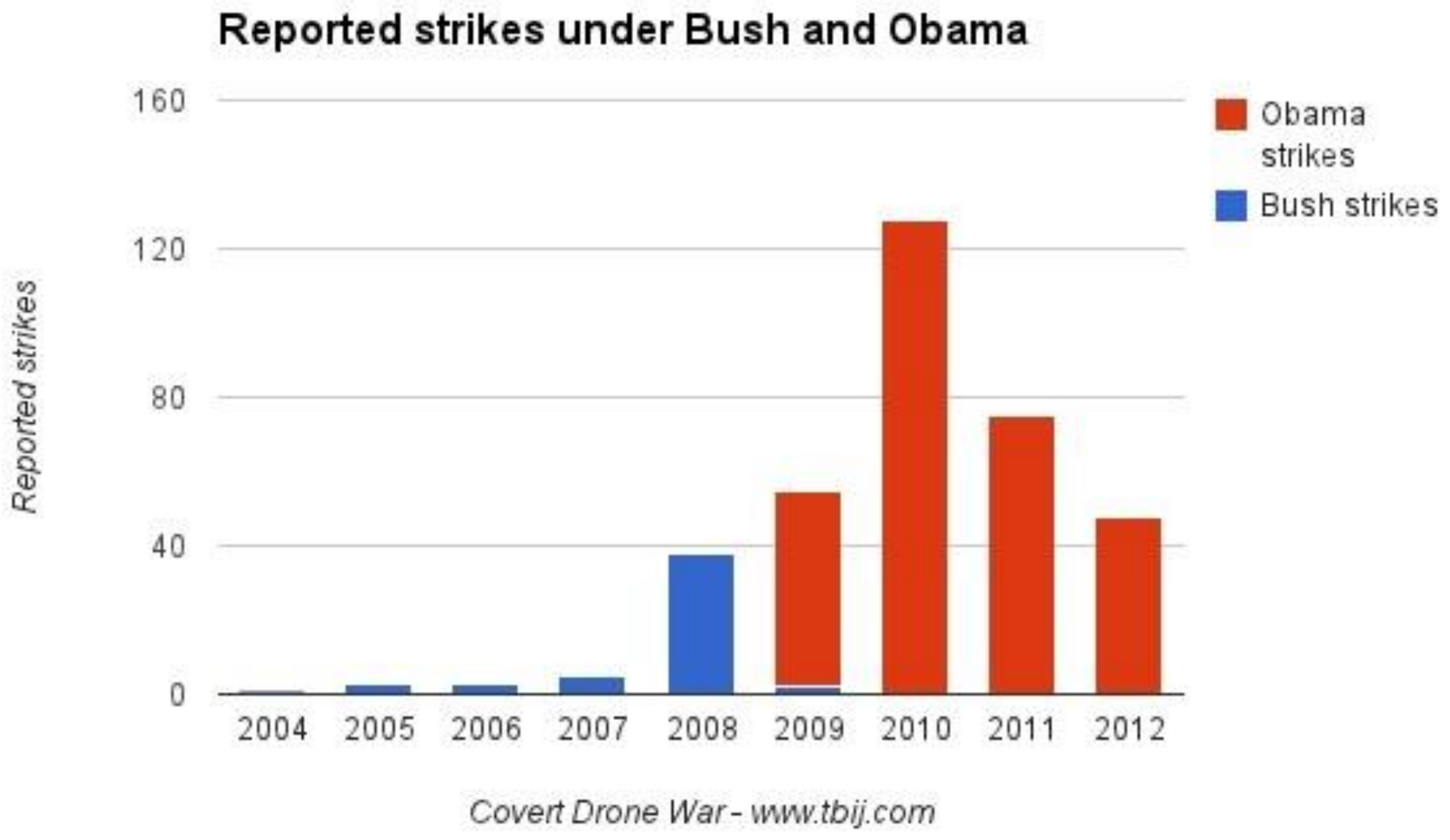
STEALING THE FIRE

CYBER WAR AND OTHER TOOLS THAT GOT AWAY FROM US…

WOT 5 OLLI

No Class March 10th

DRONE NUMBERS ARE “CLASSIFIED” BUT THE TREND IS CLEAR



Reported strikes under Bush and Obama

Covert Drone War - www.tbij.com

Three different Drone Programs:

USAF – Africa, Iraq Libya, Syria – acknowledged program

JSOC – Somalia, Yemen – not public

CIA Drone program – mostly AfPak border, Syria

Drones both the platform for Surveillance and end users of the data- combining Analysis and Operations Realms.

17 minutes in the life of a drone, 2010.

- Fort Meade, NSA "pings" a phone call in Afghanistan through electronic dragnet. Phone a disposable, but call to known safe house.
- Voice analysis match to HPT. Linguists come in to make human verification.
- CIA Counter terrorism notified. CIA Drone redirected to region.
- Nevada Air Pilot navigates, video, heat signatures transmitted.
- Legal Analysis of Target, Collateral Damage potential.
- Nevada "fires" weapon – electronic pulse through fiber optic cables to Europe, Satellite to Predator weapons.

