Newsweek

Did Hayden's Flawed Decisions make America More Vulnerable?

Patrick Eddington

December 8, 2017

Retired Gen. Michael Hayden, former director of the NSA and CIA (and now, a national security analyst at CNN), has recently emerged as a leading critic of the Trump administration, but not so long ago, he was widely criticized for his role in the post-9/11 surveillance abuses. With the publication of his memoir, *Playing to the Edge: American Intelligence in the Age of Terror*, Hayden launched his reputational rehab campaign.

Like most such memoirs by high-level Washington insiders, Hayden's tends to be heavy on self-justification and light on genuine introspection and accountability. Also, when a memoir is written by someone who spent their professional life in the classified world of the American Intelligence Community, an additional caveat is in order: The claims made by the author are often impossible for the lay reader to verify. This is certainly the case for *Playing to The Edge*, an account of Hayden's time as director of the NSA, and subsequently, the CIA.

Fortunately, with respect to at least one episode Hayden describes, litigation I initiated under the Freedom of Information Act (FOIA) has produced documentary evidence of Hayden's role in the 9/11 intelligence failure and subsequent civil liberties violations. The consequences of Hayden's misconduct during this time continue to be felt today. First, some background.

The War Inside NSA, 1996 to 2001

By the mid-1990s, a group of analysts, cryptographers, and computer specialists at NSA realized that the growing volume of digital data on global communications circuits was both a potential gold mine of information on drug traffickers and terrorist organizations, as well as a problem for NSA's largely analog signals intelligence (SIGINT) collection, processing, and dissemination systems. As recounted in the documentary *A Good American*, three NSA veterans—Bill Binney, Ed Loomis, and Kirk Wiebe—set out to solve the problem of handling an ever-increasing stream of digital data while protecting the 4th Amendment rights of Americans against warrantless searches and seizures.

Through their Signals Intelligence Automation Research Center (SARC), they had, by 1999, developed a working prototype system, nicknamed THINTHREAD. A senior Republican House Permanent Select Committee on Intelligence (HPSCI) staffer, Diane Roark, was so impressed with what Binney, Loomis, and Wiebe had developed, that she helped steer approximately $3 million to the THINTHREAD project to further its development. But by April 2000, Roark and

the SARC team had run into the ultimate bureaucratic roadblock for their plan: Hayden, who had recently been installed as NSA director.

He had his own, preferred solution to the same problem the SARC team had been trying to solve. As Hayden noted in his memoir:

Our answer was Trailblazer. This much-maligned (not altogether unfairly) effort was more a venture capital fund than a single program, with our investing in a variety of initiatives across a whole host of needs. What we wanted was an architecture that was common across our mission elements, interoperable, and expandable. It was about ingesting signals, identifying and sorting them, storing what was important, and then quickly retrieving data in response to queries.
It was, of course, a description that fit THINTHREAD perfectly—except for the collection and storage of terabytes of digital junk. THINTHREAD's focus on metadata mining and link analysis was designed to help analysts pinpoint the truly important leads to follow while discarding irrelevant data. Hayden's concept mirrored that of his successor, Keith Alexander, who also had a "collect it all" mentality.

In his memoir, Hayden spoke of the need to "engage industry" (p. 20) in the effort to help NSA conquer the challenge of sorting through the mind-numbing quantity of digital data, but even Hayden admitted that "When we went to them for things nobody had done yet, we found that at best they weren't much better or faster than we were" (page 20).

That should've been Hayden's clue that NSA would be better off pursuing full deployment of THINTHREAD, a proven capability. But Hayden chose to pursue his industry-centric approach instead, and he tolerated no opposition or second-guessing of the decision he'd made.

In April 2000, Hayden's message to the NSA workforce made it clear that any NSA employees who went to Congress to suggest a better way for the NSA to do business would face his wrath. Even so, the THINTHREAD team pressed on, managing to get their system deployed to at least one NSA site in a test bed status, working against a real-world target. Meanwhile, Roark continued to push NSA to make the program fully operational, but Hayden refused, and just three weeks before Sept. 11, 2001, further development of THINTHREAD was terminated in favor of the still hypothetical TRAILBLAZER program.

