Cybersecurity Challenges

Thinking Globally – Acting Locally

CHRIS EVANS
MARCH, 2017

How Did I Get Here?

- 10 Years in the United States Air Force
  - Communications Officer, Air Force Red Team
- 9 Years Cybersecurity Consulting with Delta Risk
  - Strategy, Risk Management, Assessments, Exercises, Training
- 2 Months(!) at Stash
  - Co-Founder and Chief Information Security Officer

STASH® DELTA RISK A CHERTOFF GROUP COMPANY U.S. AIR FORCE NASA JPL USC ILLINOIS INSTITUTE OF TECHNOLOGY

Talk Objectives

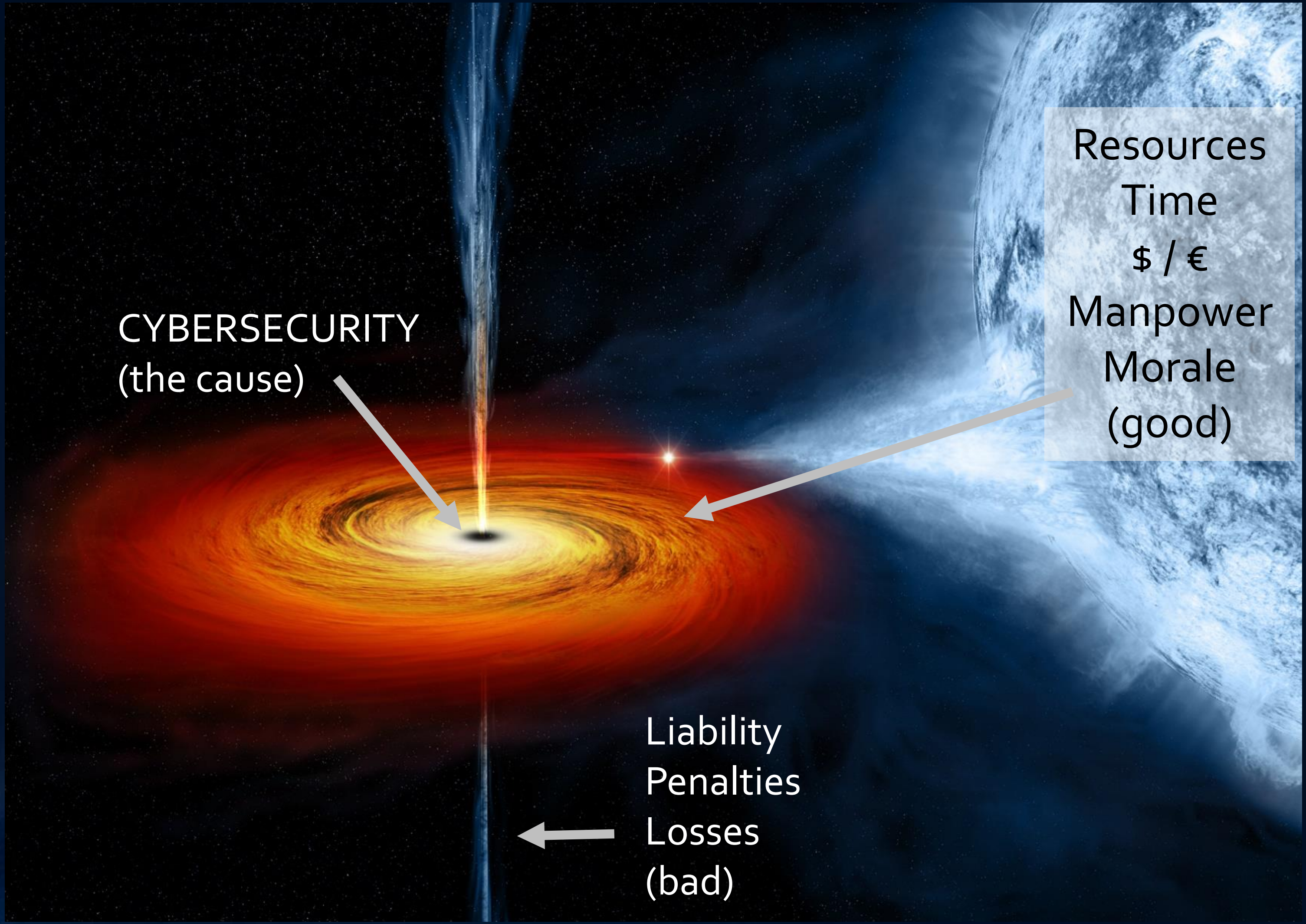
- Present a Non-Traditional View of Cybersecurity Challenges
- Discuss Why We are Currently Losing the Cyber “War”
- Highlight How We can Shift to a Winning Strategy

A Global View of the Internet

- The Internet is a Fragile Place – Whether We Know It or Not!

Video TBD

Cybersecurity (a general view)



CYBERSECURITY
(the cause)

Resources
Time
$ / €
Manpower
Morale
(good)

Liability
Penalties
Losses
(bad)

NASA

Cybersecurity (another viewpoint)

- We are at war
  - Conventional / Insurgency / Cold / Undeclared?
  - Asymmetric / Symmetric?

