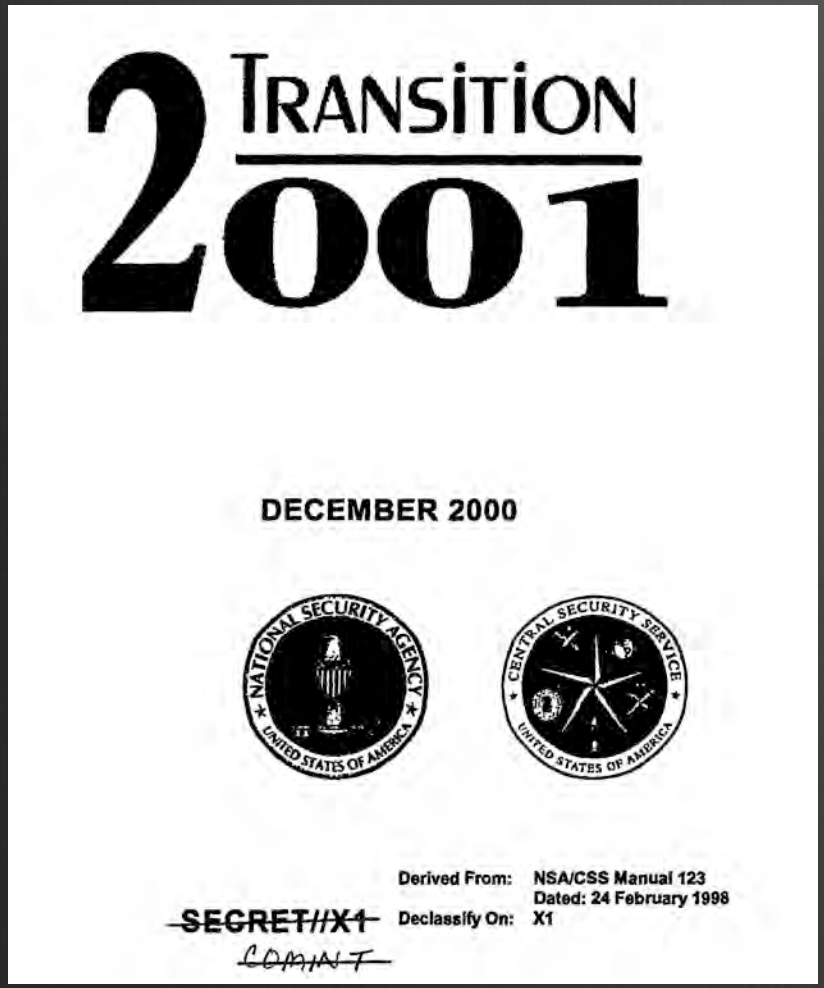
M. Jones, Columbia @nescioquid

NSA 2001



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.**

Three changes

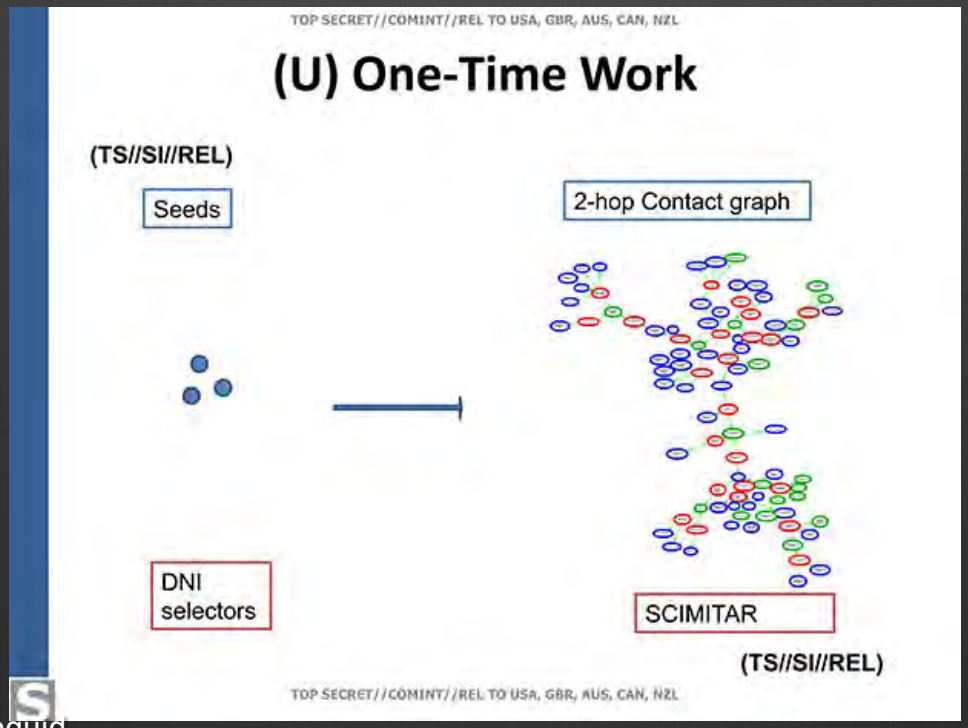
1. severity of volume

- Mid 1990s
  - Volume of communications foremost problem for the NSA
- Mid 2000s
  - Email title: “Volume is our Friend.”
- Late 2000s
  - “Golden Age of SigInt” (Signals Intelligence)

2. legality of querying

Late 1990s

Dept. of Justice rejects legality of a novel scheme to contact chain telephony and Internet as violation of 4th Amendment



2. legality of querying

Late 1990s

DOJ rejects legality of a novel scheme to contact chain telephony and Internet metadata while encrypting the identity of US persons as violation of 4th Amendment

2008 secret Justice department memo

contact chaining and other metadata analysis do not qualify as the 'interception' or 'selection' of communications . . . .

Thus: no search and seizure under 4th amendment

3. banality of hacking

1997

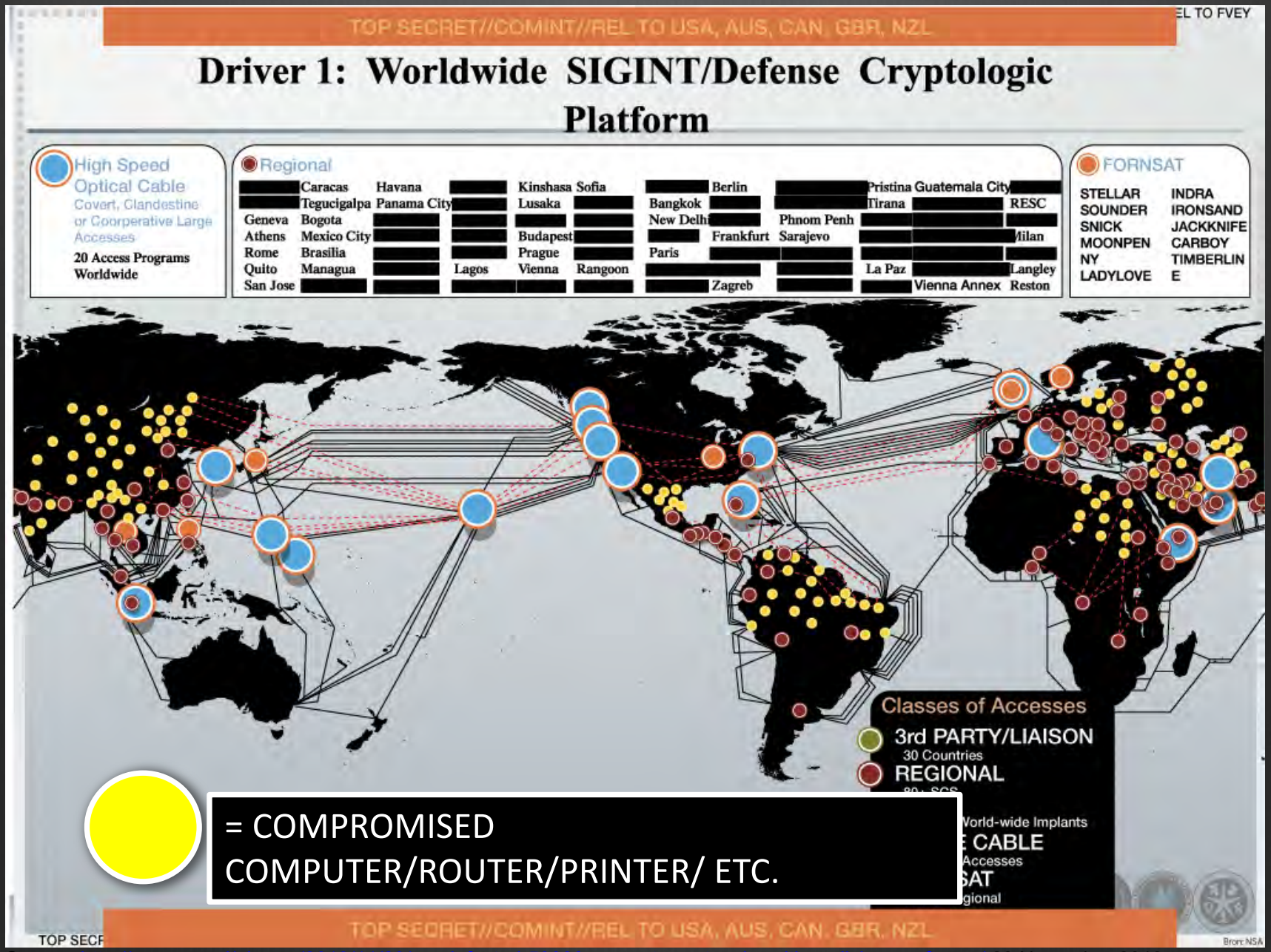
The US Secretary of Defense assigned primary responsibility for Computer Network Attacks (CNA) to the NSA, securing NSA a central role in information warfare—post cold war future

Mid 2000s

Distributed XKeyscore database offered the option to “Show me all the exploitable machines in country X.”

2013

“The United States Government has mature capabilities and effective processes for cyber collection.”



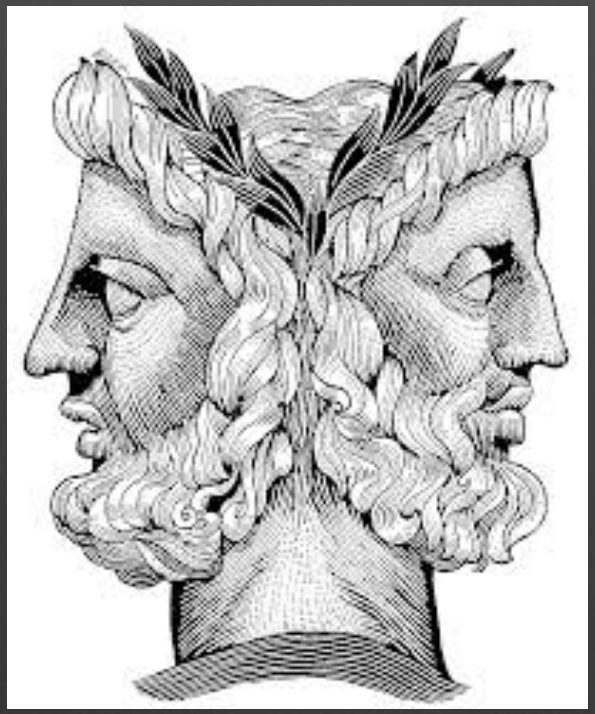
Source: http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/ 23 November 2013

“own the Net”

Janus Faced Agency

SigInt

Exploit communications



Information Assurance

Protect Communications

(COMSEC)

Exploitation >> comsec

- **Secret** risk analyses

  that national security best served by:

- Weakening encryption standards >> strongest encryption

- Retaining malware exploits >> systematic patching

“in ur interwebz, sploiting ur dataz”

NSA talk title, August 2008

M. Jones, Columbia @nescioquid

M. Jones, Columbia @nescioquid

Well, duh!

The job of the NSA is to collect and analyze communications, what did you expect them to do?

