The Intercept_

THE MOST INTRIGUING SPY STORIES FROM 166 INTERNAL NSA REPORTS

Micah Lee, Margot Williams

May 16 2016, 11:37 a.m.

10

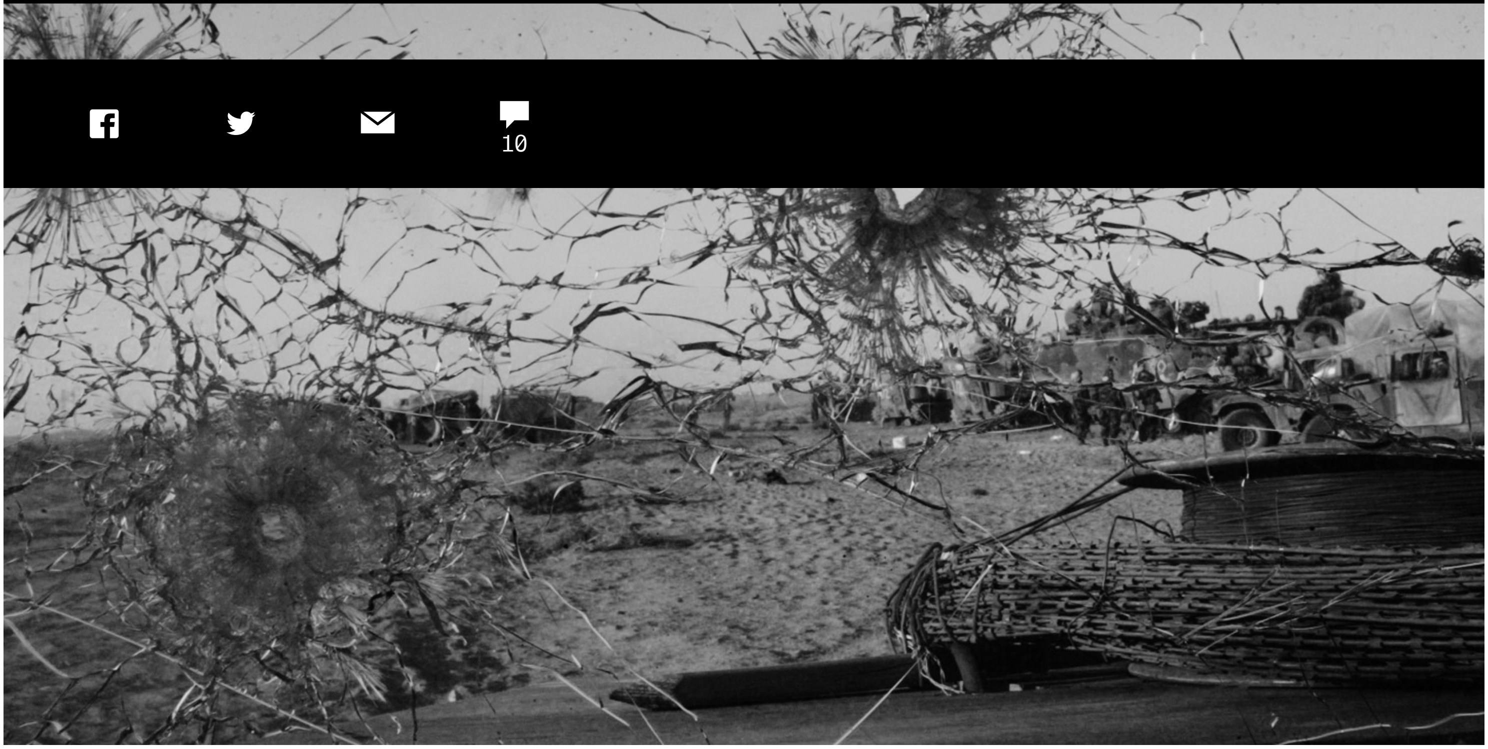


Photo: Joe Raedle/Getty Images

SNOWDEN ARCHIVE —THE SIDTODAY FILES

[redacted] months of 2003, the National Security Agency saw demand for its services spike as a new war in Iraq, as well as ongoing and profound changes in how people used the internet, added to a torrent of new agency work related to the war on terror, according to a review of 166 articles from a restricted agency newsletter.

