

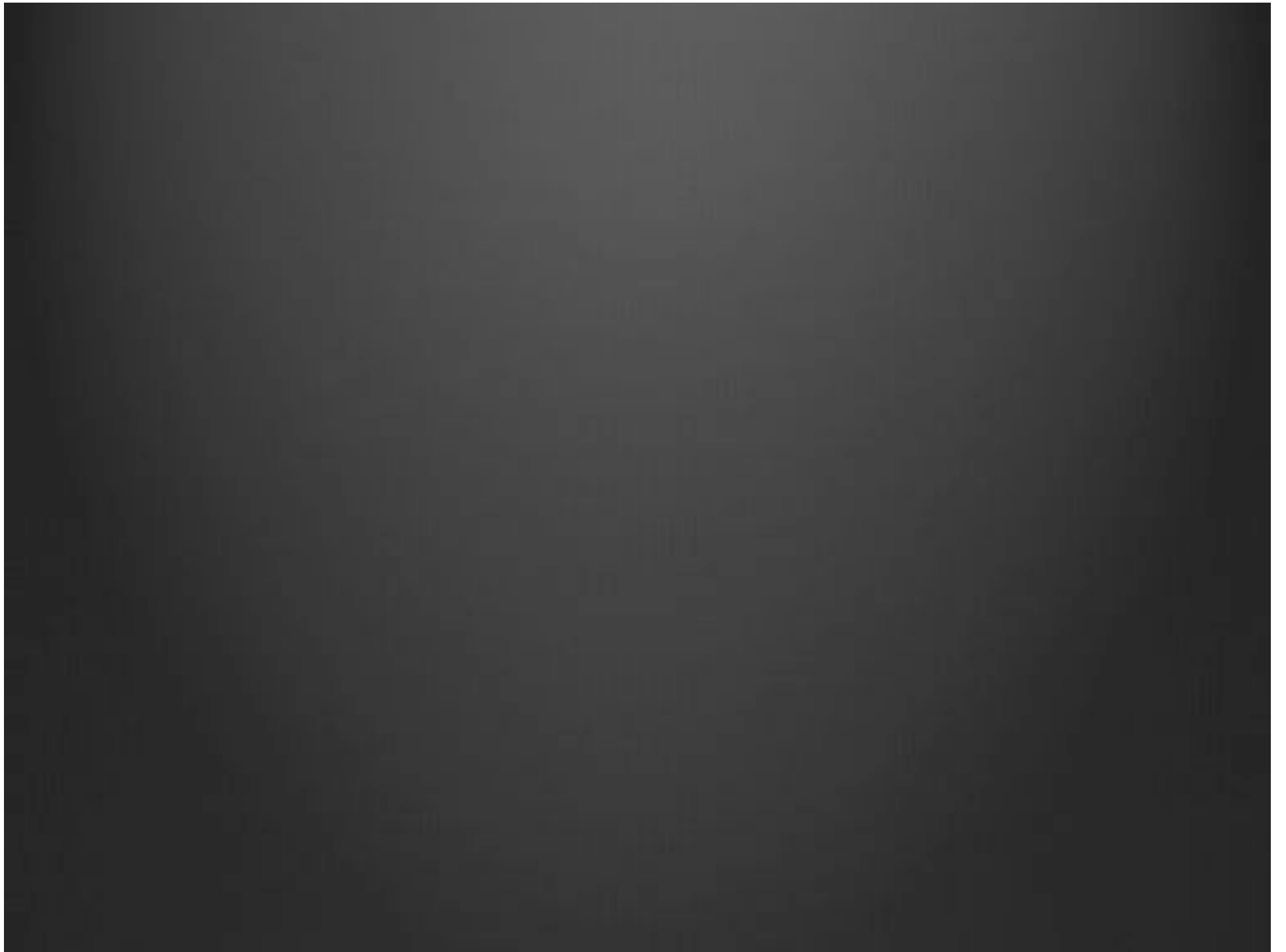
BH2015 slides surveillance & post-Westphalia states

Matthew Jones

History, Columbia

mjones@columbia.edu

@nescioquid



NSA 2001

2 TRANSITION 2001

DECEMBER 2000



Derived From: NSA/CSS Manual 123
Dated: 24 February 1998
Declassify On: X1

~~SECRET//X1~~

CONFIDENTIAL

The Fourth Amendment is as applicable to eSIGINT as it is to the SIGINT of yesterday and today. **The Information Age will however cause us to rethink and reapply the procedures, policies and authorities born in an earlier electronic surveillance environment.**