- Films on Drones:

- The Good Kill; https://www.youtube.com/watch?v=lY2EBKuLzW8&list=RDzWmEZAl4sxc&index=5

- Eye in the Sky https://www.youtube.com/watch?v=CqWIbG7_xn0

Drone Evolution

1991 Laser Guided Weapons expensive, malfunctioned depending on the weather. Bandwidth problem. Email, fax, couriers still in use. 3 day targeting to strike lag.

1991 – No Fly Zones in Iraq, Balkans push to have cheaper surveillance

1995 Satellite feeds from Surveillance showing mass graves, troop withdrawals…

1996 Khobar tower bombings – push to move more surveillance back to the U.S.

1998 In Kosovo – GPS solution to the laser guided weapon problem.

> JDAM – a kit that could be attached to make any bomb a "smart bomb" 1/50 the cost of a cruise missile, 1/20th the cost of a laser guided bomb. Still not attached to drones.

2000 Predator Base established in Uzbekistan. Bin Laden spotted, provokes debate on legality of strike, time lag too long for a strike.

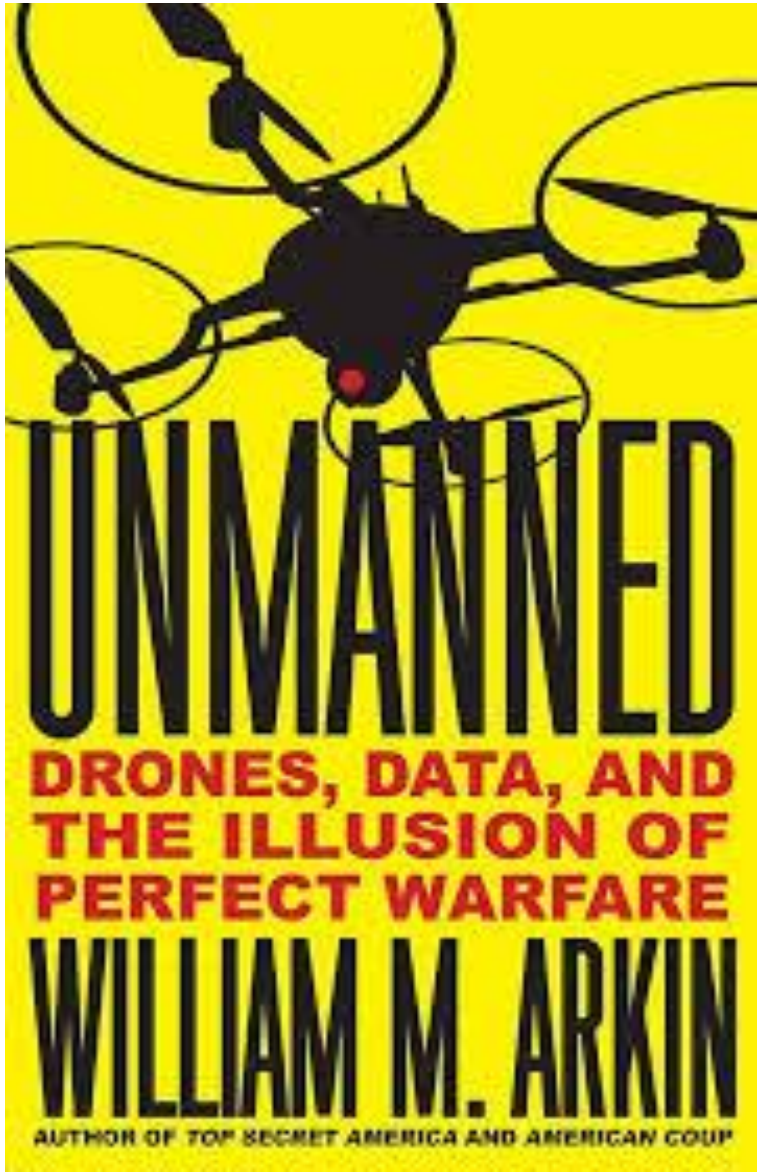
2001 Afghanistan a perfect war for ISR development – no targets except humans…

2004-5 The real impulse for drone warfare with rise of insurgencies after Occupation…

June 2003 1st US IED death.

2001 50 Drones to 2015 8,000 in use.

Funding 2001 $350 m annually– 2013 $5 B annually


UNMANNED
DRONES, DATA, AND THE ILLUSION OF PERFECT WARFARE
WILLIAM M. ARKIN
AUTHOR OF TOP SECRET AMERICA AND AMERICAN COUP

2015 book

Sharing of information across platforms and organizations becomes both a Tactical and a Financial Issue

Bandwidth issue - 2003 one Predator using 10x the bandwidth of the entire U.S. military in 1991!

