University of Wroclaw
Institute of Informatics

Igor Tryhub

"No Such Agency. The history and future of the NSA. What are normal activities of such institutions in democratic countries and beyond their borders?"

Wroclaw 2016

Organization and History

In the early stages of the Cold War in the United States there was no single authority responsible for radio intelligence. Relevant units were in aviation, the army and navy, but were independent and their responsibilities often overlap. For coordination in accordance with the law on national security in 1947, Armed Forces Security Agency (AFSA) was created. Beginning in June 1950, the Korean War showed the inefficiency of the new agency: the military high command were dissatisfied with the quality supplied to them strategic information. Due to the uncertain authority and ill-established cooperation with other services, AFSA was another body which carries out exploration, rather than to combine existing. The investigation of failures of the AFSA lead to decision to establish a new body with more powers, and give him all the functions of electronic intelligence. So, the secret directive of President Truman on October 24, 1952 was established by the National Security Agency.

Creation of the NSA was kept secret until 1957 the agency is not mentioned in any official document. Only in 1957 it was mentioned in the annual United States Government Manual as "separately organized agency within the Ministry of Defense, under the direction and control of the Secretary of Defense ... that performs highly specialized technical functions in support of the intelligence activities of the United States".[1]

Despite the mystery that surrounds the agency over the years have been revealed some of its work, e.g.:

- recordings of conversations of Leonid Brezhnev with the highest level Soviet dignitaries conducted with telephone installed in the limousine of the Secretary of the CPSU;
- chats of the dictator of Panama, Manuel Antonio Noriega, with his lover, which captured information that helped to identify the Libyans responsible for the bombing of a passenger plane a Pan Am in 1988;
- recordings of telephone conversations Colombian cocaine lord Pablo Escobar, allowing to locate his whereabouts.

Throughout the Cold War, the NSA hostilely treated the attempts by writers and journalists to lift the veil of secrecy over the organization. Works on cryptography rarely appeared in the press, as most researches were classified. When in 1967, David Kahn was preparing for the publication of the book "Codebreakers", which included some information on the techniques used in the NSA, the agency tried to prevent its publication. In 1982, a book of James Bamford "The Puzzle Palace" was published - the first book entirely dedicated to the NSA. The author used the documents which access was granted in accordance with the Freedom of Information Act. Trying to prevent the publication of the book, the government changed the degree of secrecy of certain documents. To this day, the book remains virtually the only full-scale work dedicated to NSA.[2]

The National Security Agency (NSA) is therefore an intelligence organization of the United States government, responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes (aka SIGINT).

Foreign analogs of the NSA are:

- Russia: Special Communications Service of Russia
- UK: Government Communications Headquarters
- Canada: Communications Security Establishment Canada
- France: Frenchelon.

The Central Security Service (CSS) is an agency of the United States Department of Defense, which was established in 1972 to integrate the National Security Agency (NSA) and the Service Cryptologic Elements (SCE) of the United States Armed Forces in the field of signals intelligence, cryptology and information assurance at the tactical level.[3]

Although many of NSA's programs rely on "passive" electronic collection, the agency is authorized to accomplish its mission through active clandestine means,[4] among which are physically bugging electronic systems[5] and allegedly engaging in sabotage through subversive software.[6] Moreover, NSA maintains physical presence in a large number of countries across the globe, where its Special Collection Service (SCS) inserts eavesdropping devices in difficult-to-reach places. SCS collection tactics allegedly encompass "close surveillance, burglary, wiretapping, breaking and entering".[7]

Due to a secret agreement concluded in 1947, so-called UKUSA Agreement (United Kingdom - United States of America Security Agreement) combines the operations of a radio intelligence in Australia, Canada, New Zealand, the United States and Great Britain. Despite cooperation through the UKUSA agreement, there was no shortage of events such as concealing of important information and mutual suspicion. The headquarters of the CIA created a special headquarters for just such projects.

