

**UCLA**  
**limn**

**Title**

The Spy Who Pwned Me

**Permalink**

<https://escholarship.org/uc/item/5300241s>

**Journal**

limn, 1(8)

**Author**

Jones, Matthew L.

**Publication Date**

2017-06-22

**Copyright Information**

This work is made available under the terms of a Creative Commons Attribution-ShareAlike License, available at <https://creativecommons.org/licenses/by-sa/3.0/>

# THE SPY WHO

HOW DID WE GET TO STATE-SPONSORED HACKING?  
**MATT JONES** TRACES THE LEGAL AUTHORITIES AND  
TECHNICAL CAPACITIES THAT HAVE TRANSFORMED THE  
POWER OF THE NATION-STATE SINCE THE 1990S.

# PWNED ME



## U.S. INTELLIGENCE OFFICERS DISCUSS

Chinese espionage in dramatically different terms than they use in talking about the Russian interference in the U.S. presidential election of 2016. Admiral Michael Rogers, head of NSA and U.S. Cyber Command, described the Russian efforts as “a conscious effort by a nation state to attempt to achieve a specific effect” (Bocugno 2016). The former director of NSA and subsequently CIA, General Michael Hayden, argued, in contrast, that the massive Chinese breach of records at the U.S. Office of Personnel Management was “honorable espionage work” of a “legitimate intelligence target” (American Interest 2016; Gilman et.al 2017). Characterizing the Chinese infiltration as illegal hacking or warfare would challenge the legitimacy of state-sanctioned hacking for acquiring information and would upset the norms permitting every state to hack relentlessly into each other’s information systems.

The hairsplitting around state-sanctioned hacking speaks to a divide between the doctrinal understanding of intelligence professionals and the intuitions of non-professionals. Within intelligence and defense circles of the United States and its close allies, peacetime hacking into computers with the primary purpose of stealing information is understood to be radically different than using hacked computers and the information from them to cause what are banally called “effects”—from breaking hard drives or centrifuges, to contaminating the news cycles of other states, to playing havoc with electric grids. One computer or a thousand, the size of a hack doesn’t matter: scale doesn’t transform espionage into warfare. Intent is key. The Chinese effort to steal information: good old espionage, updated for the information age. The Russian manipulation of the election: information or cyber warfare.

Discussing the OPM hack, Gen. Hayden candidly acknowledged,

*If I as director of CIA or NSA would have had the opportunity to grab the equivalent [employee records] in the Chinese system, I would not have thought twice... I would not have asked permission. I would have launched the Starfleet, and we would have brought those suckers home at the speed of light.<sup>1</sup>*

Under Hayden and his successors, NSA has certainly brought suckers home from computers worldwide. Honorable computer espionage has become multilateral, mundane, and pursued at vast scale.<sup>2</sup>

In February 1996 John Perry Barlow declared to the “Governments of the Industrial World,” that they “have no sovereignty where we gather”—in cyberspace (Barlow 1996). Whatever their naivety in retrospect, such claims in the 1990s from right and left, from civil libertarians as well as defense hawks, justified governments taking preemptive measures to maintain their sovereignty. Warranted or not, the fear that the Internet would weaken the state fueled its dramatic, mostly secret, expansion at the beginning of the current century. By understanding the ways state-sponsored hacking exploded from the late 1990s onward, we see more clearly the contingent interplay of legal authorities and technical capacities that created the enhanced powers of the nation-state.

How did we get a mutual acceptance of state-sanctioned hacking? In a legal briefing for new staff, NSA tells a straightforward story of the march of technology. The movement from telephonic and other communication to the mass “exploitation” of computers was “a natural transition of the foreign collection mission of SIGINT” (signals intelligence). As communications moved from telex to computers and switches, NSA pursued those same communications” (NSA OGC n.d.). Defenders of NSA and its partner agencies regularly make similar arguments:

anyone unwilling to accept the necessity of government hacking for the purposes of foreign intelligence is seen as having a dangerous and unrealistic unawareness of the threats nations face today. For many in the intelligence world today, hacking into computers and network infrastructures worldwide is, quite simply, an extension of the long-standing mission of “signals intelligence”—the collection and analysis of communications by someone other than the intended recipient.

Contrary to the seductive simplicity of the NSA slide, little was natural about the legalities around computer hacking in the 1990s. The legitimization of mass hacking into computers to collect intelligence wasn’t technologically or doctrinally pre-given, and hacking into computers didn’t—and doesn’t—easily equate to earlier forms of espionage. In the late 1990s and 2000s, information warfare capacities were being developed, and authority distributed, before military doctrine or legal analysis could solidify.<sup>3</sup> Glimpsed even through the fog of classification, documents from the U.S. Department of Defense and intelligence agencies teem with discomfort, indecision, and inter-necine battles that testify to the uncertainty within the military and intelligence communities about the legal, ethical, and doctrinal use of these tools. More “kinetic” elements of the armed services focused on information warfare within traditional conceptions of military activity: the destruction and manipulation of the enemy command and control systems in active battle. Self-appointed modernizers demanded a far more encompassing definition that suggested the distinctiveness of information warfare and, in many cases, the radical disruption of traditional kinetic warfare.