Radical two fold difference

Breadth

Depth

NSA >9/11: depth abroad

- not just foreign leaders, militaries, and intelligence
- not just the communications passing between phones or computers, but access to the full contents of computers, phones and routers themselves of millions of people and organizations
- Banality of hacking: at least 80K “implants”
  - Millions of devices systematically scanned as exploitable
  - “lightweight implants” used to map internal networks just in case
  - “enable” other activities

NSA >9/11: domestic breadth

- Breadth
  - Systematic collection of *domestic* telephony and (until lately) internet metadata
  - Able to collect large numbers of communications into, out of, and traversing the US
  - Including a large number of "incidental" communications of US persons
  - Including keeping *all* encrypted communications indefinitely

“modernizing” the law

Telephones/Internet usage

Individual Phone dialing info w/o Warrant

to

Collect all telephony metadata worldwide

Espionage

Capturing a particular set of communications

to

Cracking computers at great scale

“modernizing” the law

- Ignore *scale*
- Ignore power of operations on scale
- Ignore danger of operations on scale

- BIG DATA Crowd: Volume changes things

M. Jones, Columbia @nescioquid

Paradigm shift

The volume has been pumped up

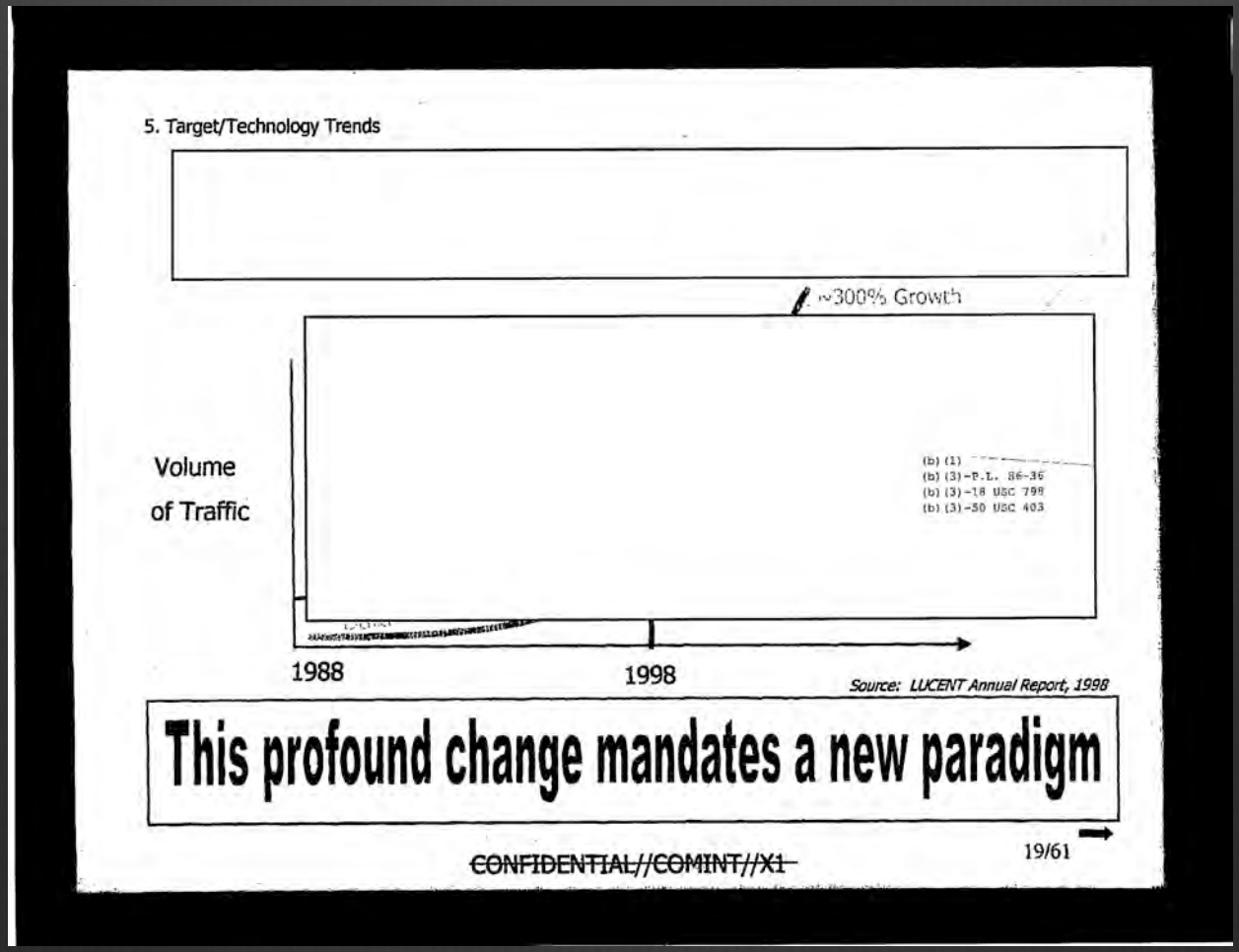
M. Jones, Columbia @nescioquid

Volume

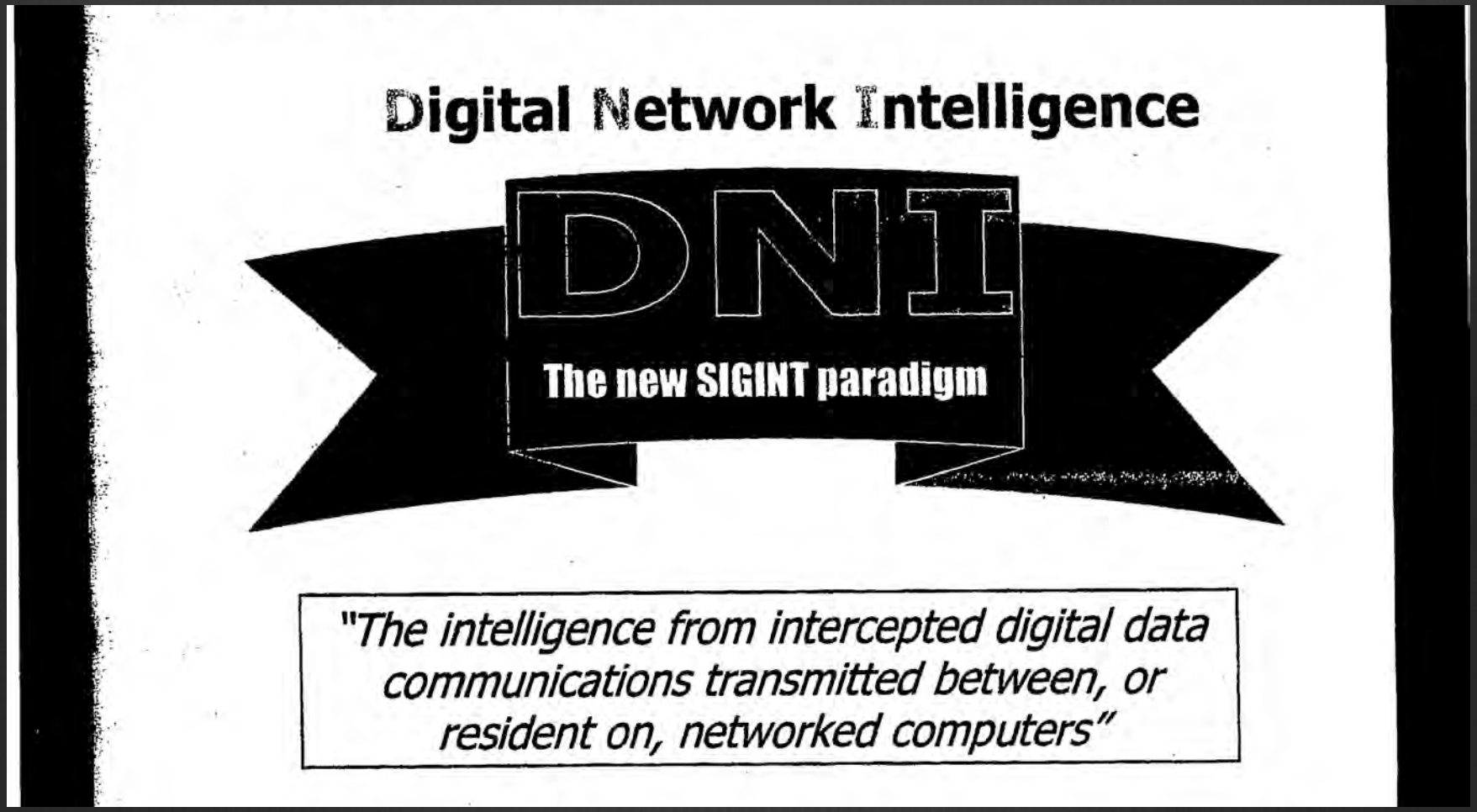
"Let me add to all of that the third biggest challenge facing us, and that is volume. And I could just end the sentence there and everything is said. [Paragraph Redacted] That gives you some idea of the daunting challenge volume presents, forcing us to look for new technologies."

redacted, "Confronting the Intelligence Future (U) An Interview with William P. Crowell, NSA's Deputy Director (U)." 1996