The Intercept today is releasing the first three months of *SIDtoday*, March 31 through the end of June 2003, using files provided by NSA whistleblower Edward Snowden. In addition, we are releasing any subsequent 2003 installments of *SIDtoday* series that began during this period. The files are available for download here.

We combed through these files with help from other writers and editors with an eye toward finding the most interesting stories, among other concerns.

SIDtoday was launched just 11 days into the U.S. invasion of Iraq by a team within the NSA's Signals Intelligence Directorate. SID is arguably the NSA's most important division, responsible for spying on the agency's targets, and *SIDtoday* became, as Peter Maass documents in an accompanying article, an invaluable primer on how the NSA breaks into and monitors communications systems around the world.

At the outset, *SIDtoday* declared that its mission was to "bring together communications from across the SIGINT Directorate in a single webpage" and that one of its key areas of focus would be providing "information on the Iraq Campaign and Campaign Against Terrorism." And, indeed, the first issues of *SIDtoday* document how the agency paved the way for the Iraq War with diplomatic intelligence, supported the targeting of specific enemies in Iraq, and continued servicing existing "customers" like the Department of the Interior and the Department of Agriculture, whose appetite for signals intelligence grew sharply after the Sept. 11 attacks.

While the agency was helping in Iraq, NSA personnel were also involved in interrogations at Guantánamo Bay, *SIDtoday* articles show, working alongside the military and CIA at a time when prisoners there were treated brutally. *The Intercept*'s Cora Currier describes the NSA's involvement with the interrogations in a separate story, one that also documents how the agency helped with the capture and rendition to Guantánamo of a group of Algerian men in Bosnia.

Other highlights from this set of documents follow below, alongside links to the relevant originals.

U.S. Marines from the 2nd Battalion, 8th Regiment enter the southern Iraqi city of Nasiriyah, March 23, 2003. Photo: Eric Feferberg/AFP/Getty Images

Shock and Awe: The Iraq War in SID

In the first months of the Iraq War, *SIDtoday* articles bragged about the NSA's part in the run-up to the invasion and reflected the Bush administration's confidence that Saddam Hussein had hidden weapons of mass destruction.

At the United Nations, readers were told, "timely SIGINT played a critical role" in winning adoption of resolutions related to Iraq, including by providing "insights into the nuances of internal divisions among the five permanent members of the U.N. Security Council."

When the military deployed to Iraq, SIGINT came too. Maj. Gen. Richard J. Quirk III, then a deputy director of SID, put out an "urgent" call for additional SIGINT analysts to volunteer for 90- to 120-day field deployment, stressing that "SIGINT is wired into our military operations as never before." NSA's Iraq War tasks would include "researching possible locations of stockpiled WMD material." The Geospatial Exploitation Office, placed on 24/7 watch, provided "near-real-time tipping of communications associated with Iraqi leadership and other high-value targets."

POW Pfc. Jessica Lynch being loaded into a military helicopter on her way out of Iraq, April 2, 2003. Photo: CENTCOM/Getty Images

Just three days into the campaign, on March 23, 2003, Pfc. Jessica Lynch and five others were taken prisoner after their convoy from the 507th Maintenance Company went off course near Nasiriyah, Iraq, and lost 11 soldiers in the ensuing attack. On April 1, Special Operations commandos rescued Lynch from her bed at the Saddam Hussein General Hospital in Nasiriyah, swooping down in Black Hawk helicopters and firing explosive charges. (It later emerged that Iraqi forces had previously left the hospital.)

In “SID Support to POW Rescue,” Chief of Staff Charles Berlin revealed that the Lynch rescue was aided by blueprints from the Japanese construction firm that originally built the hospital, blueprints rounded up as the rescue was being planned and sent “as digital files” to the commandos “literally minutes before the aircraft departed with the strike team” on April 1. Information about the hospital had been collected by a dedicated Underground Facility Support Cell created by the NSA in 2002 as part of an interagency effort to assess “the infrastructure and vulnerabilities of underground facilities used by hostile governments or military forces.”