Graphic TBD

Graphic TBD

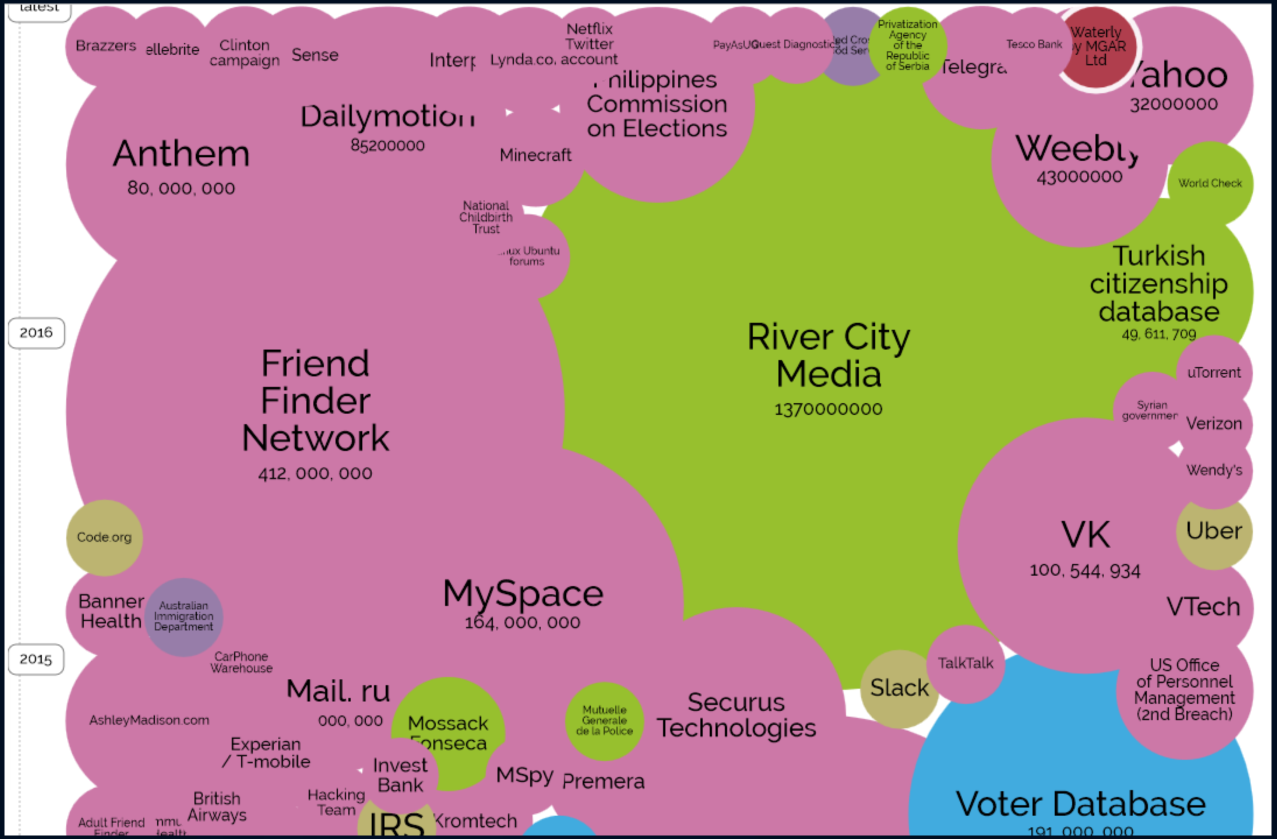
This Cyber War Stuff is Expensive

- Extreme difference in cost to attack versus cost to defend
- Stats on impact to financial, morale, intellectual property, etc TBD

Work in Progress

Is There a Doubt We are Losing this War?

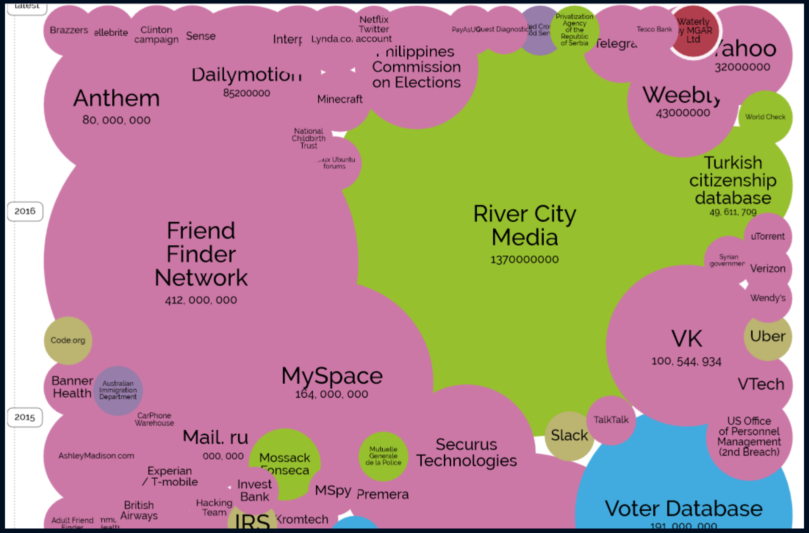
- Magenta = Hacked
- Red = Poor Security Practices
- Light Blue = Insider
- Green = Lost Computer / Media

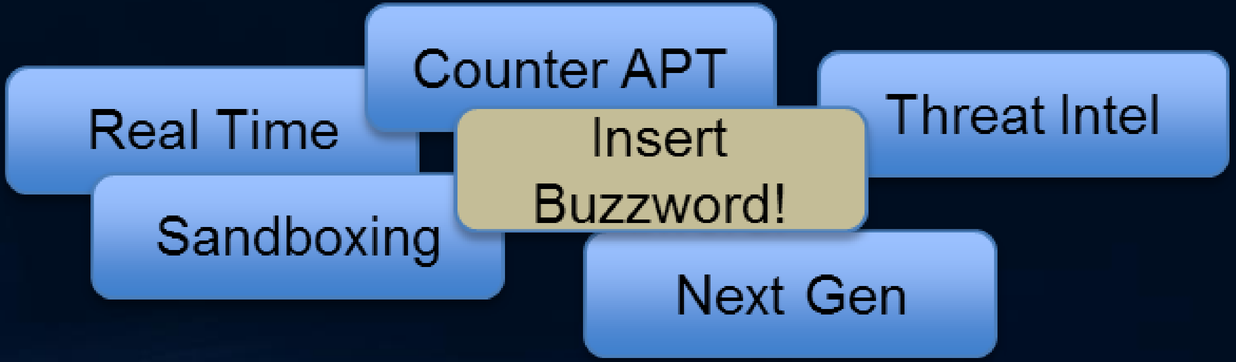


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

How Can This Be?