Transiting US

TOP SECRET//SI//ORCON//NOFORN

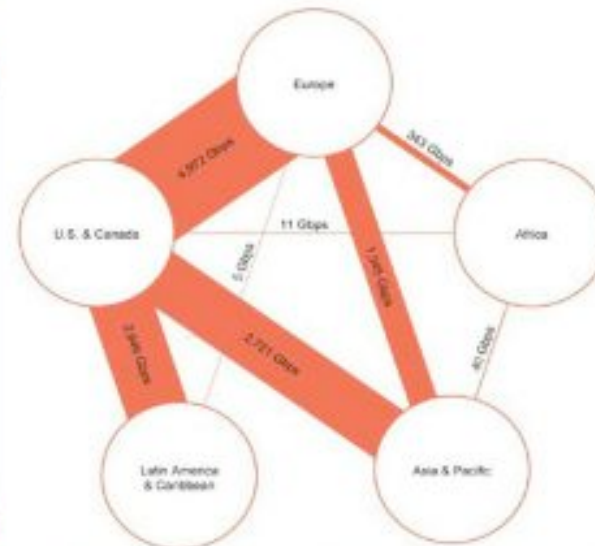


(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



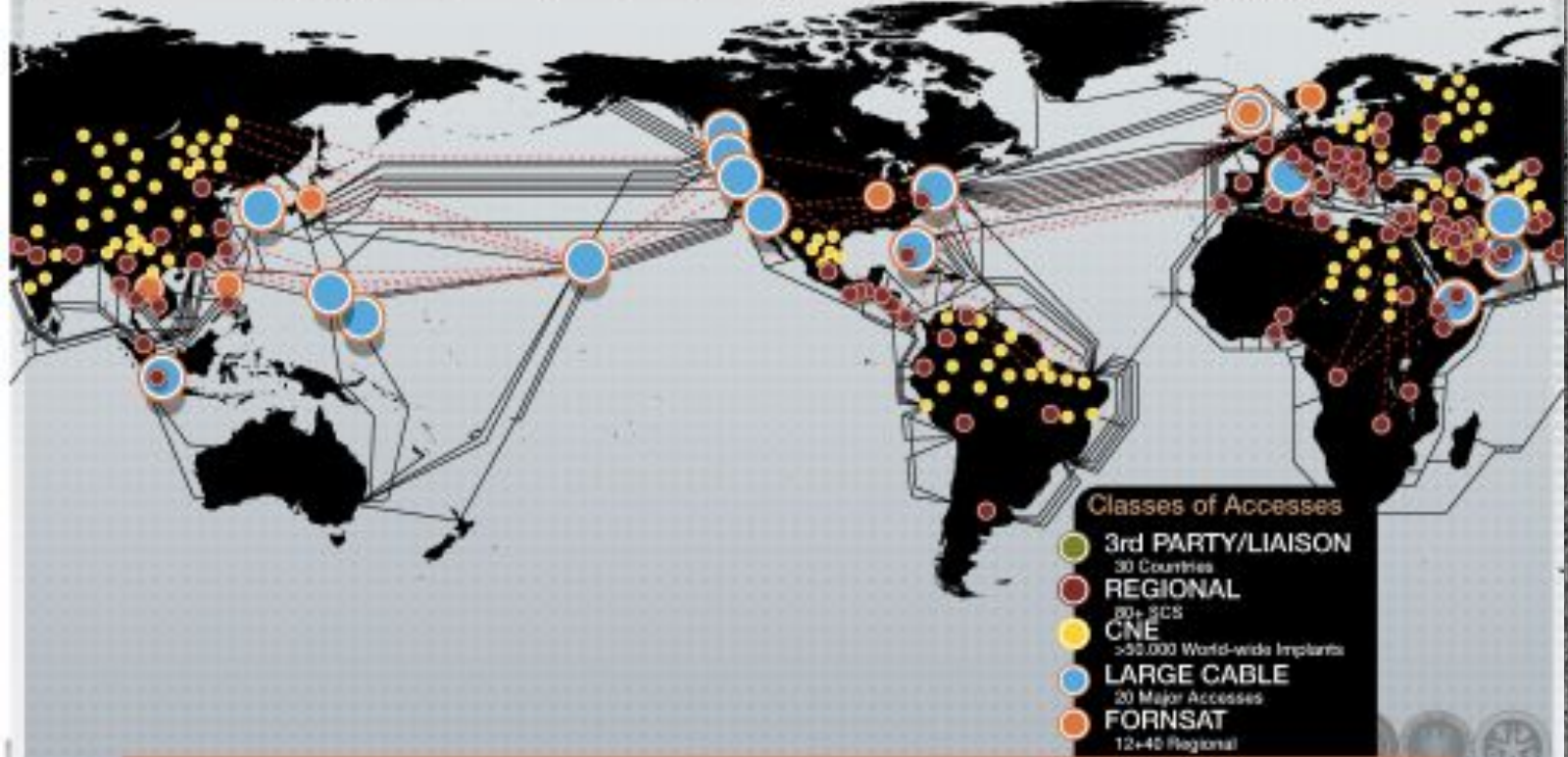
International Internet Regional Bandwidth Capacity in 2011