The number of employees and an annual budget of the Agency is classified information. There are various estimates of these numbers: the number of employees at headquarters is estimated at 20,000-38,000 people. In addition, about 100,000 electronic warfare specialists, psychological warfare and cryptography work in US military bases around the world.[2] By scattered estimated budget of the NSA may be from 3.5 to 13 billion USD., Which makes it the most funded intelligence agency of the world.[8]

Budget of US intelligence in 2013 (in billions USD):

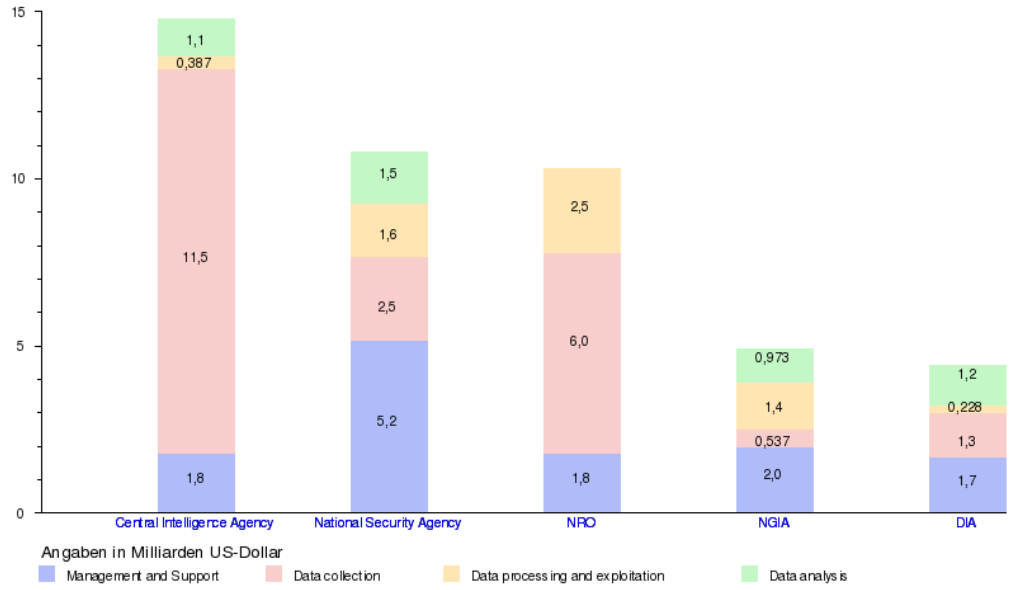


Image source: https://de.wikipedia.org/wiki/National_Security_Agency

Fort Meade is the main center for encryption studies of the NSA. Its computer research center is considered to be the largest concentration of mathematicians in the world. Fort Meade is able to fully sustain all of its vital functions. It has its own power station, television network, police

office, libraries, cafes, bars, various social facilities, including schools and kindergarten. Two glass buildings in the complex were built in 1984 and 1986 and are equipped with protection against electronic intelligence. National Security Agency is the largest employer and second largest recipient of electricity in Maryland.

In Utah, there was being built a largest data center, which would allow to store 5 zettabytes of data.[9] The total cost of the data center was projected to be between $1.5 billion up to $2 billion, and construction was supposed to be completed in September 2013.[10]

After the collapse of the Soviet Union and the Cold War, the NSA, as well as the CIA and the DIA, and other intelligence agencies of the United States, were looking for other new activities such as electromagnetic intelligence (ELINT) data collection.

NSA is the main operator of the global interception system "Echelon". In 1990, in order to maintain its budget in the changed conditions of the agency had to change their field of activity. In the early 1990s, surveillance of the collapsed Soviet Union, and especially Russia, remained to be its main task, as in this part of the globe is placed considerable nuclear capability. Later on, it redefined its priority as obtaining not military, but economic data. The object of observation began, many countries - allies of the United States, whose banks, trading and industrial companies successfully compete in the global market with US partners.

After the suicide terrorist attacks on the World Trade Center and the Pentagon on 11 September 2001, "terrorism" has become a foreground of its activities.

The topic of the NSA and its activity brings a lot of controversies and therefore is being actively discussed in the society. As a result, there have even appeared 11 movies that try to warn us about the NSA:[11]

- Mercury Rising (1998)
- Enemy Of The State (1998)
- The Simpsons Movie (2007)
- The Forgotten (2004)
- Good Will Hunting (1997)
- Starman (1984)
- Sneakers (1992)
- Live Free Or Die Hard (2007)
- Grosse Point Blank (1997)
- The Iron Giant (1999)
- Echelon Conspiracy (2009)

Methods and Scope of Activity

Training of specialists for the NSA is carried out at the National Institute of Cryptography. This academic institution trains not only for the NSA, but also for several other units of the Ministry of Defense. In addition, the NSA pays for the training of its employees in leading US colleges and universities, as well as in military colleges of the Ministry of Defense.