"Rover" Gave Special Op troops on the ground their own window into what the drones were seeing, their own channel to pilots and to the integration of intelligence. (Weight goes from 50 lbs to 4 lbs, accessing at least 40 different data streams).

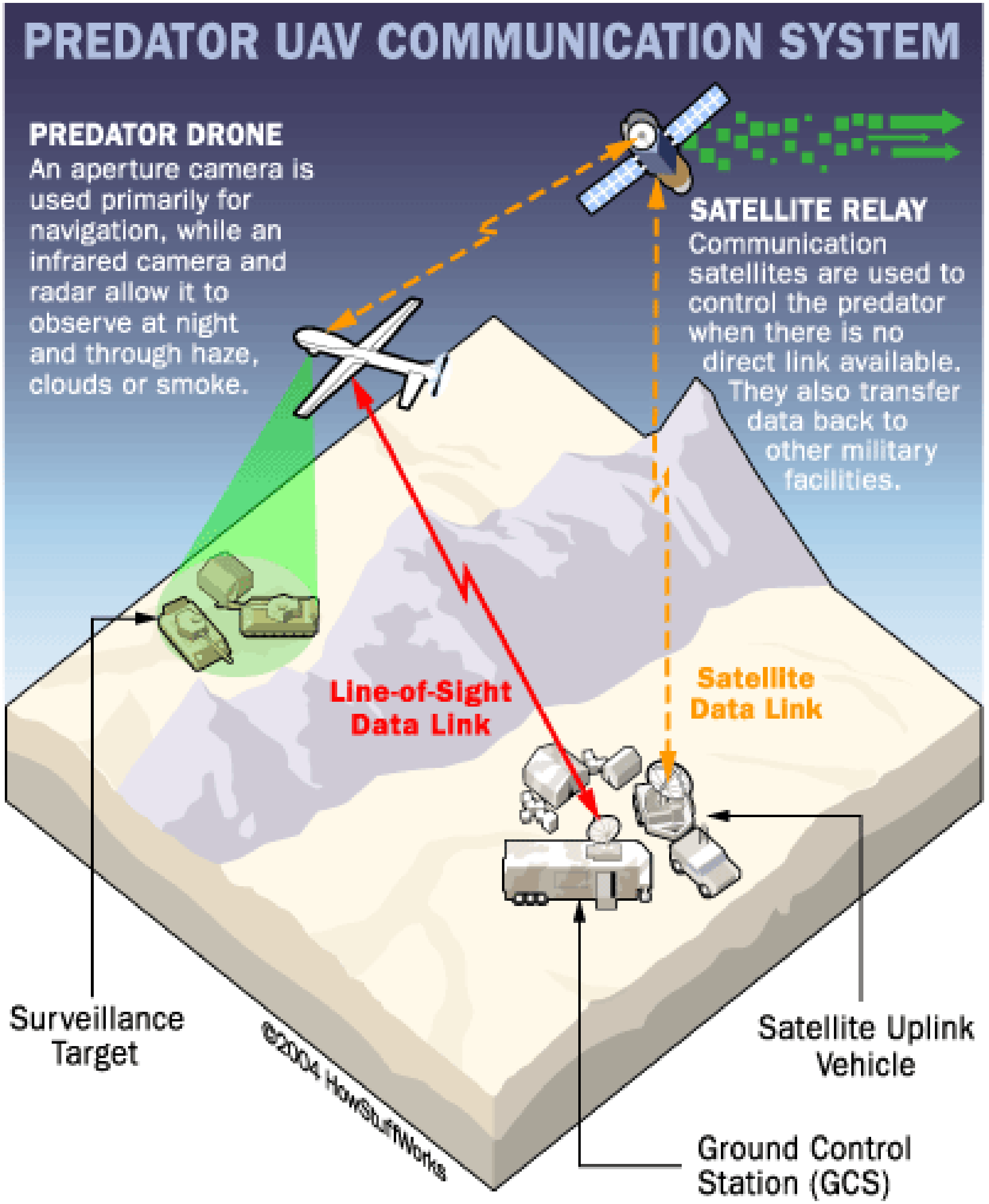
Enhanced troop safety – but who is setting overall policy?

What does "eyes on target" mean here? Rules of Engagement shift.

