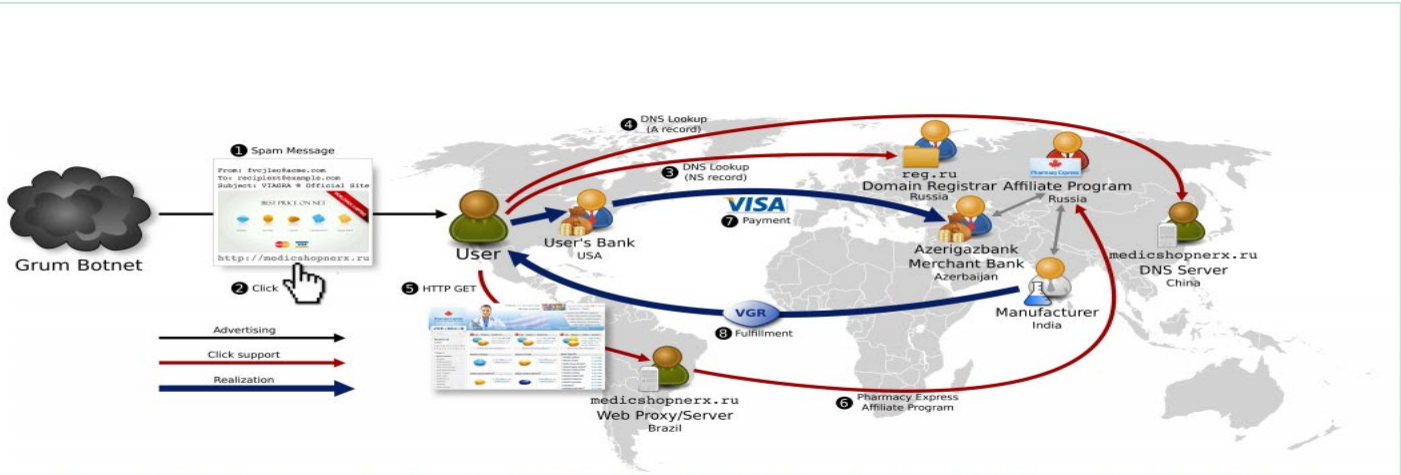
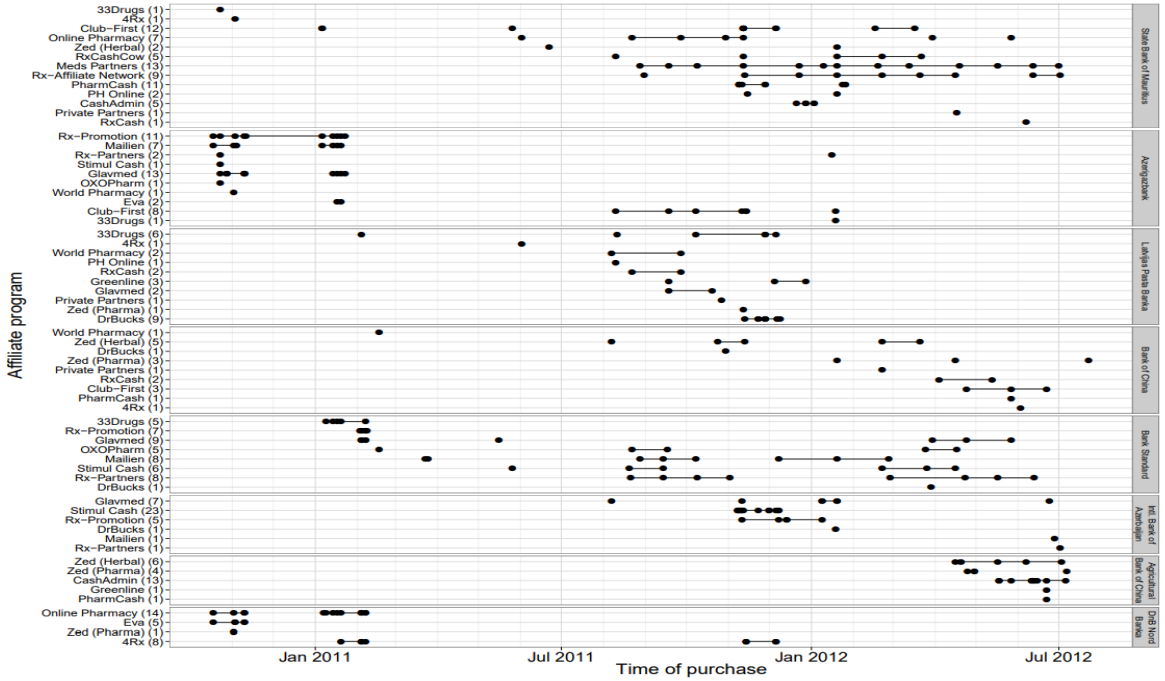


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

"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

RSAC 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 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**.

About Offensive Security

RSAC Sandbox

- 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
@DAlperovitch

“Apply” Slide

RSAC Sandbox

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