CORE SECRETS: NSA SABOTEURS IN CHINA AND GERMANY

BY PETER MAASS AND LAURA POITRAS *@maassp*

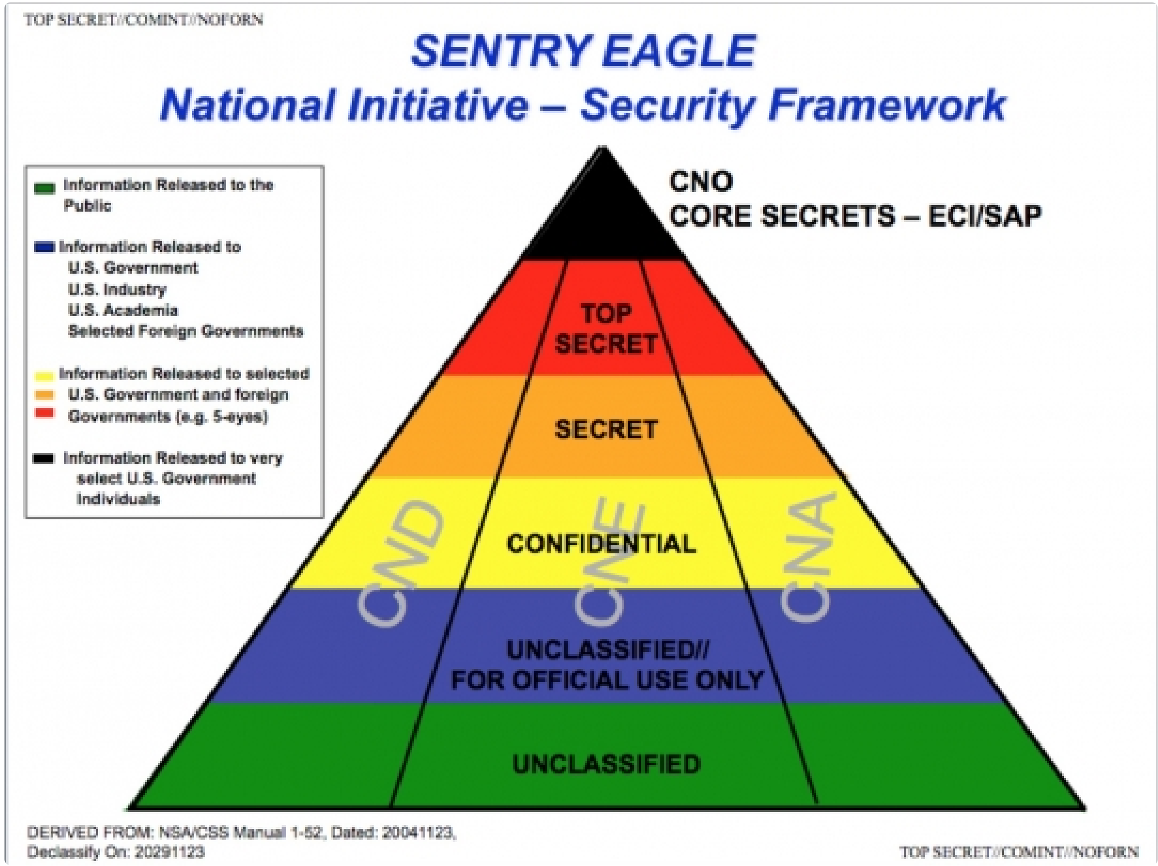
10/11/2014

The National Security Agency has had agents in China, Germany, and South Korea working on programs that use "physical subversion" to infiltrate and compromise networks and devices, according to documents obtained by *The Intercept*.

The documents, leaked by NSA whistleblower Edward Snowden, also indicate that the agency has used "under cover" operatives to gain access to sensitive data and systems in the global communications industry, and that these secret agents may have even dealt with American firms. The documents describe a range of clandestine field activities that are among the agency's "core secrets" when it comes to computer network attacks, details of which are apparently shared with only a small number of officials outside the NSA.