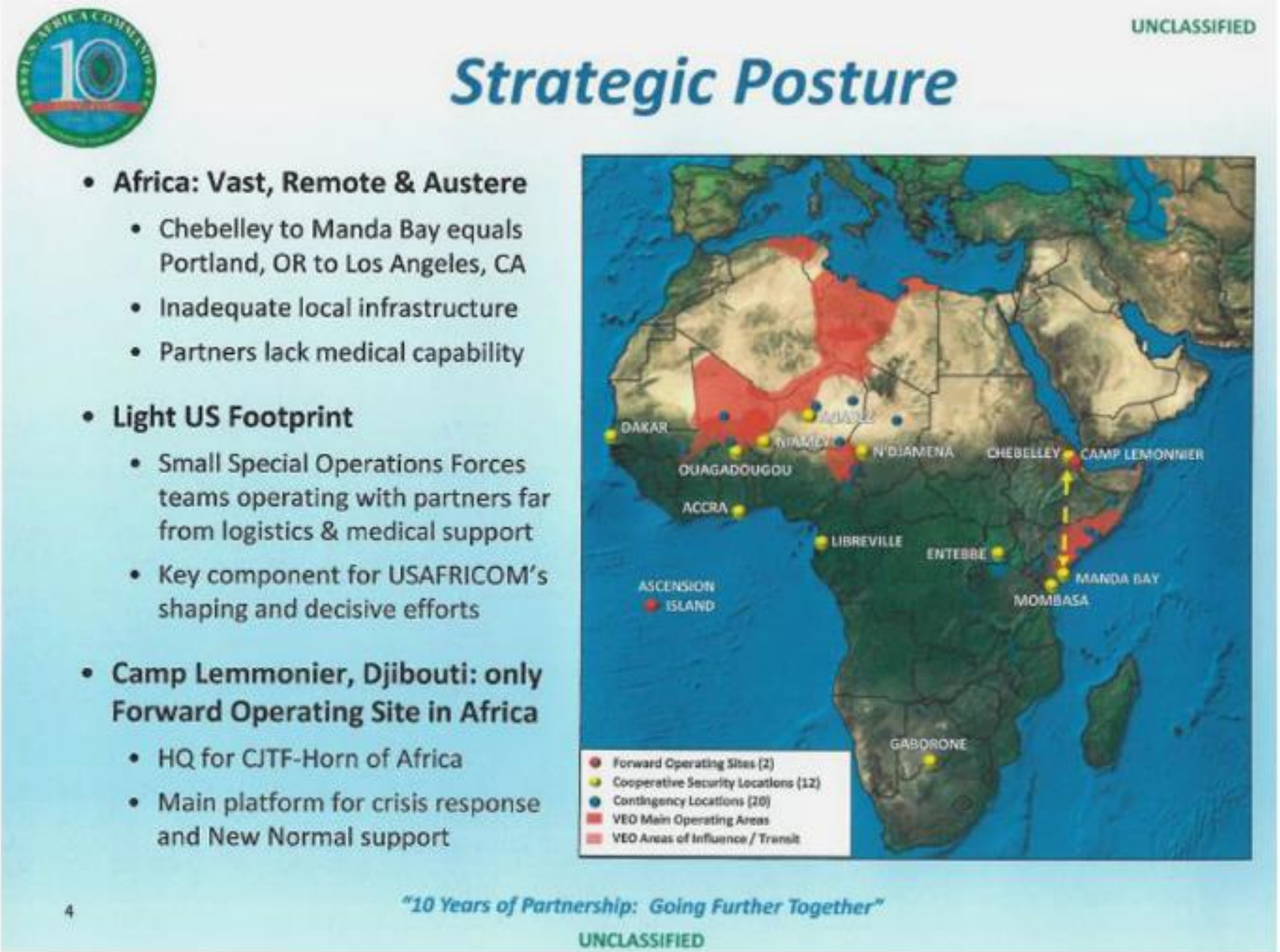
Regional Ground Control Stations are needed for bases, launch and recovery of drones.

Once launched, drones can be piloted by satellite link.

Pilots, intelligence, ground troops, can all share parts of the intelligence feed.



PREDATOR UAV COMMUNICATION SYSTEM
PREDATOR DRONE
An aperture camera is used primarily for navigation, while an infrared camera and radar allow it to observe at night and through haze, clouds or smoke.
SATELLITE RELAY
Communication satellites are used to control the predator when there is no direct link available. They also transfer data back to other military facilities.
Line-of-Sight Data Link
Satellite Data Link
Surveillance Target
©2004 HowStuffWorks
Satellite Uplink Vehicle
Ground Control Station (GCS)



UNCLASSIFIED

Strategic Posture

- **Africa: Vast, Remote & Austere**
  - Chebelley to Manda Bay equals Portland, OR to Los Angeles, CA
  - Inadequate local infrastructure
  - Partners lack medical capability
- **Light US Footprint**
  - Small Special Operations Forces teams operating with partners far from logistics & medical support
  - Key component for USAFRICOM's shaping and decisive efforts
- **Camp Lemmonier, Djibouti: only Forward Operating Site in Africa**
  - HQ for CJTF-Horn of Africa
  - Main platform for crisis response and New Normal support

DAKAR
NIAMEY
N'DJAMENA
OUAGADOUGOU
ACCRA
LIBREVILLE
ENTEBBE
CHEBELLEY
CAMP LEMONNIER
MANDA BAY
MOMBASA
ASCENSION ISLAND
GABORONE
● Forward Operating Sites (2)
● Cooperative Security Locations (12)
● Contingency Locations (20)
🟥 VEO Main Operating Areas
🟥 VEO Areas of Influence / Transit

4

"10 Years of Partnership: Going Further Together"

UNCLASSIFIED

U.S. Africa Command's "Strategic Posture" – listing 34 military outposts – from a 2018 briefing by Science Advisor Peter E. Teil. Image: U.S. Africa Command

2018 Briefing Slide on U.S. Africom

"Inadequate Local Infrastructure"

"Light footprint?"