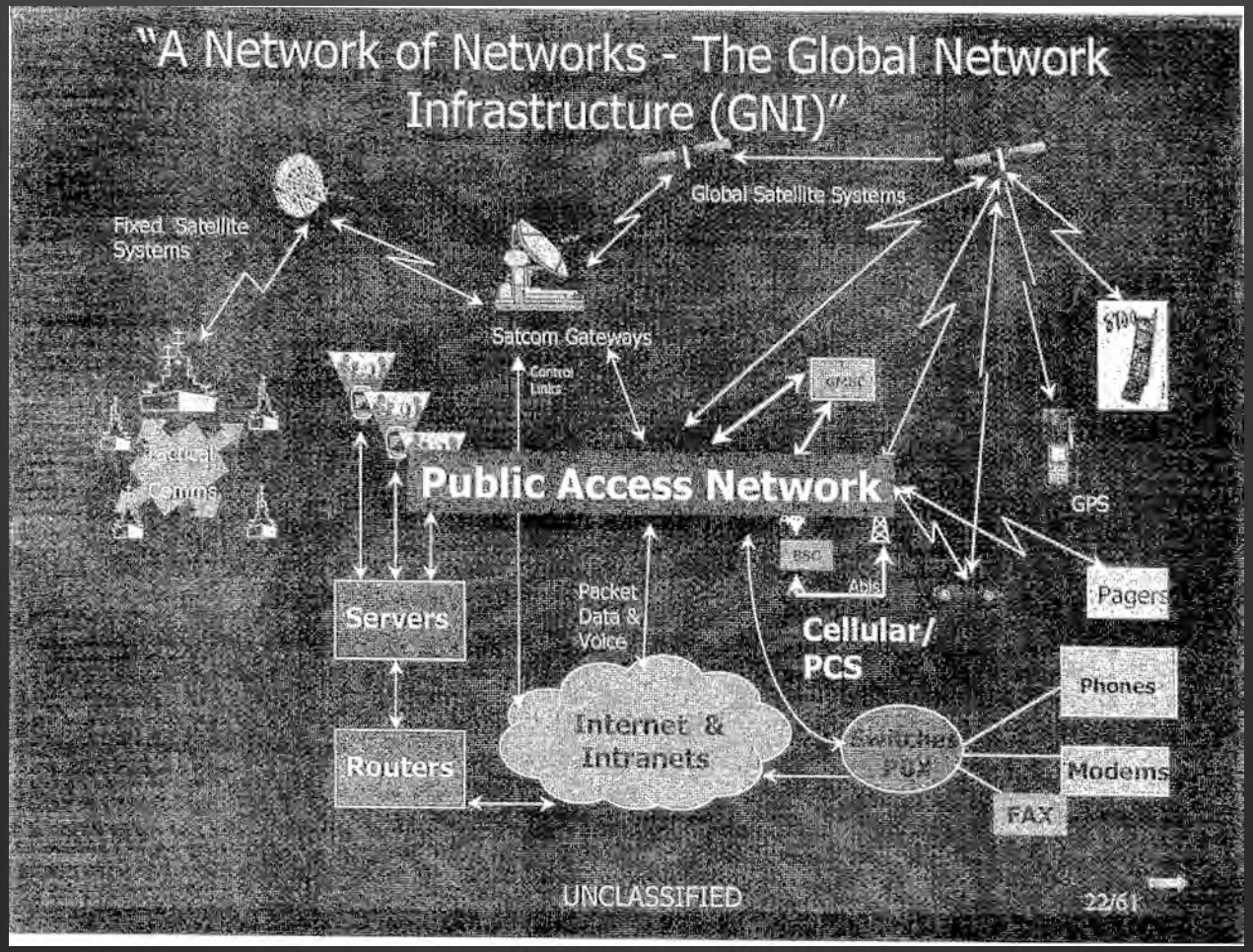
Paradigm shift



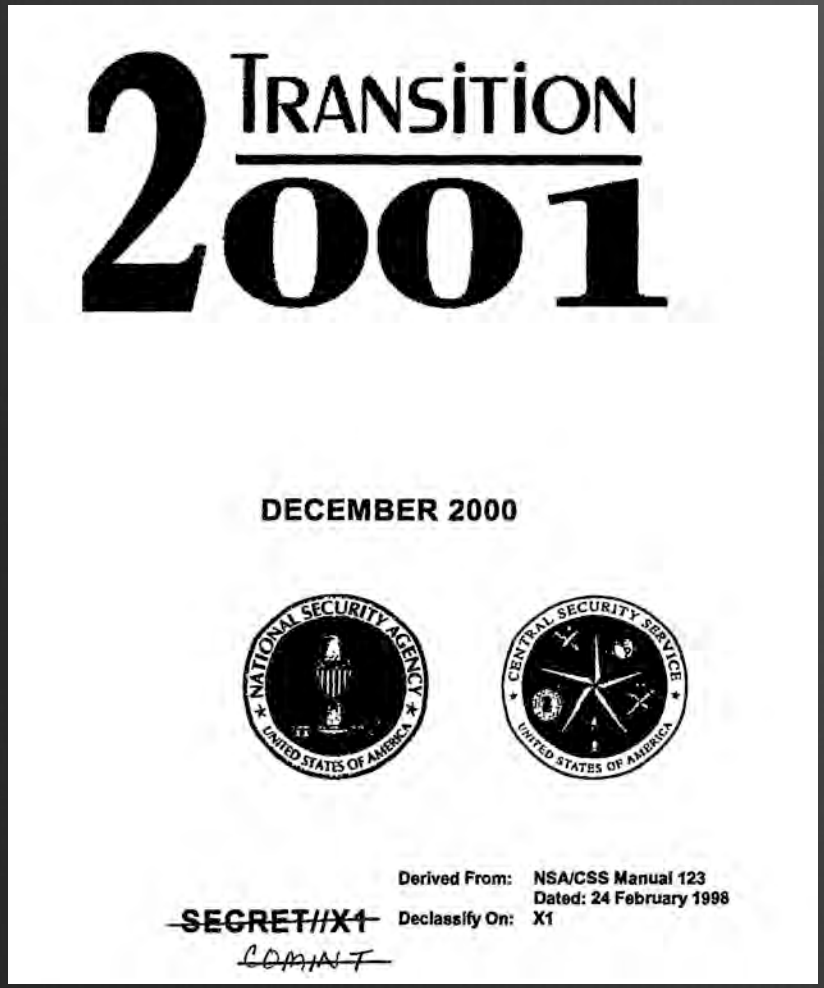
Paradigm shift



What to exploit? c. 1999



NSA 2001

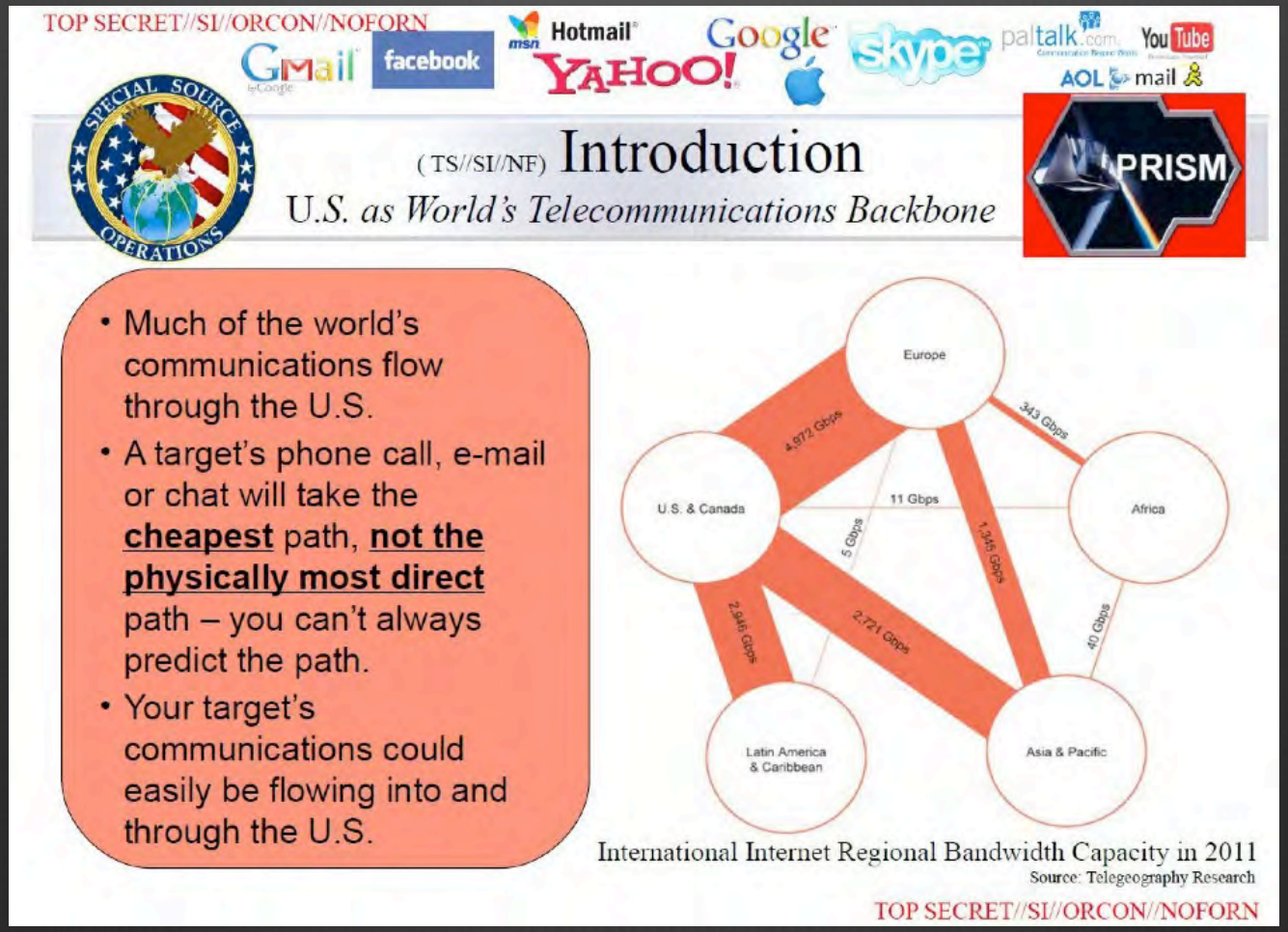


The Fourth Amendment is as applicable to eSIGINT as it is to the SIGINT of yesterday and today. **The Information Age will however cause us to rethink and reapply the procedures, policies and authorities born in an earlier electronic surveillance environment.**

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**.
- National Security Agency/Central Security Service, "National Security Agency/Central Security Service Transition 2001", p. 32.

Transiting US

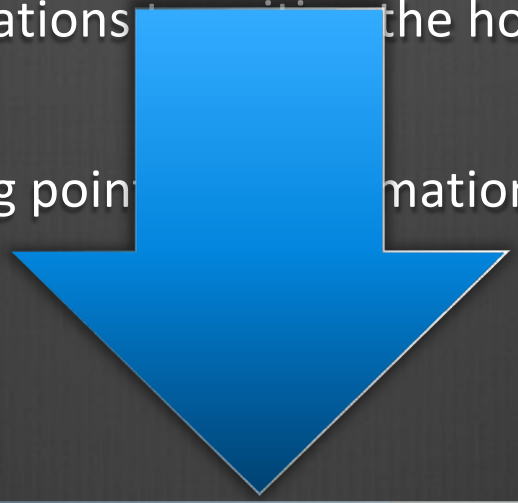


“modernizing” the law

Non-US signals in the homeland

1) Foreign communications [illegible] the homeland

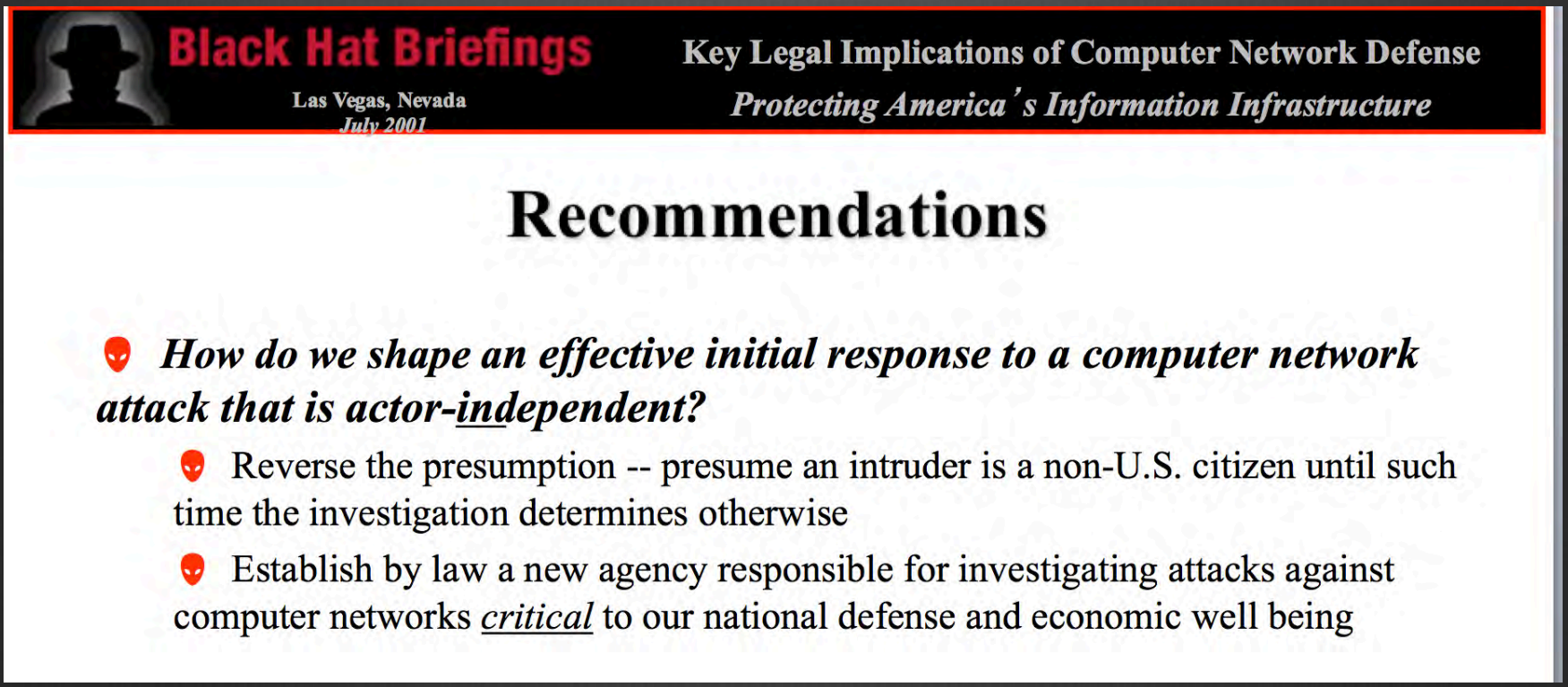
2) Domestic launching poin[illegible]mation warfare from foreign sources



Impossibility of treating as *domestic* law enforcement subject to 4th Amendment

Necessity to treat as *defense* issue in the first instance

Δ(presumption)



Gary Sharp (soon after counsel for IO/DNO/Cyber at DOD….)

4th revised

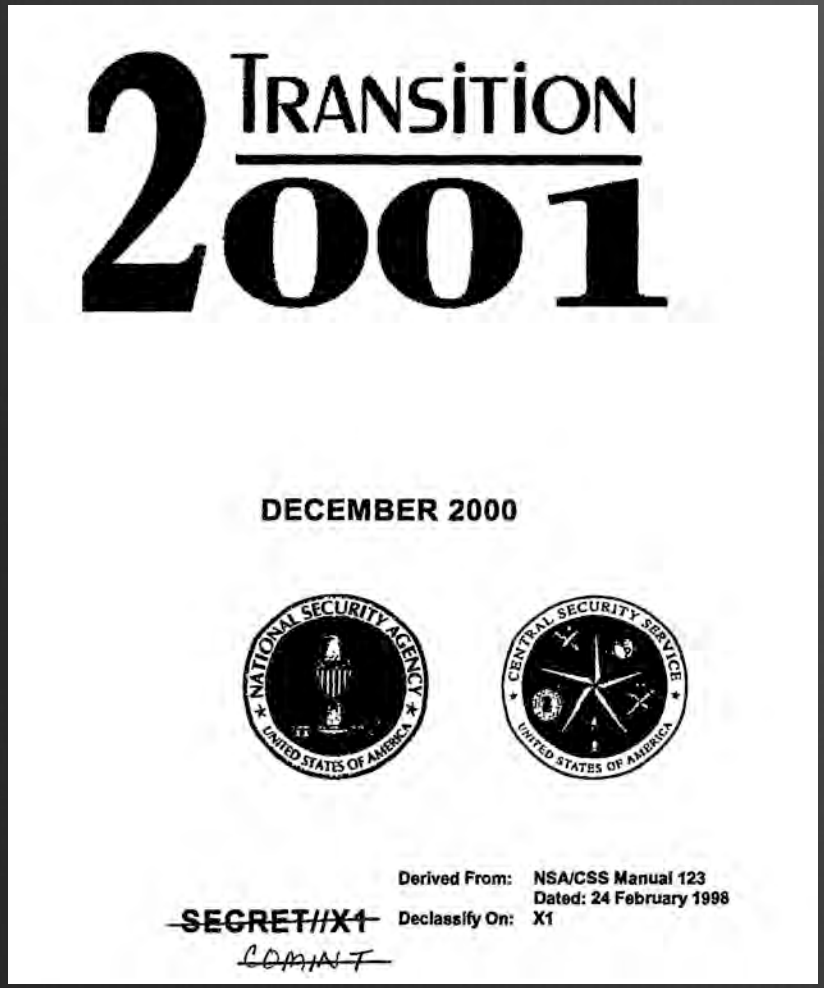
- Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment . . . senior leadership must understand that today's and tomorrow's mission will demand a powerful, permanent presence on a global telecommunications network that **will host the 'protected' communications of Americans as well as the targeted communications of adversaries**.
- National Security Agency/Central Security Service, "National Security Agency/Central Security Service Transition 2001", p. 32.