"It's something that many people have been wondering about for a long time," said Chris Soghoian, principal technologist for the American Civil Liberties Union, after reviewing the documents. "I've had conversations with executives at tech companies about this precise thing. How do you know the NSA is not sending people into your data centers?"

Previous disclosures about the NSA's corporate partnerships have focused largely on U.S. companies providing the agency with vast amounts of customer data, including phone records and email traffic. But documents published today by *The Intercept* suggest that even



TOP SECRET//COMINT//NOFORN

SENTRY EAGLE
National Initiative – Security Framework

🟩 Information Released to the Public

🟦 Information Released to
U.S. Government
U.S. Industry
U.S. Academia
Selected Foreign Governments

🟨 🟧 🟥 Information Released to selected U.S. Government and foreign Governments (e.g. 5-eyes)

⬛ Information Released to very select U.S. Government Individuals

CNO
CORE SECRETS – ECI/SAP

TOP SECRET

SECRET

CONFIDENTIAL

UNCLASSIFIED//
FOR OFFICIAL USE ONLY

UNCLASSIFIED

CND

CNE

CNA

DERIVED FROM: NSA/CSS Manual 1-52, Dated: 20041123,
Declassify On: 20291123

TOP SECRET//COMINT//NOFORN

as the agency uses secret operatives to penetrate them, companies have also cooperated more broadly to undermine the physical infrastructure of the internet than has been previously confirmed.

In addition to so-called “close access” operations, the NSA’s “core secrets” include the fact that the agency works with U.S. and foreign companies to weaken their encryption systems; the fact that the NSA spends “hundreds of millions of dollars” on technology to defeat commercial encryption; and the fact that the agency works with U.S. and foreign companies to penetrate computer networks, possibly without the knowledge of the host countries. Many of the NSA’s core secrets concern its relationships to domestic and foreign corporations.

Some of the documents in this article appear in a new documentary, *CITIZENFOUR*, which tells the story of the Snowden disclosures and is directed by *Intercept* co-founder Laura Poitras. The documents describe a panoply of programs classified with the rare designation of “Exceptionally Compartmented Information,” or ECI, which are only disclosed to a “very select” number of government officials.

Sentry Eagle

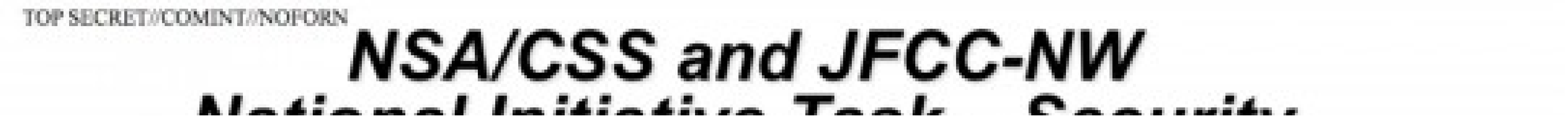
The agency’s core secrets are outlined in a 13-page “brief sheet” about Sentry Eagle, an umbrella term that the NSA used to encompass its most sensitive programs “to protect America’s cyberspace.”

“You are being indoctrinated on Sentry Eagle,” the 2004 document begins, before going on to list the most highly classified aspects of its various programs. It warns that the details of the Sentry Eagle programs are to be shared with only a “limited number” of people, and even then only with the approval of one of a handful of senior intelligence officials, including the NSA director.

“The facts contained in this program constitute a combination of the greatest number of highly sensitive facts related to NSA/CSS’s overall cryptologic mission,” the briefing document states. “Unauthorized disclosure…will cause exceptionally grave damage to U.S. national security. The loss of this information could critically compromise highly sensitive cryptologic U.S. and foreign relationships, multi-year past and future NSA investments, and the ability to exploit foreign adversary cyberspace while protecting U.S. cyberspace.”