DoD IG Investigation vs. Hayden's memoir

As Loomis noted in his own account of the THINTHREAD-TRAILBLAZER saga, within days after the 9/11 attacks, NSA management ordered key components of THINTHREAD—the system Hayden had rejected—to be integrated (without the inclusion of 4th Amendment compliance software) into what would become known as the STELLAR WIND warrantless surveillance program. Terrified that the technology they'd originally developed to fight foreign threats was being turned on the American people, Loomis, Binney, and Wiebe retired from the NSA at the end of October 2001.

Over the next several months, they would attempt to get the Congressional Joint Inquiry to listen to their story, but to no avail. By September 2002, the trio of retired NSA employees, along with

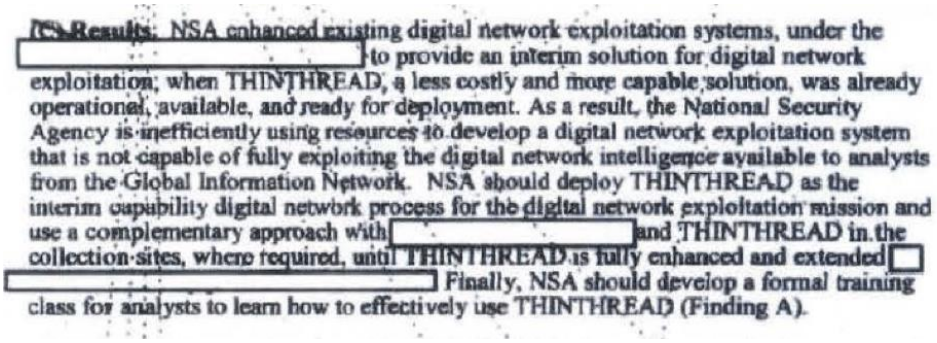
Roark, decided to file a Defense Department Inspector General (DoD IG) hotline complaint, in which they alleged waste, fraud, and abuse in the TRAILBLAZER program. Inside NSA, they still had an ally—a senior executive service manager named Tom Drake, who had become responsible for the remnants of THINTHREAD after the SARC team had resigned. Drake became the key source for the subsequent DoD IG investigation, which resulted in a scathing, classified report completed in December 2004.

The TRAILBLAZER-THINTHREAD controversy subsequently surfaced in the press, and I followed the reporting on it while working as a senior staffer for then-Representative Rush Holt (D-N.J.), a HPSCI member at the time. Once Holt was appointed to the National Commission on Research and Development in the Intelligence Community, I asked for and received copies of the published DoD IG reports dealing with the THINTHREAD and TRAILBLAZER programs. The 2004 report remains the most damning IG report I've ever read, and after Holt announced his departure from Congress in 2014, I decided to continue my own investigation into this episode as an analyst at the Cato Institute. In March 2015, I filed a FOIA request seeking not only the original 2004 DoD IG report, but all other documents relevant to the investigation. After being stonewalled by DoD and NSA for nearly two years, Cato retained the services of Loevy and Loevy of Chicago to prosecute a FOIA lawsuit to help get the documents I sought. In July 2017, the Pentagon released to me a still heavily redacted version of the 2004 DoD IG report. But there are fewer redactions in my copy than there were in the version provided to the Project on Government Oversight (POGO) in 2011, and it provides the clearest evidence yet that Hayden's account of the THINTHREAD-TRAILBLAZER episode in his memoir is simply not to be believed.