The first known official Department of Defense definition of “Information Warfare,” promulgated in an only recently declassified 1992 document, comprised:

1 In conversation with Gerard Baker, June 15, 2015. Available at link.

2 For the current state of international consensus on cyber espionage among international lawyers, see Schmitt 2017, rule 32.

3 See Berkowitz 2003:59-65; Rattray 2003; Rid 2016:294-339 and Kaplan 2016

## Authority to conduct CNE

- (S) EO 12333 assigns NSA the Signals Intelligence (SIGINT) Mission, **which includes COMINT and in turn CNE.**
- (U) CNE evolved as a natural transition of the foreign intelligence collection mission of SIGINT. As communications moved from telex to computers and switches, NSA pursued those same communications.
- (U) 2 type of CNE activities:
  - (U) **Collection Activities-** designed to acquire foreign intelligence information from the target computer system.
  - (S) **Enabling Activities-** designed to obtain or facilitate access to the target computer system for possible later CNA, or force use of alternate communication systems.

Classification: TOP SECRET//COMINT//Rel 4  
EYES/20291123

FIGURE 1: "Authority to Conduct CNE."  
(NSA OFFICE OF GENERAL COUNSEL, N.D.8)

and dissemination of information has been a stumbling block in gaining understanding and acceptance of the concepts surrounding information warfare" (Kuehl 1997). Information warfare had to encompass collection of intelligence, deception, and propaganda, as well as more warlike activities such as deletion of data or destruction of hardware. Exploitation had to become peaceful.

Around 1996, a new doctrinal category, "Computer Network Exploitation" (CNE), emerged within the military and intelligence communities to capture the hacking of computer systems to acquire information from them.<sup>5</sup> The definition encompassed the acquisition of information but went further. "Computer network exploitation" encompassed collection and enabling for future use. The military and intelligence communities produced a series of tortured definitions. A 2001 draft document offered two versions, one succinct,

*Intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) or networks.*

and the other clearer about this "enabling":

*Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. CNE is composed of two types of activities: (1) enabling activities designed to obtain or facilitate access to the target computer system where the purpose includes foreign intelligence collection; and, (2) collection activities designed to acquire foreign intelligence information from the target computer system (Wolfowitz 2001:1-1).*

*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 systems from such attacks (DODD TS 3600.1 1992:1).*

Under this account, warfare included "exploitation": the acquiring of information from an adversary's computers whether practiced on or by the United (ibid.:4).<sup>4</sup> A slightly later figure (Figure 2) illustrates this inclusion of espionage in information warfare.

According to an internal NSA magazine, information warfare was "one of the new buzzwords in the hallways" of the Agency by 1994 (Redacted 1994:3). Over the next decade, the military services competed with NSA and among themselves over the

definition and partitioning of information warfare activities. One critic of letting NSA control information warfare worried about "the Intelligence fox being put in charge of the Information Warfare henhouse" (Rothrock 1997:225).

Information warfare techniques were too valuable only to be used in kinetic war, a point Soviet strategists had long made. By the mid-1990s, the U.S. Department of Defense had embraced a broader doctrinal category, "Information Operations" (DODD S-3600 1996). Such operations comprised many things, including "computer network attack" (CNA) and "computer network defense" (CND) as well as older chestnuts like "psychological operations." Central to the rationale for the renaming was that information warfare-like activities did not belong solely within the purview of military agencies and they did not occur only during times of formal or even informal war. One influential strategist, Dan Kuehl, explained, "associating the word 'war' with the gathering

4 Drawn from the signals intelligence idiolect, "exploitation" means, roughly, making some qualities of a communication available for acquisition. With computers, this typically means discovering bugs in systems, or using pilfered credentials, and then building robust ways to gain control of the system or at least to exfiltrate information from it.

5 Computer Network Exploitation (CNE) was developed alongside two new doctrinal categories emerging in 1996: more aggressive "Computer Network Attack," (CNA) which uses that access to destroy information or systems, and "Computer Network Defense" (CND). For exploitation versus attack, see (Owens et. al. 2009; Lin 2010:63).