M. Jones, Columbia @nescioquid

“The Information Age,” huh?

The issue of domestic intelligence gathering and surveillance needs to be revisited. […] intelligence gathering and surveillance are the first line of deterrence and defense against all forms of cyberattack. [CSIS Homeland Defense: Information Warfare, p. 191]

NSA 2001



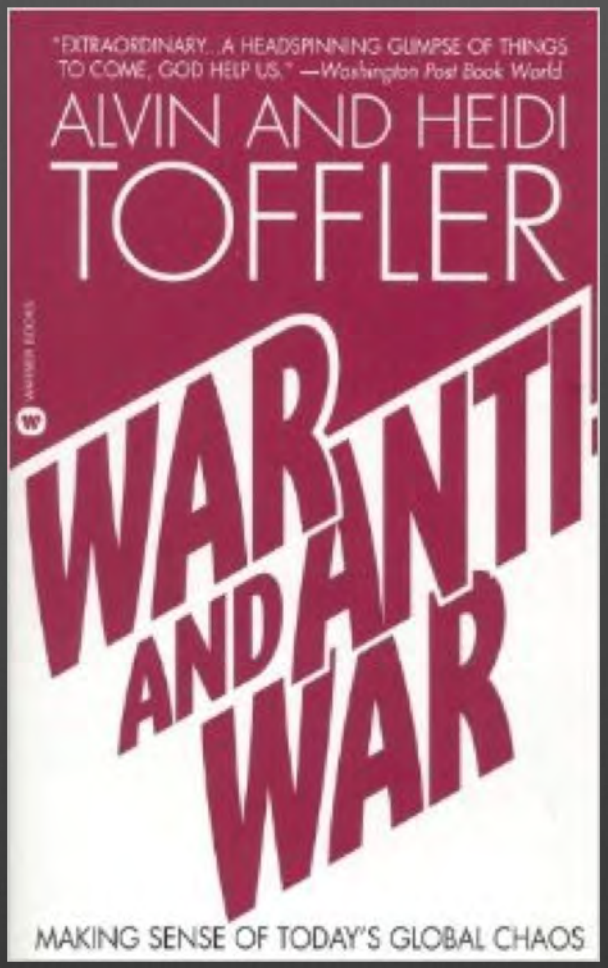
The Fourth Amendment is as applicable to eSIGINT as it is to the SIGINT of yesterday and today. **The Information Age will however cause us to rethink and reapply the procedures, policies and authorities born in an earlier electronic surveillance environment.**

Block Periodization

A Taxonomy for Information Warfare: Three Waves, Three Schools of Thought

WAVE	FIRST (AGRARIAN)	SECOND (INDUSTRIAL)	THIRD (INFORMATION)
PHYSICAL SECURITY PROVIDED BY	A Warrior Class, Mercenaries, Militia	Professional Citizens	Information Knowledgeable Leaders
DOMINANT SOCIAL, POLITICAL, ECONOMIC FORCE	Tribe, City, State	Nation-State	Global Conglomerates
ECONOMY DOMINATED BY	Trade	Money	Symbols
WAR CHARACTERIZED BY	Representational Conflict	Mass Armies	Information Attacks
ULTIMATE DESTRUCTIVE CAPABILITY	Gunpowder	Weapons of Mass Destruction	Critical Information Deletion
INFORMATION IN WARFARE	YES	YES	YES
INFORMATION TECHNOLOGY IN WARFARE	NO	YES	YES
INFORMATION WARFARE	NO	NO	YES

Toefler


"EXTRAORDINARY...A HEADSPINNING GLIMPSE OF THINGS TO COME, GOD HELP US." —Washington Post Book World
ALVIN AND HEIDI
TOFFLER
WAR
AND
ANTI
WAR
MAKING SENSE OF TODAY'S GLOBAL CHAOS

Two regimes of conflict

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

Two regimes of conflict

- De-territorialized, non-Westphalian, Information age
  - Porous nations and non-state actors
    - “homeland” no “sanctuary”
    - Grotian paradigm gone baby gone
  - 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

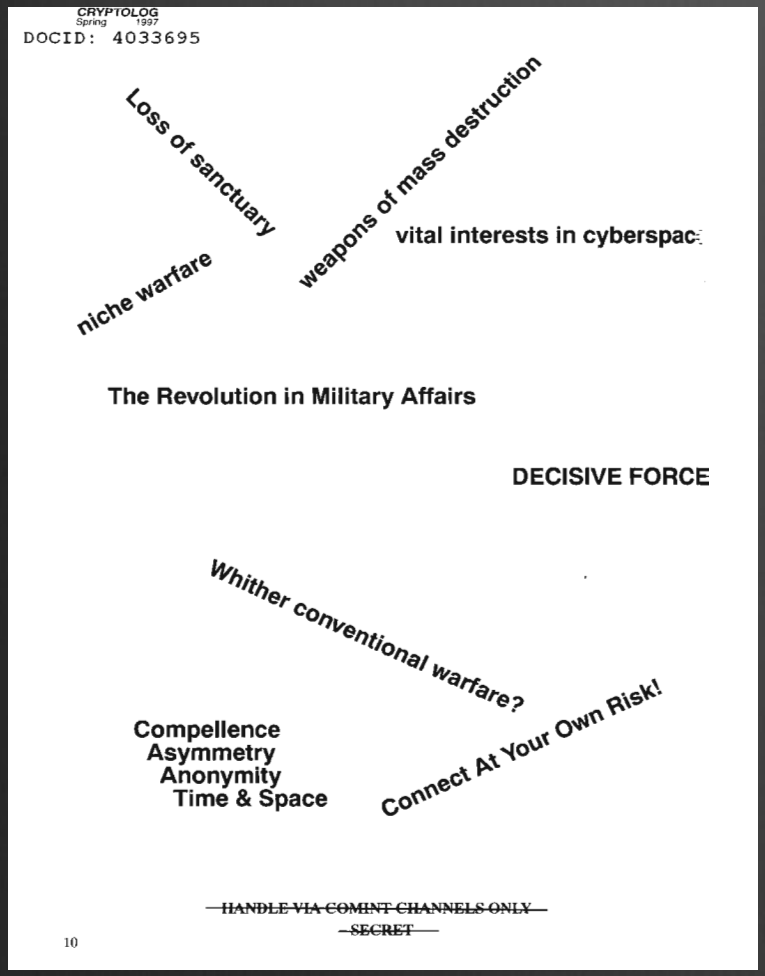
Information war has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the U.S. economy will increasingly rely on complex, interconnected network control systems for such necessities as oil and gas pipelines, electric grids, etc. […]

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

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

DSB Summer Study 2000

Loss of sanctuary



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]

NSA Cryptolog Magazine,1997

M. Jones, Columbia @nescioquid

“modernizing” < 9/11

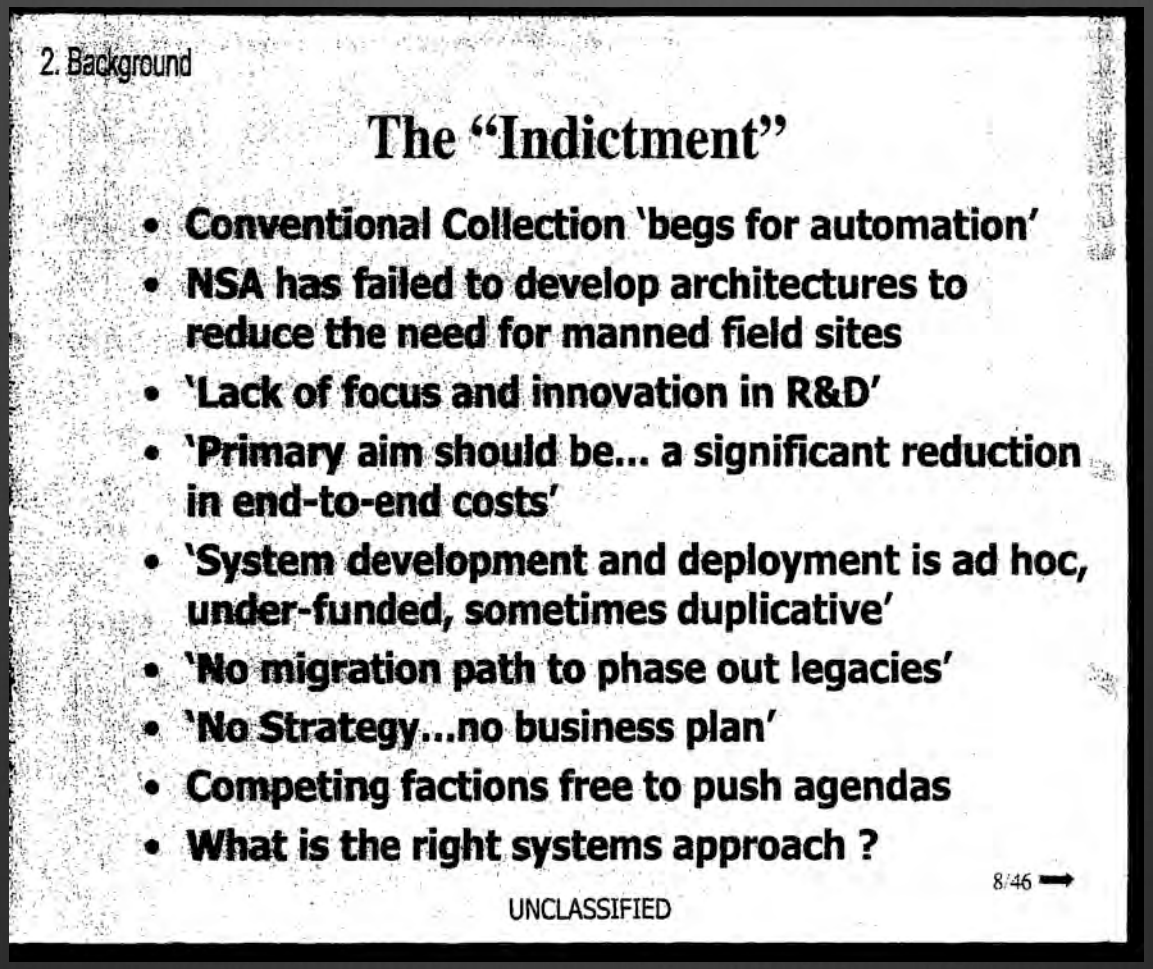
- Deterritorializing regime working within constitutional one
- Setting wheels in motion to
  - Allow interception of foreign packets transiting US
  - Weaken intelligence / domestic crime boundary
  - Allow NSA to play significant role in scanning US
    for vulnerabilities or attacks in action (Critical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

PATRIOT ACT emerges with weeks of 9/11

Contested < 9/11

- NSA/FBI lost “Crypto wars” (a shock)
- NSA considered by many a cold war relic in 1990s
  - NSA lost responsibility for civilian digital infrastructure to NIST
  - Peace dividend killing budget
  - BLEEDING mathematical and CS talent
- Armed services fighting for control of Information Warfare
- NSA UNLIKELY to get its form of “MODERNIZATION” of law

Contested < 9/11

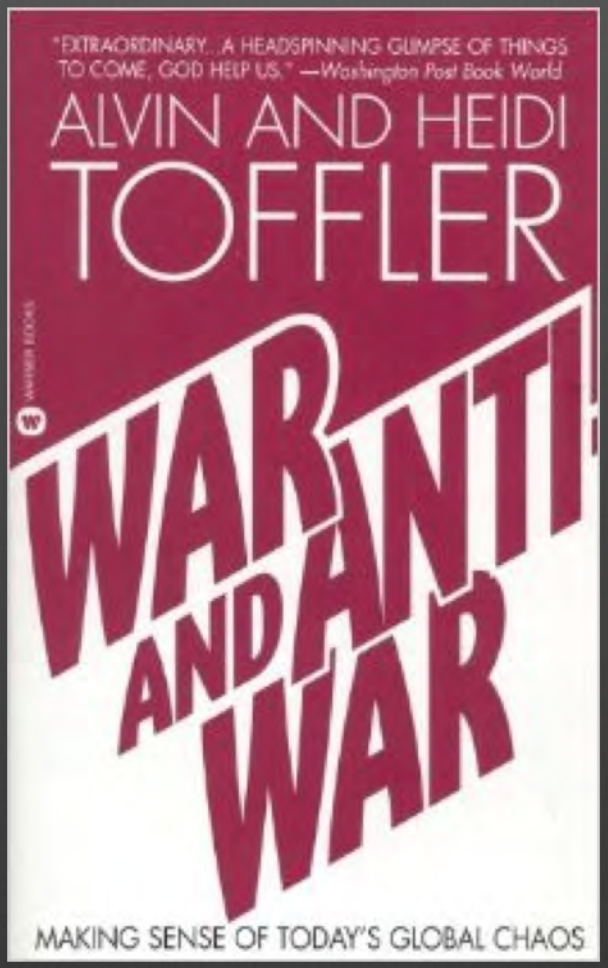


Congressional Indictment of NSA FY 1999 Authorization; Clapper report

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

Toefler



Fighting terrorism, in particular, requires extremely fine graded information and new computerized techniques for getting it. […]

M. Jones, Columbia @nescioquid

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.