On The IG Investigation Itself

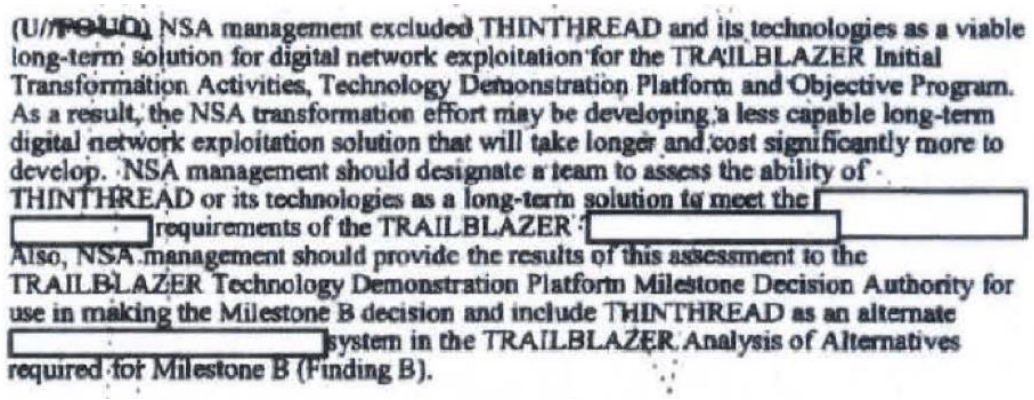
On page 26 of his memoir, Hayden's only mention of the IG investigation is a single sentence: "Thin Thread's advocates filed an IG (inspector general) complaint against Trailblazer in 2002." Hayden makes no mention of the efforts he and his staff made to downplay THINTHREAD to the IG, or the climate of fear that Hayden and his subordinates created among those who worried TRAILBLAZER was a programmatic train wreck, and that THINTHREAD could, in fact, provide NSA with exactly the critical "finding the needle in the haystack" capability it needed in the digital age.

In its Executive Summary (page ii), the DoD IG report agreed THINTHREAD was the better solution and should be deployed:



(U) **Results.** NSA enhanced existing digital network exploitation systems, under the [redacted] to provide an interim solution for digital network exploitation; when THINTHREAD, a less costly and more capable solution, was already operational, available, and ready for deployment. As a result, the National Security Agency is inefficiently using resources to develop a digital network exploitation system that is not capable of fully exploiting the digital network intelligence available to analysts from the Global Information Network. NSA should deploy THINTHREAD as the interim capability digital network process for the digital network exploitation mission and use a complementary approach with [redacted] and THINTHREAD in the collection sites, where required, until THINTHREAD is fully enhanced and extended [redacted] Finally, NSA should develop a formal training class for analysts to learn how to effectively use THINTHREAD (Finding A).

And the DoD IG made it clear that NSA management—meaning Hayden—had deliberately excluded THINTHREAD as an alternative to TRAILBLAZER at a clear cost to taxpayers:

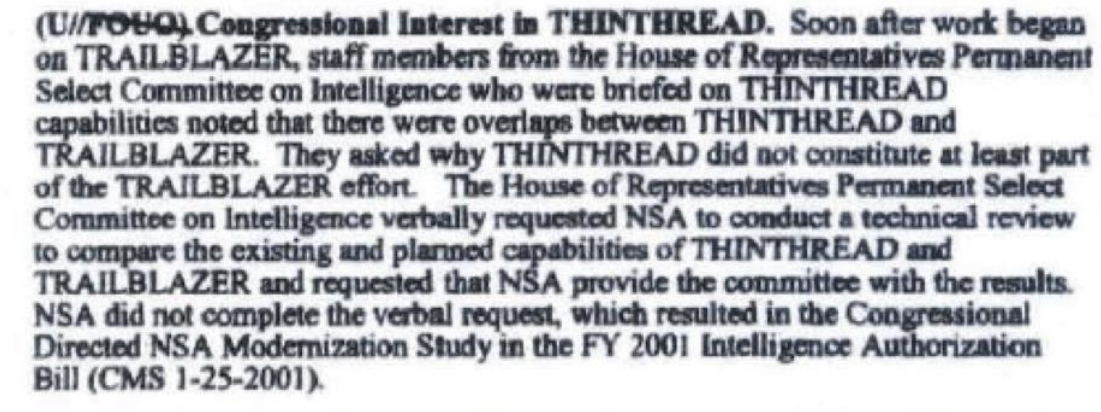

(U//~~FOUO~~) NSA management excluded THINTHREAD and its technologies as a viable long-term solution for digital network exploitation for the TRAILBLAZER Initial Transformation Activities, Technology Demonstration Platform and Objective Program. As a result, the NSA transformation effort may be developing a less capable long-term digital network exploitation solution that will take longer and cost significantly more to develop. NSA management should designate a team to assess the ability of THINTHREAD or its technologies as a long-term solution to meet the [redacted] requirements of the TRAILBLAZER [redacted] Also, NSA management should provide the results of this assessment to the TRAILBLAZER Technology Demonstration Platform Milestone Decision Authority for use in making the Milestone B decision and include THINTHREAD as an alternate [redacted] system in the TRAILBLAZER Analysis of Alternatives required for Milestone B (Finding B).

