This is an excerpt on intelligence technology deficiencies taken from the declassified Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, Report of the U.S. Senate Committee on Intelligence and the U.S. House Permanent Committee on Intelligence, December 2002, declassified version released on July 9, 2004.

Source of report:

http://a257.g. a kamaitech.net/7/257/2422/24 jul 20031400/www.gpoaccess.gov/serialset/creports/pdf/full report errata.pdf

PDF, 858 pages, 5.4MB

JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF **SEPTEMBER 11, 2001**

REPORT

OF THE

U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE

AND

U.S. HOUSE PERMANENT SELECT COMMITTEE ON **INTELLIGENCE**

TOGETHER WITH ADDITIONAL VIEWS

DECEMBER 2002

between al-Mihdhar and the *USS Cole* bombing necessary to open a criminal investigation. FBI attorneys took the position that criminal investigators "CAN NOT" (emphasis original) be involved and that criminal information discovered in the intelligence case would be "passed over the wall" according to proper procedures. An agent in the FBI's New York field office responded by e-mail, [page 387] "Whatever has happened to this, someday someone will die and, wall or not, the public will not understand why we were not more effective in throwing every resource we had at certain problems." Again, FBI Headquarters applied FISA "walls" to a non-FISA case.

The USA PATRIOT Act, enacted in response to September 11, provided unambiguous authority for the Attorney General and other law enforcement officials to disclose to the Director of Central Intelligence foreign intelligence collected in the course of a criminal investigation. The Act also requires that intelligence be "a significant purpose" of a FISA search rather than "the purpose." These provisions were intended to reduce, if not remove restrictions that had grown up around FISA operations. The Foreign Intelligence Surveillance Review Court, in its first opinion since being established in 1979, has affirmed that the Act permits the free flow of intelligence to prosecutors, who may direct and control FISA surveillances.

XI. Technology Gaps

Technology is critical to the Intelligence Community's efforts to collect, analyze, and disseminate information on terrorist identities, locations, capabilities, plans, and intentions. The Joint Inquiry examined a number of issues in order to assess how well-postured the Community was in regard to its use of technology as well as its understanding of the use of technology by terrorists. The NSA, which, of all the intelligence agencies, relies the most on technical collection, received most of the attention.

A. Technology Gaps at NSA

Al-Qa'ida members employed a variety of communications technologies, including modern ones such as [______], in the conduct of their activities. In his testimony, NSA Director Lt. Gen. Hayden lamented the fact that terrorists have access to the three-trillion-dollar-a-year communications industry. The Joint

Inquiry attempted to examine NSA's current and planned capabilities to exploit these types of modern communications as well as the tools being used and developed to help linguists and analysts process and share the volumes of information collected. In addition, the Joint Inquiry [page 388] examined the health of the technical collection platforms from which the majority of counterterrorism intelligence information is derived.

The assessment presented below draws on testimony, interviews, and some NSA documentation.

		—].	
[Page 389]			
[
].		
[]		
] .			
_			
[<u>]</u>		
[
].		
[

[Page 390] [—————————].	-
J.	
F. Selection and Filtering for [<u> Communications</u>
Much of NSA's pre-September 11 success agains	st terrorist targets was due to the ability to
[—————————————————————————————————————	ed on [———] interest rather
than randomly choosing among millions of communicati	ons. With the proliferation of multimedia
communications, even better selection and filtering technique.	niques will be required.
One area of increased attention is [
] an area in which NSA ha	s made only limited progress. [———
]. Unfortunately, NSA's selection	capabilities suffer from a critical
deficiency, [] . The solution to
this deficiency is well understood and estimated to cost l	ess than \$1 million to implement.
However, the Joint Inquiry learned in interviews that eve	en though [———] have been
available for many years, and even though NSA has had	recent significant funding increases, the
program manager is still "scrounging" for funds to pay for	or this upgrade that would not be
completed until 2004.	
G. Analyst Tools	
NSA often did not provide analysts with sufficien	nt tools to exploit the data collected. For
example, NSA in 1998 did not have the capability to [
], NSA's Analysis and Pro	duction Chief, noted, "At that time the
systems that were in place were high tailored, not integra	table. The plug and play was only
beginning to come into play at that point in time. So a ta	ilored solution that you might be able to
architect at home wasn't necessarily one that you could d	leploy across [———] or
within a CT shop." [] noted, however, that this	capability now existed.
[Page 391]	
However, field operators still do not have such to	ols, even though they were available at
NSA Headquarters after September 11. During a visit to	the [],