Source: TeleGeography Research

TOP SECRET//SI//ORCON//NOFORN

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

| | | | | | | | | | | | | | | | | |
|---|------------------------|-------------|-------------|----------|-----------|--------------|----------------|--|--|--------|-------|----------|-----------------------|---------|-----------|-------|
| <p>High Speed Optical Cable Covert, clandestine or Cooperative Large Accesses 26 Access Programs Worldwide</p> | <p>Regional</p> | | | | | | | | | | | | <p>FORNSAT</p> | | | |
| | Caracas | Havana | Kinshasa | Soňa | Berlin | Prizna | Guatemala City | | | | | | | | STELLAR | INDRA |
| | Tripoli | Algiers | Lusaka | | Bangkok | Tripoli | RESC | | | | | | | SOUNDER | IRONSAND | |
| | Geneva | Bogota | Panama City | | New Delhi | Phoenix Park | | | | | | | | SNICK | JACKKNIFE | |
| | Athens | Mexico City | | Budapest | Frankfurt | Sarajevo | | | | | | | | MOONPEN | CARBOY | |
| | Rome | Brasilia | | Prague | Paris | | | | | | | | | NY | TIMBERLIN | |
| Quito | Managua | | Lagos | Varna | Kangon | | | | | La Paz | | LADYLOVE | E | | | |
| San Jose | | | | Zagreb | | | | | | Vienna | Armas | Rosten | | | | |



Classes of Accesses

- 3rd PARTY/LIAISON
30 Countries
- REGIONAL
80+ SCS
- CNE
>50,000 World-wide Implants
- LARGE CABLE
20 Major Accesses
- FORNSAT
12+40 Regional

4th revised

- ⊗ Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment . . . senior leadership must understand that today's and tomorrow's mission will demand a powerful, permanent presence on a global telecommunications network that **will host the 'protected' communications of Americans as well as the targeted communications of adversaries.**

Loss of sanctuary

2000

S
u
m
m
e
r

DSB

S
t
u
d
y

2000

9600

***Threat to the Homeland
How We Got Here?***

- Politics
 - ❖ Dissolution of the Soviet Union
 - ❖ U.S. symmetric dominance makes us target for asymmetric attack
 - ❖ As only superpower, United States is a target
- Technology
 - ❖ Widespread availability and low cost of biological, chemical and information warfare technology
 - ❖ Global pool of skilled human resources
 - ❖ Internet as C³
 - ❖ Fragility of complex, interdependent society

6

Information war has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the U.S. economy will increasingly rely on complex, interconnected network control systems for such necessities as oil and gas pipelines, electric grids, etc. [...]

the U.S. homeland may no longer provide a sanctuary from outside attack.

--RAND report on Cyberwar exercises
"What Makes Cyberwar Different?"

Two regimes of conflict

- ⊗ Ye olde Westphalian order:
 - ⊗ Among sovereign, territorial nations
 - ⊗ some (US) with robust formal rights for citizens (US persons)
 - ⊗ Externally focused forces (DOD, CIA, MI-6, &c)
 - ⊗ Domestically focused forces (FBI, MI-5, &c.)
 - ⊗ “Hobbesian” relations among nations