On Defying Congress

Hayden's fury at the SARC team keeping HPSCI staffer Roark in the loop about their progress was palpable, as he made clear on page 22 of his book:

The alliance with HPSCI staffer Roark created some unusual dynamics. I essentially had several of the agency's technicians going outside the chain of command to aggressively lobby a congressional staffer to overturn programmatic and budget decisions that had gone against them internally. That ran counter to my military experience—to put it mildly.

But Binney, Loomis, and Wiebe didn't owe their allegiance to Hayden—they owed it to the Constitution and the American people. And to be clear, Roark was the driver behind briefing and information requests, performing her mandated oversight role, a fact Hayden clearly resented—to the point that he was willing to defy her requests, as the IG report noted on page 2:


(U//~~FOUO~~) **Congressional Interest in THINTHREAD.** Soon after work began on TRAILBLAZER, staff members from the House of Representatives Permanent Select Committee on Intelligence who were briefed on THINTHREAD capabilities noted that there were overlaps between THINTHREAD and TRAILBLAZER. They asked why THINTHREAD did not constitute at least part of the TRAILBLAZER effort. The House of Representatives Permanent Select Committee on Intelligence verbally requested NSA to conduct a technical review to compare the existing and planned capabilities of THINTHREAD and TRAILBLAZER and requested that NSA provide the committee with the results. NSA did not complete the verbal request, which resulted in the Congressional Directed NSA Modernization Study in the FY 2001 Intelligence Authorization Bill (CMS 1-25-2001).

That defiance of a congressional request went further, as the DoD IG noted on page 99 of their report:

(U//~~FOUO~~) **Management Comments.** NSA recommended that the audit report emphasis NSA's cooperation and responsiveness to Congress.

(~~S//NF~~) **Audit Response.** Information in congressional records notes that NSA did not explain to congress why THINTHREAD did not constitute at least some part of TRAILBLAZER. Instead, NSA delayed deploying THINTHREAD. Although the THINTHREAD deployment study showed that not being fully documented would not have a negative effect on mission capability, NSA chose to document THINTHREAD before completing its deployment. Most of THINTHREAD deployments could have been completed prior to our audit. The THINTHREAD deployment plan was inadequate.

[redacted]

Hayden didn't just stiff-arm Roark, he stiff-armed the entire committee.

On Incompetent Program Management and Priorities

Hayden makes clear in his memoir (page 20) that he wanted an orderly approach to the digital traffic problem, even if it meant taking a lot of time to do it:

Our program office had a logical progression in mind: begin with a concept definition phase, then move to a technology demonstration platform to show some initial capability and to identify and reduce technological risk. Limited production and then phased deployment would follow. The DoD IG investigators viewed Hayden's approach as ill-considered (p. 4):

NSA (b)(3) 50 USC 3605

[redacted]

A. The NSA Interim Solution to Urgent National Security Needs (U)

(~~TS//SI~~) The NSA deployed enhanced legacy systems and services under the [redacted] although requirements could have been satisfied better with an existing and more capable and less costly system, THINTHREAD. Those conditions occurred because NSA:

- (U//~~FOUO~~) did not consider THINTHREAD as an alternative solution to a quick reaction capability requirement for an interim digital network exploitation system after the September 11, 2001, terrorist attacks; and
- (U//~~FOUO~~) did not follow the recommendations of internal and external technical reviews completed in 2001 that recommended:
  1. (U//~~FOUO~~) deploying THINTHREAD as the interim solution for digital network exploitation; and
  2. (U//~~FOUO~~) extending and enhancing the capabilities of THINTHREAD;
- (~~TS//SI~~) delayed deployment of THINTHREAD to collection sites as directed by Congress in FY 2002; and

(~~S~~) As a result, NSA initiated and used [redacted] as an interim digital network exploitation solution, which NSA plans to use until FY 2009. [redacted] is not capable of fully exploiting the digital network intelligence available to analysts from the global information network and costs significantly more to develop, field, and maintain than THINTHREAD.