"Shaping efforts?"

"The New Normal?"

With drones, the technology has become the strategy.

Homeland Scene: Quinn on Syria. https://www.youtube.com/watch?v=4yw8HycLbnM

US Foreign Policy and National Security Policy on Surveillance driven-Autopilot (Arkin)

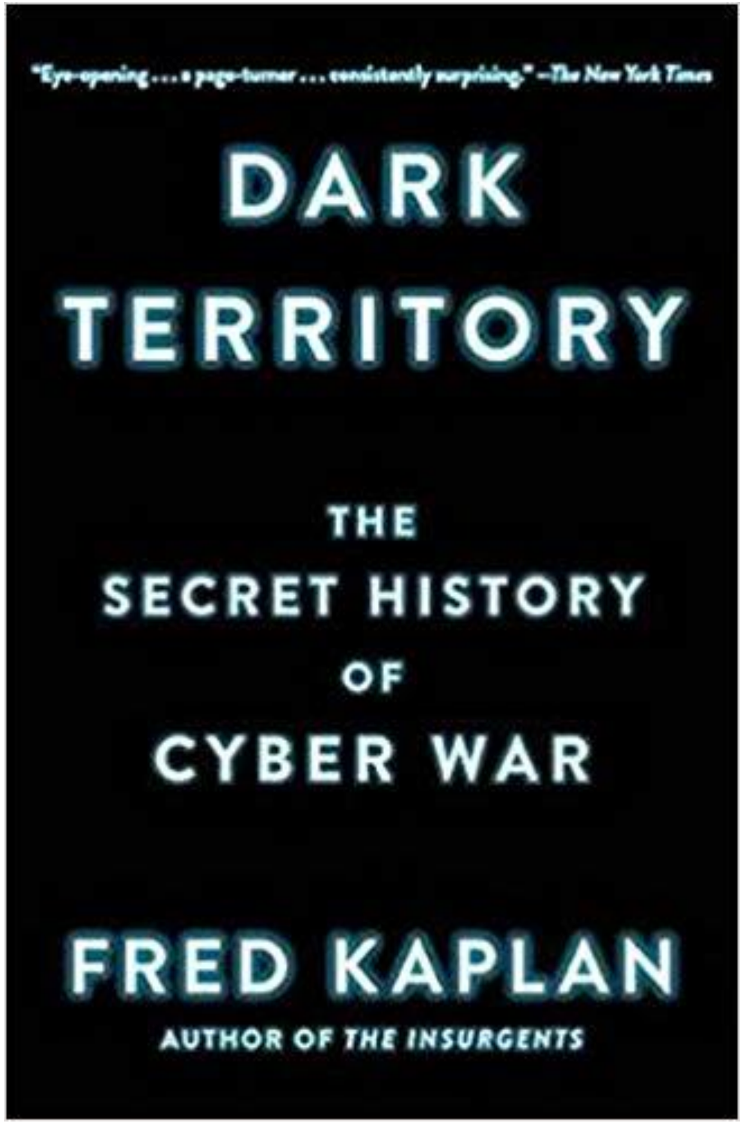
- Lack of Division between CIA/Defense/NSA. Designing Data to fit policies, not vice versa. A constant hunt for more data as the solution.

- "Vextering" – The thrill of the vector hunt in an age of instant communications overtakes the ability for other voices to weigh in.

- The PPT and the Death of Policy Review. Constantly tweaked PPTs have halted the longer process of consensus building and debate in older policy formations.

- Focus on "Kills" statistics ignores the blowback from Drone wars.

- An Assumption the data and technology advantage will remain.
  (In 2015 About 90 nations use drones, about 50 produce them.)



"Eye-opening . . . a page-turner . . . consistently surprising." —The New York Times

DARK TERRITORY

THE SECRET HISTORY OF CYBER WAR

FRED KAPLAN

AUTHOR OF *THE INSURGENTS*

Another Area where the Technology is Setting Policy ?

CyberSpace

1983 Film "War Games" raised the issue of cyber security with Reagan and the JCS.

Is this an issue of domestic or international security? Who should have the expertise?

https://www.youtube.com/watch?v=KXzNo0vR_dU

Mid 1990s, "Cyber" enters the vocabulary.

1994 1st Commercially available browsers, dot.com revolution puts everything online.

The private encryption industry emerges alongside hacking economy.

fort Meade, Mayland.
Good afternoon.