Joint Inquiry personnel found [——] linguists frustrated	d with Headquarters support for language
tools. In fact, one of their primary concerns was the inab	oility to display [—————
]. They noted that they could purchase software of	on the local economy that can display
[] but are prohibited from de	oing so because the software is not an
"approved application" for their computer platform. "W	hen they officially requested such a
capability through official channels, they were told that s	something could be available in 18
months." They noted that some computers they still use	are 1993 vintage UNIX machines that
cannot even display ordinary graphical user interfaces co	prrectly due to color graphics limitations.

H. Collection Platforms

NSA collects signals intelligence using a variety of methods or platforms. Often these platforms, which have a sizable infrastructure investment, serve a myriad of intelligence missions. In identifying these critical platforms, the Joint Inquiry examined statistics on counterterrorism-related reporting. The following chart shows the source of counterterrorism reports per technical collection platform both pre- and post-September 11:

Collection Platform	All	All	Percent
	Counterterrorism	Counterterrorism	Increase
	Reports 10 May 01	Reports 11 Sep 01	
	- 10 Sep 01	- 11 Jan 02	
[]	[]	[]	[]

NSA spending increases after September 11, however, are not focused on several of the most productive sources of counterterrorism information. [————] [Page 392]

[
].
The evidence suggests that an effective counterterrorism effort requires [
]. In testimony, Lt. Gen. Hayden acknowledged, [
]. Lt.
Gen. Hayden also stated that in his effort to develop capabilities against new communications
technologies by the end of the 1990s, "This meant taking money away from current, still active,
still producing activities " Since the attacks, NSA has focused on its transformation strategy.
Lt. Gen. Hayden testified:
"Shortly after September 11 th , I had a meeting of my senior leaders. I asked them the following question: Is there any part of our transformation roadmap that we should change as a result of the attacks? Unanimously, they responded, 'No, but we need to accelerate these changes.' With the money the President has requested and Congress has provided, we have done just that."
NSA's commitment to the future viability of the [
unclear, despite their value.

XII. Technical Collection of Terrorist Communications

[Responsibility for most of the technical collection of terrorist communications falls under the purview of the National Security Agency, although the CIA and the FBI also conduct technical collection against terrorism. NSA and other agencies learned valuable information from intercepting terrorist communications and prevented several planned attacks. Indeed, numerous

officials throughout the policy and Intelligence Community told the Joint Inquiry that [page 393] Signals Intelligence (SIGINT) was a valuable source of information on al-Qa'ida. Exploitation of terrorist communications, however, was uneven at best and suffered from insufficient investment. Al-Qa'ida was only one of several high priority targets and a difficult one].

A. NSA's Organizational Structure for Collecting Terrorist Communications

Within the NSA, the Signal	s Directorate, which was created in February 2001 by
combining the Operations and Tech	hnology Directorates, has the primary SIGINT mission. Within
the Signals Directorate, the Counter	rterrorism Product Line has the lead for counterterrorism
] :
• [];
r	1
• [];
• [];
- [1,
• [
];
• [];
• [].

B. SIGINT and the September 11 Attacks

Prior to 11 September 2001, NSA had no specific information indicating the date, time, place, or participants in an attack on the United States. Numerous NSA personnel, including

Lt. [page 394] General Hayden, the Director of the NSA (DIRNSA), repeatedly related this conclusion to the Joint Inquiry.

[NSA had intercepts on September 10, 2001 that, in retrospect, appear to relate to the September 11 attacks. These intercepts were processed on September 11 (after the terrorist attacks) and reported early on September 12, 2001. Although each of the products referred to something occurring the following day, neither intercept had specifics on the attack, location, or targets. This wording was similar to other non-specific threats occasionally reported by NSA over the past several years].

