June 24, 2016

E-mails from inside the NSA bureaucracy

Earlier this month, the NSA declassified a huge set of internal e-mails, following FOIA-requests about the issue of whether Edward Snowden had raised concerns about the NSA's surveillance programs through proper channels inside the agency.

> Download the declassified e-mails (very large pdf)

Here, we will take a look at the administrative details these internal NSA e-mails provide. Next time we will see what their content says about the concerns that Snowden claimed to have raised.

Internal e-mail from NSA director Michael Rogers. In the signature block we see his NSA Net and SIPRNet e-mail addresses and his non-secure phone number (all redacted)

E-mail addresses
Except from the classification markings, the NSA's internal e-mails aren't very different from those exchanged by most other people around the world. But they do show for example some details about the internal communications networks of the agency.

From the signature blocks underneath the e-mails we learn that, depending on their function and tasks, NSA employees have e-mail addresses for one or more of the following four computer networks:

- NSANet for messages classified up to Top Secret/SCI (Five Eyes signals intelligence). On this network the address format for e-mail is jjdoe@nsa

- JWICS for messages classified up to Top Secret/SCI (US intelligence). The address format is jjdoe@nsa.ic.gov

- SIPRNET for messages classified up to Secret (mainly US military). The address format is jjdoe@nsa.mil

- UNCL for unclassified messages, likely through NIPRNet. The address format is jjdoe@nsa.gov

  > See for more: US military and intelligence computer networks

For e-mail, all NSA employees have display names in a standardized format: first comes their family name, given name and middle initial, sometimes followed by "Jr" or a high military rank. Then follows "NSA" and the proper organizational designator, then "USA" for their nationality and finally "CIV" for civilian employees, "CTR" for contractors, "USN" for Navy, "USA" for Army or "USAF" for Air Force members.

Thus, the display name of the current NSA director is "Rogers Michael S ADM NSA-D USA USN", while that of the previous director was "Alexander Keith B GEN NSA-D USA USA". In 2012, Snowden had the display name "Snowden Edward J NSA-FHX4 USA CTR":

![E-mail from Snowden as systems administrator in Hawaii, August 2012](image)

The organizational designator FHX4 is interesting. FH stands for Field station Hawaii, but X4, being unit 4 of division X, is still a mystery. The field station divisions have the same designators as those at NSA headquarters, where there's also a division X, but so far no document gave an indication what it does.

The signature block shows that Snowden worked as a systems administrator for Dell’s Advanced Solutions Group and that he was deployed at the Technology Department of NSA’s Cryptologic Center in Hawaii, more specifically at the Office of Information Sharing. The latter has the organizational designator (F)HT322 and is therefore different from that in Snowden’s display name.

---

The phones of US Director of National Intelligence James Clapper
Something about the use of selectors: correlations and equations
A look at the latest French laws on intelligence collection
How NSA contact chaining combines domestic and foreign phone records
Section 215 bulk telephone records and the MAINWAY database
Leaked documents that were not attributed to Snowden
How NSA targeted the Venezuelan oil company PDVSA

"It's actually straight up interesting but also weird how weirdly, wonderfully detailed this blog about hyper secure communications is.” — Gizmodo.com

---

**Pages**

- Home
- INDEX
- Links
- Abbreviations and Acronyms
- NSA Nicknames and Codewords
- NSA's organizational designations
- NSA's Legal Authorities
- NSA Glossary
- The US classification system
- SIGINT Activity Designators (SIGADs)
- GCHQ Codewords and Abbreviations
- CSE Codewords and Abbreviations
- BND Codewords and Abbreviations
- Telephony Abbreviations
- Internet abbreviations

**Total Pageviews**

Total Pageviews

---

**Popular Posts**

- How Obama's BlackBerry got secured
- New phones aboard Air Force One
In the declassified messages we only see display names, not the actual e-mail addresses behind them. Therefore, only the classification markings on the messages provide an indication on which network they were exchanged.

From an e-mail that was declassified earlier we know that in April 2013 Snowden used the address "esnowd@nsa.ic.gov", which is the format for the JWICS network, but was apparently used on NSANet.*

From one of the declassified e-mails about NSA's internal investigation it seems that Snowden had just two mail accounts: "we have his TS (Top Secret) NSANet email and his UNCLASSIFIED nsa.gov email", but this is followed by some redacted lines.*

Finally, the signature blocks of some NSA employees also provide a link to their dropbox for sending them files that may be too large for e-mail. Such dropboxes have addresses like "http://urn.nsa.gov/dropbox/ [...]".