The document does not provide any details on the identity or number of government officials who were supposed to know about these highly classified programs. Nor is it clear what sort of congressional or judicial oversight, if any, was applied to them. The NSA refused to comment beyond a statement saying, “It should come as no surprise that NSA conducts targeted operations to counter increasingly agile adversaries.” The agency cited Presidential Policy Directive 28, which it claimed “requires signals intelligence policies and practices to take into account the globalization of trade, investment and information flows, and the commitment to an open, interoperable, and secure global Internet.” The NSA, the statement concluded, “values these principles and honors them in the performance of its mission.”

Sentry Eagle includes six programs: Sentry Hawk (for activities involving computer network exploitation, or spying), Sentry Falcon (computer network defense), Sentry Osprey (cooperation with the CIA and other intelligence agencies), Sentry Raven (breaking encryption systems), Sentry Condor (computer network operations and attacks), and Sentry Owl (collaborations with private companies). Though marked as a draft from 2004, it refers to the various programs in language indicating that they were ongoing at the time, and later documents in the Snowden archive confirm that some of the activities were going on as recently as 2012.



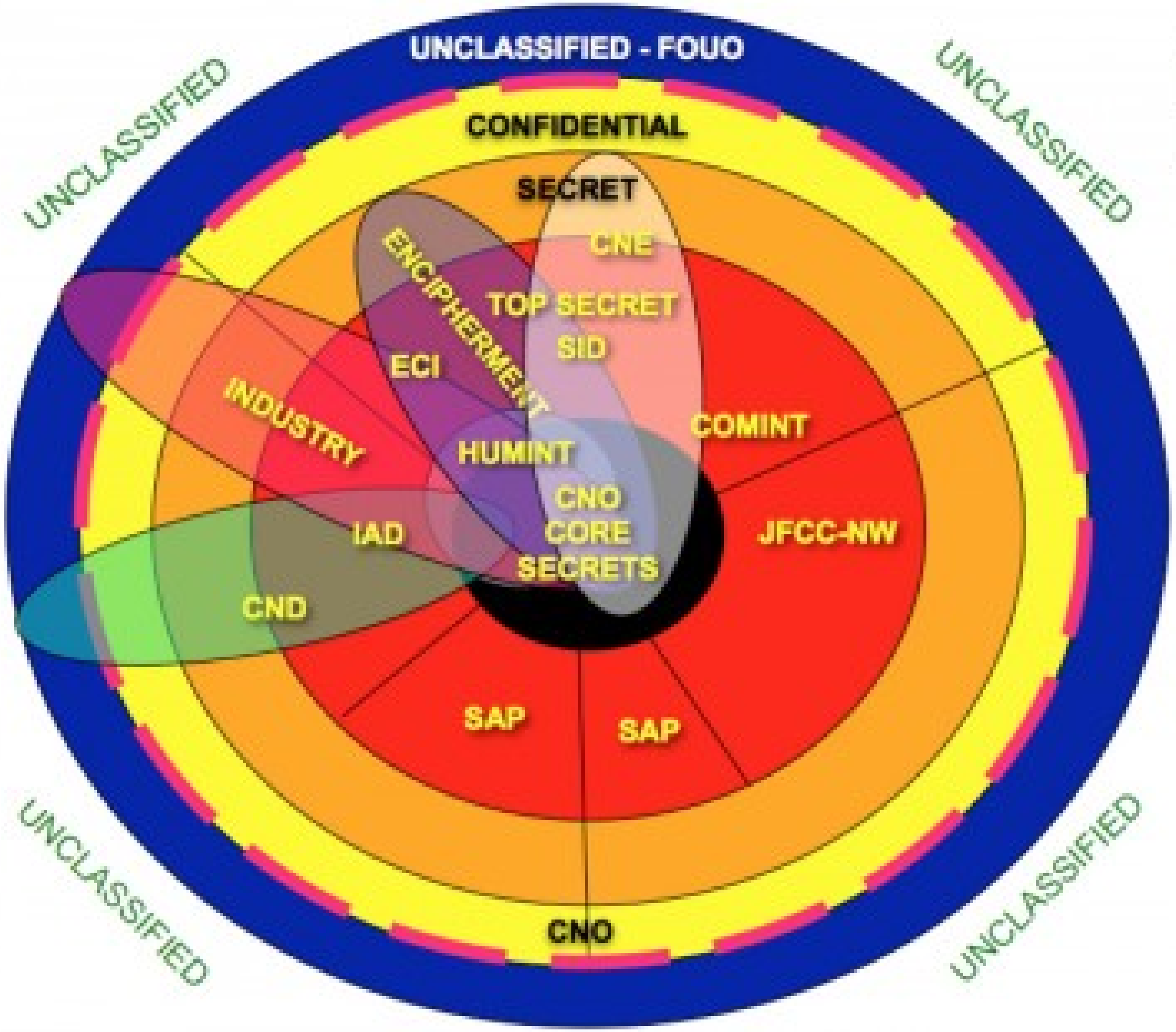
TOP SECRET//COMINT//NOFORN

NSA/CSS and JFCC-NW

National Initiative Task – Security

National Initiative Task – Security Framework

SAP Authority	NSA/CSS/JFCC-NW SAPS		
DNI	CNE		
DoD		CND	CNA



🟩 Information Released to the Public

🟦 Information Released to
U.S. Government
U.S. Industry
U.S. Academia
Selected Foreign Governments

🟨 🟧 🟥 Information Released to selected U.S. Government and foreign Governments (e.g. 5-eyes)

⬛ Information Released to very select U.S. Government Individuals

TOP SECRET//COMINT//NOFORN

TAREX

One of the most interesting components of the “core secrets” involves an array of clandestine activities in the real world by NSA agents working with their colleagues at the CIA, FBI, and Pentagon. The NSA is generally thought of as a spying agency that conducts its espionage from afar—via remote commands, cable taps, and malware implants that are overseen by analysts working at computer terminals. But the agency also participates in a variety of “human intelligence” programs that are grouped under the codename Sentry Osprey. According to the briefing document’s description of Sentry Osprey, the NSA “employs its own HUMINT assets (Target Exploitation—TAREX) to support SIGINT operations.”