Even before President Bush declared an end to major combat operations in Iraq on May 1, 2003, NSA was preparing its history of the war. Record management officers were given guidance on how to preserve records from the operation, and the general staff was told how to preserve even “seemingly mundane things.”

Soon after the president’s “Mission Accomplished” victory speech, some NSA staff returned from deployment. But the role of signals intelligence in Iraq was not over. The NSA provided “time-sensitive SIGINT” support, including a “summary of contacts,” to aid the May 22, 2003, capture of a top Baathist official, Aziz Sajih Al-Numan, “king of diamonds” in the deck of playing cards that featured U.S. Central Command’s wanted Iraqis. Al-Numan was caught within 25 hours after the Army contacted NSA to request support. “Well done to all involved in his capture!” a *SIDtoday* article declared.

In June, the “ace of diamonds,” Saddam’s secretary Abid Hamid Mahmud al-Tikriti, was captured thanks to “near-real-time tipping [of geospatial intelligence] to the Special Operations Forces engaged in the hunt,” along with rapid translation of intercepted conversations, *SIDtoday* bragged.

As the end of the quarter approached, *SIDtoday* reported on portents of continued resistance and warned, “The scope of hostilities is greater than many may realize,” and, separately, that “Iraq is still a troubled environment and much work needs to be done.”

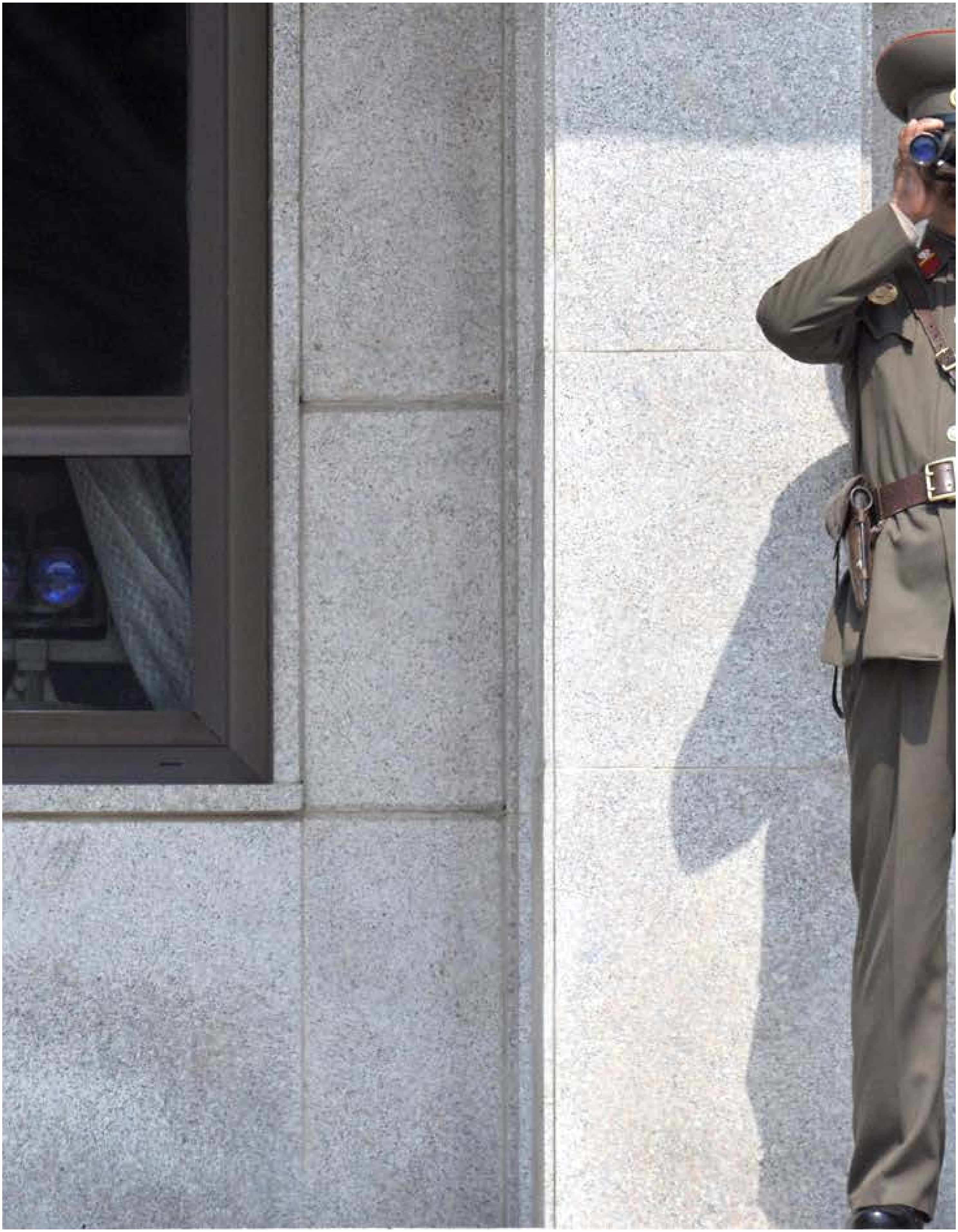
Additional *SIDtoday* articles about Iraq are available here.