The NSA conducts polygraph tests of employees. For new employees, the tests are meant to discover enemy spies who are applying to the NSA and to uncover any information that could make an applicant pliant to coercion. As part of the latter, historically EPQs or "embarrassing personal questions" about sexual behavior had been included in the NSA polygraph.[12] The NSA also conducts five-year periodic reinvestigation polygraphs of employees, focusing on counterintelligence programs. In addition the NSA conducts aperiodic polygraph investigations in order to find spies and leakers; those who refuse to take them may receive "termination of employment", according to a 1982 memorandum from the director of the NSA.[13]

Excerpt from Defense Security Service (DSS) polygraph brochure given to NSA applicants:

Image source: http://www.dss.mil/multimedia/polygraph_videos/polygraph.pdf

NSA has a group of computer scientists, engineers and mathematicians, who conduct research on a wide class of problems. The Agency is working with commercial and academic partners as well as with other government organizations to explore new analytical methods and computer platforms. Their research areas include:[14]

- Knowledge bases
- Ontologies
- Intelligence Value Estimation
- Language analytics
- Voice analytics
- User Modeling/Cognitive Science

Quite often, the majority of them does not even know what they are doing indeed. For example, as reported by the British media, it was the case with a group of about 40 employees of British Telecom. As it turned out, these people had no relation to the NSA neither to the British signals intelligence, but nevertheless they intercepted all - from the embassy correspondence and business messages to personal birthday greetings.

The Agency command makes every effort to remain in the shadows. For years, its staff members, if asked about the place of work, had no right to mention the names and had to answer, e.g. "The Department of Defense (DoD)". Civilian employees of the agency are subjects to numerous limitations, for example, they are allowed to use only dentists checked by a security guard of the NSA, and also must inform about marriages of their relatives with a foreigner. Such a high level of secrecy has led over time to humorous translations of a shortcut NSA as "No Such Agency" or "Never Say Anything".

In 2013, the extent of the NSA's secret surveillance programs was revealed to the public by Edward Snowden. According to the leaked documents, the NSA intercepts the communications of over a billion people worldwide, many of whom are American citizens, and tracks the movement of hundreds of millions of people using cellphones. Most such interceptions did not meet the legal requirements underpinning the agency's work. Internationally, research has pointed to the NSA's ability to surveil the domestic internet traffic of foreign countries through "boomerang routing".[15] As an example of boomerang routing, let us consider how a University of Toronto student visits the Ontario Student Assistance Program (OSAP) web-site (which server is just few blocks away) from a campus computer:

Image source: https://www.youtube.com/watch?v=F_v0VMvjcI8

The ISP sends the data to its New York switching center, where there is a good reason to believe to be intercepted by the NSA without a warrant. From New York a student's data is forwarded to Chicago - another city where the NSA is strongly suspected of setting up a warrantless wiretapping operations. In Chicago it connects with the ISP for the interior government, which then carries the data back to Toronto to deliver to OSAP's computers. This entire trip takes a fraction of a second, but is not necessarily efficient and exposes foreigner's data to the US spine.

A PRISM presentation slide showing the flow of data in the world:

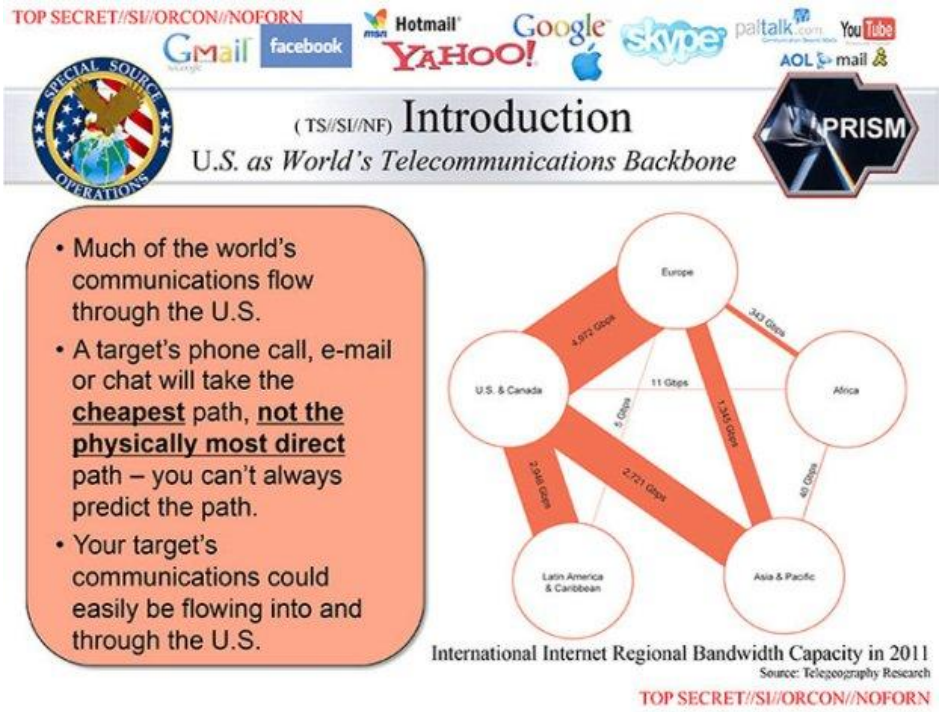


Image source:
http://technologie.gazeta.pl/internet/1,104530,14065176,Czy_mozemy_uniknac_podsluchu__Co_zrobic_ _zeby_obronic.html

NSA intercepts and analyzes the data of foreign countries in the area of radio communications, telephone, internet and emissions of all kinds of radar and missile guidance systems, and coordinates all activities of the United States in the field of cryptanalysis and cryptosecurity. Its two main tasks include breaking the code and cipher systems of other countries and protection of information systems security (INFOSEC) of US communications, including communications of the White House.

The day-to-day work of the CSS is to capture enemy signals (radar, telemetry, radio/satellite communications) using the means of the involved service. For example, the Navy has special submarines for tapping undersea cables; the Air Force operates aircraft with sophisticated antennas and processing gear to listen to enemy radar and radio; and on the ground, the Army operates similar eavesdropping equipment.[16]

The basis of the NSA's technical infrastructure is the Echelon spy system. In a simplified form of "Echelon" works in the following manner. The sources of information are the Internet, e-mail, telephone, fax, telex. At the initial stage of the captured data is transferred to specialized computers. They are called dictionaries and equipped with disk arrays, the capacity of which is estimated at terabytes. Further on, these texts are scanned with excavation methods to allocate an array of interesting pieces of information or individual voices. The principle is similar to that used by the search engines, but unlike them, "Echelon" works in real time and in the course of, say, the telephone conversation decides if a message is interesting or not. "Echelon" has a variety of languages, and is familiar with the professional slang (such as of drug traffickers or weapon dealers) and special vocabulary, knows the nicknames of the major political figures of the leading countries of the world.

In addition, experts believe that the NSA learned to get a "voice print", which, according to them, is as unique as a fingerprint. Due to the available voice occurrence (specimen) in computer memory, any voice can be quickly identified within audio stream. In other words, if the "Echelon" has once registered the voice of a man, then it can track the conversation from any device in the world.

In the second phase, the scanned messages selected with computers from around the world fall into the information storage unit. There they are recorded, sorted by topic (e.g., "military affairs", missile or nuclear technology, terrorism, politics, guns, drugs, smuggling) and sent for further analysis. Then specially designed for each topic program analyzes the information on given topics. From the selected in the first stage 10,000 messages only 100-200 can appear truly important.

In the fourth stage, after which the materials tend to fall on the table of major officials in the US administration, is an expert review of staff from relevant departments of NSA in Fort Meade for each of the received 100-200 messages.

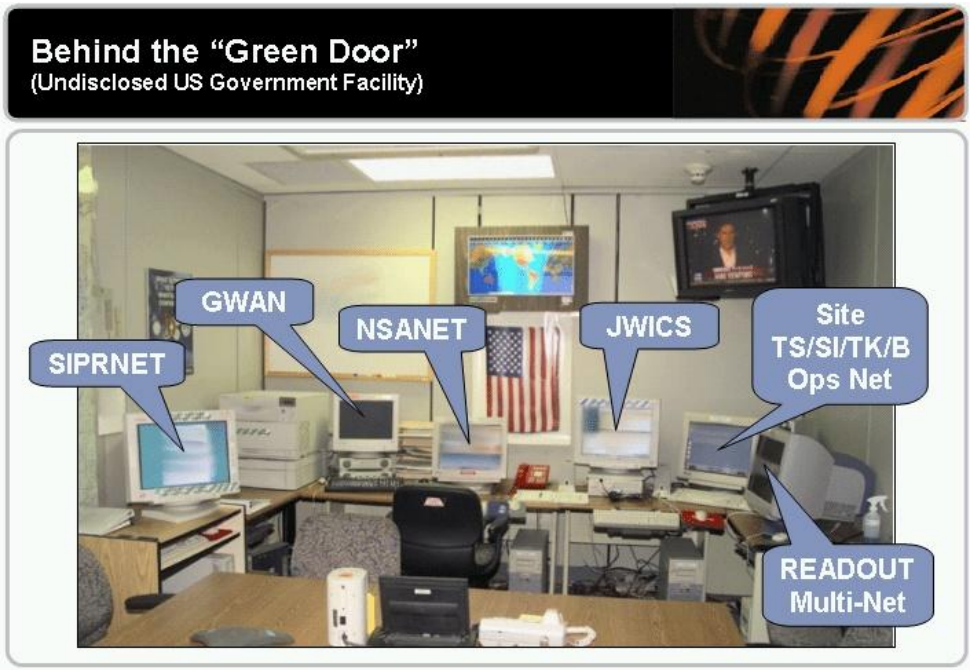
PRISM is another clandestine surveillance program under which the United States National Security Agency (NSA) collects internet communications from at least nine major US internet companies.[17] Since 2001 the United States government has increased its scope for such surveillance, and so this program was launched in 2007. The potential monitoring targets are users of certain services that are not US citizens or US citizens, whose contacts include foreigners! It specifies that the most interesting are the people living outside the United States. PRISM authorizes the Agency to obtain a variety of information: view e-mail, listen to voice and video chat, view photos, videos, track transferred files, to learn other details from social networks.

According to the intelligence services' allegations, due to the court decision many large companies had to commit to an active co-operation with intelligence services, providing them access to servers of Microsoft (Hotmail), Google (Google Mail), Yahoo!, Facebook, YouTube, Skype, AOL, Apple and Paltalk. [18]

The amount of data that was obtained in August of 2013 under the NSA Internet Surveillance, was 29 petabytes per day.[19] Experts also say that the system is able to analyze and memorize up to 3 billion messages a day.

In order to protect its own data from external interception, a highly secured computer network consisting of fiber-optic and satellite communication channels is used. NSANet is almost completely separated from the public internet. The network allows NSA personnel and civilian and military intelligence analysts anywhere in the world to have access to the agency's systems and databases. This access is tightly controlled and monitored. For example, every keystroke is logged, activities are audited at random and downloading and printing of documents from NSANet are recorded.[20]

Secure communications room with separate computer terminals for access to SIPRNET, GWAN, NSANET, and JWICS (2007):



In the headquarters of the National Security Agency also operates a large printing facility and a microprocessors plant for a powerful computer park, which also runs the National School of Cryptology.

Controversies and Scandals

Some critics blame the system "Echelon" in that it deals not only with finding and identifying terrorist bases, routes of drug trafficking and political and diplomatic intelligence, which would be natural, but also is used for large-scale commercial theft, international commercial espionage and invasion of privacy . For example, the British journalist Duncan Campbell and his New Zealand counterpart Nicky Hager drew public attention to the fact that in 1990 the system "Echelon" has been involved in industrial espionage to considerably greater extent than for military and diplomatic purposes. Examples cited by journalists, included wind turbine technology developed by the German company "Enercon", and speech recognition technology, owned by Belgian company "Lernout & Hauspie".[21]

It was revealed that the NSA intercepts telephone and internet communications of over a billion people worldwide, seeking information on terrorism as well as foreign politics, economics[22] and "commercial secrets".[23] In a declassified document it was revealed that 17,835 phone lines were on an improperly permitted "alert list" from 2006 to 2009 in breach of compliance, which tagged these phone lines for daily monitoring.[24] As few as eleven percent of these monitored phone lines met the agency's legal standard for "reasonably articulable suspicion" (RAS).