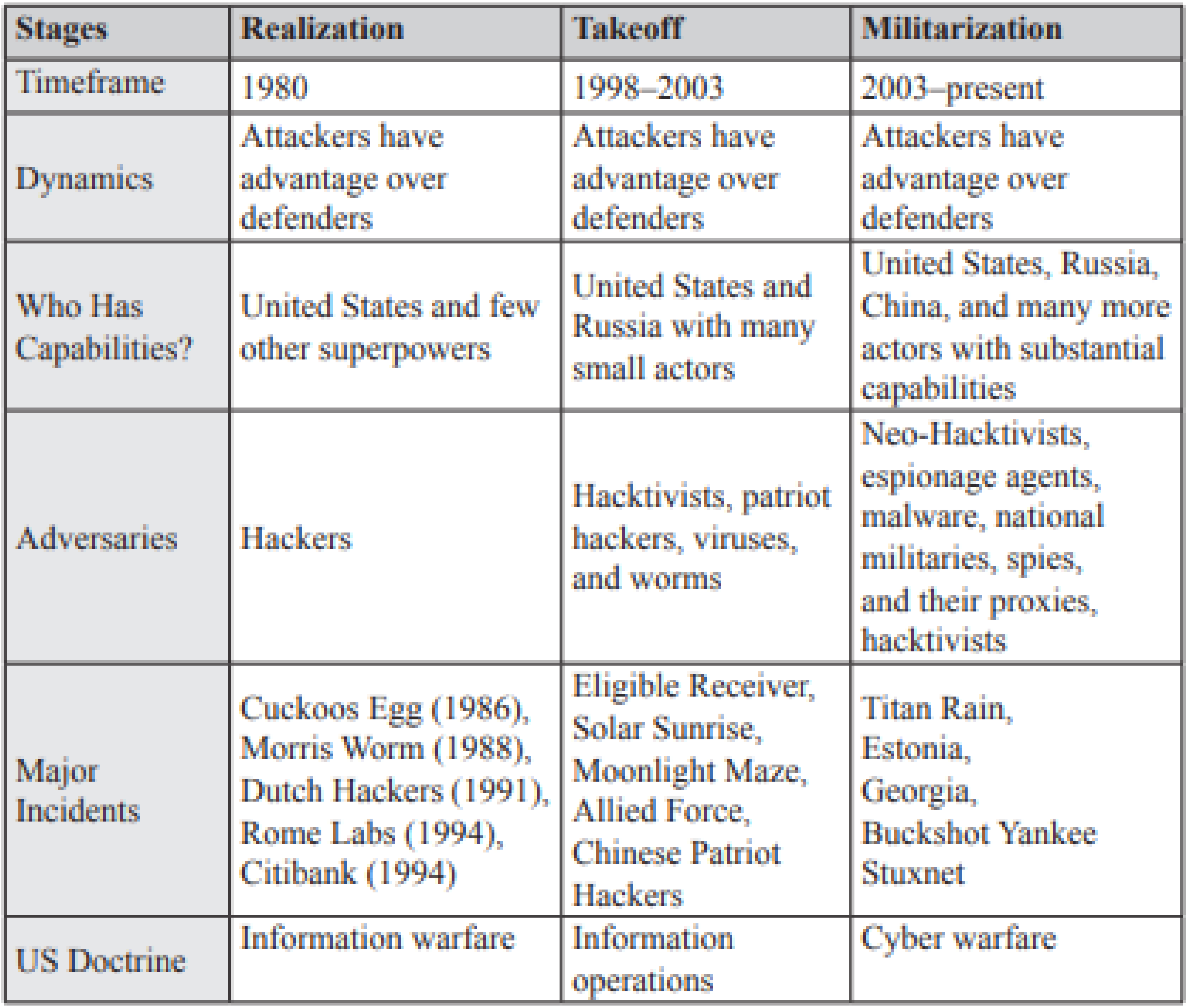
1992 Film Sneakers https://www.youtube.com/watch?v=coDtzN6bXAM (reality more likely to be 16 year olds)

New awareness of "critical national infrastructure." (Both "brick and mortar" and information networks).

Data Systems Create Vulnerabilities – Automated management, Environmental sensors; Personnel Systems…

The 1997 Presidential Commission leaves no one happy – public or private with proposals for cyber security.

1995 Oklahoma City Bombing



Stages	Realization	Takeoff	Militarization
Timeframe	1980	1998–2003	2003–present
Dynamics	Attackers have advantage over defenders	Attackers have advantage over defenders	Attackers have advantage over defenders
Who Has Capabilities?	United States and few other superpowers	United States and Russia with many small actors	United States, Russia, China, and many more actors with substantial capabilities
Adversaries	Hackers	Hacktivists, patriot hackers, viruses, and worms	Neo-Hacktivists, espionage agents, malware, national militaries, spies, and their proxies, hacktivists
Major Incidents	Cuckoos Egg (1986), Morris Worm (1988), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot Hackers	Titan Rain, Estonia, Georgia, Buckshot Yankee Stuxnet
US Doctrine	Information warfare	Information operations	Cyber warfare

Figure 1: Phases of Cyber Conflict History

Cyber Strategy evolves from reactions to major incidents

1998 Solar Sunrise Attack

DOD notes a coordinated system of attacks against US army, navy, intelligence sites worldwide.