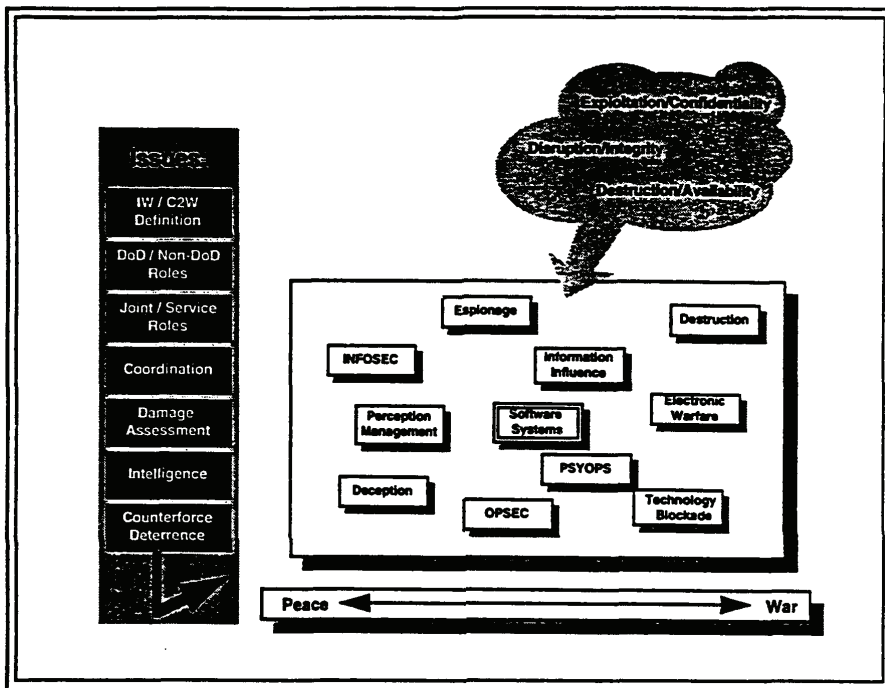


FIGURE 2: "Information Warfare."

(FIELDS AND MCCARTHY 1994: 27)

FIGURE 3 (BELOW): Information warfare is different.

(ANDREWS 1996:3-2).

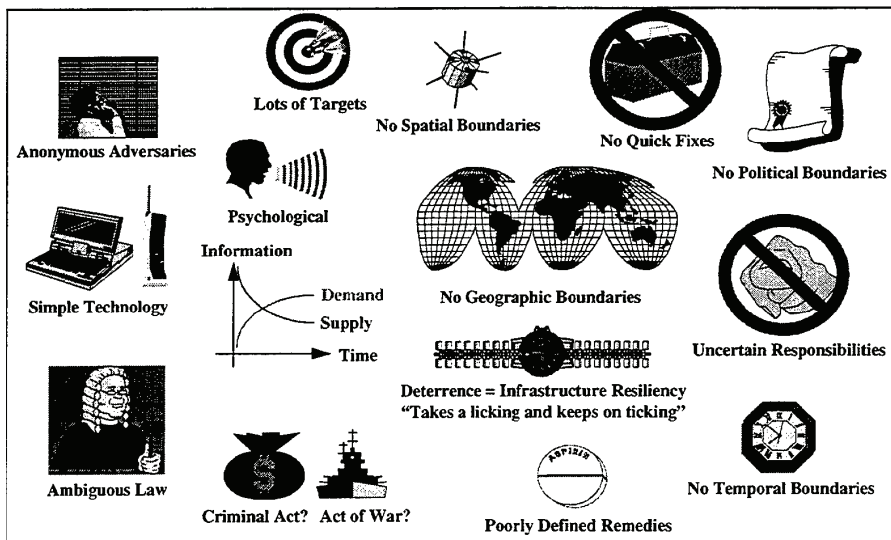
category, "enabling" was hived off from *offensive warfare*, to clarify that exploiting a machine—hacking in and stealing data—was not an attack. It was espionage, whose necessity and ubiquity everyone ought simply to accept.

The new category of CNE subdued the protean activity of hacking and put it into an older legal box—that of espionage. The process of hacking into computers for the purpose of taking information and enabling future activities during peacetime was thus grounded in pre-existing legal foundations for signals intelligence. In contrast to the flurry of new legal authorities that emerged around computer network attack, computer network exploitation was largely made to rest on the hoary authorities of older forms of signals intelligence.<sup>6</sup>

A preliminary DoD document captured this domestication of hacking in 1999:

*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. . . . international reaction is likely to depend on the practical consequences of the activity. If lives are lost and property is destroyed as a direct consequence, the activity may very well be treated as a use of force. 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 1999:40; emphasis added).

In justifying computer espionage, military and intelligence thinkers rested on a Westphalian order of ordinary state



Enabling operations were carefully made distinct from *affecting* a system, which takes on a war-like demeanor. Information operations involved "actions taken to affect adversary information and information systems, while defending one's own information and information systems" (CJCSI 3210.1A 1998). CNE was *related to* but was not in fact an informa-

tion "operation." A crucial 1999 document from the CIA captured the careful, nearly casuistical, excision of CNE from Information Operations: "CNE is an intelligence collection activity and while not viewed as an integral pillar of DoD IO doctrine, it is recognized as an IO-related activity that requires deconfliction with IO" (DCID 7/3 2003: 3). With this new

6 Especially NSCID-6 and Executive Order 12,333. The development of satellite reconnaissance had earlier challenged mid twentieth century conceptions of espionage. For a vivid sense of the difficulty of resolving these challenges, see (Falk 1962: 45-82).

relations with long standing norms. At the very moment that the novelty of state-sanctioned hacking for information was denied, however, a range of strategists and legal thinkers expounded how the novelty of information warfare would necessitate a radical alteration of the global order.

**BEYOND WESTPHALIA**

Mirroring Internet visionaries of left and right alike, military and defense wonks in the 1990s detailed how the Net would undermine national sovereignty. An article in RAND's journal in 1995 explained,

*Information war has no front line. Potential battlefields are anywhere networked systems allow access—oil and gas pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack*

*(Rand Research Review 1995; emphasis added.)*

In this line of thinking, a wide array of forms of computer intrusion became intimately linked to other forms of asymmetric dangers to the homeland, such as biological and chemical warfare.