According to a 2012 classification guide describing the program, TAREX “conducts worldwide clandestine Signals Intelligence (SIGINT) close-access operations and overt and clandestine Human Intelligence (HUMINT) operations.” The NSA directs and funds the operations and shares authority over them with the Army’s Intelligence and Security Command. The guide states that TAREX personnel are “integrated” into operations conducted by the CIA, FBI, and Defense Intelligence Agency. It adds that TAREX operations include “off net-enabling,” “supply chain-enabling,” and “hardware implant-enabling.”

According to another NSA document, off-net operations are “covert or clandestine field activities,” while supply-chain operations are “interdiction activities that focus on modifying equipment in a target’s supply chain.”

The NSA’s involvement in supply-chain interdiction was previously revealed in *No Place to Hide*, written by *Intercept* co-founder Glenn Greenwald. The book included a photograph of intercepted packages being opened by NSA agents, and an accompanying NSA document explained the packages were “redirected to a secret location” where the agents implanted surveillance beacons that secretly communicated with NSA computers. The document did not say how the packages were intercepted and did not suggest, as the new documents do, that interception and implants might be done by clandestine agents in the field.

The TAREX guide lists South Korea, Germany, and Beijing, China as sites where the NSA has deployed a “forward-based TAREX presence;” TAREX personnel also operate at domestic NSA centers in Hawaii, Texas, and Georgia. It also states that TAREX personnel are assigned to U.S. embassies and other “overseas locations,” but does not specify where. The document does not say what the “forward-based” personnel are doing, or how extensive TAREX operations are. But China, South Korea, and Germany are all home to large telecommunications equipment manufacturers, and China is known to be a key target of U.S. intelligence activities.

Although TAREX has existed for decades, until now there has been little information in the public domain about its current scope. A 2010 book by a former Defense Intelligence Agency officer, Lt. Col. Anthony Shaffer, described TAREX operations in Afghanistan as consisting of "small-unit, up-close, intelligence-gathering operatives. Usually two-to-three man units."