Post-westphalian warfare

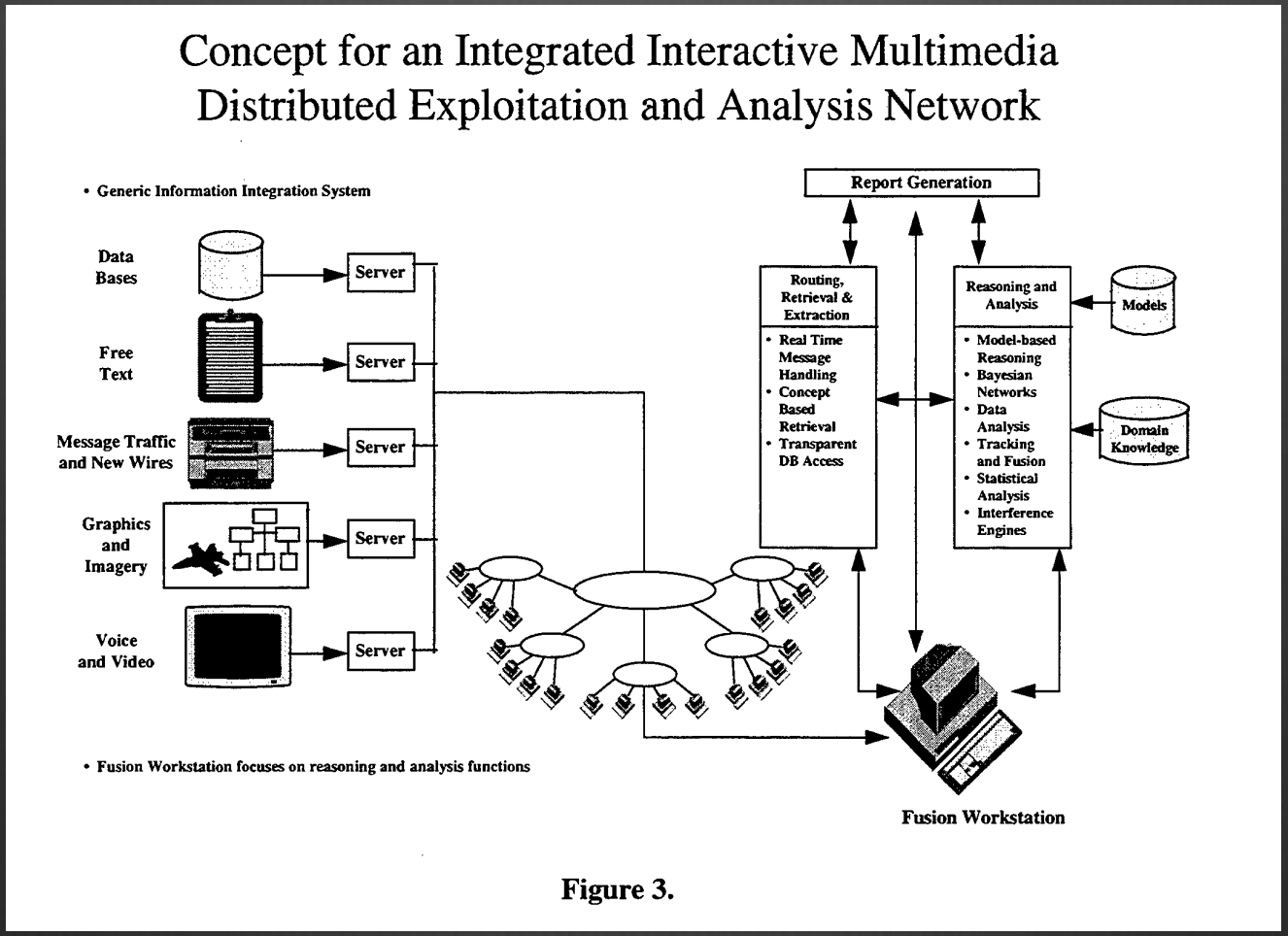


Figure 3.

Andrews, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," appendix B.

Total Information Awareness

LACK OF IRONY A REASONED FACT NOT JUST A FACT

M. Jones, Columbia @nescioquid

“Evidence Extraction and Link Discovery”

“The Evidence Extraction and Link Discovery (EELD) program will develop automated discovery, extraction and linking of sparse evidence in large amounts of classified and unclassified data sources. . . . .It will then link together related items that comprise potential terrorist groups or scenarios, and learn patterns of different groups or scenarios to identify new organizations or emerging threats.”

--Statement by Dr. Tony Tether Director Defense Advanced Research Projects Agency Before the Subcommittee on Military Research and Development Committee on Armed Services House of Representatives (6/26/2001)

M. Jones, Columbia @nescioquid

EELD

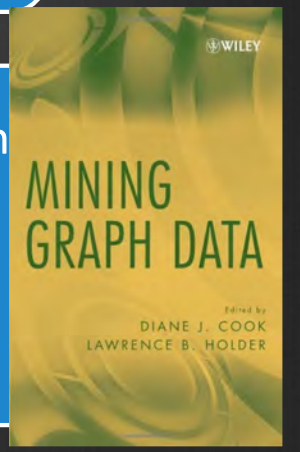
Academic Centers

The KOJAK Group Finder: Connecting the Dots via Integrated Knowledge-Ba… Statistical Reasonin…

(USC)

Graph-based Structural Pattern Learning

(UT-Arlington)



Transformative R…

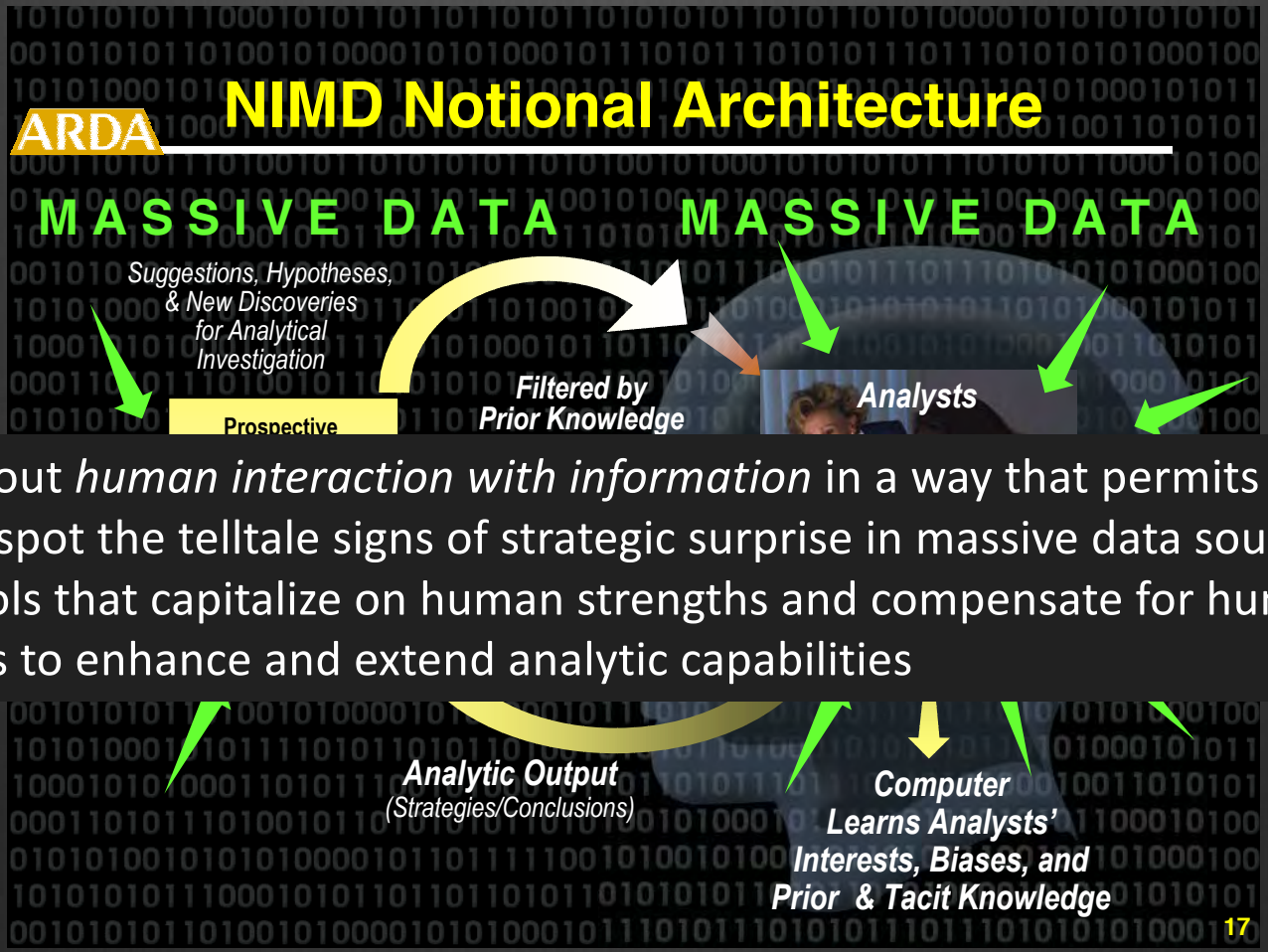
(Knowledge… Labor…

UMass Amherst …

M. Jones, Columbia, @nesciquid

Source: unclassified final reports, available at www.dtic.mil

Advanced Research and Development Activity c. 2002



NIMD is about *human interaction with information* in a way that permits intelligence analysts to spot the telltale signs of strategic surprise in massive data sources - building tools that capitalize on human strengths and compensate for human weaknesses to enhance and extend analytic capabilities

Exploiting the law

Making up Metadata

Computer Network Exploitation

M. Jones, Columbia @nescioquid

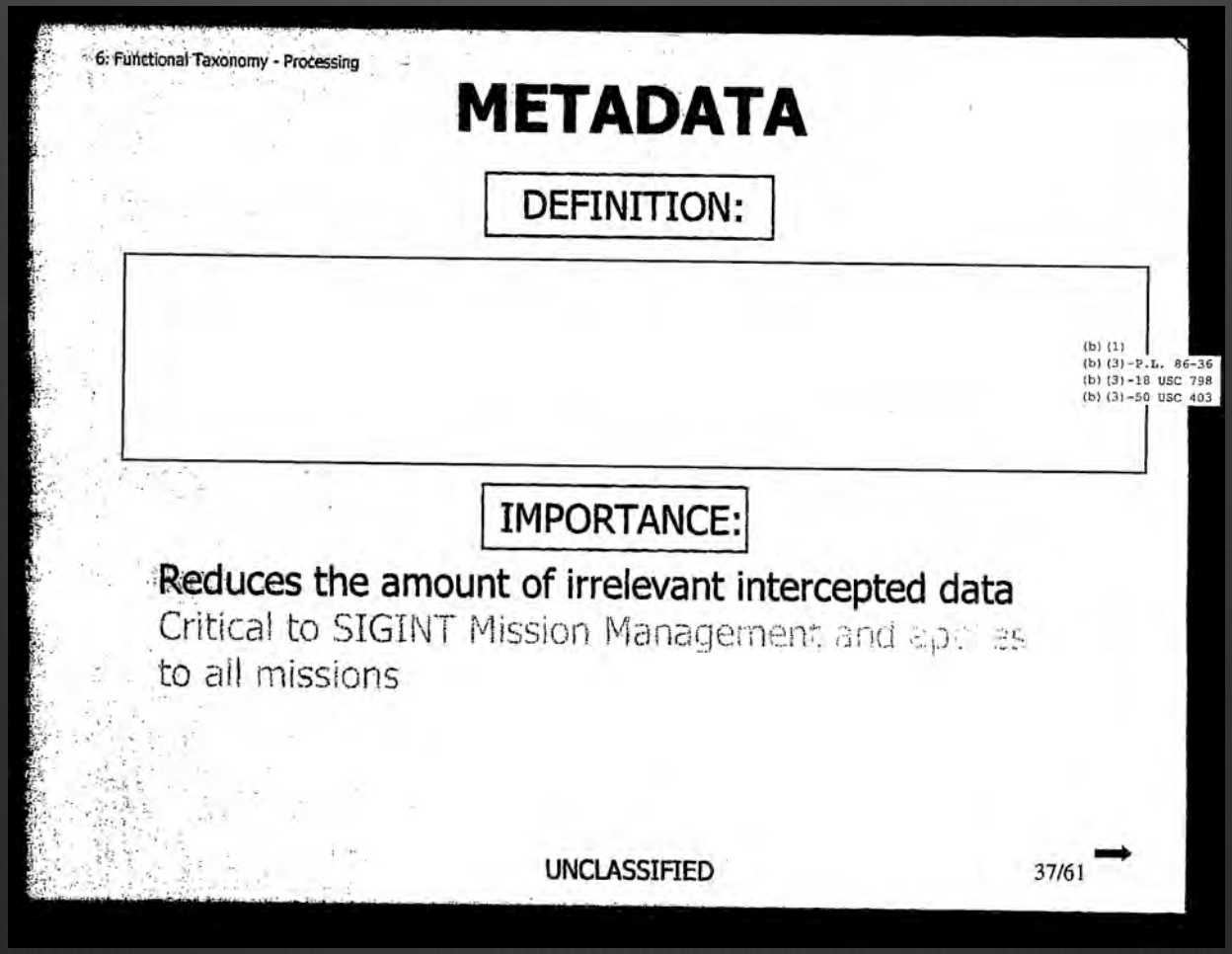
M. Jones, Columbia @nescioquid

Exploiting the law

Making up Metadata

M. Jones, Columbia @nescioquid

Definition too secret…



6: Functional Taxonomy - Processing

METADATA

DEFINITION:

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 403

IMPORTANCE:

Reduces the amount of irrelevant intercepted data
Critical to SIGINT Mission Management and applies to all missions

UNCLASSIFIED 37/61

Smith v. Maryland (1979)

- Supreme Court held that users of telephony have no "reasonable expectation of privacy" in the phone numbers they dial even as they have a reasonable expectation of privacy in the spoken content of their calls.
  - Give dialing information willingly to phone company
  - "Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." (*Smith v. Maryland*, at 743.)