The porousness of the state in the global information age accordingly demanded an expansion—a hypertrophy—of state capacities and legal authorities at home and abroad to compensate. The worldwide network of surveillance revealed in the Snowden documents is a key product of this hypertrophy. In the U.S. intelligence community, the challenges of new technologies demanded rethinking Fourth Amendment prohibitions against unreasonable search and seizure. In a document intended to gain the support of the incoming presidential administration, NSA explained in 2000,

*Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment and*

**Diversity is the Password to Your Career Satisfaction at NSA.**

**Engineers...Computer Scientists...Mathematicians... Language Specialists**

Unparalleled diversity in the technologies of the future and in all types of assignments awaits you at the National Security Agency. At NSA, we're charged with the unique missions of collecting, analyzing and assessing foreign signals, as well as with safeguarding our government's vital communications and ensuring its massive computer systems. To carry out these unique missions, we continually develop the most sophisticated technologies and advanced techniques, often years in advance of their commercial use. At NSA, you'll find the kind of equipment, support facilities and technical assistance that many companies and private labs dream about, including a computer complex so vast that it's measured in acres.

NSA's diversity of 21st century technologies also gives you the opportunity to move freely among a wide variety of organizations and assignments within the Agency and for resultant rapid career advancement.


We currently have positions available for individuals with interests and experience in the following areas:

- Electrical Engineering**  
(Minimum of BS/EE required)  
Electrical Engineers work across the technological and functional spectrum. Opportunities range from fundamental research through advanced development, small to large system design and prototype development, developmental test and evaluation, field installation and operational support.
- Computer Security and Networking**  
Hardware and Software Design, Development and Interface  
Microprocessor Implementation and Programming  
LSI/VLSI Analog and Digital Design  
Secure Communications and Analysis
- Signals Analysis and Processing**  
RF and Microwave Systems  
Speech Processing  
Logic Design  
Contract Management  
C/AD/AM  
Systems Acquisition  
Optics  
EW  
Systems Architecture and Design
- Computer Science**  
(Minimum of BS in Computer Science required)  
Our Computer Scientists work with Electrical Engineers and Mathematicians across the frontier of finite state machine development and applications.
- Networking**  
Computer Security Applications  
Graphics
- Systems Design and Analysis**  
Software Engineering  
Operating Systems  
DBMS
- Mathematics**  
(Minimum of BA/BS in Math required)  
Work in a challenging research environment using a variety of mathematical concepts, including algebra, probability theory, statistics, Galois theory and group theory.
- Cryptanalysis**  
**Cryptography**  
**Algorithm Development**
- Computer Architecture**  
**Operations Research**  
**Mathematical Engineering**

**Language**  
(Minimum of BA in specified language or native proficiency)  
As a Language Specialist, you'll be transcribing, translating, analyzing or reporting on material that involves matters of utmost concern to the security of the United States.

- Slavic
- Near Eastern
- Asian
- African

In addition to the challenges and career rewards of diverse projects, NSA offers competitive salaries and benefits plus, most importantly, the opportunity to make your own crucial contribution to an informed and secure environment for our nation's policymaking. Discover your password to job satisfaction today. Send your resume to:

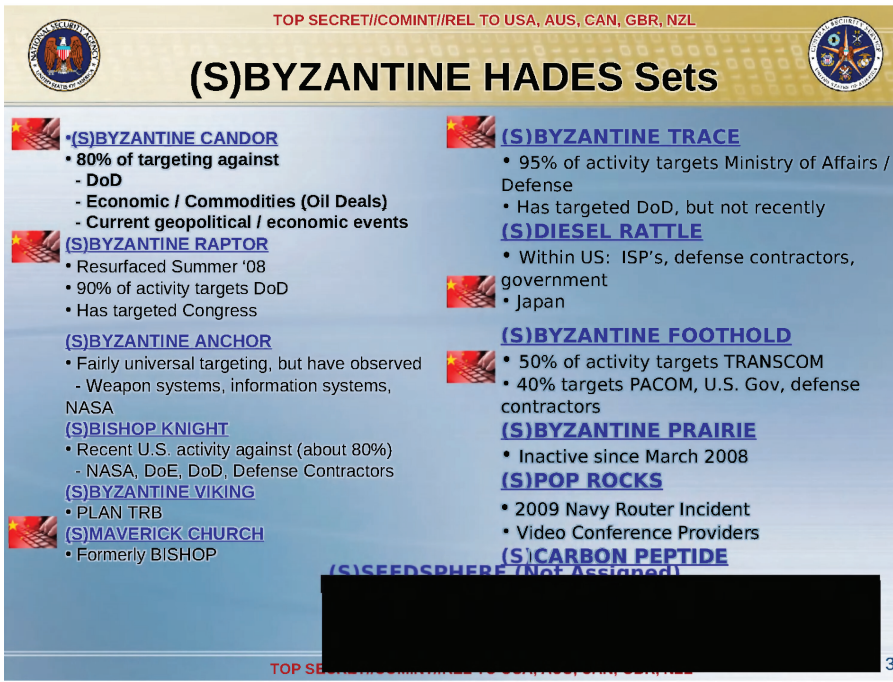
 Unheard of Career Opportunities  
NATIONAL SECURITY AGENCY  
ATTN: M323 (IAD)  
Fort Meade, MD 20778-6000  
U.S. citizenship required  
We are an equal opportunity employer