In an effort to place the September 10 messages in perspective, General Hayden testified, "I should also note that [over a period of time] earlier that summer we had intercepted and reported over 30 such imminent attack messages and that since September 11 [NSA continues to report similar activities]."

In fact, following September 11, there was a flurry of similar [——] intercepts that were not associated with any terrorist attacks:

• [—		
• [];
• [
	—]; and	
• [——		
[Page 395]	—].	

C. A Chronological Review of NSA Collection Efforts Against al-Qa'ida

[In the years before the September 11 attacks, NSA steadily increased its collection on al-
Qa'ida. Initial Intelligence Community efforts focused on Bin Ladin himself as a terrorist
financier. As the 1990s wore on, this effort expanded to collection on Bin Ladin's associates and
the al-Qa'ida organization. [————————————————————————————————————
-
].
The following review is largely drawn from Joint Inquiry interviews. It highlights
important milestones in NSA's collection against al-Qa'ida.
[
]. Bin Ladin was viewed almost exclusively by the
Intelligence Community as a terrorist financier until 1996].
[In 1996, CTC established its Bin Ladin unit as the Intelligence Community focal point for
tracking Bin Ladin. [
]. The first phase of the unit's Bin Ladin project was strategic information
gathering, [———]. It was at this
point that the Intelligence Community began focusing on the Bin Ladin target as a terrorist support
network in addition to being a terrorist financier].
[
].
[Page 396]

[Before Bin Ladin issued his February 1998 anti-American fatwa, [
]. Following the <i>fatwa</i> , the Director of
NSA appealed to [] partners, few of which were focused on counterterrorism at the
time, for counterterrorism assistance. [
[Following the August 1998 East Africa Embassy bombings, NSA instituted a much high
operations tempo, which never really subsided. After the bombings, at the request of FBI's New
York Field Office, NSA provided all reports that appeared related to the attacks. This information
was useful to the FBI].
Un the fell of 1000 NCA lest the chility to listen to Din Lodin on his catallite phone. This
[In the fall of 1998, NSA lost the ability to listen to Bin Ladin on his satellite phone. This
loss was probably the result of, among other things, a media leak. [
].
[
l
1.
In February 1999, the Department of State demarched the Taliban, [
].
[Page 397]

[
L
].
The Millennium threat surge began in November 1999. The Millennium threat was a top
priority for the entire Intelligence Community, and NSA personnel worked around the clock
supporting CIA's disruption campaign. During this time, Jordanian officials arrested terrorists
linked to al-Qa'ida. [
].
[
Constant of the control of the contr
Several other advances occurred throughout 2000. [——————————————————————————————————
].
[Page 398]
Following the USS Cole bombing in October 2000, NSA consolidated some of its
counterterrorism efforts [

TOP SECRET
].
[By the winter of 2000, NSA noted a general rise in threat activity. The Intelligence
Community assessed the threat to be mostly oriented abroad. In spring 2001, NSA noted another
significant rise in threat activity. Again, the Intelligence Community assessed the threat to be
directed abroad].
[Throughout June and July 2001, another rise in threat activity was identified. NSA analysts noted vague communications traffic indicating that something was afoot. Intelligence Community speculation centered on whether the likely target was abroad. The U.S. military was sufficiently concerned that an attack would occur on the Arabian Peninsula that "ThreatCon Delta" was declared and all ships in the area were sent to sea].
[Military customers asked NSA/CT analysts if the threat were real. NSA counterterrorism analysts reviewed the evidence and were confident that it was. [

[In the spring, the Intelligence Community reported indications that an attack may have been postponed. The Joint Inquiry was told that this led the Intelligence Community to believe that a real terrorist attack had been averted].