The NSA tracks the locations of hundreds of millions of cellphones per day, allowing them to map people's movements and relationships in detail.[25] It reportedly has access to all communications made via Google, Microsoft, Facebook, Yahoo, YouTube, AOL, Skype, Apple and Paltalk, and collects hundreds of millions of contact lists from personal email and instant messaging accounts each year. It has also managed to weaken much of the encryption used on the Internet (by collaborating with, coercing or otherwise infiltrating numerous technology companies), so that the majority of Internet privacy is now vulnerable to the NSA and other attackers.[26]

The NSA supplies foreign intercepts to the DEA, IRS and other law enforcement agencies, who use these to initiate criminal investigations. Federal agents are then instructed to "recreate" the investigative trail via parallel construction (in order to conceal how the investigation actually began).[27] By hiding the origin of investigation, the DEA could be hiding evidences from the people arrested. This might jeopardize people's constitutional right to a fair trial.

The NSA also spies on influential Muslims to obtain information that could be used to discredit them, such as their use of pornography. The targets, both domestic and abroad, are not suspected of any crime but hold religious or political views deemed "radical" by the NSA.[28]

Rules of XKeyscore (a formerly secret computer system first used by the United States National Security Agency for searching and analyzing global Internet data) reveal that the NSA tracks users of privacy-enhancing software tools, including Tor, the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in Cambridge, Massachusetts, and readers of the Linux Journal.[29]

As part of a plan to discredit "radicalizers", the NSA is also involved in planning to blackmail people with "SEXINT", the practice of monitoring and/or indexing the potential target's sexual activity and pornographic preferences of internet users in an effort to later use the information for blackmail.[30] Those targeted had not committed any apparent crime nor were charged with one.

The espionage group named the Equation Group, described by discoverers from Kaspersky Labs as one of the most advanced in the world as of 2015, is suspected of being a part of NSA. The

group's known espionage methods have been documented to include interdiction (interception of legitimate CDs sent by a scientific conference organizer by mail), and the "unprecedented" ability to infect and be transmitted through the hard drive firmware of several of the major hard drive manufacturers, and create and use hidden disk areas and virtual disk systems for its purposes, a feat demanding access to the manufacturer's source code of each to achieve.[31]:16–18

Computers seized by the NSA due to interdiction (secret interception of electronics shipment for the purpose of implanting bugs before they reach their destination) are often modified with Cottonmouth, a physical device that can be inserted in the USB port of a computer in order to establish remote access to the targeted machine. The NSA can establish Bridging (networking) "that allows the NSA to load exploit software onto modified computers as well as allowing the NSA to relay commands and data between hardware and software implants."

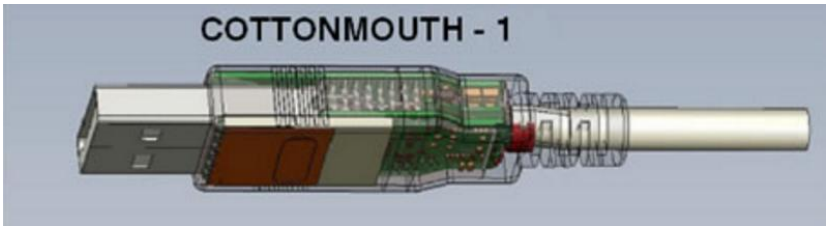


Image source:
http://www.spiegel.de/static/happ/netzwelt/2014/na/v1/pub/img/USB/S3223_COTTONMOUTH-I.jpg

In 1999 Microsoft was accused in having a predefined master asymmetrically encrypted key for Windows NT implemented by NSA because an encryption code had component named _NSAKEY. That variable contained a 1024-bit public key. These allegations were corroborated later.

NSA was also embroiled in some minor controversy concerning its involvement in the creation of the Data Encryption Standard (DES), a standard and public block cipher algorithm used by the U.S. government and banking community. During the development of DES by IBM in the 1970s, NSA recommended changes to some details of the design. There was suspicion that these changes had weakened the algorithm sufficiently to enable the agency to eavesdrop if required, including speculation that a critical component—the so-called S-boxes—had been altered to insert a "backdoor" and that the reduction in key length might have made it feasible for NSA to discover DES keys using massive computing power. It has since been observed that the S-boxes in DES are particularly resilient against differential cryptanalysis, a technique which was not publicly discovered until the late 1980s, but which was known to the IBM DES team.

Perhaps because of previous discussions, participation of NSA in the selection of a successor to DES was limited to performance testing. The agency subsequently certified algorithms to protect information of classified character. Allegedly, widely used hash functions SHA-1 and SHA-2 were also designed at the NSA.

Apart from that, NSA promoted the inclusion of a random number generator called Dual_EC_DRBG in the U.S. National Institute of Standards and Technology's 2007 guidelines. This led to speculation of a backdoor which would allow NSA access to data encrypted by systems using that pseudo random number generator.[32]

Legality

The Foreign Intelligence Surveillance Act, the law on surveillance of foreign intelligence services, adopted in 1976 by the US Congress, sets out the principles of the secret surveillance of people suspected of espionage in the United States. Other rights relating to limit the scope of the NSA wiretap used by the agency to the foreign communications, meaning that one of the callers should be located within the United States and the other outside it. Monitoring the citizens of their own country is generally prohibited.

However, the NSA may eavesdrop connectivity of extraterritorial institutions (such as embassies and consulates) within the territory of the country without any limitations. A special order is required in case an employee of the embassy uses a telephone located outside the extraterritorial territory of the diplomatic mission. During one phase of the Shamrock (Minaret) operation, approximately 1,800 American citizens appeared on a watch list. Among them were people like Martin Luther King, Jr., actress Jane Fonda, singer Joan Baez and the renowned pediatrician, Dr. Benjamin Spock. During Shamrock Operation the NSA has compiled cases on 75,000 American citizens.

U.S. District Judge William Pauley ruled that the NSA's collection of telephone records is legal and valuable in the fight against terrorism. In his opinion, he wrote, "a bulk telephony metadata collection program is a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data" and noted that a similar collection of data prior to 9/11 might have prevented the attack.[33]

In April 2009, officials of the US Department of Justice acknowledged that the NSA led a large-scale collection of information from internal communications of US citizens abusing their authority, but at the same time claimed that the actions were unintentional and have since been corrected.[34]

In March 2015 Wikipedia founder Jimmy Wales and Wikimedia Foundation Executive Director Lila Tretikov has informed about submitting a lawsuit against the National Security Agency spying on users through Wikipedia:[35]

"As a result, whenever someone abroad is to view or edit a page in the "Wikipedia", it is likely that the NSA monitors these actions, including the content of the read or sent to print, as well as other information that may be related a physical location of the person or a his/her possible identity. These actions are confidential and private: they can reveal everything - from person's political and religious beliefs to his/her sexual orientation and state of health", - emphasized the article. NYT notes that one of the documents, which published the NSA whistleblower Edward Snowden, defines "Wikipedia" as an object of observation, along with other major sites such as CNN.com, Gmail and Facebook. "Harm to Wikimedia and hundreds of millions of people who visit our sites, is obvious: the ubiquitous surveillance has a chilling effect. It stifles free speech and the free exchange of knowledge, which Wikimedia was created for"- wrote Wales and Tretikov.[36]

Fourth Amendment to the United States Constitution states:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Nevertheless, the U.S. government has aggressively sought to dismiss and challenge Fourth Amendment cases raised against it, and has granted retroactive immunity to ISPs and telecoms participating in domestic surveillance.[37] The U.S. military has acknowledged blocking access to parts of The Guardian website for thousands of defense personnel across the country,[38] and blocking the entire Guardian website for personnel stationed throughout Afghanistan, the Middle East, and South Asia.

Before 2015, the NSA paid billions of dollars to telecommunications companies in order to collect data from them.[39] While companies such as Google and Yahoo! claim that they do not provide "direct access" from their servers to the NSA unless under a court order, the NSA had access to emails, phone calls and cellular data users. With the new bill getting passed in May, 2015 is known as the U.S.A. Freedom Act. It will enable the NSA to continue hunting for terrorists by analyzing telephone links between callers but "keep the bulk phone records in the hands of phone companies". Telecommunications companies would not provide the NSA with bulk information. The companies would allow the disposal of data in every 18 months.[40]

So, instead of trying (unsuccessfully, unless we are extremely proficient in computers and feel a big oppression) to cheat the system, we might want to think about something else - the change in the law. If we cannot (and, let's be honest, we do not want to, because it makes our lives more convenient) restrict the collection of data, let's have its access and use strictly regulated. Moreover, these regulations should apply not only to the security services, but also to companies. Only in this way can we ensure that we keep even the remnants of privacy.[41]

References

1. David Kahn. Агентство национальной безопасности //Взломщики кодов = The Codebreakers. — Центрполиграф, 2000. — p.480 — (Секретная папка). —ISBN 5-227-00678-4.
2. Encyclopedia of Espionage, Intelligence and Security / Ed. by K. Lee Lerner, Brenda Wilmoth Lerner. — 1 edition. — Gale, 2003. — Vol. 2. — P. 351-353. — ISBN 978-0-7876-7546-2.
3. https://www.nsa.gov/about/central_security_service/css_insignia.shtml
4. https://www.gpo.gov/fdsys/pkg/WCPD-2008-08-04/pdf/WCPD-2008-08-04-Pg1064.pdf
5. Malkin, Bonnie. NSA surveillance: US bugged EU offices. The Daily Telegraph, June 30, 2013
6. Ngak, Chenda. NSA leaker Snowden claimed U.S. and Israel co-wrote Stuxnet virus, CBS, July 9, 2013
7. Lichtblau, Eric (February 28, 2001). "Spy Suspect May Have Revealed U.S. Bugging; Espionage: Hanssen left signs that he told Russia where top-secret overseas eavesdropping devices are placed, officials say". Los Angeles Times. p. A1. Archived from the original on April 17, 2001.
8. Пыхалов И. В. АНБ //Спецслужбы США. — СПб.: ОЛМА-ПРЕСС, 2002. — ISBN 5-7654-1504-0.
9. http://telecombloger.ru/16255
10. http://www.wired.com/2012/03/ff_nsadatacenter/all/1
11. http://www.avclub.com/article/no-such-agency-11-movies-that-tried-to-warn-us-abo-98901
12. Bauer, Craig P. (2013). Secret History: The Story of Cryptology. CRC Press. p. 359. ISBN 9781466561861.
13. Bamford. Body of Secrets. p. 538.
14. https://www.nsa.gov/research/computer_info_sci_research/index.shtml
15. Obar, Jonathan A.; Clement, Andrew (2013). "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty". TEM 2013: Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association (Victoria, June 5–7, 2012). Retrieved June 3, 2014.
16. https://fas.org/irp/eprint/css.htm
17. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
18. http://lenta.ru/articles/2013/06/10/bigbro/
19. http://www.zdnet.com/article/nsa-hunger-demands-29-petabytes-of-data-a-day/
20. http://theweek.com/articles/463381/how-single-tech-could-spy-world
21. http://www.webcitation.org/66Jmuc30R
22. http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html
23. https://www.washingtonpost.com/politics/kerry-to-face-questions-on-nsa-spying-during-south-america-trip/2013/08/12/afdab47e-0382-11e3-88d6-d5795fab4637_story.html
24. http://www.theverge.com/2013/9/10/4716642/nsa-illegally-searched-15000-suspects-phone-records-according-to
25. https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?hpid=z1
26. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0
27. http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805
28. http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html
29. http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html
30. http://cyberlaw.stanford.edu/blog/2013/11/nsa-sexint-abuse-you%E2%80%99ve-all-been-waiting
31. https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
32. http://www.webcitation.org/6CYqAu1fE
33. https://web.archive.org/web/20131228162843/http://www.indyposted.com/227717/judge-says-nsas-data-collection-legal/
34. http://www.nytimes.com/2009/04/16/us/16nsa.html
35. http://www.pravda.ru/news/world/northamerica/usacanada/11-03-2015/1251879-wiki-0/#sthash.2ktEQgNI.dpuf
36. http://www.rbc.ru/technology_and_media/11/03/2015/54ffbf329a794775e5d33f9d
37. http://arstechnica.com/security/2008/02/democrats-fail-to-block-telecom-immunity-provision/
38. http://www.theguardian.com/world/2013/jun/28/us-army-blocks-guardian-website-access
39. https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html
40. http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=1
41. http://technologie.gazeta.pl/internet/1,104530,14065176,Czy_mozemy_uniknac_podsluchu__Co_zrobic__zeby_obronic.html