Two regimes of conflict

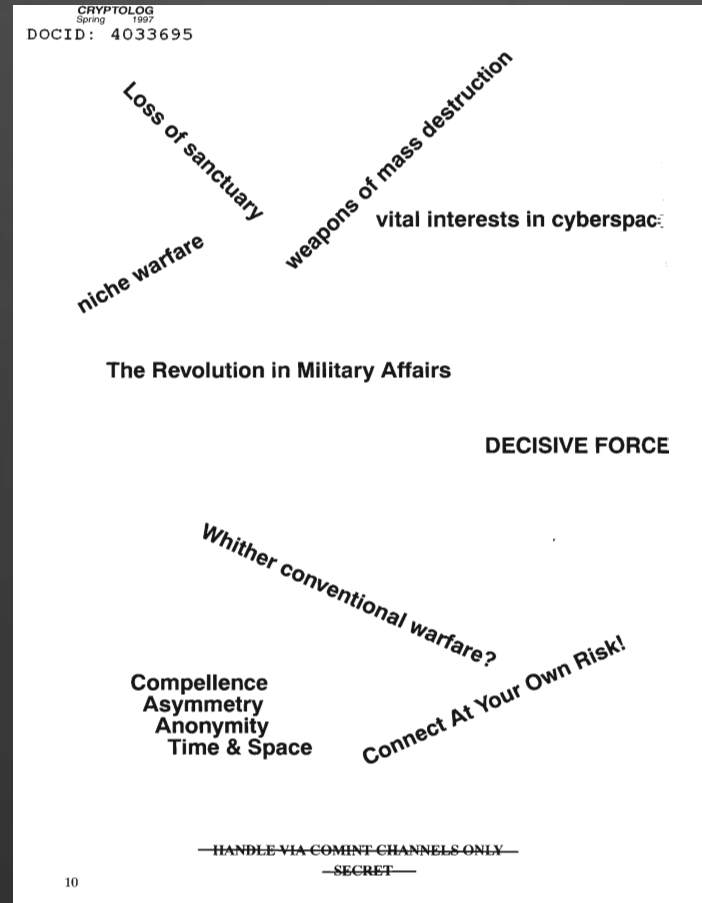
- ⊗ De-territorialized, non-Westphalian, Information age
 - ⊗ Porous nations and non-state actors
 - ⊗ “homeland” no “sanctuary”
 - ⊗ Asymmetrical warfare anywhere
 - ⊗ Dissolving of Defense/law enforcement boundary
 - ⊗ Dissolving of foreign/not foreign
 - ⊗ “Critical infrastructure” at risk
 - ⊗ Dissolving of economic/non-economic
 - ⊗ Foucault being read in DoD and RAND

Loss of sanctuary



In the new era, a sharp distinction between 'foreign' and 'domestic' no longer apply. We do not equate national security with 'defense.'" (Hart-Rudman, *Roadmap to National Security*)


Loss of sanctuary



NSA Cryptolog Magazine, 1997

“modernizing” < 9/11

- ⊗ Deterritorializing regime working within constitutional one
- ⊗ Setting wheels in motion to
 - ⊗ Allow interception of foreign packets transiting US
 - ⊗ Weaken intelligence / domestic crime boundary
 - ⊗ Allow NSA to play significant role in scanning US for vulnerabilities or attacks in action (Critical Infrastructure)
 - ⊗ Allow NSA, CIA, and DOD more involvement in fighting asymmetric warfare in US more generally



PATRIOT ACT
emerges with
weeks of 9/11

Much contested < 9/11

- ⊗ Clinton era Office of Legal Counsel in 1997-2000
 - ⊗ Sharply uphold boundary between
 - ⊗ Domestic law enforcement
 - ⊗ Grand juries
 - ⊗ Wiretaps
 - ⊗ Intelligence Community
 - ⊗ Reject plan to contact-chain US persons



Shock necessary

- ⊗ DSB 2001 report (< 9/11/2001)
- ⊗ Because the targets of information operations will be civilian as well as military, defending against such attacks will require close cooperation between the public and private sectors. Such cooperation is mildly controversial today, but **a sophisticated attack on public and private networks will likely make cooperation not just politically acceptable but politically necessary. When that happens, the legal regime needed to respond to the attack will likely be put in place quickly by politicians anxious to be seen as part of the solution. [85-86]**

Post-westphalian data mining

- ⊗ “the application of evolving techniques that already are employed widely in the industrial sector for searching, merging, sorting and correlating data in multiple independent data bases, can be applied to the transnational terrorist problem to provide intelligence analysts with more effective tools than are now available to help them discover the identities, capabilities, intentions and plans, of foreign and domestic threat groups.”
 - ⊗ Hermann and Welch, *The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats. Volume III (Supporting Reports)*, section 4A, p. 6.