Hunting a Russian Mobster, “Mr. Kumarin”

In an example of highly targeted intelligence gathering, the NSA spent “many months” acquiring the phone number of a Russian organized crime figure and began intercepting his calls, according to a May 2003 article. The intelligence work was sparked by the State Department, which in 2002 requested information on the leader of the Tambov crime syndicate in Russia, referred to only as “Mr. Kumarin,” and about any links between the syndicate and Russian President Vladimir Putin.

In 2009, the Russian authorities tried and convicted Vladimir

Kumarin, who had changed his name to Vladimir Barsukov, for fraud and money laundering. The *New York Times* compared him to a "Russian John Gotti." He was sentenced to 14 years in prison.



A North Korean soldier looks south through binoculars at the truce village of Panmunjom in the demilitarized zone dividing North and South Korea on April 9, 2009. Photo: Jung Yeon-Je/AFP/Getty Images

Uncovering North Korean Nuclear Efforts

As previously shown, NSA signals intelligence was used to inform negotiations over U.N. resolutions against Iraq in early 2003. But that wasn't the only time the agency influenced diplomacy: In 2002, signals intelligence ignited a confrontation between North Korea and the U.S., according to a *SIDtoday* article from April 2003. NSA eavesdroppers discovered that North Korea was developing a uranium enrichment capability in violation of an agreement with the U.S. When the State Department presented the evidence at a meeting in Pyongyang that October, the North Koreans admitted it was true, the article said, setting off the clash.

"The ONLY source of information on this treaty violation was SIGINT derived from North Korean external communications," an NSA manager wrote in *SIDtoday*. "This is both a SIGINT success story and an example of how cross-organizational collaboration can produce key intelligence. Hats off to everyone involved!"

Orbital Signals Intelligence

For more than 30 years, one *SIDtoday* article from June 2003 explained, the NSA had tapped into communications from foreign satellites. Though the program associated with this monitoring, FORNSAT, has been previously disclosed, this document adds important context. For example, it made FORNSAT sound like an intelligence gold mine, having "consistently provided … over 25 percent of end product reporting." It also explained what sorts of information the NSA gleaned from satellites — "intelligence derived from diplomatic communications … airline reservations and billing data … traffic about terrorists, international crime, weapons of mass destruction … international finance and trade."

The problem, at the time the article was written, was that FORNSAT was in "dire need of upgrade" because it was "primarily engineered for voice" communications and needed to shift to intercepting more digital communications, including digital video. It also needed to be expanded to tap into mobile satellite phone systems, which "use hundreds of spot beams. Our 13 fixed FORNSAT sites cannot provide the necessary access."