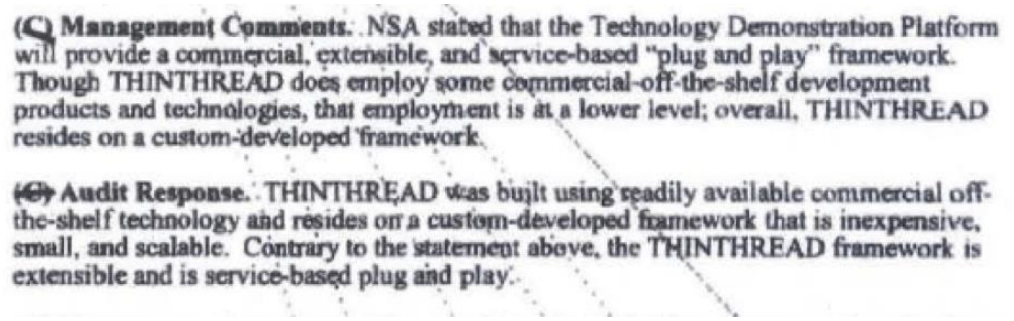
In other words, Hayden had learned nothing from his mistake in sand-bagging THINTHREAD prior to 9/11, and he kept the original, full program on ice even after the loss of nearly 3,000 American lives and daily concerns in the months after the terrorist attacks about possible "sleeper cells" and follow-on attacks.

On THINTHREAD's scalability

Hayden argues in his memoir (page 22) that THINTHREAD was not deployable across all NSA elements:

The best summary I got from my best technical minds was that aspects of Thin Thread were elegant, but it just wouldn't scale. NSA has many weaknesses, but rejecting smart technical solutions is not one of them.

The DoD IG investigators disagreed, as this response to Hayden's team at the time makes clear (p. 106):



(C) **Management Comments.** NSA stated that the Technology Demonstration Platform will provide a commercial, extensible, and service-based "plug and play" framework. Though THINTHREAD does employ some commercial-off-the-shelf development products and technologies, that employment is at a lower level; overall, THINTHREAD resides on a custom-developed framework.

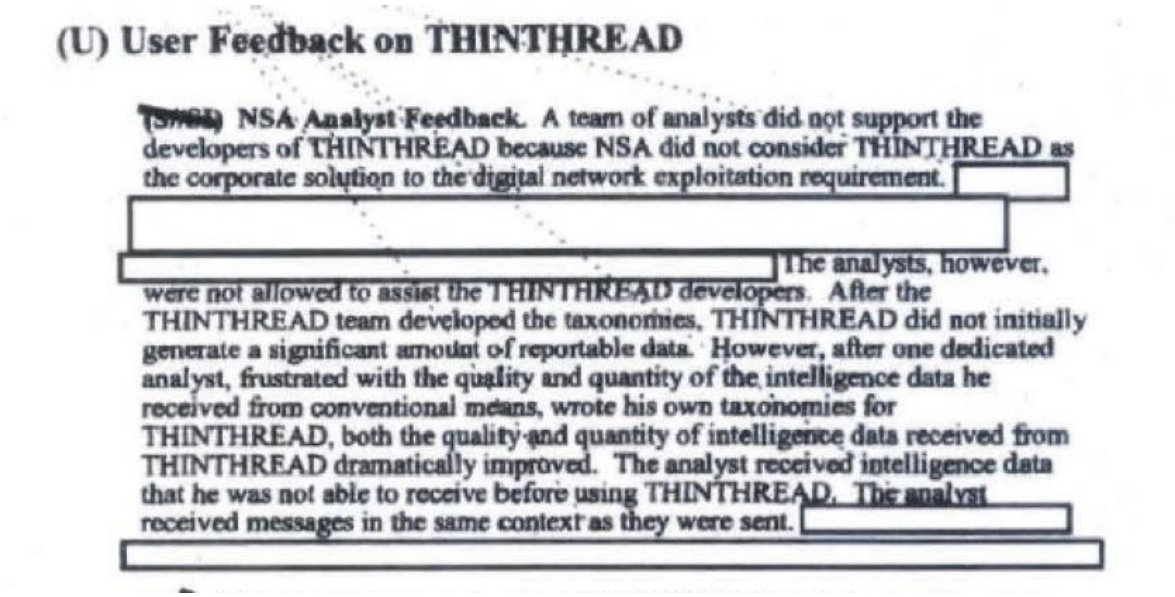
~~(C)~~ **Audit Response.** THINTHREAD was built using readily available commercial off-the-shelf technology and resides on a custom-developed framework that is inexpensive, small, and scalable. Contrary to the statement above, the THINTHREAD framework is extensible and is service-based plug and play.