Gathering passwords, implanting "sniffing" programs that could gather data, covering their tracks…

Iraq? Russia? Chinese military?

https://www.wired.com/2008/09/video-solar-sun/
FBI produced film to raise awareness of the problem.

The 9-11 Effect – Into the Grey Zone in a time of crisis

Post 9-11 CIA and NSA cultivating relationships with both black and white hat hackers. Buying "Zero Days" on the Black Market

Exploiting the lack of legal guidelines.

> Example: the firm "Endgame" in Fairfax, VA, was known as the Halibuton of Hackers. Private contractor operating at the grey zone.
>
> Their program, "Bonesaw" pulled internet data to show which software ran on machines around the globe, linked to publicly available techniques to hack it.

2014 The Hackers Collective "Anonymous" published information on CIA/NSA grey zone activities – industry anger with intelligence industry.

Mid 2000s - From Cybersecurity to Cyberwarfare

2007 Estonia punished with Russian (?) Cyber attack on utilities

2008 "Worms" found in International Space Station computers

2009 Creation of Cyber Command – from 900 people to over 15,000 today.

2010 Stuxnet hits the news

2014 Russian cyber war in Ukraine (defense, power and electoral systems)

2015 Information theft in private sphere – personal data, patents, etc.

2017 from Malware to Ransomware Attacks

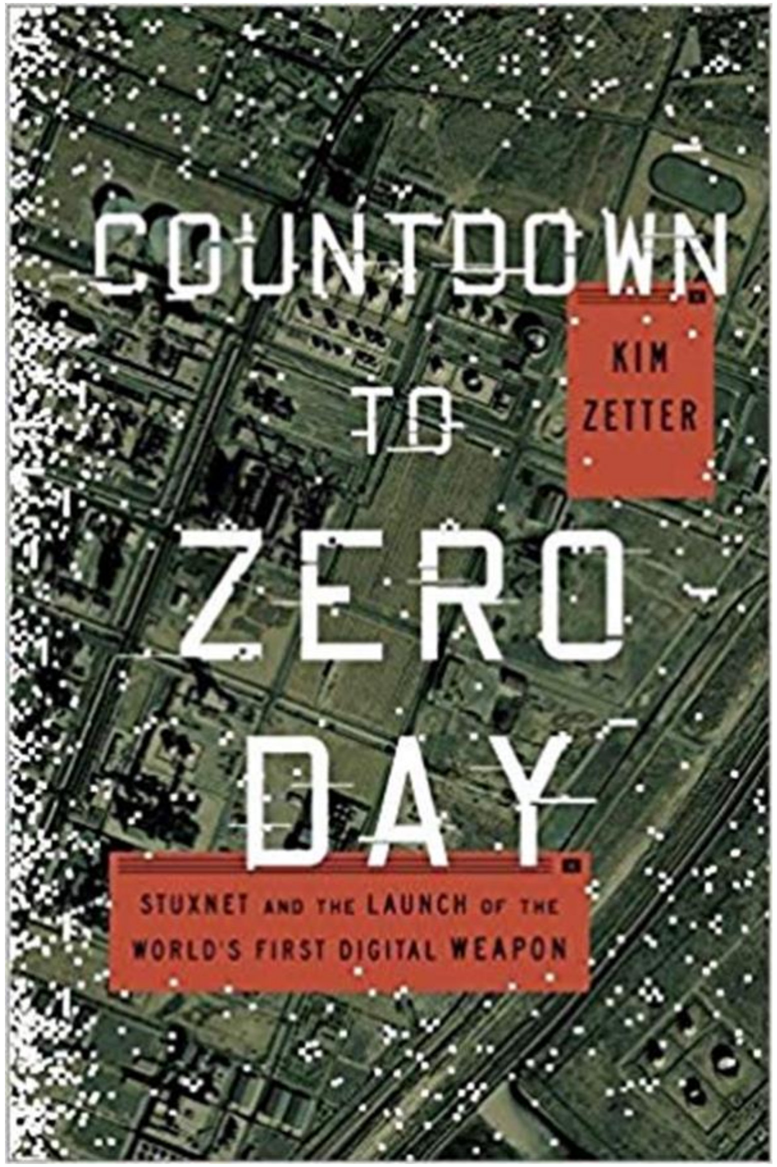
Stuxnet: The Weapon that Prevented War with Iran or the weapon that expanded the battlefield?