*all applicable laws. But 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*

*(NSA 2000:32).*

The briefing for the future president and his advisors delivered the hard truths of the new millennium. In the mid- to late 1990s, technically minded circles in

the Departments of Defense and Justice, in corners of the Intelligence Community, and in various scattered think tanks around Washington and Santa Monica began sounding the call for a novel form of homeland security, where military and law enforcement, the government and private industry, and domestic and foreign surveillance would necessarily mix in ways long seen as illicit if not illegal. Constitutional interpretation, jurisdictional divisions, and the organization of bureaucracies alike would need to undergo dramatic—and painful—change. In a remarkable draft "Road Map for National Security" from 2000, a centrist bi-



**FIGURE 4:** NSA's list of major Chinese CNE efforts, called "BYZANTINE HADES." (REDACTED-NTOC 2010).

*perspective (i.e., low cost of entry, few tangible observables, a diverse and expanding target set, increasing amounts of 'freely available' information to support target development, and a flexible base of deployment where being 'in range' with large fixed field sites isn't important) present a particularly difficult problem for the defense... before you get too excited about this 'target-rich environment,' remember, General Custer was in a target-rich environment too! (Redacted 1997: 9; emphasis added).*

The Air Force and NSA pioneered computer security from the late 1960s: their experts warned that the wide adoption of information technology in the United States would make it the premier target-rich environment (Hunt 2012). NSA's capacities developed as China, Russian, and other nations dramatically expanded their own computer espionage efforts (see figure 4 for the case of China c. 2010).

By 2008, and probably much earlier, the Agency and its close allies probed computers worldwide, tracked their vulnerabilities, and engineered viruses and worms both profoundly sophisticated and highly targeted. Or as a key NSA hacking division bluntly put it: "Your data is our data, your equipment is our equipment—anytime, anyplace, by any legal means" (SID Today 2006: 2).

While the internal division for hacking was named "Tailored Access Operations," its work quickly moved beyond the highly tailored—bespoke—hacking of a small number of high priority systems. In 2004, the Agency built new facilities to enable them to expand from "an average of 100–150 active implants to simultaneously managing thousands of implanted targets" (SID Today 2004a:2). According to Matthew Aid, NSA had built tools (and adopted easily available open source tools) for scanning billions of digital devices for vulnerabilities; hundreds of operators were covertly "tapping into thousands of foreign computer systems" worldwide (Aid 2013). By 2008, the Agency's

partisan group argued, "in the new era, sharp distinctions between 'foreign' and 'domestic' no longer apply. We do not equate national security with 'defense'" (U.S. Commission on National Security 2001). 9/11 proved the catalyst, but not the cause, of the emergence of the homeland security state of the new millennium. The George W. Bush administration drew upon this dense congeries of ideas, plans, vocabulary, constitutional reflection, and an overlapping network of intellectuals, lawyers, ex-spies, and soldiers to develop the new homeland security state. This intellectual framework justified the dramatic leap in the foreign depth and domestic breadth of the acquisition, collection, and analysis of communications of NSA and its Five Eyes partners, including computer network exploitation.

### THE GOLDEN AGE OF SIGINT

In its 2000 prospectus for the incoming presidential administration, the NSA included an innocent sounding clause: "in close collaboration with cryptologic and Intelligence Community partners, establish tailored access to specialized communications when needed" (National Security Agency 2001: 4). Tailored access

meant government hacking—CNS. In the early 1990s, NSA seemed to many a cold-war relic, inadequate to the times, despite its pioneering role in computer security and penetration testing from the late 1960s onward. By the late 2010s, NSA was at the center of the "golden age of SIGINT" focused ever more on computers, their contents, and the digital infrastructure (NSA 2012: 2).

From the mid 1990s, NSA and its allies gained extraordinary worldwide capacities, both in the "passive" collection of communications flowing through cables or the air and the "active" collection through hacking into information systems, whether it be the president's network, Greek telecom networks during the Athens Olympics, or in tactical situations throughout Iraq and Afghanistan (see Redacted-Texas TAO 2010; SID Today 2004).

Prioritizing offensive hacking over defense became very easy in this context. An anonymous NSA author explained the danger in 1997:

*The characteristics that make cyber-based operations so appealing to us from an offensive*



FIGURE 5: Worldwide SIGINT/Defense Cryptologic Platform, n.d., (HTTPS://ARCHIVE.ORG/DETAILS/NSA-DEFENSE-CRYPTOLOGIC-PLATFORM.)

forms of metadata such as calling records from legal protection stems from the intelligence value of studying metadata at scale. The collection of the metadata of one person, on this view, is not legally different from the collection of the metadata of many people, as the U.S. Foreign Intelligence Surveillance Court has explained:

*[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.<sup>7</sup>*

Yet metadata is desired by intelligence agencies just because it is revealing at scale. Since their inception, NSA and its Commonwealth analogues have focused as much on working with vast databases of “metadata” as on breaking cyphered texts. NSA’s historians celebrate a cryptographical revolution afforded through “traffic analysis” (Filby 1993). From reconstructing the Soviet “order of battle” in the Cold War to seeking potential terrorists now, the U.S. Government has long recognized the transformative power of machine analysis of large volumes of metadata while simultaneously denying the legal salience of that transformative power.