- A lot of big organizations on this list
- Organizations with big budgets
- Lots of security technology already in play
- Real Time, Counter APT, Next Gen, Advanced <BLAH>




Counter APT

Real Time

Threat Intel

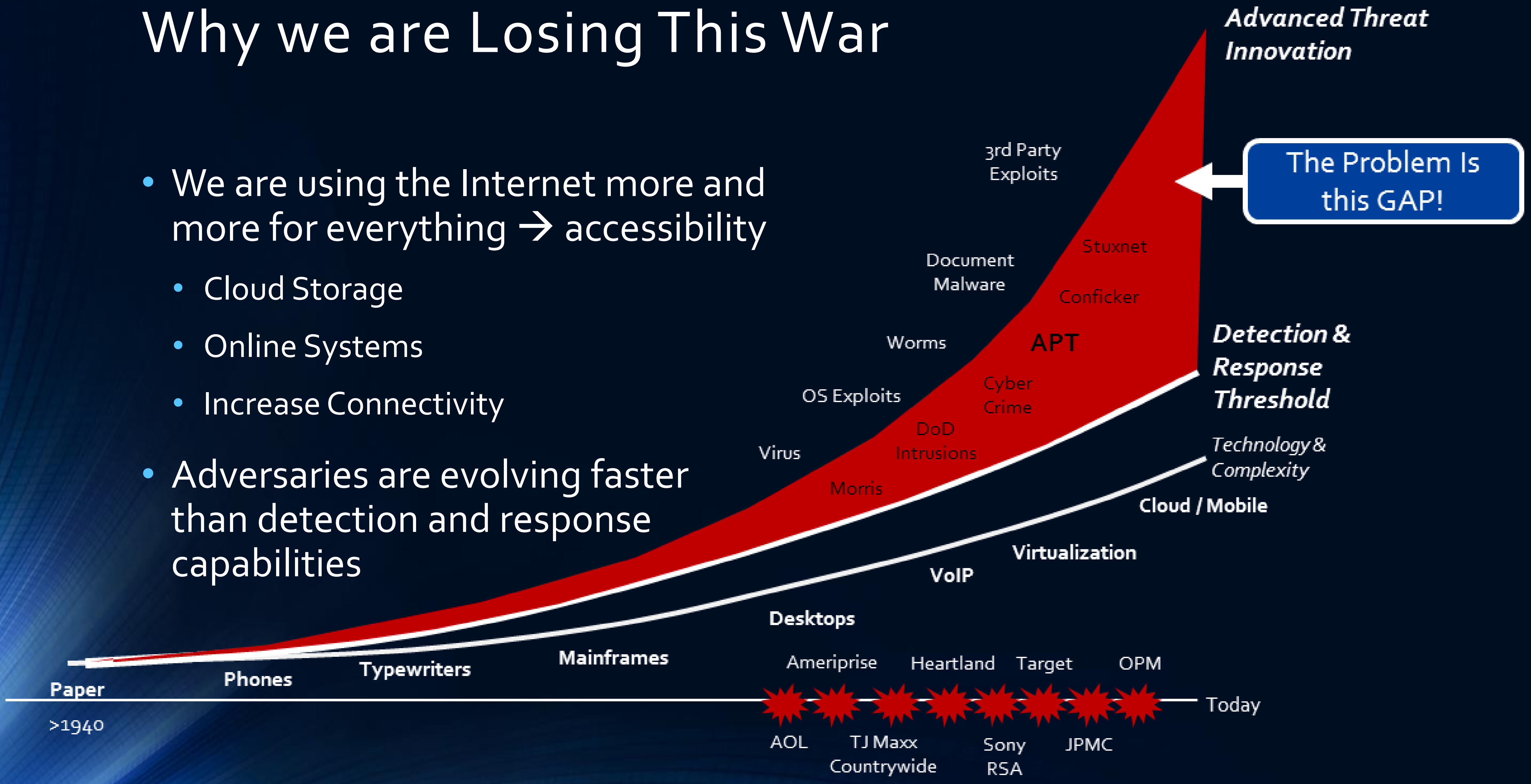
Insert Buzzword!

Sandboxing

Next Gen

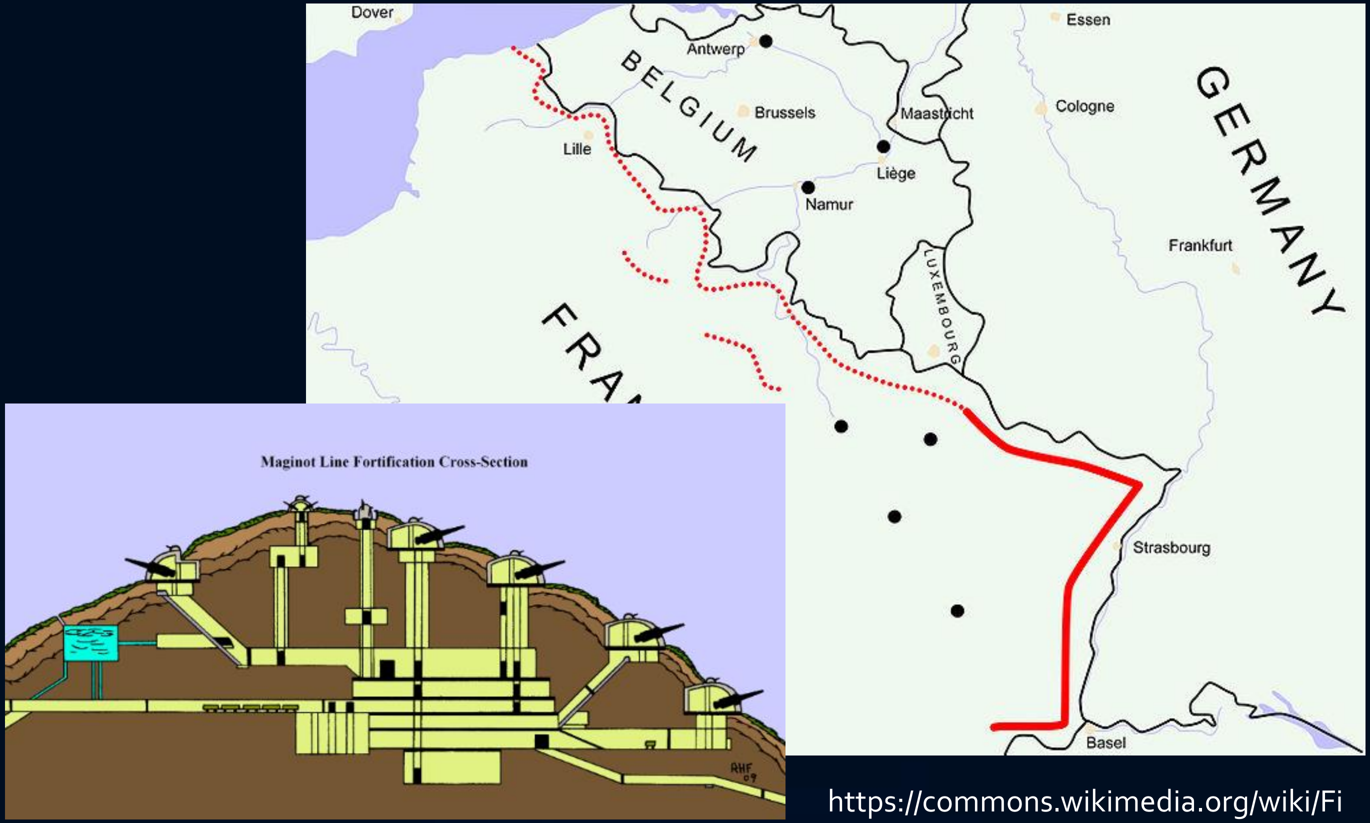
Why we are Losing This War

- We are using the Internet more and more for everything → accessibility
  - Cloud Storage
  - Online Systems
  - Increase Connectivity
- Adversaries are evolving faster than detection and response capabilities



An Analogy from History – The Maginot Line

- Expansive and Expensive Defenses
- Built to Keep "Something" Out
- Successful? Worth the Expense?

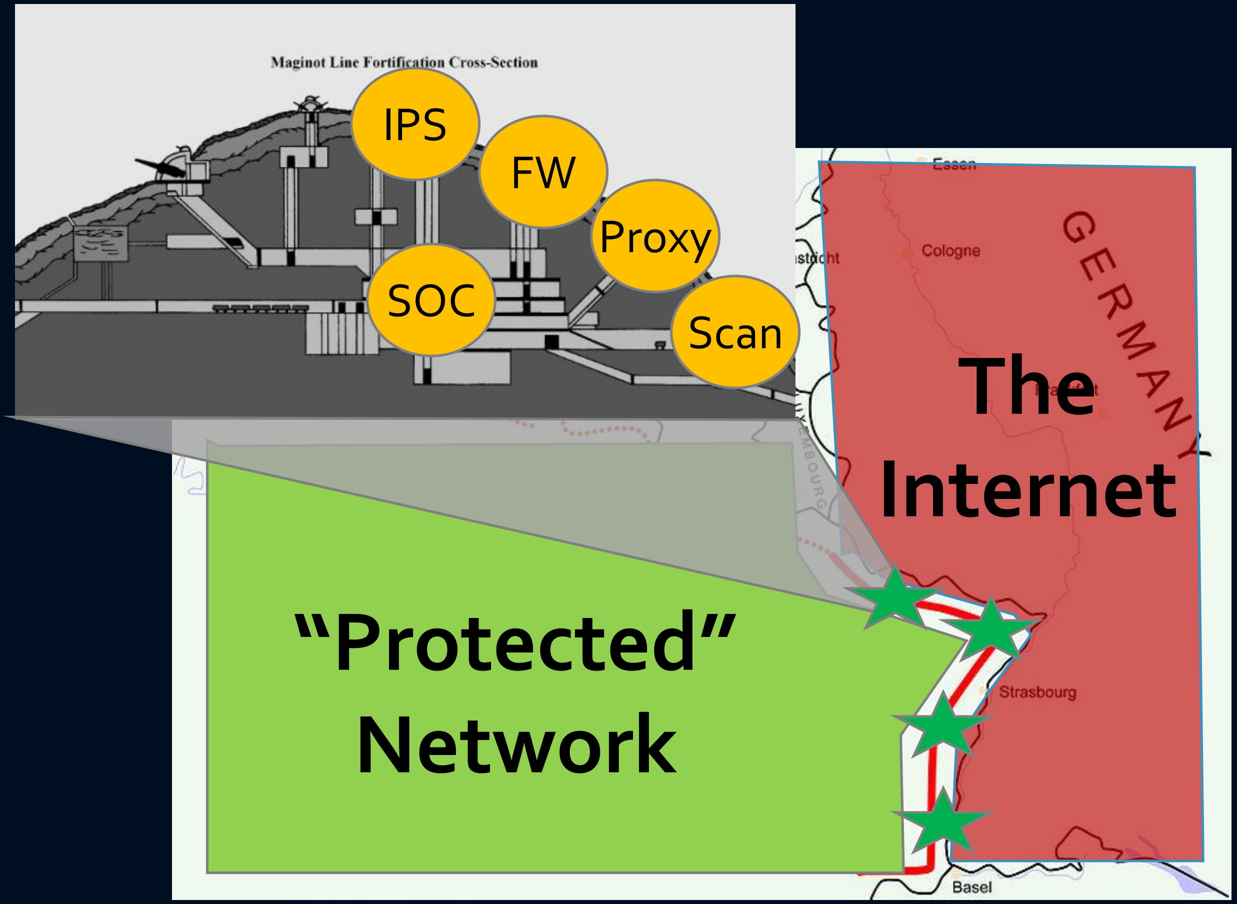


https://www.pinterest.com/mojo1944/maginot-line/

https://commons.wikimedia.org/wiki/File:Maginot_Line_ln-en.jpg

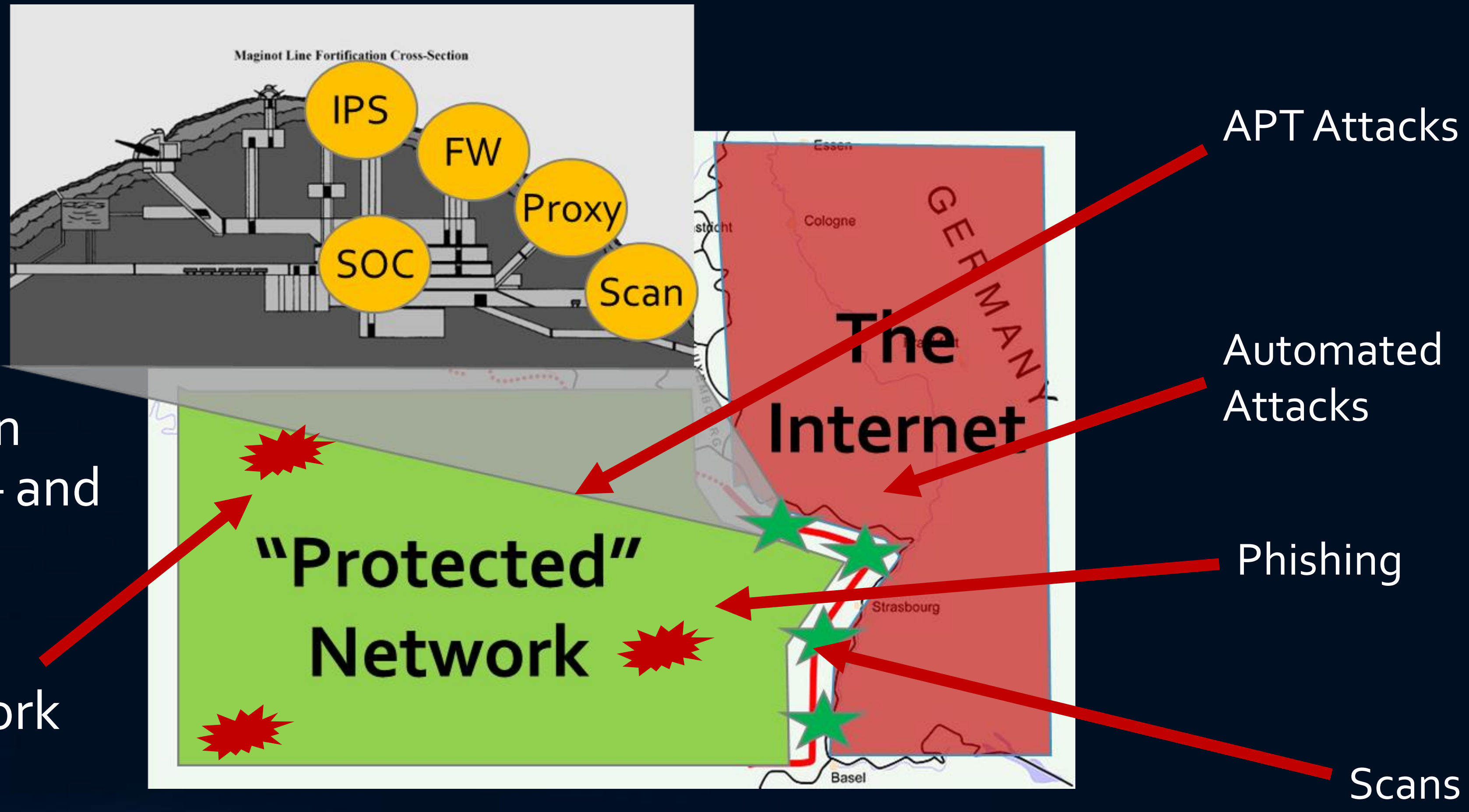
Does This Look Familiar?

- Expansive and Expensive Defenses
- Built to Keep "Something" Out
- High Reliance on Technology
- Depends on "Looking in the Right Direction"
- Successful? Worth the Expense?



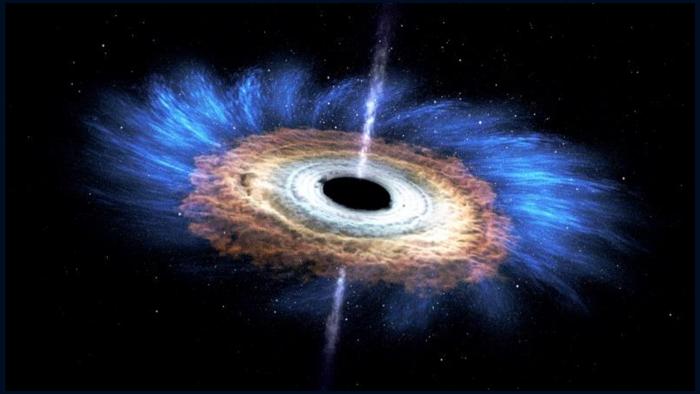
This Strategy is Being Bypassed…

- Most networks look like this
- Advanced attackers find ways in
- We're fighting on multiple fronts – and not just cyber
- There is also an insurgency at work



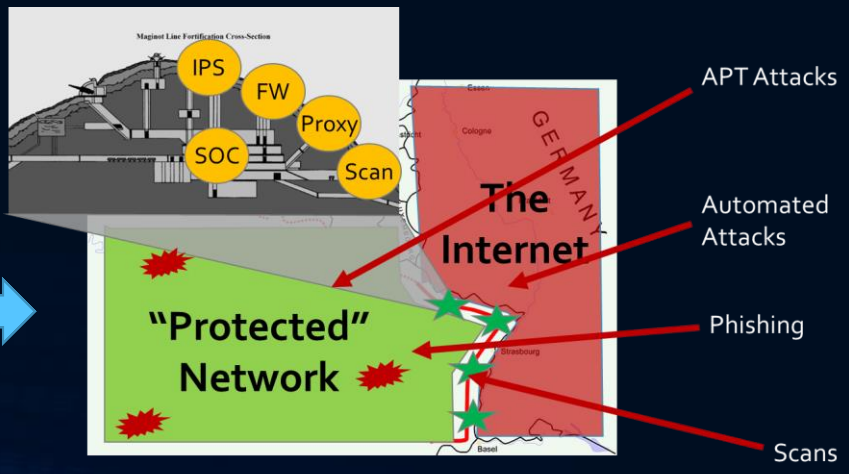
The Traditional View of Cybersecurity

- Analyst -> “It’s is a CHORE”
- CISO -> “I have to do it”
- CFO -> “It’s a Cost Center”
- CEO/Board -> “I don’t want fiduciary impacts”
- Regulator -> “You better do it or ELSE”
- Policy Maker -> “I can make this better”



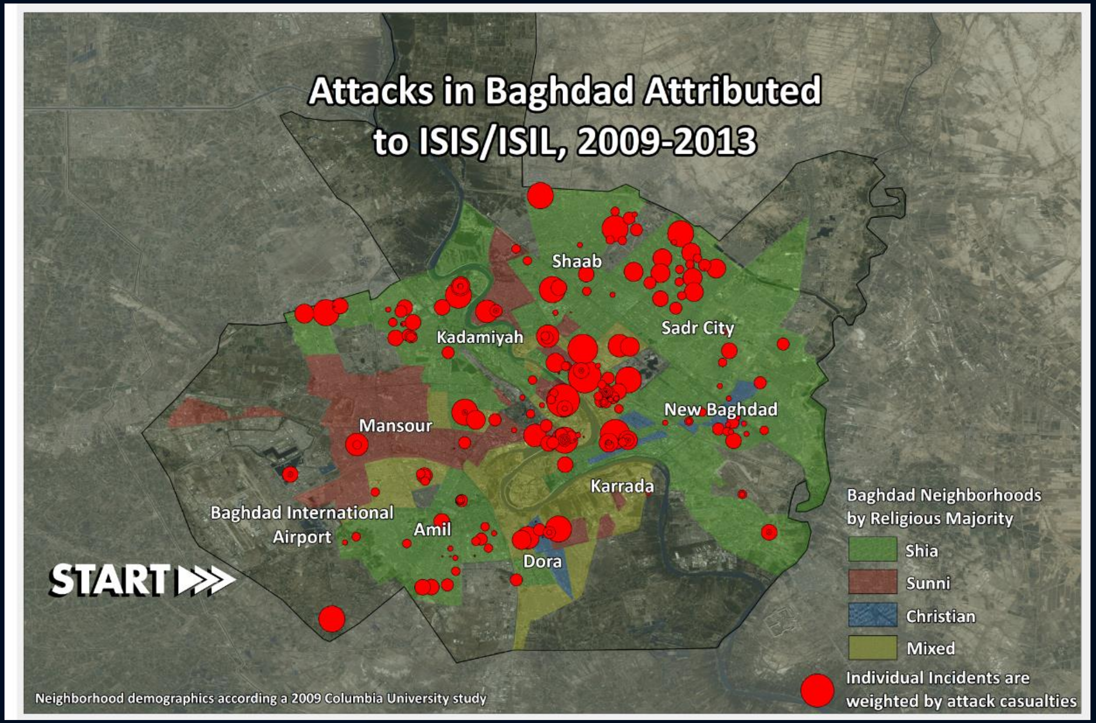
Remember that black hole?!

How can we fix this?



Another Military Analogy

- We are not fighting a conventional war
- We are fighting an insurgency
- Unclear who the attackers are
- Unclear where attacks originate
- Unclear when the attacks will happen
- Unclear where the **Battlefield** is
- Attackers use different tactics
  We should probably do that too!


Attacks in Baghdad Attributed to ISIS/ISIL, 2009-2013
Shaab
Kadamiyah
Sadr City
New Baghdad
Mansour
Karrada
Baghdad International Airport
Amil
Dora
START ⋙
Baghdad Neighborhoods by Religious Majority
🟩 Shia
🟥 Sunni
▨ Christian
🟨 Mixed
● Individual Incidents are weighted by attack casualties
Neighborhood demographics according a 2009 Columbia University study

WarOnTheRocks.com

Counter-Insurgency Tactics

- SURGE!
- Intelligence and Analysis
- Early Warnings and Indicators
- Clear Identification
- Continuous Vigilance – Always on Alert
- Allied / Multi-National Operations
- Real-Time Communications
- New Technology / Tools
- Are there equivalents in network defense terms?