On THINTHREAD's effectiveness

On page 21 of his book, Hayden gives the reader the impression that THINTHREAD was not that good at actually finding real, actionable intelligence:

We gave it a try and deployed a prototype to Yakima, a foreign satellite (FORNSAT) collection site in central Washington State. Training the system on only one target (among potentially thousands) took several months, and then it did not perform much better than a human would have done. There were too many false positives, indications of something of intelligence value when that wasn't really true. A lot of human intervention was required.

An analyst who had actually used THINTHREAD after its initial prototype deployment in November 2000 had a very different view (p. 16):



(U) User Feedback on THINTHREAD

(TS//SI) NSA Analyst Feedback. A team of analysts did not support the developers of THINTHREAD because NSA did not consider THINTHREAD as the corporate solution to the digital network exploitation requirement. [redacted] The analysts, however, were not allowed to assist the THINTHREAD developers. After the THINTHREAD team developed the taxonomies, THINTHREAD did not initially generate a significant amount of reportable data. However, after one dedicated analyst, frustrated with the quality and quantity of the intelligence data he received from conventional means, wrote his own taxonomies for THINTHREAD, both the quality and quantity of intelligence data received from THINTHREAD dramatically improved. The analyst received intelligence data that he was not able to receive before using THINTHREAD. The analyst received messages in the same context as they were sent. [redacted]

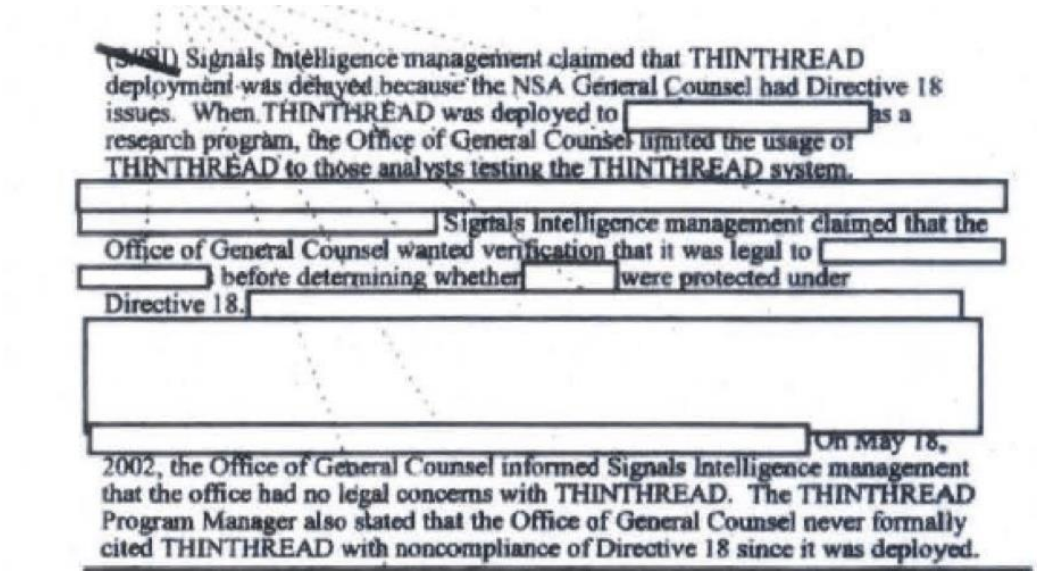
The second to last sentence is worth repeating: "The analyst received intelligence data that he was not able to receive before using THINTHREAD." "*Not able to receive" from any other NSA system or program*. Had THINTHREAD been deployed broadly across NSA and focused on al-Qaeda, it could have helped prevent the 9/11 attacks, as the SARC team and Roark have repeatedly claimed.