"Under Cover" Agents

The most controversial revelation in Sentry Eagle might be a fleeting reference to the NSA infiltrating clandestine agents into "commercial entities." The briefing document states that among Sentry Eagle's most closely guarded components are "facts related to NSA personnel (under cover), operational meetings, specific operations, specific technology, specific locations and covert communications related to SIGINT enabling with specific commercial entities (A/B/C)."

It is not clear whether these "commercial entities" are American or foreign or both. Generally the placeholder "(A/B/C)" is used in the briefing document to refer to American companies, though on one occasion it refers to both American and foreign companies. Foreign companies are referred to with the placeholder "(M/N/O)." The NSA refused to provide any clarification to *The Intercept*.

The document makes no other reference to NSA agents working under cover. It is not clear whether they might be working as full-time employees at the "commercial entities," or whether they are visiting commercial facilities under false pretenses. The CIA is known to use agents masquerading as businessmen, and it has used shell companies in the U.S. to disguise its activities.

There is a long history of overt NSA involvement with American companies, especially telecommunications and technology firms. Such firms often have employees with security clearances who openly communicate with intelligence agencies as part of their duties, so that the government receives information from the companies that it is legally entitled to receive, and so that the companies can be alerted to classified cyber threats. Often, such employees have previously worked at the NSA, FBI, or the military.

But the briefing document suggests another category of employees—ones who are secretly working for the NSA without anyone else being aware. This kind of double game, in which the NSA works with and against its corporate partners, already characterizes some of the agency's work, in which information or concessions that it desires are surreptitiously acquired if corporations will not voluntarily comply. The reference to "under cover" agents jumped out at two security experts who reviewed the NSA documents for *The Intercept*.

“That one bullet point, it’s really strange,” said Matthew Green, a cryptographer at Johns Hopkins University. “I don’t know how to interpret it.” He added that the cryptography community in America would be surprised and upset if it were the case that “people are inside [an American] company covertly communicating with NSA and they are not known to the company or to their fellow employees.”

The ACLU’s Soghoian said technology executives are already deeply concerned about the prospect of clandestine agents on the payroll to gain access to highly sensitive data, including encryption keys, that could make the NSA’s work “a lot easier.”

“As more and more communications become encrypted, the attraction for intelligence agencies of stealing an encryption key becomes irresistible,” he said. “It’s such a juicy target.”

Of course the NSA is just one intelligence agency that would stand to benefit from these operations. China’s intelligence establishment is believed to be just as interested in penetrating American companies as the NSA is believed to be interested in penetrating Chinese firms.

“The NSA is a risk [but] I worry a lot more about the Chinese,” said Matthew Prince, chief executive of CloudFlare, a server company. “The insider threat is a huge challenge.” Prince thinks it is unlikely the NSA would place secret agents inside his or other American firms, due to political and legal issues. “I would be surprised if that were the case within any U.S. organization without at least a senior executive like the CEO knowing it was happening,” he said. But he assumes the NSA or CIA are doing precisely that in foreign companies. “I would be more surprised if they didn’t,” he said.

Corporate Partners

The briefing sheet’s description of Sentry Owl indicates the NSA has previously unknown relationships with foreign companies. According to the document, the agency “works with specific foreign partners (X/Y/Z) and foreign commercial industry entities” to make devices and products “exploitable for SIGINT”—a reference to signals intelligence, which is the heart of the NSA’s effort to collect digital communications, such as emails, texts, photos, chats, and phone records. This language clarifies a vague reference to foreign companies that appears in the secret 2013 budget for the intelligence community, key parts of which were published last year from the Snowden archive.

The document does not name any foreign companies or products, and gives no indication of the number or scale of the agency's ties to them. Previous disclosures from the Snowden archive have exposed the agency's close relationships with foreign intelligence agencies, but there has been relatively little revealed about the agency gaining the help of foreign companies.