As in the case of metadata, U.S. legal work on hacking into computers does not consider scale as legally significant. Espionage at scale used to be tough going: the very corporeality of sifting through physical mail, or garbage, or even setting physical wiretaps, or other devices to capture microwave transmissions scale only with great expense, difficulty, and potential for discovery (Donovan 2017).

distributed XKeyscore database and search system offered its analysts the option to “Show me all the exploitable machines in country X,” meaning that the U.S. government systematically evaluated all the available machines in some nations for potential exploitation and catalogued their vulnerabilities. Cataloging at scale is matched by exploiting machines at scale (National Security Agency 2008). One program, *Turbine*, sought to “allow the current implant network to scale to large size (millions of implants)” (Gallagher and Greenwald 2014). The British, Canadian, Australian partner intelligence agencies play central roles in this globe-spanning work.

**THE DISANALOGY WITH ESPIONAGE**

The legal status of government hacking to exfiltrate information rests on an analogy with traditional espionage. Yet the scale and techniques of state hacking strain the analogy. Two lawyers associated with U.S. Cyber Command, Col. Gary Brown and Lt. Col. Andrew Metcalf, offer two examples: “First, espionage used to be a lot more difficult. Cold Warriors did not anticipate the wholesale plunder of our industrial secrets. Second, the techniques of cyber espionage and cyber attack are often identical, and cyber espionage is usually a necessary prerequisite for cyber attack” (Brown and Metcalf 1998:117).

The colonels are right: U.S. legal work on intelligence in the digital age has tended to deny that scale is legally significant. The international effort to exempt sundry

Scale provided a salutary limitation on surveillance, domestic or foreign. As with satellite spying, computer network exploitation typically lacks this corporeality, barring cases of getting access to air-gapped computers, as in the case of the StuxNet virus. With the relative ease of hacking, the U.S. and its allies can know the exploitable machines in a country X, whether those machines belong to generals, presidents, teachers, professors, jihadis, or eight-year olds.

Hacking into computers unquestionably alters them, so the analogy with physical espionage is imperfect at best. A highly-redacted Defense Department “Information Operations Policy Roadmap” of 2003 underscores the ambiguity of “exploitation versus attack.” The document calls for clarity about the definition of an attack, both against the U.S. (slightly redacted) and by the U.S. (almost entirely redacted). “A legal review should determine what level of data or operating system manipulation constitutes an attack” (Department of Defense 2003:52). Nearly every definition—especially every classified definition—of computer network exploitation includes “enabling” as well as exploitation of computers. The military lawyers Brown and Metcalf argue, “Cyber espionage, far from being simply the copying of information from a system, ordinarily requires some form of cyber maneuvering that makes it possible to exfiltrate information. That maneuvering, or ‘enabling’ as it is sometimes called, requires the same techniques as an operation that is intended solely to disrupt” (Brown and Metcalf 1998:117) “Enabling” is the key moment where the analogy between traditional espionage and hacking into computers breaks down. The secret definition, as of a few years ago, explains that enabling activities are “designed to obtain or facilitate access to the target computer system for possible later” computer network attack. The enabling function of an implant placed on a computer, router, or printer is the preparation of the space of future battle: it’s as if every time a spy entered a locked room to plant a bug, that bug contained a nearly unlimited capacity to materialize a bomb or other

7 Quotation from secret decision with redacted name and date, p. 63, quoted in Amended Memorandum Opinion, No. BR 13-109 (Foreign Intelligence Surveillance Court August 29, 2013).



device should distant masters so desire. An implant essentially grants a third-party control over a general-purpose machine: it is not limited to the exfiltration of data. Installing an implant within a computer is like installing a cloaked 3-D printer into physical space that can produce a photocopier, a weapon, and a self-destructive device at the whim of its master. One NSA document put it clearly: “Computer network attack uses similar tools and techniques as computer network exploitation. If you can exploit it, you can attack it” (SID Today 2004b).

In a leaked 2012 Presidential Policy Directive, the Obama administration clarified the lines between espionage and information warfare explicitly to allow that espionage may produce results akin to an information attack. Amid a broad array of new euphemisms, CNE was transformed into “cyber collection,” which “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: 2-3). The bland term ‘cyber effects’ is defined as “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. The creation of effects akin to attack need not require the international legal considerations of war, only the far weaker legal regime around espionage. With each clarification, the gap between actual government hacking for the purpose of obtaining information

and traditional espionage widens; and the utility of espionage as a category for thinking through the tough policy and legal choices around hacking diminishes.