On THINTHREAD's legality

Hayden claims in his memoir (page 24) that NSA's lawyers viewed THINTHREAD as illegal: Sometime before 9/11, the Thin Thread advocates approached NSA's lawyers. The lawyers told them that no system could legally do with US data what Thin Thread was designed to do. Thin Thread was based on the broad collection of metadata that would of necessity include foreign-to-foreign, foreign-to-US, and US-to-foreign communications. In other words, lots of US person data swept up in routine NSA collection.

In fact, as the SARC team noted in *A Good American*, THINTHREAD's operational concept was just the opposite: scan the traffic for evidence of foreign bad actors communicating with Americans, segregate and encrypt that traffic, and let the rest go by. No massive data storage problem, no mass spying on Americans.

And the account the DoD IG investigators got from NSA's Office of General Counsel (page 20) flatly contradicts Hayden's memoir:



(S//SI) Signals Intelligence management claimed that THINTHREAD deployment was delayed because the NSA General Counsel had Directive 18 issues. When THINTHREAD was deployed to [redacted] as a research program, the Office of General Counsel limited the usage of THINTHREAD to those analysts testing the THINTHREAD system.

[redacted] Signals Intelligence management claimed that the Office of General Counsel wanted verification that it was legal to [redacted] before determining whether [redacted] were protected under Directive 18. [redacted] On May 16, 2002, the Office of General Counsel informed Signals Intelligence management that the office had no legal concerns with THINTHREAD. The THINTHREAD Program Manager also stated that the Office of General Counsel never formally cited THINTHREAD with noncompliance of Directive 18 since it was deployed.

The "Directive 18" in question is United States Signals Intelligence Directive 18, which governs NSA's legal obligations regarding the acquisition, storage, and dissemination of data on U.S. persons.

As you can probably imagine, I could cite many other instances of Hayden's rewriting of the history of the THINTHREAD-TRAILBLAZER episode, but if you want as much of the story as is currently available, I suggest you read the entire (though still heavily redacted) version of the DoD IG report I obtained in July.

The Story Goes On

What's remarkable is that Congress was well aware of Hayden's misconduct and mismanagement while at NSA, but it still allowed him to become the head of my former employer, the CIA. Meanwhile, Roark's personal example of integrity and fidelity to congressional oversight were rendered meaningless by her then-boss, House Intelligence Committee Chairman (and former CIA operations officer) Porter Goss's (R-FL) failure to fully investigate the THINTHREAD-TRAILBLAZER disaster, and by his Senate colleagues who elected to confirm Hayden to head the CIA by a vote of 78-15. Hayden definitely got one thing very right: He knew he could snow House and Senate members and get away with it.

My FOIA lawsuit is ongoing, and additional document productions are—hopefully—just a few months away. To date, DoD is continuing to invoke the NSA Act of 1959 to keep many details of this saga—especially the amount of money squandered on TRAILBLAZER—from public view. For me, that's actually a key issue in this case—testing the proposition as to whether NSA, utilizing the 1959 law, can conceal indefinitely waste, fraud, abuse, or even criminal conduct from public disclosure.

But the larger policy issue for me is laying bare, using a real-world case study, a prime example of a hugely consequential congressional oversight failure. The SARC team and Roark continue to argue that had THINTHREAD been fully deployed by early 2001, the 9/11 attacks could've

been prevented. Drake asserts in *A Good American* that post-attack testing of THINTHREAD against NSA's PINWALE database uncovered not only the attacks that happened, but ones that didn't for various reasons.

And the SARC team and Roark maintain that THINTHREAD could have accomplished NSA's digital surveillance and early warning mission without the kinds of constitutional violations seen or alleged with programs like the PATRIOT Act's Sec. 215 telephone metadata program or the FISA Amendments Act Sec. 702 program, the latter currently set to expire at the end of this month and the subject of multiple legislative reform proposals.

None of this was examined by either the Congressional Joint Inquiry or the 9/11 Commission, which means the real history of how the 9/11 attacks happened has yet to be written.

Also pending are two Office of Special Counsel investigations into aspects of this episode—one involving Drake, and the other looking at former Assistant DoD IG John Crane, as I've written previously on this site. I'll have more to say on all of this as documents become available or as events warrant.

Patrick G. Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute.