thegrugq@gmail.com
g@comae.io

OUTLINE

- Cyber is a new dimension
- Cyber is people and information
- Cyber is Calvinball

Attempting to synthesize the various aspects of cyber conflict: technology, information, people, data

CONFLICT

- Advantage: develop and exploit advantage
  - Disadvantage: arrange for the opposition to have
- Dislocation: render opposition’s strength irrelevant
- Confrontation: engage their strength
- Balance: dynamic situations lead to adaptation
  - The opposition will not play along with your plan

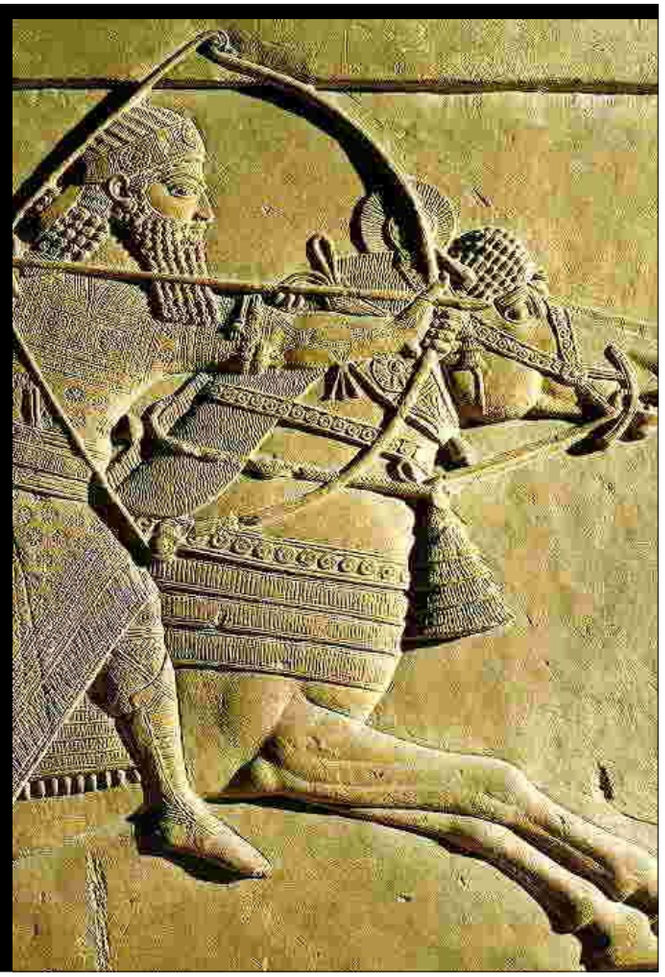
A BRIEF HISTORY OF WAR

THE BEGINNING

TWO DOMAINS: LAND + SEA

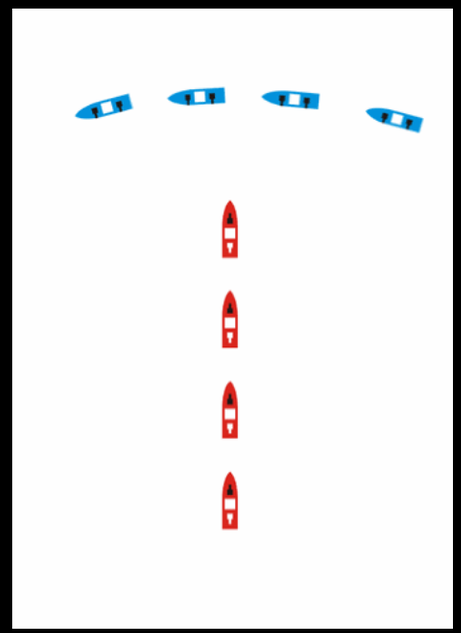
LAND

- Advantage/Disadvantage
  - Location: in front, behind, sides, rear
- Dislocation
  - Overwhelm, better tech (rare), better position
- Balance
  - Maneuver war



SEA

- Advantage/Disadvantage
  - Position, tactics (crossing the T)
- Dislocation
  - Overwhelm, tech,

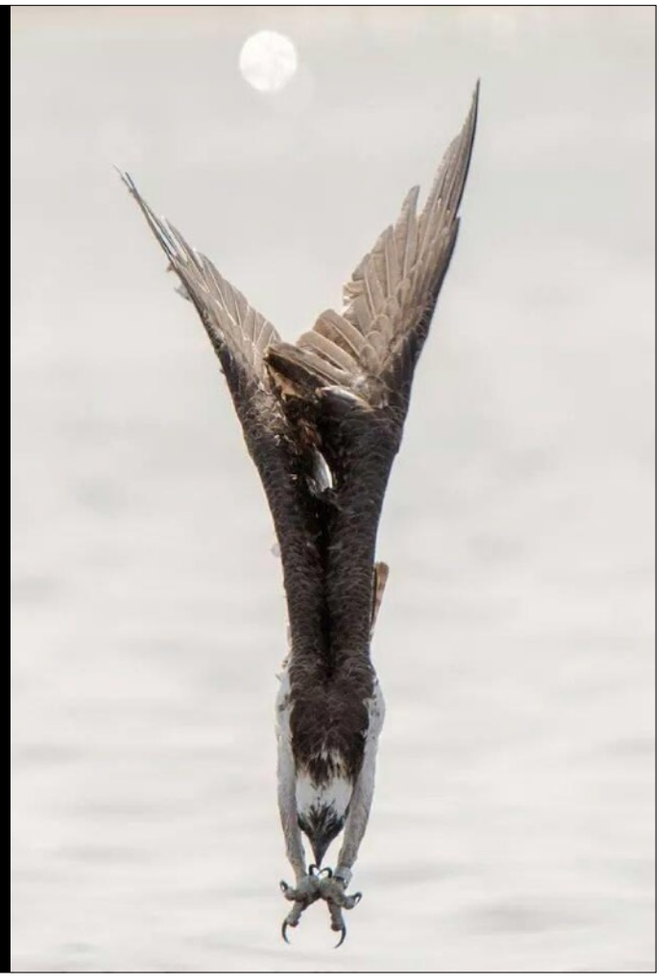


NEW DOMAINS

- Air - the third domain
  - 1910s
- Space - the fourth domain
  - 1960s
- Cyber - the fifth domain
  - 1980s

AIR WAR

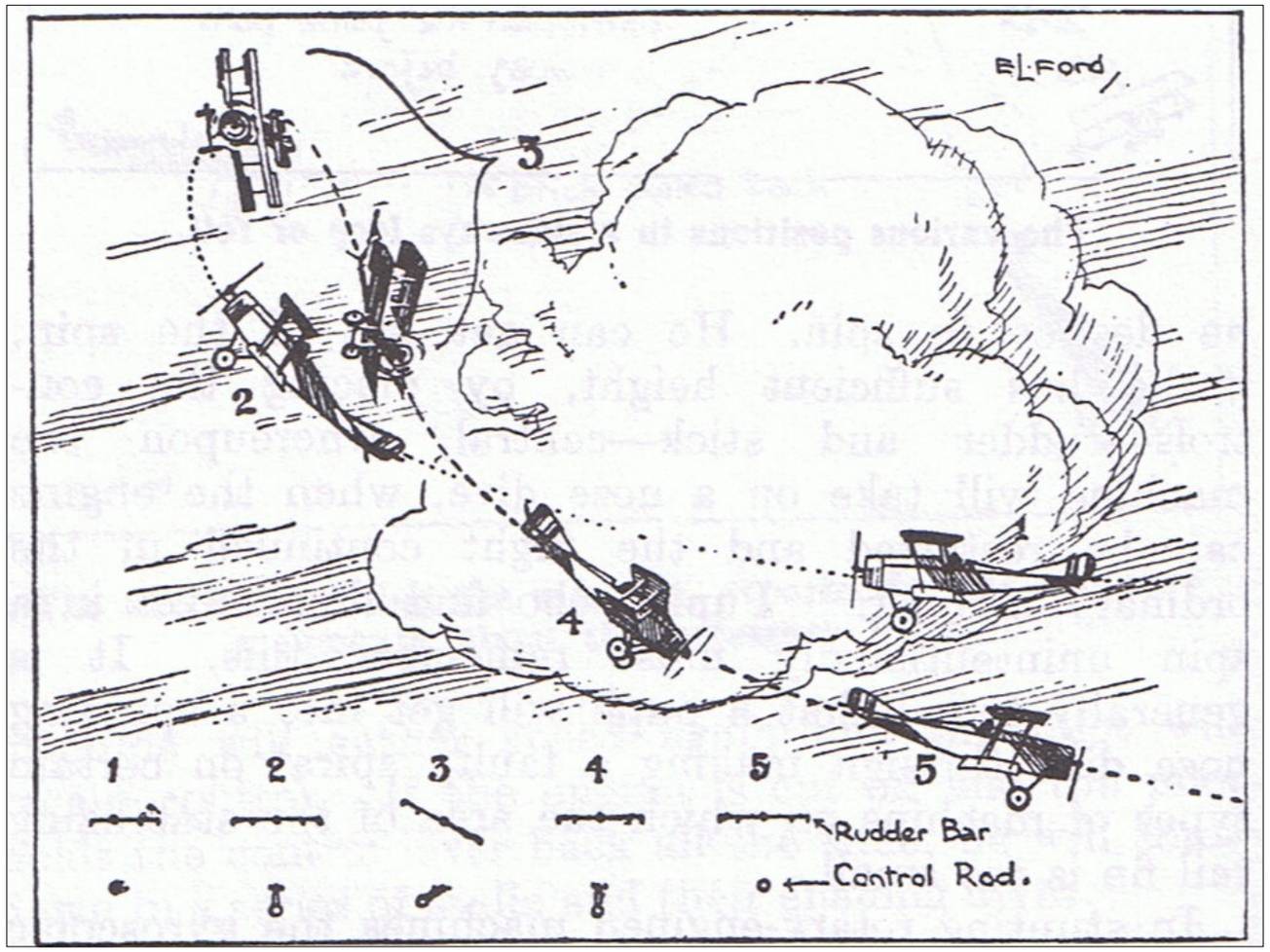
THE FIRST NEW DOMAIN



AIR - 3D

No aerofoils, the Fokker mono-wing used wing warping. The Immelmann turn is a hack to compensate for limitations of the technology, much as a hacker would discover and exploit. The plane was so bad that to land you had to “blip” (turn off fuel flow) to the engine… do it repeatedly to slow down, a mistake and the engine explodes.

https://youtu.be/gfh7X4Jsgak?t=91


E.L.Ford
1
2
3
4
5
5
Rudder Bar
Control Rod.

- Theory:
  - Create planes with high maneuverability to allow skilled pilots to best less skilled pilots
- Praxis:
  - Show up with more planes, above and behind the target, and ambush them

- Theory got wrong — Advantage was not a matter of individual skill. That is a fair fight. Fighting fair is a gamble
- Praxis revealed — Advantage came from the usual factors, location and overwhelming force.

- Advantage/Disadvantage
  - Location: above, below
    - Reconnaissance flights and fashion
- Dislocation: location based, above and behind
- Confrontation: dogfights

CHAPTER I

The New Form of War

THE TECHNICAL MEANS OF WARFARE

AERONAUTICS OPENED up to men a new field of action, the field of the air. In so doing it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable. In actual fact, aeronautics was widely employed in warfare long before any civilian use was made of it.[1] Still in its infancy at the outbreak of the World War, this new science received then a powerful impetus to military development.

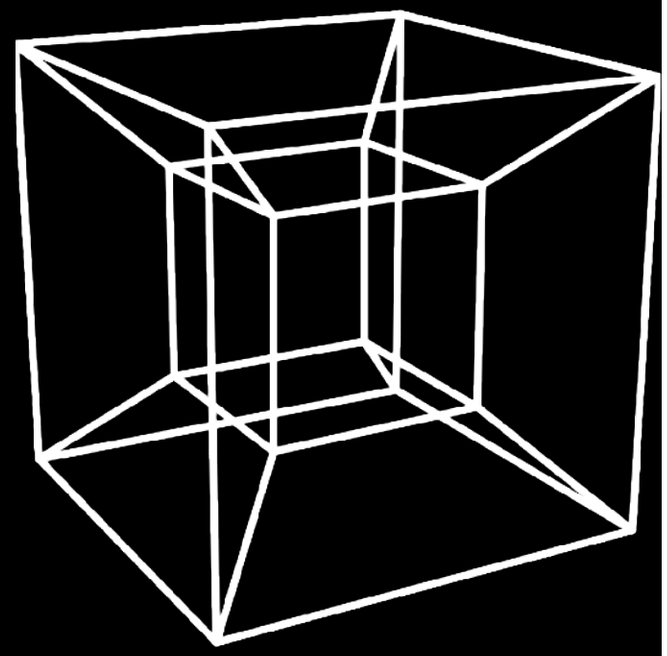
The practical use of the air arm was at first only vaguely understood. This new arm had sprung suddenly into the field of war; and its characteristics, radically different from those of any other arm employed up to that time, were still undefined. Very few possibilities of this new instrument of war were recognized when it first appeared. Many people took the extreme position that it was impossible to fight in the air; others admitted only that it might prove a useful auxiliary to already existing means of war.

At first the speed and freedom of action of the airplane—the air arm chiefly used in the beginning—caused it to be considered primarily an instrument of exploration and reconnaissance. Then gradually the idea of using it as a range-finder for the artillery grew up. Next, its obvious advantages over surface means led to its being used to attack the enemy on and behind his own lines, but no great importance was attached to this function because it was thought that the airplane was incapable of transporting any heavy load of offensive materiel. Then, as the need of counteracting enemy aerial operations was felt, antiaircraft guns and the so-called pursuit planes came into being.

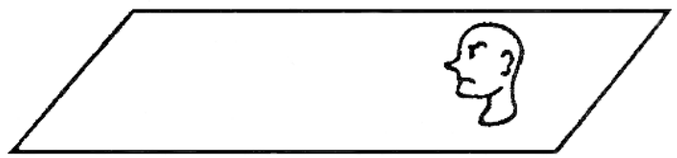
The Command of the Air - Giulio Douhet (pub 1921, revised 2nd ed published 1927)
“air power”… strategy for the air… this new domain.

CYBER

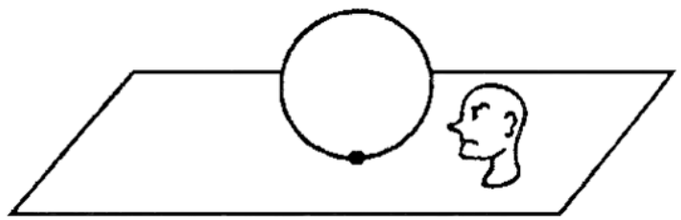
THE FIFTH DOMAIN



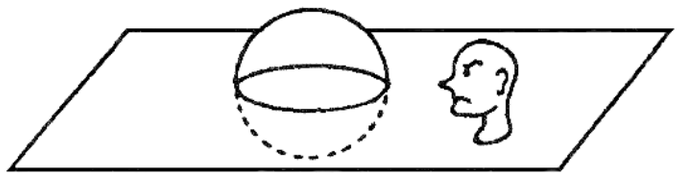
CYBER IS A NEW
DIMENSION



View from flat land. A 1D plane



The intersection appears as a point



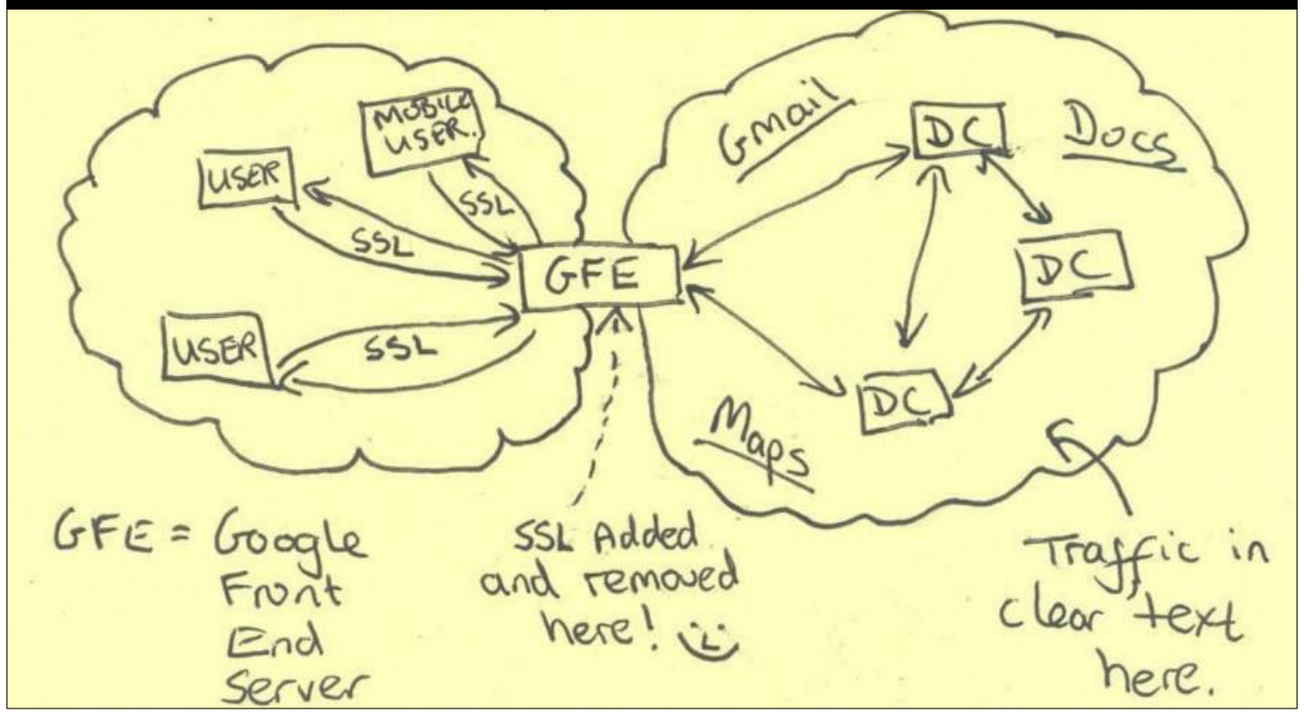
The intersection appears as a line from 1D.
From 2D it is a circle.
From 3D it is a sphere…
Cyber requires viewing that extra dimension

- Dimensions are relevant where they intersect with the world
- Cyber has four intersections
  - Active
  - Passive
  - Physical
  - Cognitive

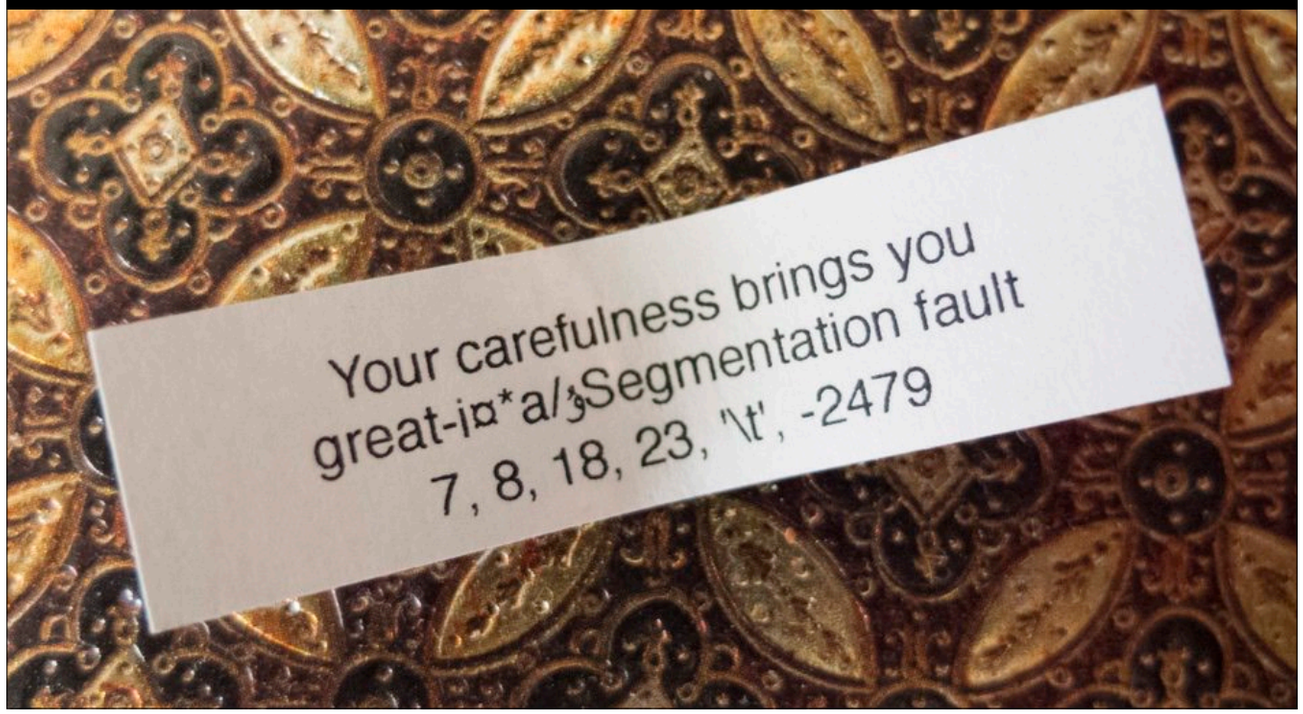
ACTIVE

Actively changing data, accessing a system, interacting with things…
8200 vs. PLO finances.

PASSIVE

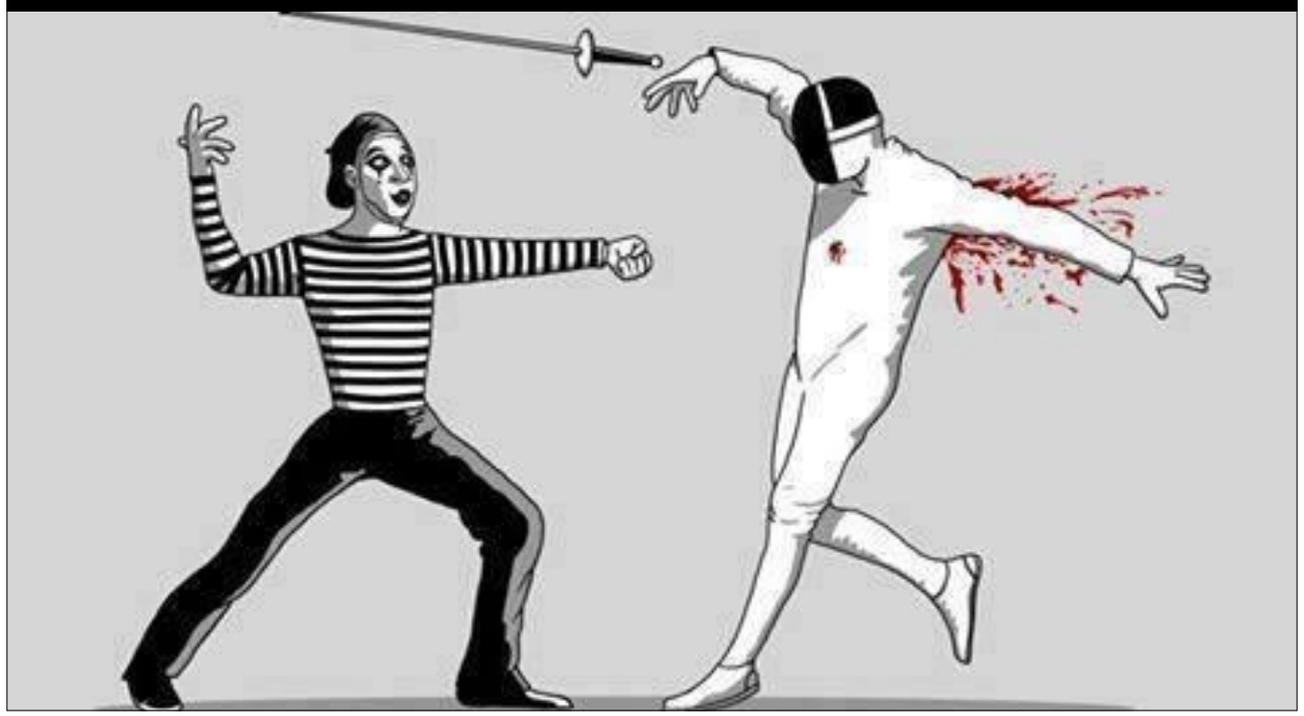

MOBILE USER
USER
SSL
SSL
GFE
USER
SSL
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.

PHYSICAL

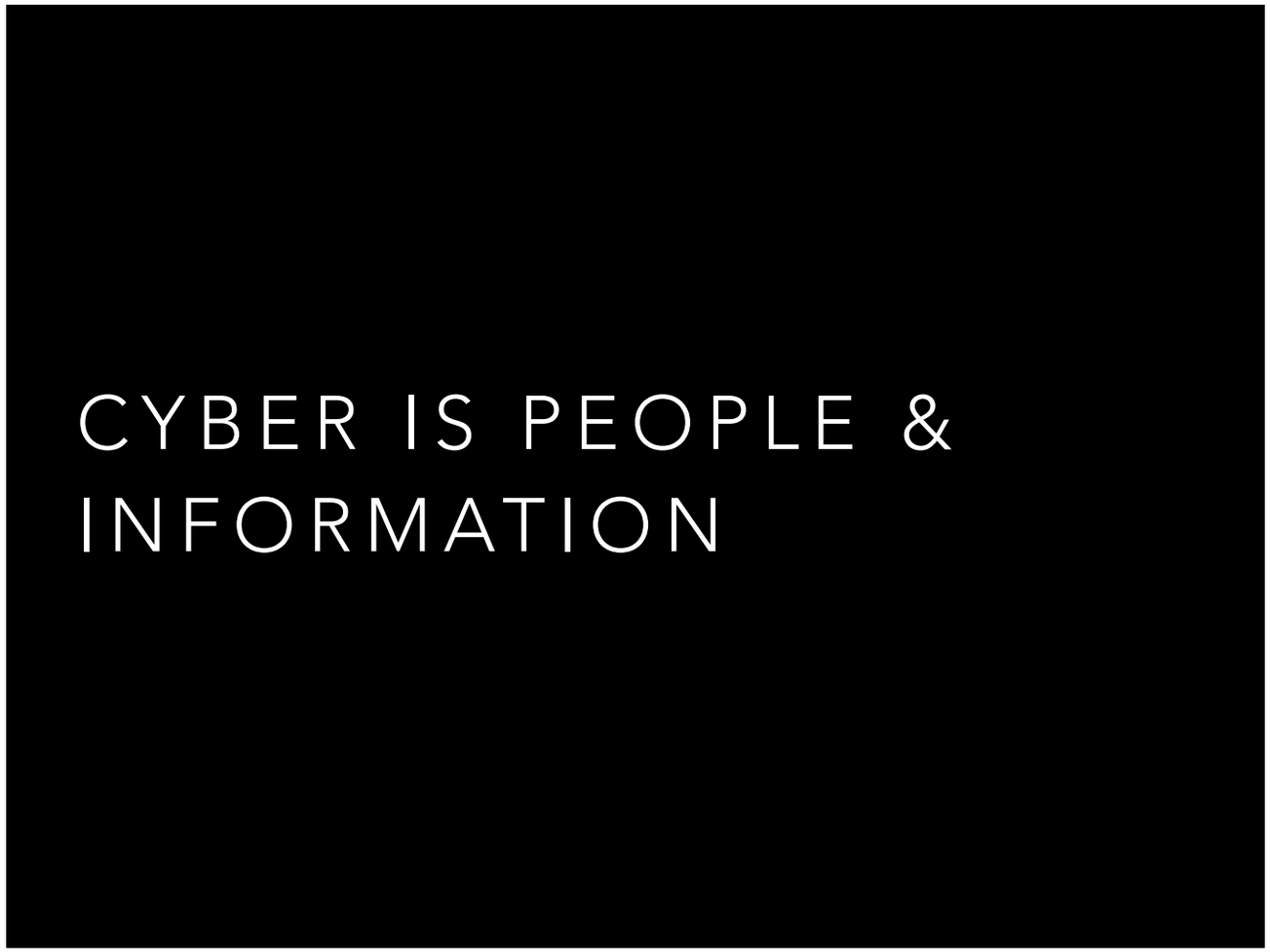


Stuxnet is the classic example, but NotPetya (shut down factories, including Durex), and also Lazarus vs. SWIFT… physically getting money out.

COGNITIVE



This is getting big play now cause PSYOPS, Information Warfare, Influence Ops, Perception Management, etc. are in the news… but cyber is just an information environment. It enables these ancient techniques from Berneys (and Goebbels, and Sefton Delmer, etc) .. propaganda.



Game theory k-level..

If you understand that cyber isn’t computers, but really people and info, then you can k-level your opponent… but you need to exploit that, which means you need players, teams..

BUREAUCRACY IS AN ENABLER
OF CYBER CAPABILITY

"Bureacracy is hard."

–MARA TAM

TEAMS

FACTORS OF TEAM CAPABILITY

- Adaptability
- Agility
- Speed
- Creativity
- Cohesion

DAVE AITEL'S META

ORG STRATEGIES

Meta-Style	Advantages	Disadvantages
Operators Mega-Team	Scalability allows for wide reach with a hands on touch, which in turn allows for being able to have high levels of covert and persistent presence!	Leaks or internal penetration can be fatal to a wide range of efforts. Training a huge team on any more than a handful of toolsets becomes difficult. Operators are not super-technical, which means mistakes get made.
Fully Automated Suite – No operators just linguists and programmers	Quick to run operations. Entirely scalable. Reliable to a fault.	Only certain exploits will fit the platforms. Platforms require massive investment. No feedback loop. QA is a nightmare.
Remote Worms	No need for operators! Fire and forget – faster than your opponent can react.	Impossible to predict impact of events. Toolkit is burnt after use, typically.
Many small teams of contractors	Highly innovative. Needs very little initial investment to ramp up.	Managing your supply chain and accompanying OPSEC is hard. Scaling this to any level is expensive.

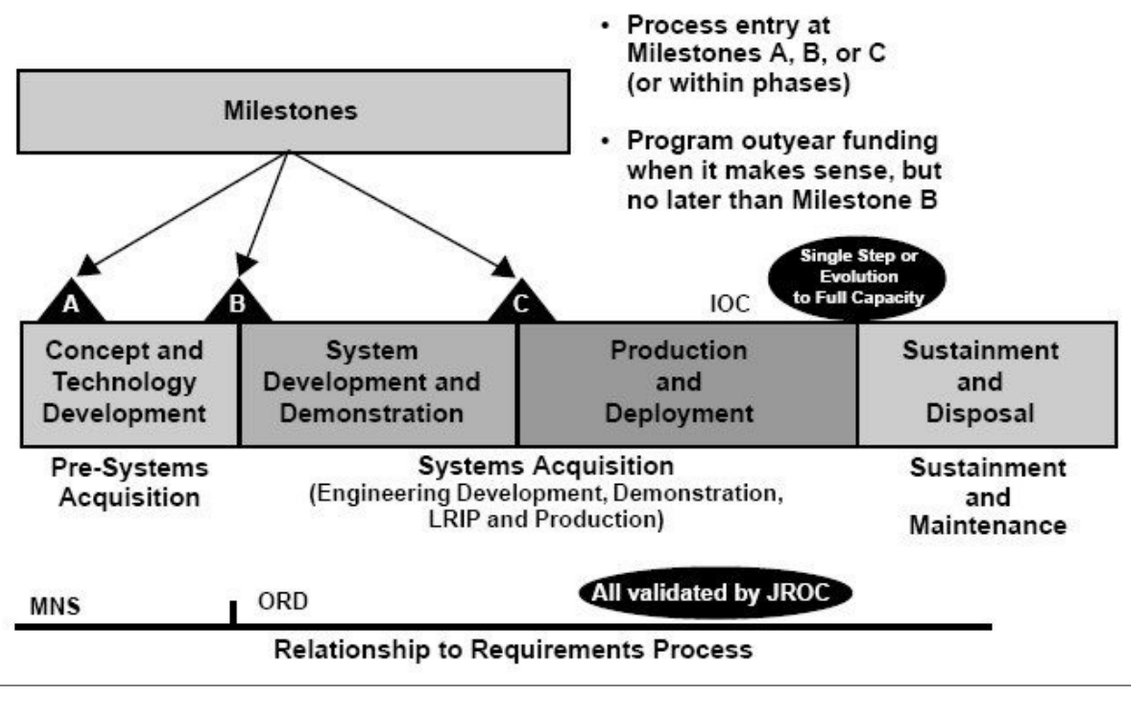
- monolithic mega team:
- Managed worm, basically:
- Ummanaged worm
- Small teams: gives a spectrum of capacity

MEGATEAM

Will always suffer because of procurement life cycle.

PROCUREMENT LIFECYCLE

WHY MEGA TEAMS SUFFER



As requirements change, you keep modifying your toolchain, because replacing it is super expensive and slow… but sometimes you have no choice because it gets burned. So, not ideal

MANAGED WORMS

- Expensive
- Fragile
- Specialized
- Dependent on programmers
  - Weaponised stackoverflow copy pasta

MANY SMALL TEAMS

Spectrum of capacity. Crucial if you want to have both HVT and “zero equities CNO”

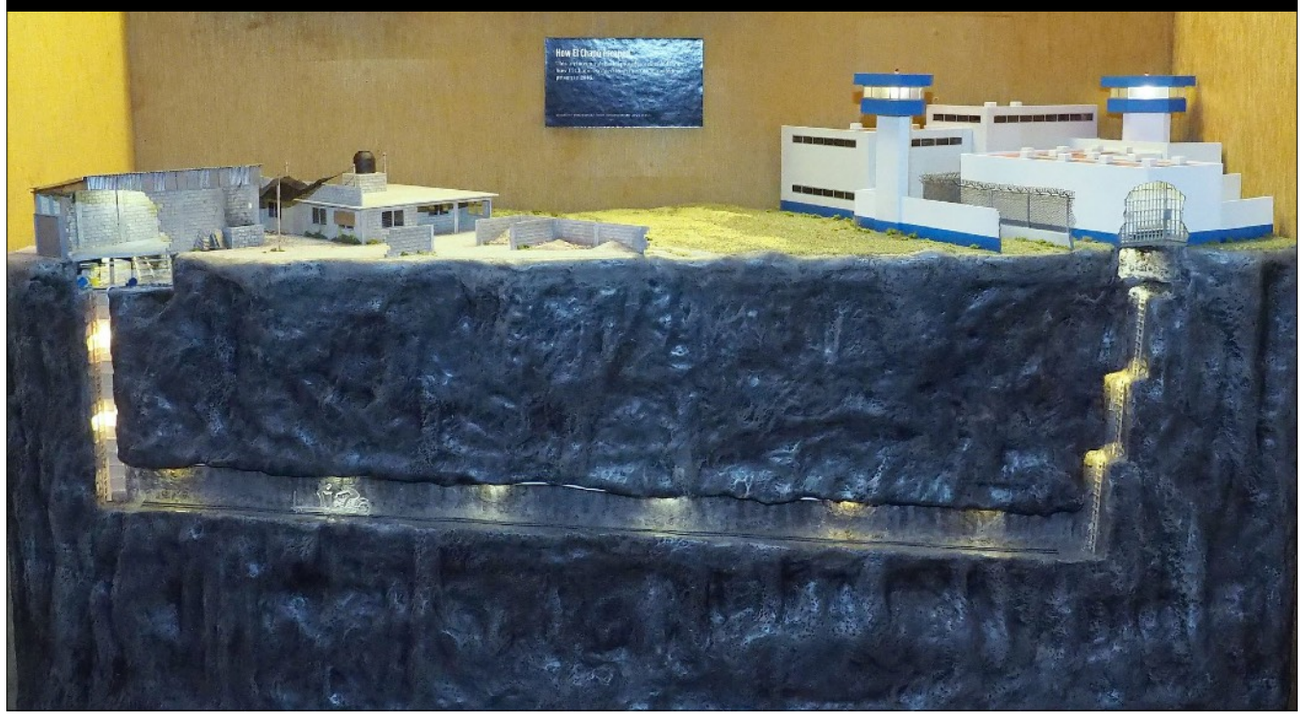
Zero equities CNO…

- Adaptability
- Agility
- Speed
- Creativity
- Cohesion

ADAPTABILITY

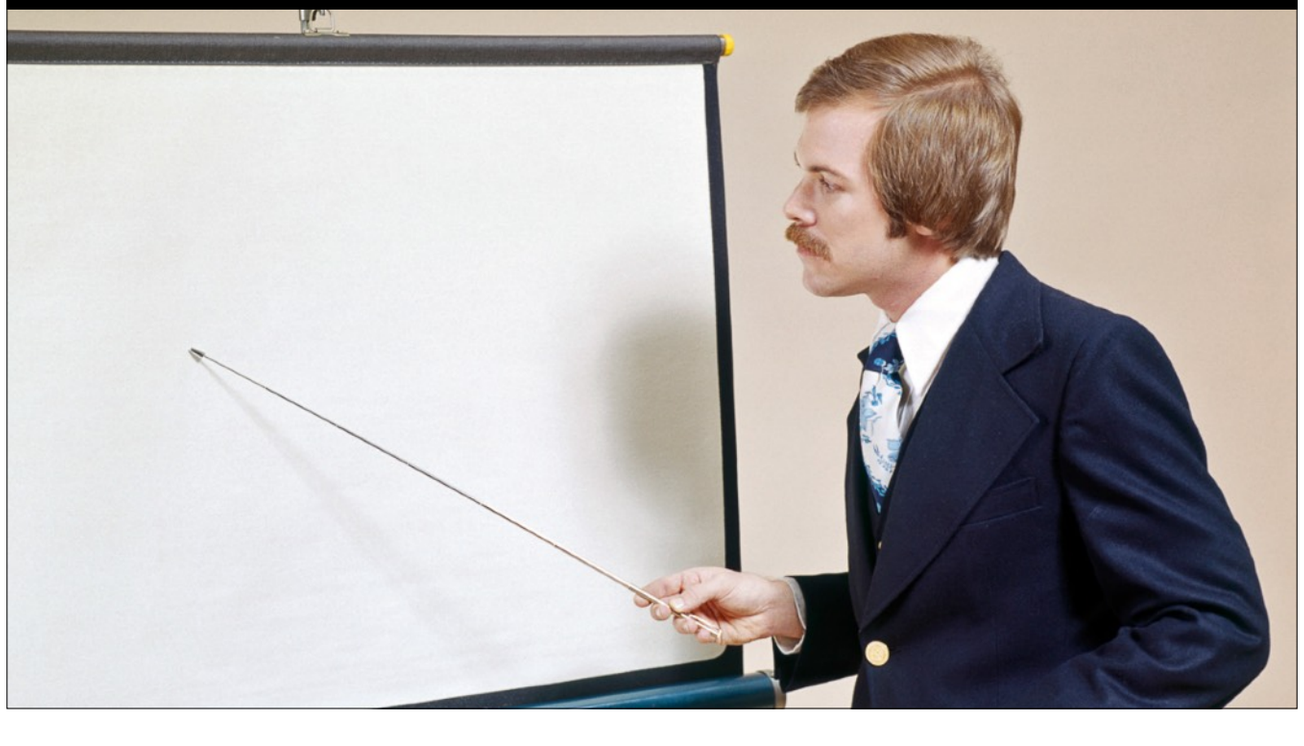
Ability to take new technology and exploit it for cyber conflict

AGILITY



Ability to adjust rapidly to changing circumstances and react appropriately… so, taking a blown op and turning it into an information op in less than 24hrs is amazing agility

SPEED



Conception to execution. Or, “how many meetings until someone can press enter?”

CREATIVITY

Ability to innovate, create new tools, techniques and methods.

COHESION

How closely does the cyber team follow the will of the executive. Is it loose, they just kinda do what they think they should.. it is tight, they do exactly what they’re told? Do the teams compete with each other or share info?


BEARS

- It’s complicated
- Private operators and orgs
- State intelligence
- Military intelligence

- Lots of teams competing
  - But also formal and informal information sharing
- Freedom to fail
  - Risk tolerant
- Multiple funding sources
- Great creativity, agility, speed, low cohesion, excellent adaptability

"A good plan, violently executed now, is better than the perfect plan next week"

–GENERAL GEORGE S. PATTON


FVEY

picture credit: @dave_daves
https://twitter.com/dave_daves/status/974564619774758912

- Authority to operate is Title 50 (espionage)
  - Authority for offensive PSYOPS is Title 10 (war)
  - Authority for defensive IO was State Dept (disbanded in the 1990s)
- Result, all cyber became espionage
  - IO becomes a k-level

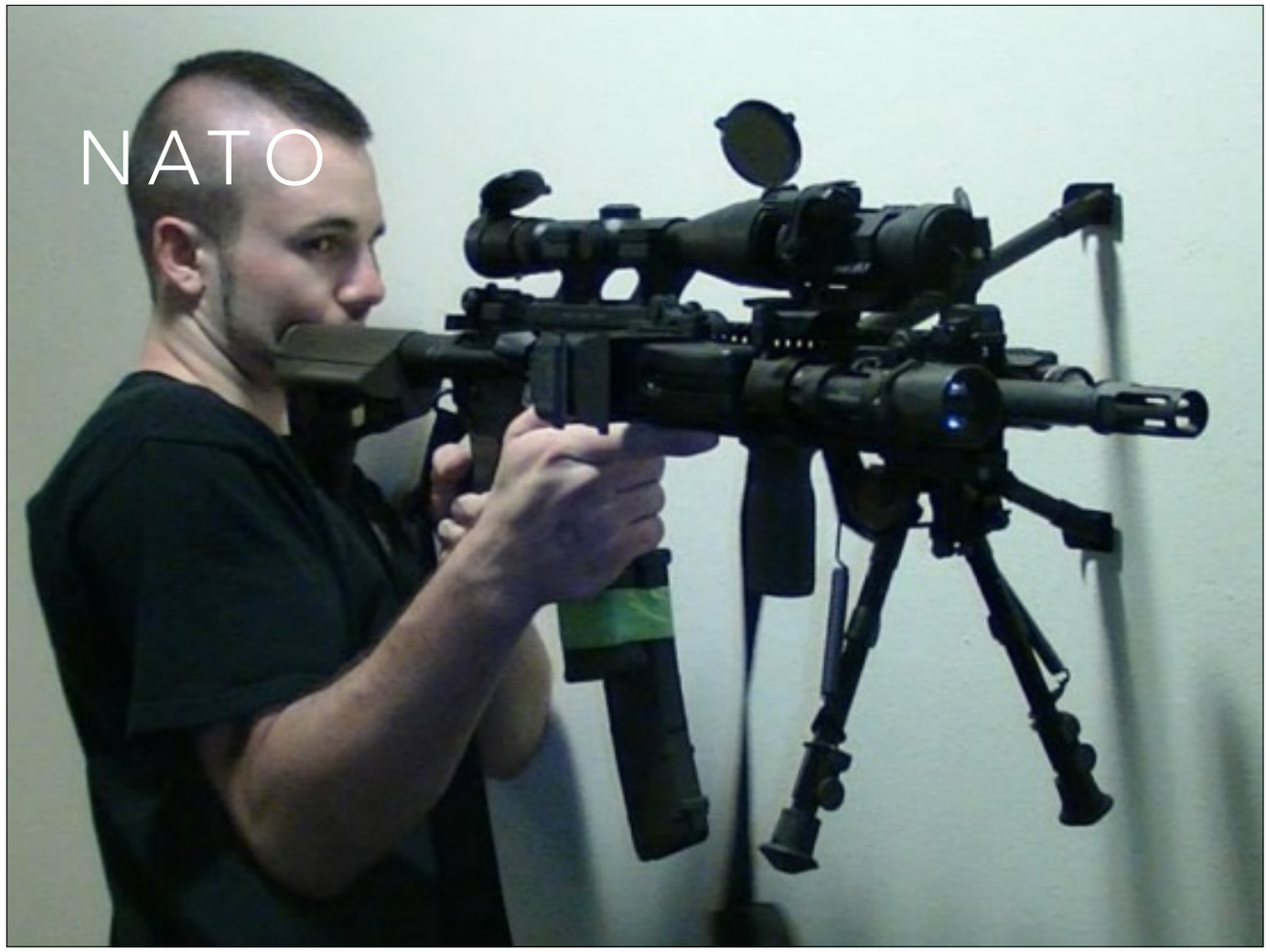
Bureaucracy is hard…

DRPK

- Money
- Low agility, adaptability, medium speed, high cohesion


CHINA

- Complicated and changing
- Loose cohesion
  - For security and deniability
- Low adaptability, agility, medium speed, mixed creativity
  - They shine on targeting, but have a spectrum of capacity


NATO

- Necessary to create NATO Cyber
  - No one is gonna share secrets
  - Create secrets together
- Basically a big “hack me” sign

Not a solution to a tough neighborhood… kids are gonna steal the tires

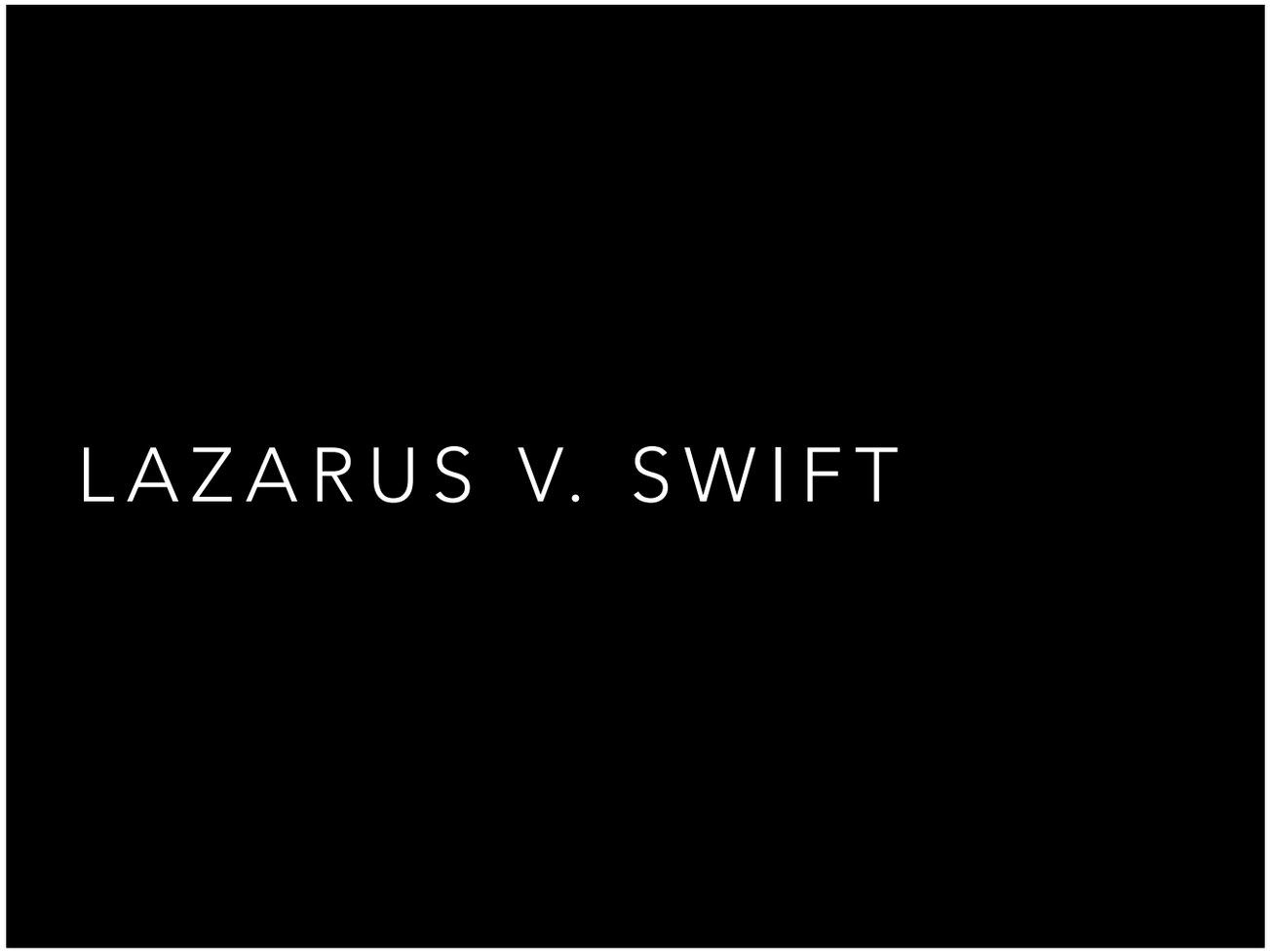
Every attack has two effects: 1) an impact, 2) a reaction… the reaction will negate the efficacy of that attack, creating diminishing returns over time. Thus attacks need to be changed, combined, innovated… etc.

CAMPAIGNS

passive, active, passive… ultimately about learning about counterintelligence — which accounts are being monitored by the FBI to see which spies have been detected. Sophisticated targeting.

STUXNET

Physical, cognitive … active, passive… a lot going on. But it was cyber.

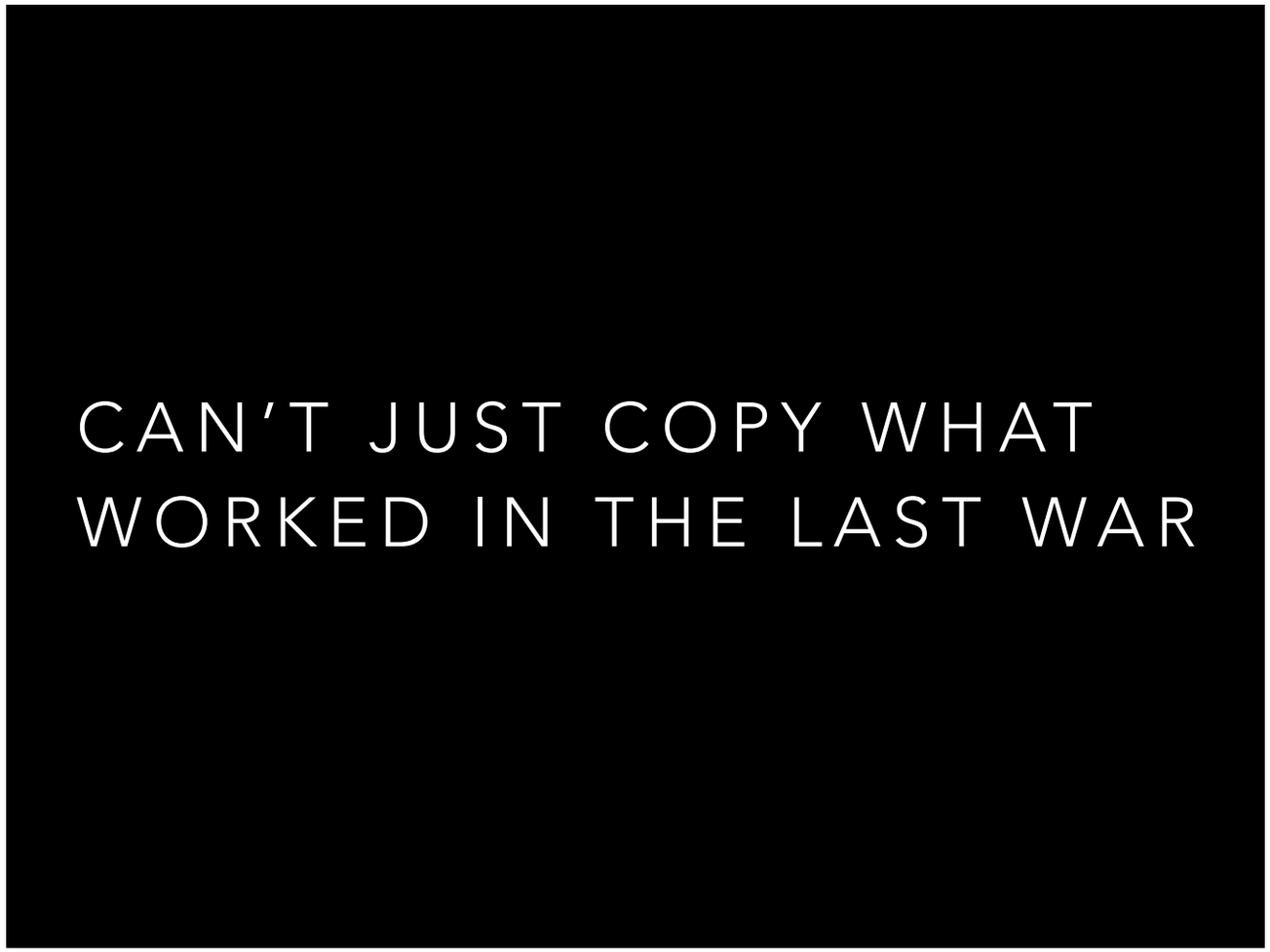


active, but ultimately physical … they had to get that money out of the bank DB into cash. Can’t be pure cyber because any change in a DB can be reversed, so it was laundered through casinos physically. Extremely complicated process to turn a SWIFT command into cash

Building a private “facebook” of data about the USG … active, clever targeting, to build a passive DB that will make it very hard to slip in undercover operatives. Also provides some capacity to do assessment and recruiting. But all in the services of intelligence and counterintelligence … how many insurance companies think “we are a nation state intelligence target?”

Purely cognitive… using information from an active and passive campaign, the data was turned into an information operation or Active Measure (or reflexive control, perception management, etc).. all just propaganda.


FINAL THOUGHTS
© CraigGoodwinPhoto



Every weapon or technique has two effects .. the first is a direct effect against the target, the second is the reaction of the target. Because of this things evolve, from the basic “patching” to more complex “harden systems against that attack technique”

Having a big “hack me” sign is not how to survive against swarms of small agile teams.

This will be interesting as other countries who are used to being the center of the world find themselves in a multipolar world and later on the periphery …

US IS GREAT AT DEVELOPING TECHNOLOGY AND TERRIBLE AT EXPLOITING IT

BLENDED OPS, NOT THE INSIDER THREAT YOU KNOW

Recruited or hired malicious insiders, not just ignorant or disgruntled or whatever… actually really malicious, and trained.

THANK YOU


QUESTIONS?