### SURVEILLING IRONY

By the end of the first decade of the 2000s, sardonic geek humor within NSA revealed in the ironic symbols of government overreach. A classified NSA presentation trolled civil libertarians: “Who knew that in 1984” an iPhone “would be big brother” and “the Zombies would be paying customers” (Spiegel Online 2013). Apple’s famous 1984 commercial dramatized how better technology would topple the corporatized social order, presaging a million dreams of the Internet disrupting wonted order. Far from undermining the ability of traditional states to know and act, the global network has created one of the greatest intensifications of the power of sovereign states since 1648. Whether espoused by cyber-libertarians or RAND strategists, the threat from the Net enabled new authorities and undermined civil liberties. The potential weakening of the state justified its hypertrophy. The centralization of online activity into a small number of dominant platforms—Weibo, Google, Facebook, with their billions of commercial transactions, has enabled a scope of surveillance unexpected by the most optimistic intelligence mavens in the 1990s. The humor is right on.

Signals intelligence is a hard habit to break—civil libertarian presidents like Jimmy Carter and Barack Obama quickly found themselves taken with being able to peek at the intimate communications of friends and foes alike, to know their negotiating positions in advance, to be three

steps ahead in the game of 14-dimensional chess. State hacking at scale seems to violate the sovereignty of states at the same time as it serves as a potent form of sovereign activity today. Neither the Chinese hacking into OPM databases nor the alleged Russian intervention in the recent US and French elections accords well with many basic intuitions about licit activities among states. If it would be naïve to imagine the evanescence of state-sanctioned hacking, it is doctrinally and legally disingenuous to treat that hacking as entirely licit based on ever less applicable analogies to older forms of espionage.

As the theorists in the U.S. military and intelligence worlds in the 1990s called for new concepts and authorities appropriate to the information age, they nevertheless tamed hacking for information by treating it as continuous with traditional espionage. The near ubiquity of state-sanctioned hacking should not sanction an ill-fitting legal and doctrinal frame that ensures its monotonic increase. Based on an analogy to spying that ignores scale, “computer network exploitation” and its successor concepts preclude the rigorous analysis necessary for the hard choices national security professionals rightly insist we must collectively make. We need a ctrl+alt+del. Let’s hope the implant isn’t persistent. ■

---

**MATTHEW L. JONES** teaches history of science and technology at Columbia. He is the author, most recently, of *Reckoning with Matter: Calculating Machines, Innovation, and Thinking about Thinking* from Pascal to Babbage. (Chicago, 2016).

---

### BIBLIOGRAPHY

- Aid, Matthew M. 2013. “Inside the NSA’s Ultra-Secret China Hacking Group,” *Foreign Policy*. June 10. [http://www.foreignpolicy.com/articles/2013/06/10/inside\\_the\\_nsa\\_s\\_ultra\\_secret\\_china\\_hacking\\_group?page=full](http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group?page=full)
- American Interest. 2015. “Former CIA Head: OPM Hack was ‘Honorable Espionage Work.’” *The American Interest*. June 16. <https://www.the-american-interest.com/2015/06/16/former-cia-head-opm-hack-was-honorable-espionage-work/>
- Andrews, Duane. 1996. “Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D),” December.
- Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation*, February 8, 1996. <https://www.eff.org/cyberspace-independence>
- Berkowitz, Bruce D. 2003. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press
- Boccagno, Julia. 2016. “NSA Chief speaks candidly of Russia and U.S. Election.” *CBS News*. November 17. <http://www.cbsnews.com/news/nsa-chief-adm-michael-rogers-speaks-candidly-of-russias-use-of-wikileaks-in-u-s-election/>
- Brown, Gary D. and Andrew O. Metcalf. 1998. “Easier Said Than Done: Legal Reviews of Cyber Weapons,” *Journal of National Security Law and Policy* 7.
- CJCSI 3210.01A. 1998. “Joint Information Operations Policy,” Joint Chiefs, November 6. [https://archive.org/details/CJCSI3210\\_01A](https://archive.org/details/CJCSI3210_01A)
- DCID 7/3. 2003. “Information Operations and Intelligence Community Related Activities.” Central Intelligence Agency, June 5. <https://fas.org/irp/offdocs/dcid7-3.pdf>

- Department of Defense. 2003. "Information Operations Roadmap," October 30. [http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info\\_ops\\_roadmap.pdf](http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf)
- DODD TS 3600.1. 1992. "Information Warfare (U)," December 21. <https://archive.org/details/14F0492Doc01DirectiveTS3600.1>
- DODD S-3600.1, 1996. "Information Operations (IO) (U)," December 9. [https://archive.org/details/DODD\\_S3600.1](https://archive.org/details/DODD_S3600.1)
- Donovan, Joan. 2017. "Refuse and Resist!" *Limn* 8, February. <http://limn.it/refuse-and-resist/>
- Falk, Richard A. 1962. "Space Espionage and World Order: A Consideration of the Samos-Midas Program," in *Essays on Espionage and International Law*. Akron: Ohio State University Press.
- Fields, Craig, and James McCarthy, eds. 1994. "Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," October. <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA286745>
- Filby, Vera R. 1993. *United States Cryptologic History, Sources in Cryptologic History*, Volume 4, *A Collection of Writings on Traffic Analysis*. Fort Meade, MD: NSA Center for Cryptological History.
- Gallagher, Ryan and Glenn Greenwald. 2014. "How the NSA Plans to Infect 'Millions' of Computers with Malware," *The Intercept*. March 12. <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>
- Gilman, Nils, Jesse Goldhammer, and Steven Weber. 2017. "Can You Secure an Iron Cage?" *Limn* 8, February. <http://limn.it/can-you-secure-an-iron-cage/>
- Hunt, Edward. 2012. "U.S. Government Computer Penetration Programs and the Implications for Cyberwar," *IEEE Annals of the History of Computing*. 34(3):4-21.
- Johnson, Philip A. 1999. "An Assessment of International Legal Issues in Information Operations," 1999, 40. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADB257057>
- Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.
- Kuehl, Dan. 1997. "Defining Information Power," *Strategic Forum: Institute for National Strategic Studies*, National Defense University, no. 115 (June). <https://web.archive.org/web/20050208041218/http://www.ndu.edu/inss/strforum/SF115/forum115.html>
- Lin Herbert S. 2010. "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, 4.
- National Security Agency/Central Security Service. 2000. "Transition 2001" December. <http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf>
- National Security Agency. 2008 "XKEYSCORE." February 25. [https://www.eff.org/files/2014/04/09/20130731-guard-xkeyscore\\_training\\_slides.pdf](https://www.eff.org/files/2014/04/09/20130731-guard-xkeyscore_training_slides.pdf)
- National Security Agency. 2012. "(U) SIGINT Strategy, 2012-2016," February 23. <https://archive.org/details/NSA-SIGINT-Strategy>
- NSA Office of General Counsel. n.d. "(U/FOUO) CNO Legal Authorities," slide 8. [https://www.aclu.org/sites/default/files/field\\_document/CNO%20Legal%20Authorities\\_0.pdf](https://www.aclu.org/sites/default/files/field_document/CNO%20Legal%20Authorities_0.pdf)
- Owens, William, Kenneth W. Dam, and Herbert S. Lin. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington D.C.: National Academies Press.
- Presidential Policy Directive (PPD)-20: "U.S. Cyber Operations Policy," October 16, 2012. <https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf>
- Rand Research Review. 1995. "Information Warfare: A Two-Edged Sword." *Rand Research Review: Information Warfare and Cyberspace Security*. Ed. A. Schoben. Santa Monica: Rand. [https://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/infor\\_war.html](https://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/infor_war.html)
- Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace*. Cambridge, Mass: MIT Press.
- Redacted. 1994 "Information Warfare: A New Business Line for NSA," *Cryptolog*. July.
- Redacted. 1997. "IO, IO, It's Off to Work We Go . . . (U)," *Cryptolog*. Spring.
- Redacted-NTOC, V225. 2010, "BYZANTINE HADES: An Evolution of Collection," June. [https://www.eff.org/files/2015/02/03/20150117-spiegel-byzantine\\_hades\\_-\\_nsa\\_research\\_on\\_targets\\_of\\_chinese\\_network\\_exploitation\\_tools.pdf](https://www.eff.org/files/2015/02/03/20150117-spiegel-byzantine_hades_-_nsa_research_on_targets_of_chinese_network_exploitation_tools.pdf)
- Redacted-Texas TAO/FTS327. 2010. "Computer-Network Exploitation Successes South of the Border," November 15. [https://www.eff.org/files/2013/11/15/20131020-spiegel-mexican\\_president.pdf](https://www.eff.org/files/2013/11/15/20131020-spiegel-mexican_president.pdf)
- Rid, Thomas. *Rise of the Machines: A Cybernetic History*. New York: W. W. Norton & Company, 2016.
- Rothrock, John. 1997. "Information Warfare: Time for Some Constructive Criticism," in *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica: Rand.
- Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. 2nd ed. Cambridge: Cambridge University Press. DOI:10.1017/9781316822524.
- SID Today. 2004. "Another Successful Olympics Story," October 6, 2004. <https://www.eff.org/document/20150928-intercept-another-successful-olympics-storypdf>
- SID Today. 2004a. "Expanding Endpoint Operations." September 17. <https://www.eff.org/document/20150117-spiegel-document-about-expansion-remote-operations-center-roc-endpoint-operations>
- SID Today. 2004b. "New Staff Supports Network Attack." October 21. <https://theintercept.com/snowden-sidtoday/3676084-new-staff-supports-network-attack/>
- SIDToday. 2006. "The ROC: NSA's Epicenter for Computer Network Operations," September 6. [https://www.eff.org/files/2015/01/23/20150117-spiegel-document\\_explaining\\_the\\_role\\_of\\_the\\_remote\\_operations\\_center\\_roc.pdf](https://www.eff.org/files/2015/01/23/20150117-spiegel-document_explaining_the_role_of_the_remote_operations_center_roc.pdf)
- Spiegel Online. 2013. "Spying on Smartphones," *SPIEGEL ONLINE*, September 9. <http://www.spiegel.de/fotostrecke/fotostrecke-101201.html>
- United States Commission on National Security/21st Century. 2001. *Road Map for National Security: Imperative for Change*. January 31. Final Draft. <https://www.hsdl.org/?abstract&did=2079>
- Wolfowitz, Paul. 2001. "Department of Defense Directive 3600.1 Draft," October.