The description of Sentry Hawk, which involves attacks on computer networks, also indicates close ties with foreign as well as American companies. The document states that the NSA "works with U.S. and foreign commercial entities…in the conduct of CNE [Computer Network Exploitation]." Although previous stories from the Snowden archive revealed a wide range of NSA attacks on computer networks, it has been unclear whether those attacks were conducted with the help of "commercial entities"—especially foreign ones. The document does not provide the names of any of these entities or the types of operations.

Green, the cryptography professor, said "it's a big deal" if the NSA is working with foreign companies on a greater scale than currently understood. Until now, he noted, disclosures about the agency's corporate relationships have focused on American companies. Those revelations have harmed their credibility, nudging customers to foreign alternatives that were thought to be untouched by the NSA. If foreign companies are also cooperating with the NSA and modifying their products, the options for purchasing truly secure telecommunications hardware are more limited than previously thought.

The briefing sheet does not say whether foreign governments are aware that the NSA may be working with their own companies. If they are not aware, says William Binney, a former NSA crypto-mathematician turned whistleblower, it would mean the NSA is cutting deals behind the backs of friendly and perhaps not-so-friendly governments.

"The idea of having foreign corporations involved without any hint of any foreign government involved is significant," he said. "It will be an alert to all governments to go check with their companies. Bring them into parliament and put them under oath."

The description of Sentry Raven, which focuses on encryption, provides additional confirmation that American companies have helped the NSA by secretly weakening encryption products to make them vulnerable to the agency. The briefing sheet states the NSA "works with specific U.S. commercial entities…to modify U.S manufactured encryption systems to make them exploitable for SIGINT." It doesn't name the commercial entities or the encryption tools they modified, but it appears to encompass a type of activity that Reuters revealed last year—that the NSA paid $10 million to the security firm RSA to use a weak random number generator in one of its encryption programs.

The avalanche of NSA disclosures since the Snowden leaks began in 2013 has shattered whatever confidence technologists once had about their networks. When asked for comment on the latest documents, Prince, the CEO of CloudFlare, began his response by saying, “We’re hyper-paranoid about everything.”

Documents:

- Sentry Eagle Brief Sheet (13 pages)
- TAREX Classification Guide (7 pages)
- Exceptionally Controlled Information Listing (6 pages)
- ECI WHIPGENIE Classification Guide (7 pages)
- ECI Pawleys Classification Guide (4 pages)
- ECI Compartments (4 pages)
- CNO Core Secrets Slide Slices (10 pages)
- CNO Core Secrets Security Structure (3 pages)
- Computer Network Exploitation Classification Guide (8 pages)
- CNO Core Secrets (7 pages)

Fact checking by Alleen Brown. Research by Margot Williams.

✉ Email the authors: peter.maass@theintercept.com, laura.poitras@theintercept.com

209 DISCUSSING

SHOW COMMENTS

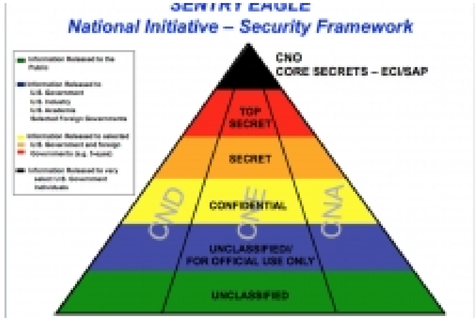
Comments closed.

RECOMMENDED

How the UAE Tried to Silence a Popular Arab Spring Activist

The FBI Director’s Evidence Against Encryption Is Pathetic

Blowing the Whistle on CIA Torture from Beyond the Grave



Core Secrets: NSA Saboteurs in China and Germany

Edward Snowden’s Girlfriend, Lindsay Mills, Moved to Moscow to Live with Him

A Wrongful Conviction Robbed William Lopez of His Freedom, and Then His Life

The NSA and Me

New Zealand Cops Raided Home of Reporter Working on Snowden Documents