Exploiting the law: metadata

Executive: secret interpretations of law

"metadata" not "interception"

Judicial: negotiation with regulatory court (FISC)

Legislative: reworking of statutory law (FISA)

From Calls to Metadata

- Warrantless wiretapping
- Pen register "use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."
- PATRIOT §216
- "the recording or decoding of electronic or other impulses to the dialing, **routing, addressing**, and signaling information utilized in the **processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications**."

Bifurcation of “communications”

- Metadata (still unnamed in PATRIOT Act)
- Content (delimited and specific)
- FBI fact sheet “Section 216 updated the law to the technology. It ensures that law enforcement will be able to collect non-content information about terrorists' communications regardless of the media they use.”

Smith v. Maryland, exploited

- Supreme Court held that users of telephony have no "reasonable expectation of privacy" in the ~~phone numbers they dial~~ their communications metadata even as they have a reasonable expectation of privacy in the content of ~~calls~~ their communications.

Everyone's metadata?

- Quotation from secret decision with redacted name and date, p. 63
- so "long as no individual has a reasonable expectation of privacy in meta data [sic], the large number of persons whose communications will be subjected to the . . . surveillance is irrelevant to the issue of whether a Fourth Amendment Search or seizure will occur."

Aggregation and privacy interests

- A later ruling:
- “Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in the Fourth Amendment interest springing into being *ex nihilo*.”
- Amended Memorandum Opinion, 8–9 (Foreign Intelligence Surveillance Court 2013), 8.

Two forms of aggregation

Classical UG stats

- Aggregation yield generalization
  - Means
  - Medians
  - Std. deviations
- No privacy interest

Data mining

- Aggregation allow to know *individual* better
  - (at least to predict many qualities about that person)
- Massive privacy interest

Traffic Analytic Revolution

- “In many respects, the break between the Black Chambers and modern cryptology is the invention of traffic analysis, the recognition that cryptologic attack can reveal information of value even when it is successful only in recovering the externals of intercepted communications.”
  - redacted, P054, “Intelligence Analysis: Production and Reporting in a Changed Environment,” *Cryptolog: The Journal of Technical Health*, no. 1 (1995): 20.

SigInt

Cryptographic Analysis

- Decrypting plain text of contents of communication
- What NSA famous for

Traffic analysis

- Reconstructing Networks of Communication, Order of Battle, etc.
- WITHOUT access to CONTENT of communications

Introduction to Traffic Analysis[1]

BY LAMBROS D. CALLIMAHOS

~~*Confidential*~~

~~CONFIDENTIAL~~

TRAFFIC ANALYSIS

Intelligence. The organization of a radio network and the manner in which messages are passed over this network reflect troop disposition, command relationships, and impending movements and preparations for military activity; therefore an analysis of net structure, traffic contacts and patterns, traffic volumes, and similar communications features, is of considerable assistance in building up a complete intelligence picture.

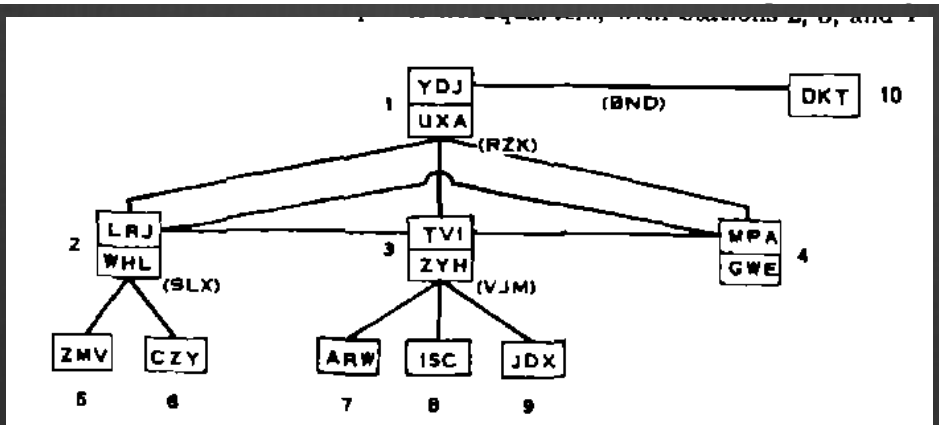


Fig. 1.

Traffic Analytic Revolution

- "The very idea that cryptologists, even when unable to produce plain text (the Holy Grail of the black chambers) could provide valuable, even life saving information to consumers, **revolutionized the field**."
  - William Nolte, "Louis W. Tordella and the Making of NSA," *Cryptolog: The Journal of Technical Health*, no. Spring 1996: iv.
- "The analytic effort to derive useful information from the **externals** of message traffic, [….], ranks as a defining event in cryptologic history. […] traffic analysis pointed to something fundamental about the cryptology of our time: **the fundamental importance of understanding not just the content of communications and the means to hide those contents but of the systems and technologies that carried those communications."**

  "Lessons Learned. Inteview with [redacted]," *Cryptolog: The Journal of Technical Health* Summer 1997: 1.

Envelopes & T/A

Summary

A hypothetical analogy using postal mail may clarify the concept of T/A in more familiar terms. In the case of postal mail, the content of the envelope would be the purview of cryptanalysis, whereas the study of the address, the return address, and the date stamp would be akin to traffic analysis. Study of these external features could reveal identification of banks, stockbrokers, credit unions, employers, doctors, dentists, friends, relatives, etc., and how often and when mail contact is maintained with these recipients. For example, T/A in this context might reveal that an individual had been diagnosed as seriously ill based on communications with doctors and insurance companies, or that the person is under financial stress based on the volume of letters from collection agencies and banks.

12333 annex

(U) Interception. The term "interception" means the acquisition by the United States Signals Intelligence System through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligence form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signal without reference to the information content carried by the signal.

Classified annex to 12333, 1988

TA from cold war to present

Cold War T/A	Post-Westphalian T/A
Electronic order of battle	Threats hidden “in the homeland”
	Massively asymmetric
All military, diplomatic, and political communications	Potentially *all* communications

M. Jones, Columbia @nescioquid

Exploiting the law

Computer network ~~attack~~ exploitation

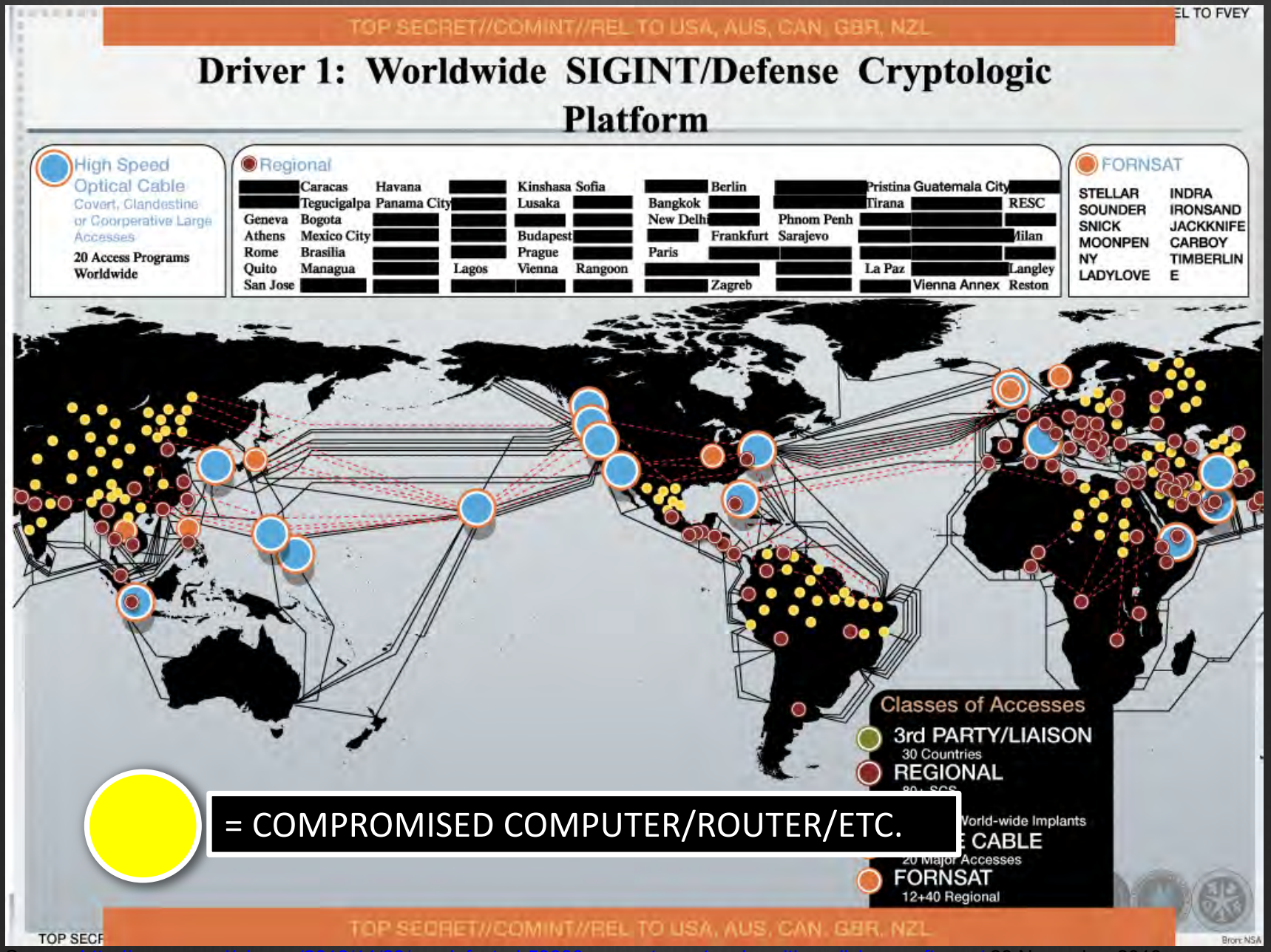
M. Jones, Columbia @nescioquid

Talking point

- Caitlin Hayden, Obama spokesperson: “The United States has made clear it gathers intelligence in exactly the same way as any other states.”

From mining data to banal cracking

- One Farsi speaking analyst describes his work on Linkedin
  - Developed DNI selectors […]. Target[ed] online activities, accounts, and associated identifiers to identify research and development efforts. . . .
  - Utilized numerous DNI and telephony databases and tools to discover new leads, …
  - Identified new targets and further developed current targets to enable TAO exploitation.



Source: http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/ 23 November 2013

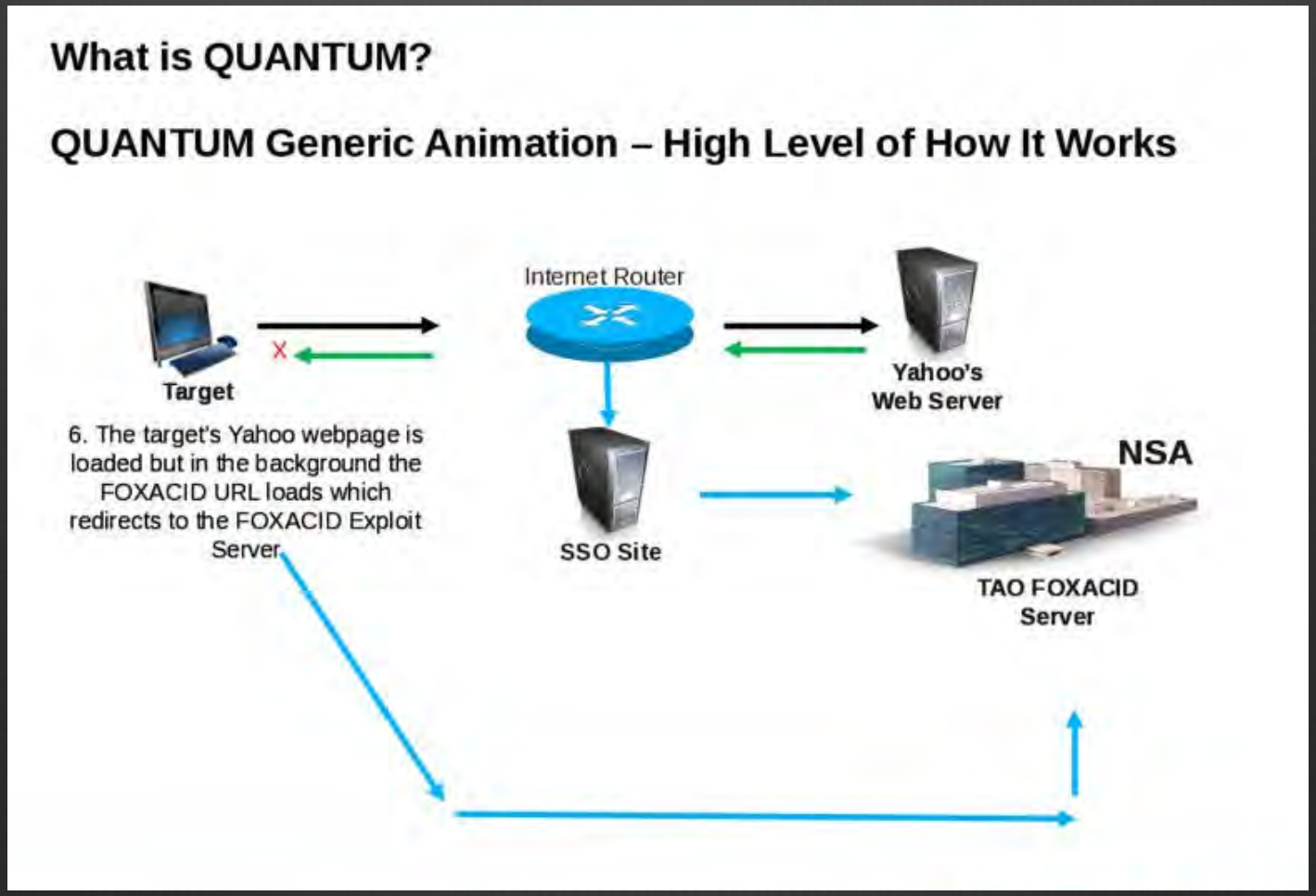
Tailored Access

Tailored Access = build malware to “enable access”

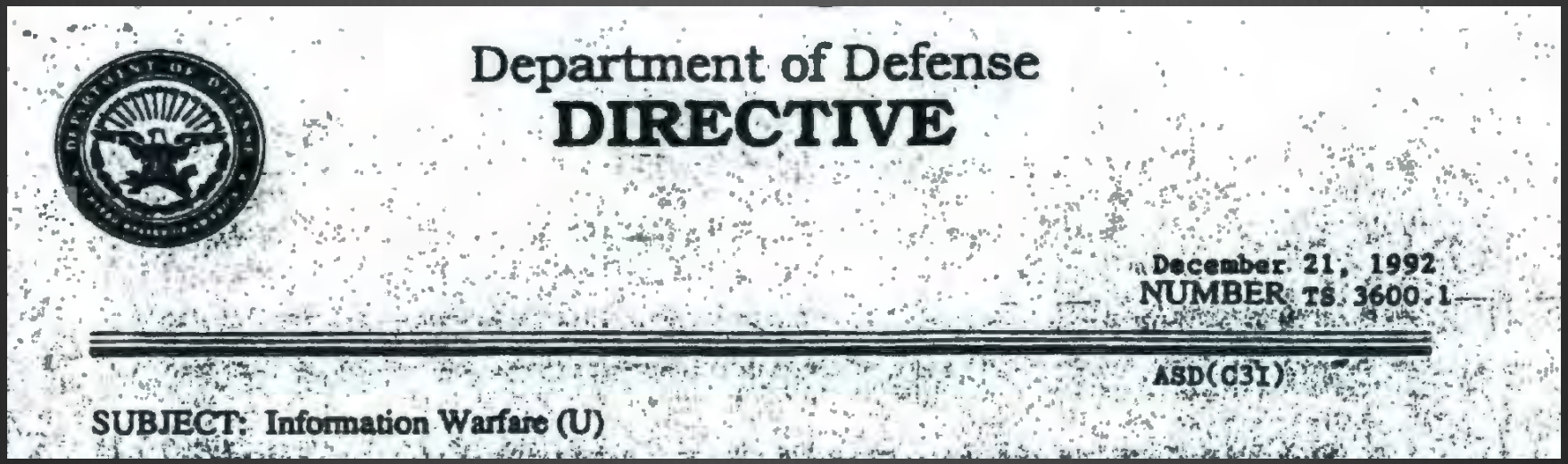
generic (W8.1, basic Tor Linux install),

highly specialized (nuclear centrifuge controller)

Tailored Access



Information Warfare 1.0



Department of Defense

DIRECTIVE

December 21, 1992
NUMBER TS 3600.1

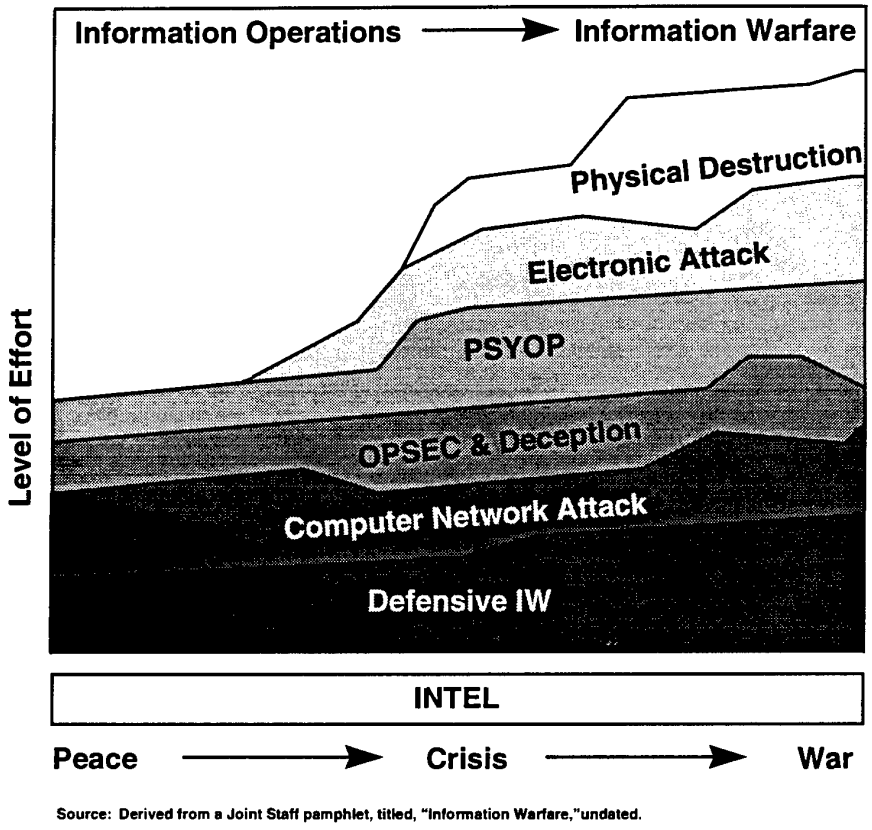
ASD(C3I)

SUBJECT: Information Warfare (U)

(U)

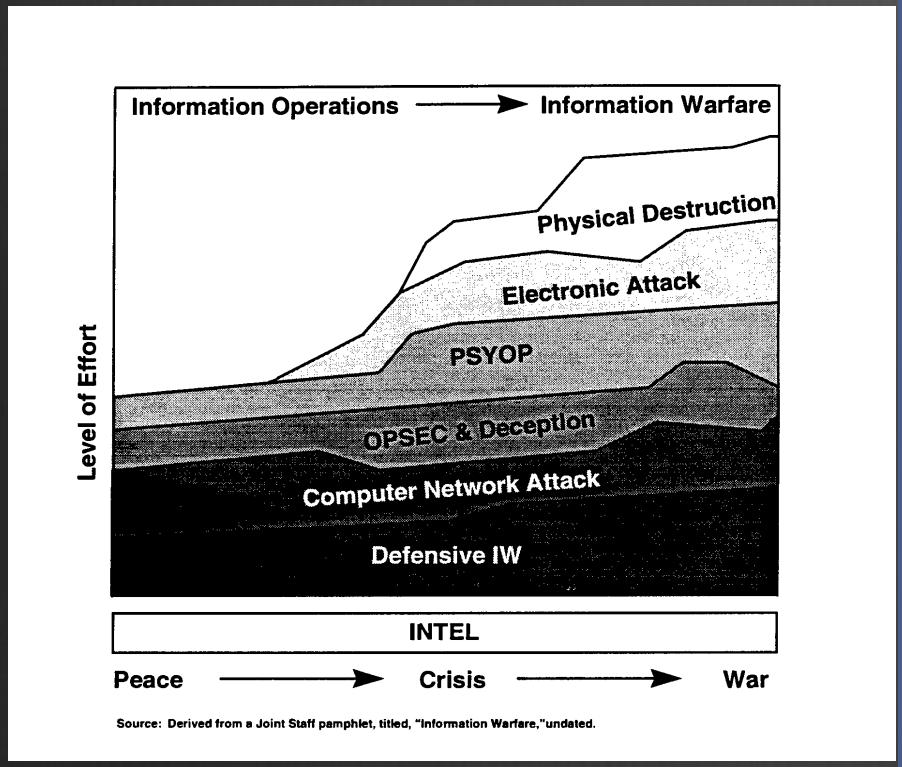
3. [redacted] Information Warfare. The competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information system through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information system from such attacks. The objective of information warfare is to attain a significant enough information advantage to enable the force overall to predominate and to do so quickly.

Computer Network Attack: a bit of honesty



Source: Derived from a Joint Staff pamphlet, titled, "Information Warfare," undated.

Computer Network Attack: euphemism



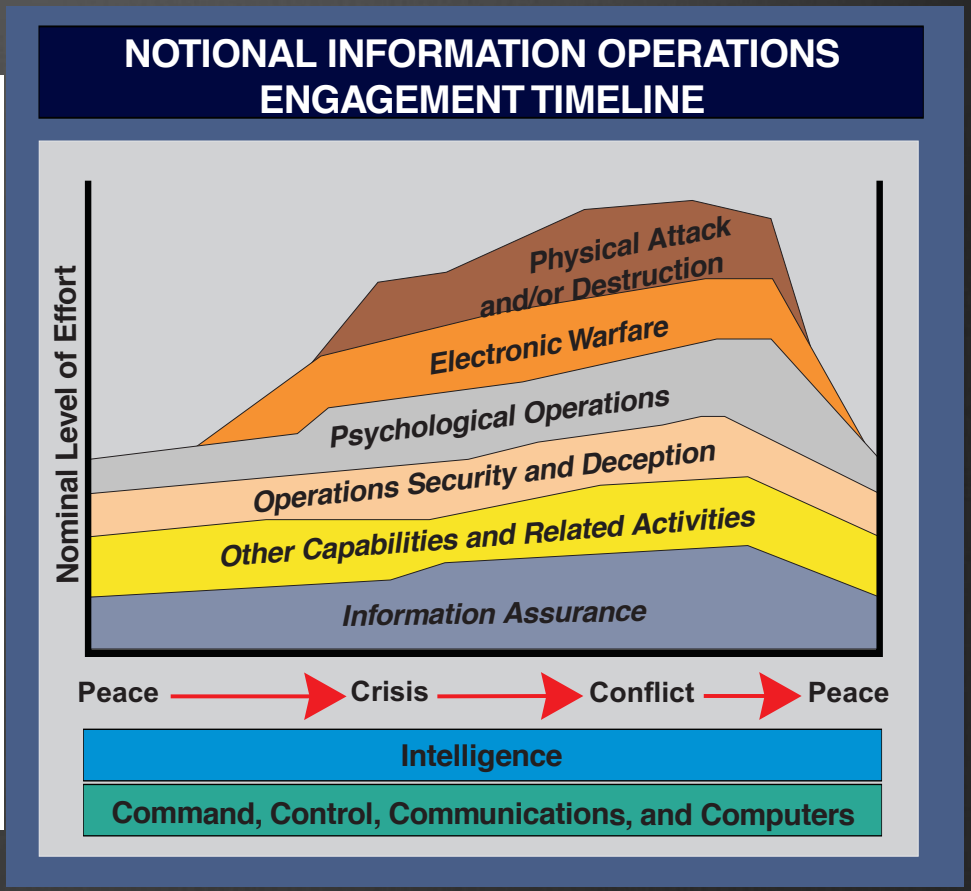


Figure II-2. Notional Information Operations Engagement Timeline

JP3-13, 1996, p. II-8

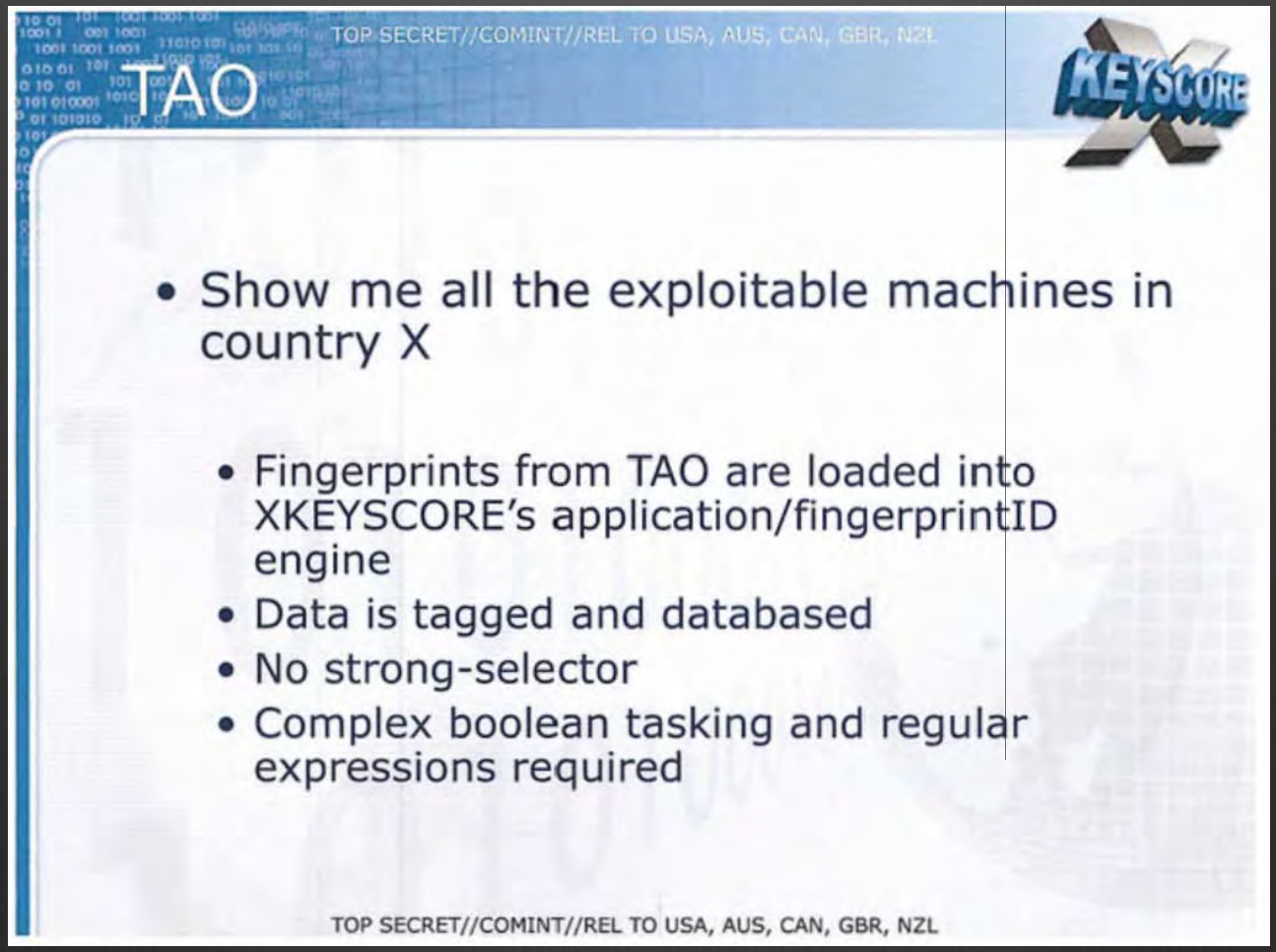
Severing “exploitation” from “attack”

- Creation of new category c 1998
- computer network exploitation [CNE]— Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
- Such cracking *not offensive warfare*—a tertium quid

CNE as espionage

- The treatment of espionage under international law may help us make an educated guess as to how the international community will react to information operations activities. . . . If the activity results only in a breach of the perceived reliability of an information system, **it seems unlikely that the world community will be much exercised**. In short, information operations activities are likely to be regarded much as is espionage - not a major issue unless significant practical consequences can be demonstrated."
- Johnson, "An Assessment of International Legal Issues in Information Operations," 40.

Not bespoke: CNE at scale



Turbine

(TS//SI//REL) TURBINE manages the active implants that make up the Active SIGINT system.
Active SIGINT offers a more **aggressive** approach to SIGINT.
We retrieve data through intervention in our targets' computers or network devices. Extract data from machine. This is: Tailored Access Operations!

One of the greatest challenges for Active SIGINT/attack is **scale**. Human "drivers" limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)
The TURBINE infrastructure will allow the current implant network to scale to large size (millions of implants) by creating a system that does **automated control implants by groups** instead of individually.
Expert System (resource and operations manager) is like the **brain** it manages the applications and functions of implants.
Decides which tools should be provided to a given implant and executes the rules on how it should be used
Decisions of the expert system are passed to the **command and control modules**, which execute the decision against the appropriate set of implants.
Diode is a device that allows connectivity from the high side to the low side network without human intervention.

“Cyber collection”

- Operations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the **primary purpose** of collecting intelligence. . . .from computers, information or communications systems, or networks with the intent to remain undetected. Cyber collection entails accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. **Cyber collection includes those activities essential and inherent to enabling cyber collection, such as inhibiting detection or attribution, even if they create cyber effects.”**

- “Presidential Policy Directive (PPD)-20: U.S. Cyber Operations Policy,” 2–3.

“Cyber effects”

- “The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.”

- Espionage, then, often will be attack in all but name.

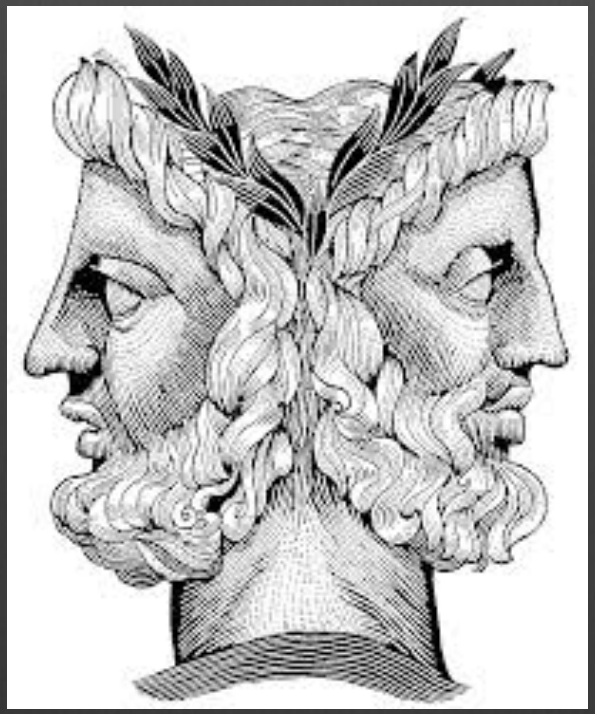
Best defense= good offence

- Active defense “requires that we have the best possible intelligence on the capabilities and intentions of potential attackers, the ability to use that knowledge to deter attacks whenever possible, and the tools and techniques necessary to detect and respond to attacks that do occur” (Minihan, Director, NSA, 1998)
- The best cyber defense, it has been decided in secret, is a cyber offence. And that offence rests on weakening some of the most obvious forms of defense.
- The NSA does not systematically help everyone patch all the holes in our laptops, our phones, our printers.

Janus Faced Agency

SigInt

Exploit communications



Information Assurance

Protect Communications

(COMSEC)

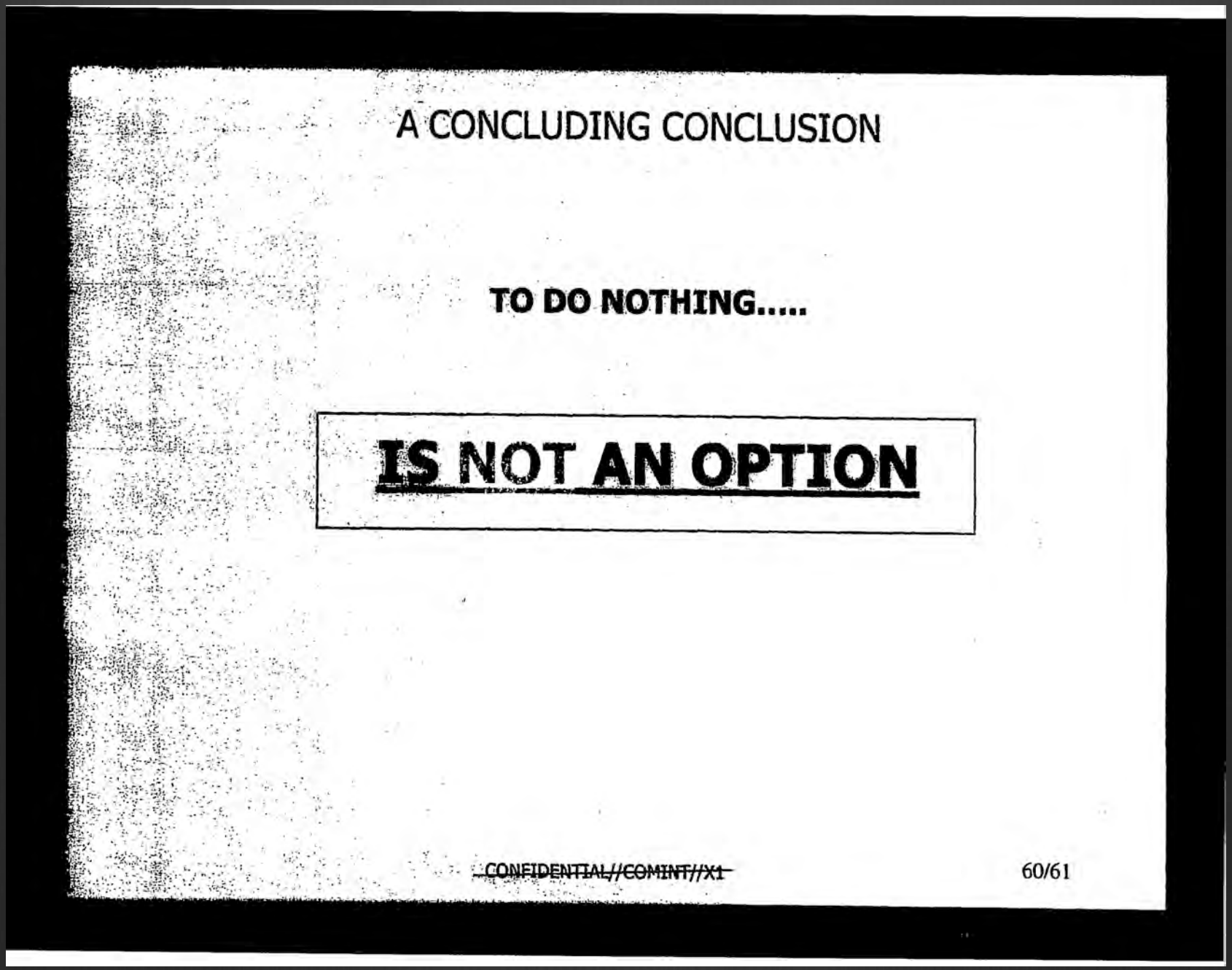
M. Jones, Columbia @nescioquid

NSA then and now

- "NSA Valued in the 1980s, Accuracy, Deep Knowledge, Thorough expertise, Productivity and Reputation […]."

- "NSA valued in the 2000s […] Speed-getting it 80 percent right now could make all the difference in saving lives. (Of course, if it were targeting information that would mean killing innocents 20 percent of the time.)"

    - redacted, "NSA Culture, 1980s to the 21st Century--a SID Perspective," *Cryptological Quarterly* 30, no. 4 (n.d.): 84.


A CONCLUDING CONCLUSION
TO DO NOTHING.....
IS NOT AN OPTION
~~CONFIDENTIAL//COMINT//X1~~
60/61