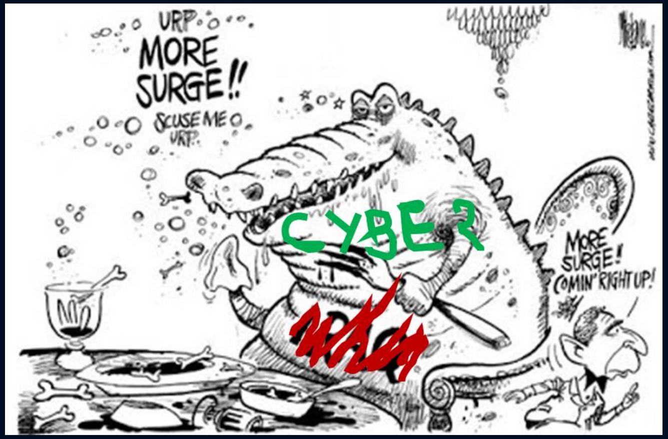
The Simpsons

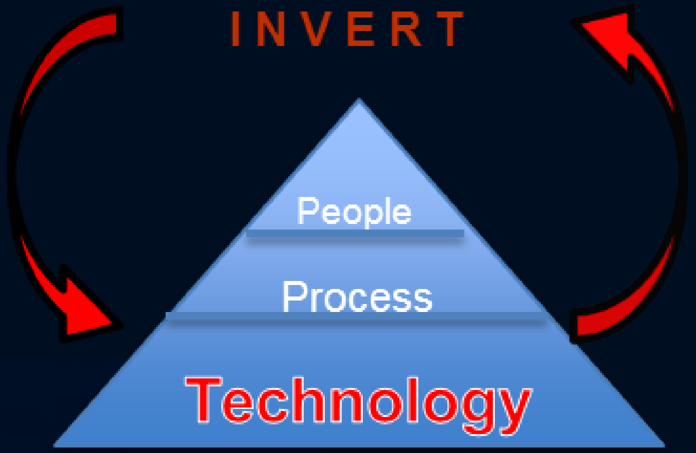
OK – It’s Bad – What Do We Do?

GENERATING “MUSK MOMENTS”

Counter-Insurgency **CYBER** Tactics

- Threat Intelligence & Fusion
- Early Warnings and Indicators
- Clean Environment
- Clear Attribution
- Continuous Monitoring
- Multi-Agency Info Sharing
- Real-Time Response
- New Technology to Assist People
- New Processes to Assist People





INVERT

People

Process

Technology

The Cyber “Environment”

- The Cyber Environment is not well defined
- It’s a unique ecosystem - much resembling a swamp:
  - Unclear where it starts and ends – you just know you’re in it
  - Unclear what’s IN there, watching you, or coming after you

JANUARY
2010

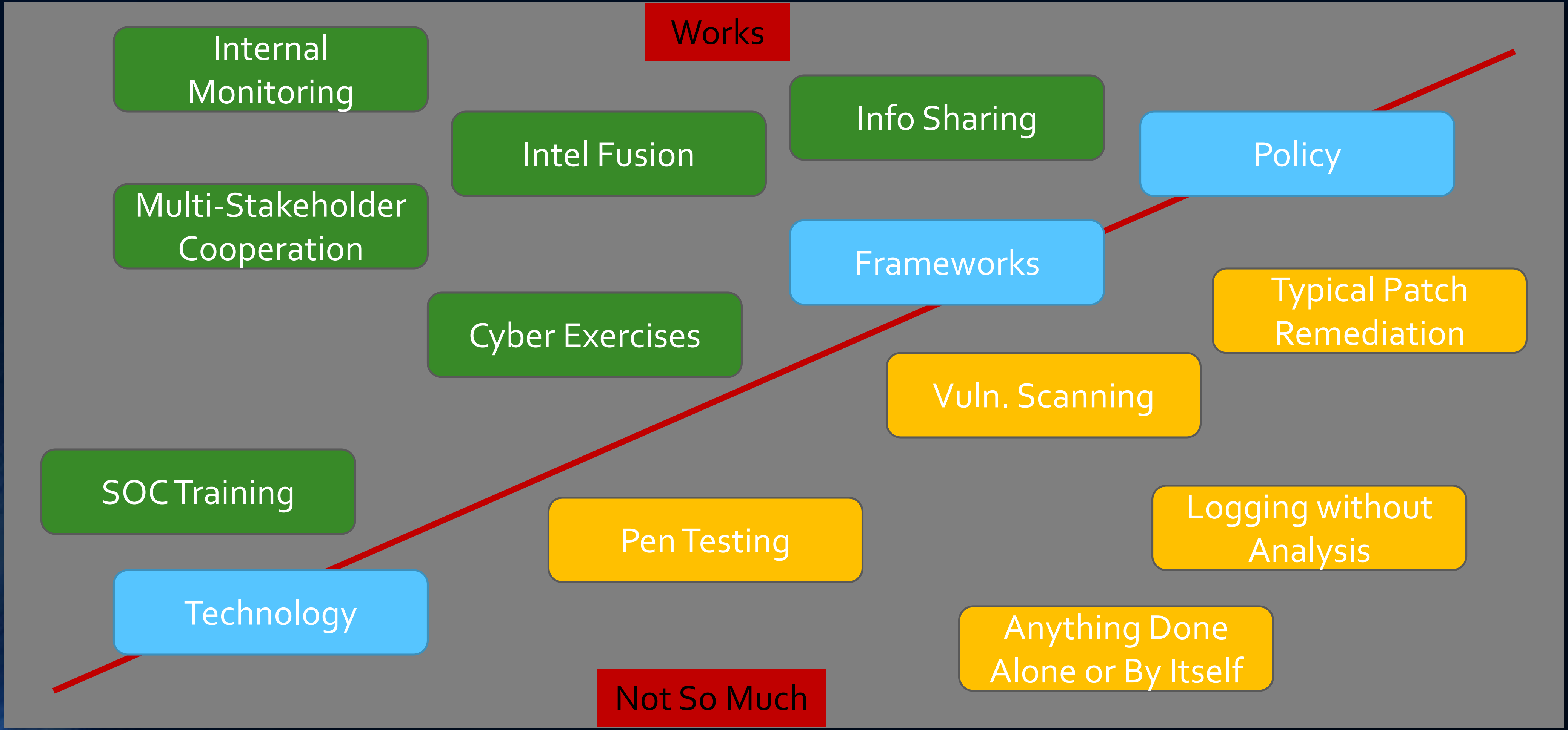
Contested Commons:
The Future of American Power
in a Multipolar World

Edited by Abraham M. Denmark and Dr. James Mulvenon
Contributing Authors: Abraham M. Denmark, Dr. James Mulvenon, Frank Hoffman, Lt Col Kelly Martin (USAF), Oliver Fritz, Eric Sterner, Dr. Greg Rattray, Chris Evans, Jason Healey, Robert D. Kaplan

Center for a New American Security

https://www.cnas.org/publications/reports/contested-commons-the-future-of-american-power-in-a-multipolar-world

What Works & What Doesn't



Works

Internal Monitoring

Intel Fusion

Info Sharing

Policy

Multi-Stakeholder Cooperation

Frameworks

Cyber Exercises

Typical Patch Remediation

Vuln. Scanning

SOC Training

Pen Testing

Logging without Analysis

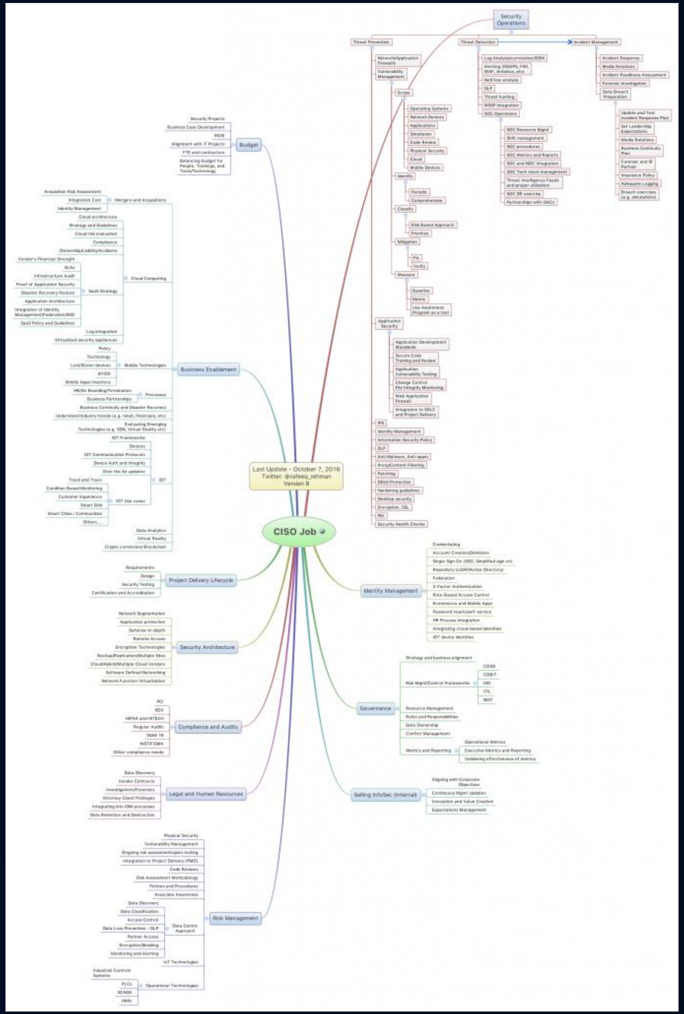
Technology

Anything Done Alone or By Itself

Not So Much

There’s Much More Too – If You Want…

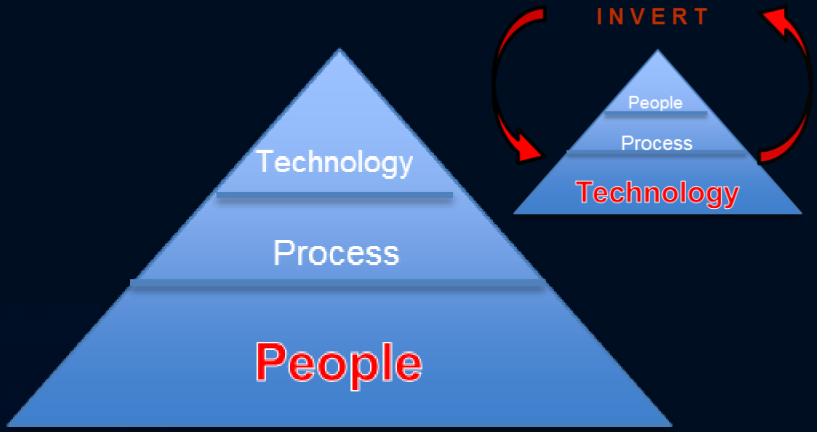
- Start now – small implementations
- Worry about being comprehensive later



http://rafeeqrehman.com/2016/10/07/announcing-ciso-mindmap-2016/

The Commonality - The “Triad”

- People, Process, Technology
- How each element breaks down individually, but combinations of the three can be effective
- (Back to maginot line as example)



What Happens When A Plan Comes Together

- Conficker Working Group
- APT-1 Release by Mandiant
- Advanced Attacker Detection
- DCiSE / DC3
- Clean Environment
- Automated Response
- Easy Compliance

http://www.memegen.com/meme/td6610

Additional Challenges

- Cross border, jurisdictional concerns, legal concerns, low cost of the att

- Go
ana C,
etc

Work In Progress

Some Models

- General: CDC, Fishing, climate sustainability,
- Clo
- Ho
- Str
- So
- CA

Work In Progress

Good Cybersecurity IS POSSIBLE

- What works: intl cooperation, threat intel, effective analysis, cor c
- Ha pre

Work In Progress

Conclusions

- Good cybersecurity is possible (with non-traditional thinking)
- It takes work, coordination, skills – all doable!
- People – detect, analyze, respond to things in the swamp
- Process – policies and processes support cleaning the swamp
- Technology – assists people, help automate, force enabler

Gracias

Thank You

CHRIS EVANS
CHRIS@STASHDADDY.COM
WWW.STASH.GLOBAL