Example of an unclassified NSA message, with in the signature block e-mail addresses for JWICS and an unclassified network, and phone numbers for the STS and the non-secure phone networks

(Nick names, work titles and phone numbers redacted)

The two black NSA headquarters buildings

OPD 2B is the wider and lower one of the two black NSA headquarters buildings

Telephone numbers

Besides e-mail addresses, many messages also have phone numbers in the signature blocks. They show numbers for one or more of the telephone systems used at NSA:

- NSTS, which stands for National Secure Telephone System and is NSA's internal telephone network for secure calls. Numbers for this network have the format 969-8765 and are often marked with "(s)" for "secure"

- STE, which stands for Secure Terminal Equipment, being a telephone device capable of encrypting phone calls on its own. Telephone numbers can be written in the format (301) 234-5678 or as STE 9076.

- BLACK, CMCL or Commercial, which are numbers for non-secure telephones that may also access the public telephone network. They have the regular format (301) 234-5678 and are often marked with "(b)" for "black" (as opposed to "red") or with "(u)" for unclassified.
TIKICUBE

Finally, releasing such a huge set of documents in which many parts had to be redacted always bears the risk that something is overlooked. That also happened this time, as in one e-mail from an investigator from NSA’s Counterintelligence Investigations unit Q311 they forgot to redact the codeword TIKICUBE:

TIKICUBE appears to be a unit of the Investigations Division Q3. Whether this might be a special unit investigating the Snowden leak isn’t clear though.

The abbreviations behind the investigators name are: CFE for Certified Fraud Examiner and CISSP for Certified Information Systems Security Professional.

We also see that this investigation division is not located at the NSA headquarters complex at Fort Meade, but at FANX. This stands for Friendship Annex, a complex of NSA office buildings in Linthicum, near Baltimore, some 12 km. or 7.5 miles north-east of Fort Meade.

The famous blue-black glass headquarters buildings are OPS 2A and OPS 2B, while the SIGINT division is apparently in the flat 3-story building from the late 1950s, designated OPS 1.
May 19, 2016

**German journalists about working with the Snowden documents**

Last Monday, the website The Intercept started publishing larger batches of documents from the Snowden trove, so they can now also be examined by the public. It's a new phase after previously documents were generally disclosed as part of journalistic reports, but the number of such publications steadily declined over the last two years.

For how it was to work with the Snowden documents can be learned from an interesting interview with two journalists from the German Magazine Der Spiegel. They not only published a whole range of articles based upon the Top Secret NSA documents, but also a book which is much more informative than that of Glenn Greenwald.

The interview with Marcel Rosenbach and Holger Stark from Der Spiegel, as well as with Svea Eckert from the German broadcaster NDR, was part of the Network Research (Netzwerk Recherche) annual conference, which was held on July 3 and 4, 2015:

![Interview with Marcel Rosenbach, Holger Stark and Svea Eckert, July 2015](image)

Because the interview is fully in German, here's an extensive summary in English, which also looks more closely at a few specific revelations:

- The Snowden documents
- The National Intelligence Priority Framework (NIPF)
- A MONSTERMIND/CYBERCOP presentation
- Eavesdropping on chancellor Merkel
- Some other issues

**The Snowden documents**

Journalists from Der Spiegel were provided with several ten thousand digital documents through the documentary film maker Laura Poitras, who had been in direct contact with Edward Snowden.

According to Holger Stark, it was clear that Snowden had sorted the documents, not very fine-grained, but he had put them in a few folders, according to topics that had his special interest, like operations of the NSA divisions TAO (hacking) and SSO (cable tapping). Rosenberg said that it looked like Snowden selected the documents based upon his concerns regarding civil liberties and that he didn't some "collect it all" scraping.
(although in the film CitizenFour, Snowden himself said: “I cast such a wide net” that it would be difficult for NSA to determine how many documents he actually took)"

The journalists tried to search and filter the documents automatically, but a huge number of them had to be read and analysed manually, and read over and over again, in order to understand what was in them and what their importance could be. For that, they also consulted experts for cryptography and network architecture as well as former NSA employees like Binney and Drake (independent intelligence experts were not mentioned).