[Page 399]

D. Technical Collection Problems and Limits at NSA

Technical collection was limited. This was due to both the nature of the target and missteps by the NSA and other U.S. government elements.

a. Difficulties of Gaining Actionable Intelligence on al-Qa'ida

[Several senior NSA officials, including the Deputy Director of NSA and Chief of the counterterrorism organization contended in interviews and testimony that information on terrorism organization.		
circumspect discussions, put them into context, and identify linkages to other known targets or		
activities. NSA's Director stated: " we do not anticipate being able to provide detailed threat		
information from SIGINT in most cases." Indeed, SIGINT did not provide significant intelligence		
to prevent other major terrorist attacks against U.S. interests such as Khobar Towers, the East		
Africa U.S. Embassies, and USS Cole].		
[However, these arguments are somewhat belied by evidence uncovered during the Joint		
Inquiry that identified several instances of communications providing some specifics in terms of		
timeframe and general location for terrorist activity. In addition, the FBI acquired toll records that		
five or six hijackers communicated extensively abroad after they arrived in the United States. The		
Intelligence Community had no information prior to September 11, 2001 regarding these		
communications, and, as a result, does not know what clues they may have contained].		
Γ		
[Page 400] [————]. The Director of NSA, testifying about the		
targeting challenges facing NSA, said "cracking into these targets is hard - very hard - and		
SIGINT operations require considerable patience – sometimes over years – before they mature."		

b. Difficulties in Adjusting to Terrorist Targets

The communications sophistication of stateless terrorists in general and al-Qa'ida in particular clearly surprised NSA officials. The rise of al-Qa'ida seemingly paralleled in some respects what NSA's Director referred to as "the telecommunications and information revolution" of the past ten years. He noted that al-Qaida operatives are skilled users of the global telecommunications infrastructure, "al-Qa'ida is in many respects different from NSA's typical SIGINT targets of the past 50 years."

In spring 2001, NSA began to change direction: rather than analyzing *what was collected*, NSA would dissect its targets' communications practices to determine *what to collect*. This is commonly referred to at NSA as *hunting* rather than *gathering*. This procedure was in its infancy when the September 11 terrorist attacks occurred.

c. Problems Keeping Pace with [—————	Advances before September 11
r	
acknowledge NSA's deficiencies in dealing with	some forms of modern communications, but was
also quick to credit his organization for working of	on the building blocks before September 11, so
that [Page 401] fielding additional capabilities aft	er September 11 was expedited].

NSA's Director apparently felt handcuffed in his effort to move forward in this area, citing his inability to "churn" (redirect) some \$200 million into "new age signals ... because we were going to erode our coverage of [other intelligence issues] as part of this effort." Indeed, General

Hayden told the Joint Inquiry that he was severely criticized on several occasions for abandoning so-called legacy communication paths in favor of developing robust new capabilities.

[There is some apparent inconsistency concerning NSA's concentration. On at least one occasion, the Director of NSA asserted that it was not so much NSA's inability to collect some modern communications, but other factors. The bulk of the information available to the Joint Inquiry, however, suggests NSA was behind the curve in this area and only began to catch up after September 11, 2001].

E. Insufficient Resources for Counterterrorism at NSA

Although NSA has had difficulty in generating consistent, accurate personnel numbers for the Joint Inquiry, it appears from interviews and the limited information provided that personnel employed in the counterterrorism organization were largely static over several years, despite repeated efforts by local managers to increase the numbers of linguists and analysts. General Hayden testified that in hindsight he would have liked to have doubled his resources against al-Qa'ida.

NSA acknowledged it had insufficient numbers of linguists and analysts on the counterterrorism target. This acknowledgment seems to have come from leadership in retrospect, while those closer to the counterterrorism problem stated to the Joint Inquiry they had been requesting personnel increases for years, mostly to little or no avail.

[Page 402]

Declining overall resources made it difficult to dramatically expand counterterrorism coverage. As discussed in more detail in a separate chapter, for much of the 1990s NSA's budget and manpower were steadily reduced to a point that all collection efforts were impeded. Cuts were "salami-sliced" across the agency rather than specifically targeted, a tactic employed by NSA for many years to cope with declines while still trying to satisfy an increasing number of intelligence requirements, and competing priorities (especially force protection requirements) that drained scarce resources, such as Arabic linguists. Funds for [______] collection, historically two of NSA's most lucrative reporting sources, were essentially put in a maintenance

mode, with investment focused on other collection sources that NSA felt needed to be developed to have a more balanced SIGINT collection system.