2004 US Strategic Command/NSA partnership exploring Cyber weapons

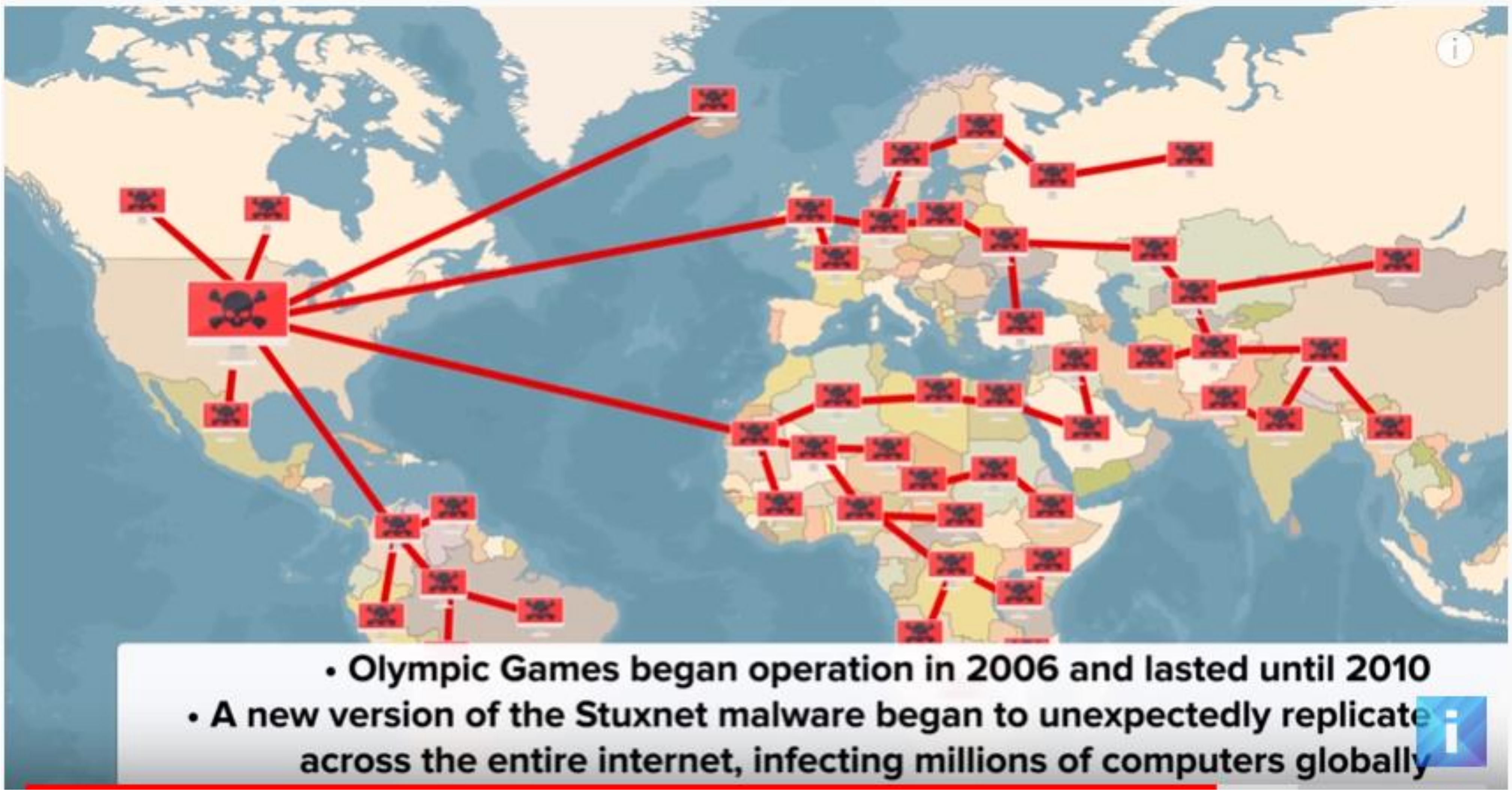
2006 Iran Nuclear Showdown - Stuxnet Virus Deployed

2007 Similar virus shut down Syrian Radar during Israeli strike

2010 Stuxnet Virus becomes public



2006 Stuxnet – First Offensive Cyber Weapon?



- Olympic Games began operation in 2006 and lasted until 2010
- A new version of the Stuxnet malware began to unexpectedly replicate across the entire internet, infecting millions of computers globally

Clip from documentary "Zero Days" https://www.youtube.com/watch?v=yCKpGIsnERY

2011 Hungry Beast short video. https://www.youtube.com/watch?v=7g0pi4J8auQ

The New Cyberwar Battleground – Public Trust?

2018 Anonymous takes on "Q Anon" which promoted conspiracy theories about Trump's struggle against the "deep state."

2020 Article in Wired Magazine https://www.wired.com/story/qanon-deploys-information-warfare-influence-2020-election/

2020 NYT article https://www.nytimes.com/2020/02/09/us/politics/qanon-trump-conspiracy-theory.html

Where do our traditional Intelligence Services fit in this new Battlespace?

A shift from language and regional expertise to technology skills

From Spying to Surveillance - emphasis on "Targeting," IET, HPTs…

Militarization of the CIA - Rush to fill out new CTC staffing at the CIA drawing on veterans, CIA staff based in military compounds overseas,

By 2005 ½ of CIA employees had 5 or fewer years at the agency! (Politico)

https://www.politico.com/magazine/story/2017/03/cia-art-spying-espionage-spies-military-terrorism-214875