Leaks Included in 5,000 "Insecurity Records"

Ten years before Edward Snowden gave a trove of NSA documents to journalists Glenn Greenwald and Laura Poitras, a "chief" within SID's Communications and Support Operations organization described in *SIDtoday* the great lengths the agency went to in order to track leaks. In a profile of the Intelligence Security Issues office within CSO, this person said that ISI scanned 350 press items daily for "cryptologic insecurities" and maintained a database called FIRSTFRUIT with "over 5,000 insecurity-related records" ranging from "espionage damage assessments" to "liaison exchanges." This

ISI profile ran as part of a broader *SIDtoday* series on the CSO organization.

Technology Pushed NSA Into the Tablet Era — and Tons of Gear Went Missing

One theme that emerges from early 2003 *SIDtoday* installments is that the NSA was grappling with how to handle advances in information technology, particularly the proliferation of mobile devices and online networks.

One article in the "Customer Relations" series described several "dynamic dissemination products" to help SID "change with … our customers," including an initiative to distribute "secret-level information" to wireless devices, a technique for disseminating "NSA product" to tablet computers, and a system to view secret documents on unclassified computers over the internet, bypassing the need for a high-security enclosed area known as a SCIF. These efforts foreshadowed Hillary Clinton's controversial use, as secretary of state, of a BlackBerry device to traffic in sensitive government information after the NSA reportedly rebuffed her request for a special secure device from the agency.

Another article highlighted that the NSA was a heavy user of mobile devices even four years before the release of the first iPhone, calling on staffers to help catalogue all computers, including "laptops, palmtops/PDAs, etc.," for an annual inventory.

The document also stated that $27 million worth of equipment remained “unaccounted for” after the prior year’s audit, which ended just two months earlier.

In addition to making secret information accessible to more people, SID was developing new systems to solve long-standing problems. The JOURNEYMAN program, described in another article, aimed to develop a system for distributing SIGINT reports to many different recipients at once across different networks with different formatting requirements. Another system, PATENTHAMMER, collected cellular, fax, and pager signals for the Special Operations Command and also allowed users to access information collected in the past.

SID was also still exploring the rapidly evolving internet. One article described how the NSA was improving its integration with the public internet via a program called OUTPARKS. Another touted the NSA’s annual SIGDEV conference, a major event in which analysts from the “five eyes” intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States share techniques for developing new SIGINT. The article noted that the 2003 SIGDEV would include workshops on “social network analysis,” “internet research,” and “wireless LANs,” that is, wifi networks.

Other NSA staff apparently required more basic forms of training. “Do you know you can make *SIDtoday* your browser homepage?” asked a June 2003 article, with instructions on changing the default homepage in the web browsers popular at the time: Netscape and Internet Explorer.

Sept. 12, 2001, shows an area of white dust and smoke at the location where the 1,350-foot towers of the World Trade Center once stood in New York City. Photo: Spaceimaging.com/Getty Images

Demand for NSA Intelligence Became "Voracious"

The Signals Intelligence Directorate is full of expert spies, but they don't choose who to spy on themselves. In the corporate lingo of

SID, the "customer" decides, customers "including all departments of the executive branch," according to the agency's website. And the demand from customers exploded in 2003, judging from a series of *SIDtoday* articles about the Customer Relationships Directorate, an office focused on ensuring that NSA's customers get what they need.

One driver of this demand was the war on terror; inbound SIGINT requests to the NSA's National Security Operations Center went from 300 in the two weeks after the Sept. 11 attacks to 1,700 by the end of the year, according to one *SIDtoday* article. Existing customers like the Department of the Interior and the Department of Agriculture "suddenly became voracious consumers" of signals intelligence, as one article from April 2003 put it, and brand new customers appeared on the scene, such as the newly created Department of Homeland Security. SID also increased its interaction with domestic law enforcement agencies like the FBI and the Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Another driver of heightened SIGINT demand was the war in Iraq. According to the document describing the NSA's role in war-related U.N. Security Council resolutions, "The number of timely SIGINT tippers delivered to [the U.S. Mission to the United Nations] during key points in the negotiations increased by a factor of four."