There was little significant, sustained reaction to the DCI's declaration of war on al-Qa'ida in 1998. Indeed, LTG Hayden (who became Director of NSA in 1999) noted that by 1998, NSA was already at a heightened counterterrorism posture and thus no additional wholesale shifts in resources were made at that time. LTG Minihan, the Director of NSA at the time of the DCI's declaration, told the Joint Inquiry that he felt the DCI was speaking for the CIA only. In his view, the DCI generally left Intelligence Community matters to the head of the Community Management Staff.

[Numerous individuals noted that counterterrorism was but one of several seemingly equally high priority targets levied on NSA prior to September 11. Although the Director of the Signals Directorate stated that in addition to al-Qa'ida, [———] was the only other Tier 0 (highest priority) target in the 1998-2001 timeframe, there did not seem to be an objective method for resource assignment within NSA, nor guidance from the DCI. The Director of NSA in his testimony referred to the PDD-35 requirements system as "cumbersome." The requirements system in place on the eve of September 11 consisted of some 1,500 standing requirements calling for some 200,000 detailed pieces of information – ad hoc requirements that were received telephonically or via e-mail, and requests for additional information. In response, NSA juggled resources to cope with competing requirements but did not make dramatic cuts in other priorities to dramatically expand counterterrorism coverage].

[Page 403]

The NSA Director also cautioned in his testimony, "If these hearings were about the war that had broken out in Korea or the crisis in the Taiwan Straits that had taken us by surprise or if we had been surprised by a conflict in South Asia or if we had lost an aircraft over Iraq or if American forces had suffered casualties in Bosnia or Kosovo, in any of these cases I would be here telling you that I had not put enough analysts or linguists against the problem. We needed more analysts and linguists across the agency, period."

F. Technical Collection at CIA

Most of the technical collection operations at the CIA have a human access element, and
the primary offices with responsibility are in the Directorate of Operations. The Counterterrorist
Center has a Technical Operations Branch that is responsible for orchestrating special technical
collection operations for terrorist targets. Some of these operations are conducted in concert with
NSA, [
].
L .
]. [Despite this [] effort, a senior CIA official testified that in
•
hindsight he would have liked to have had more [
].
G. NSA/CIA Disputes Over [
[NSA and CIA failed to agree on an approach to collect [———]
and both agencies independently developed a capability [
———]. After considerable discussion with NSA and CIA personnel, the Joint Inquiry [page
404] determined that CIA wished to have [
], and NSA said it could not deliver in the requested
timeframe. Accordingly, CIA developed its own capability while NSA continued with its
program, which ultimately was delivered some 15 months early. In the end, peace was made and
over time, NSA and CIA began to benefit from each other's capabilities].
• •

Especially during periods of budgetary shortfalls, the competitive example just cited appears particularly wasteful. To avoid similar disputes, NSA and CIA have created the Senior Partnership Advisory Group (SPAG).

H. Technical Collection at FBI

The FBI performs considerable technical collection within the United States to support its
own intelligence and criminal investigations. It also supports the collection efforts of Intelligence
Community agencies, [————————————————————————————————————
]. These activities are conducted pursuant to the authority of
the Foreign Intelligence Surveillance Act of 1978. [————————————————————————————————————
].
FBI was conducting relatively few technical collection operations against al-Qa'ida before
September 11. The intelligence produced was of relatively limited value because the targets did
not appear to be involved in significant activity.
FBI officials indicated that after September 11 a joint program had begun with NSA [——
]. FBI is responsible for collecting the information. NSA
receives the information and is responsible for reporting to the Intelligence Community and
[page 405] intelligence customers. [———]. FBI personnel maintain that collaboration [—
l can still be improved

XIII. HUMINT Collection

Three agencies in the Intelligence Community have primary responsibility for HUMINT (intelligence from human sources) collection: the CIA, the FBI, and the DIA. Before September 11, none of these agencies had collected any information through HUMINT sources warning of the September 11 attacks on the Pentagon and the World Trade Center.