Creating a "Plausible Cover" for Sensitive Intelligence Sources

Amid strong demand for intelligence, the NSA sometimes needed to alter sensitive information so it could be shared more widely. As part of *SIDtoday*'s explainer series "ConSIDer This," one unknown author from the SIGINT communications team explained how to lower the classification level of intercepted communications, or COMINT, a process known as "downgrading." The process could involve some subterfuge. "In order to downgrade COMINT, a plausible cover (i.e., collection from a less sensitive source) must exist," the article stated.

Changing of the Guard at SID

As *SIDtoday* launched in 2003, the Signals Intelligence Directorate was in the midst of a leadership change as Director Maureen Baginski moved to a new position as the FBI's head of intelligence and Maj. Gen. Quirk replaced her. Several other new managers and technical directors introduced themselves in the online newsletter's series "Getting to Know the SID Leadership Team." Also in that series: A senior technical leader complained that "voice dominates our reporting today, yet [digital information] is much more prolific in the global net" and explored reasons for this shortcoming.

The radar domes of RAF Menwith Hill in North Yorkshire dominate the skyline, Oct. 30, 2007, Harrogate, England. Photo: Christopher Furlong/Getty Images

Life Stationed Abroad for SID Staffers

Throughout the second half of 2003, employees of the Signals Intelligence Directorate contributed articles to the series "SID Around the World," a sort of collective travelogue on their tours outside the Fort Meade, Maryland, headquarters of the NSA. SID staffers seemed to most enjoy local cuisine: beer, strawberries, chocolates, and ramen, although one touted the possibility of "less than a four-hour drive" from the NSA's U.K. Menwith Hill site for a

"Taco Bell or Cinnabon fix." Interspersed with recommendations for Rhineland wineries, Japanese communal hot baths, and winter sports in Colorado were some interesting facts about NSA's global reach in 2003. The majority of signals processed at the Kunia operations center in Hawaii were collected on Okinawa. Some of the NSA's representatives in Mons, Belgium, worked in an underground bunker. The Misawa base in Japan had just 25 civilian NSA personnel, while Menwith Hill had several hundred.

SIDtoday's "Around the World" to Guantánamo Bay is part of a larger story on the NSA's role in interrogations.

Office Space: NSA Edition

SIDtoday's "A Day in the Life" series provided first-person accounts of the various jobs within the Signals Intelligence Directorate. For example, one "Day in the Life" described the work of a mathematician in the field of "diagnosis," that is, studying encryption systems in order to understand their weaknesses. "During the course of a normal day," the mathematician wrote, "I run cryptanalytic routines on UNIX desktop workstations, supercomputers, and special-purpose devices using available software tools. The routines employ standard cryptanalytic tests which search for patterns and non-random properties in data."

The series also included an article written by Maj. Gen. Quirk's executive assistant — the "conscience" of a "senior leader" — and another by a senior operations officer whose work involved entertaining Fox News personality Tony Snow before he became White House press secretary.

Peer Review for Spies: NSA's Learned Organizations

For an academic, there is no better way to improve your career than to get published in prestigious journals and to win prestigious awards. But what if your research is classified and you can't ever get the public recognition you deserve without betraying state secrets? If you work for the NSA, you look to one of the agency's Learned Organizations to receive your academic accolades.

SIDtoday included a series of articles that shines a spotlight on NSA's Learned Organizations, including the cryptanalysis-focused KRYPTOS Society; the Crypto-Linguistic Association, focused on language analysis, with events that in 2002 included a luncheon with the director of the Klingon Institute; the Collection Association, whose membership evolved from spies gathering intelligence via antennas to also include the monitoring of satellites and internet sleuthing; the Crypto-Mathematics Institute, NSA's oldest Learned Organization, founded in 1957, whose activities included an essay contest; and the International Affairs Institute.

Related Stories:

- Snowden Archive — The SIDtoday Files
- The Intercept Is Broadening Access to the Snowden Archive. Here's Why
- What It's Like to Read the NSA's Newspaper for Spies
- NSA Closely Involved in Guantánamo Interrogations,

Documents Show

CONTACT THE AUTHOR:

Micah Lee

✉ micah.lee@theintercept.com

@micahflee

Margot Williams

✉ margot.williams@theintercept.com

@MargotWilliams

10 Comments