It was possible to ask Snowden, but not in a regular or easy way, also because he wanted to stay at a distance of the journalistic work. The journalists couldn’t tell or estimate how many documents Snowden actually took. Der Spiegel got the documents unredacted but in the documents that were published, editors redacted most of the names.

Der Spiegel frequently asked NSA to review the documents they wanted to publish, in order to prevent that lives could become in danger. Sometimes NSA asked to remove things, but when it was obvious that that was for political reasons, the request was ignored. But in a few other cases Der Spiegel didn't publish or partly redacted the documents.

BOUNDLESSINFORMANT

Despite all their efforts, there were still many gaps and questions. This resulted in for example a wrong interpretation of NSA’s data visualisation tool BOUNDLESSINFORMANT. In August 2013, Der Spiegel published charts from this tool that were initially interpreted as showing how many data NSA collected from several European countries. Soon, BND and NSA denied this and explained that the charts show data that European agencies provided to the Americans.

Holger Stark admitted that their initial interpretation was apparently not correct, but that there are still many questions about this issue. One of the difficulties was that NSA and US government were not willing to respond to questions about this program, so they decided to publish their best guess. Rosenbach added that major foreign papers also shared their initial interpretation (maybe because the wrong interpretation came from Greenwald?).

BOUNDLESSINFORMANT screenshot showing metadata provided by BND

(click to enlarge)

> See also: BOUNDLESSINFORMANT only shows metadata

The National Intelligence Priority Framework (NIPF)

One document that wasn't published, but only reported about is the National Intelligence Priority Framework (NIPF), which contains the priorities for the US intelligence community as set by the White House. During the interview a part of the original NIPF document was shown for the first time:
The NIPF consists of a large matrix with each cell indicating the intersection between a state or non-state actor and an intelligence topic. A readable reconstruction of the NIPF based upon this new piece and earlier sources, can be found here (pdf).

Over time, Rosenbach and Stark learned to interpret the Snowden documents by combining information from multiple documents. A separate document, an internal NSA newsletter from December 2009, for example provided additional information about the priorities of the NIPF chart:

This newsletter says that updated versions of the NIPF are released about twice a year, and that these are run against the National SIGINT Requirements Process (NSRP), which sets the priorities for acquiring Signals Intelligence (SIGINT). The 5 levels of NIPF priorities are then translated (by the SIGINT Committee or SIGCOM) to the 9 levels of SIGINT priorities, based upon the importance of the SIGINT contribution.

The first NIPF was issued in 2003 and at that time the matrix contained over 2300 cells! There were hundreds of issues with priority 1 and 2, way too many to be manageable. So over the years the number of priorities, particularly the numbers of priority 1s and 2s had been reduced.

According to the journalists, the newsletter also explains that topics with priority 1 and 2 are meant for the president and the White House, while priority 3 is for cabinet ministers, the Chiefs of Staff and the Pentagon. For these highest priorities, covert intelligence methods are used. For priorities 4 and 5 open sources may be sufficient
and their results are mainly used for political analysis.

For the Spiegel journalists this bureaucratic process illustrates that NSA isn’t an agency that went rogue, but that they are directed by the political information needs from the White House (something that was usually conveniently ignored).

A MONSTERMIND/CYBERCOP presentation

Svea Eckert, a documentary maker for the regional German broadcaster NDR, was also present at the interview, and she had brought with her the laptop they had used for working with the Snowden documents. The computer was newly bought for this purpose and was never connected to the internet.

At NDR, Eckert was doing research for a documentary about the internet as a battle space, when a colleague of her in the US was provided with a thumb drive containing Snowden documents that had been selected on their relevance for the topic of the documentary. It wasn’t told who the middlemen for these documents were, and apparently different German news media got documents from different sources.

The source had said that for these documents only the external TAILS operating system should be used. The same system was used by other people who worked with Snowden documents, like Laura Poitras, Glenn Greenwald, and Barton Gellman. On the dedicated laptop, Eckert showed an example of what these documents look like:

In the window we see for example an internal NSA newsletter with an interview with a hacker from NSA’s TAO division, a Cyber Warfare Lexicon and a powerpoint presentation. The latter has the filename “MONSTERMIND_presentaton (copy).pptx”, but when it was opened, it actually had the cover term CYBERCOP on the front slide and it was prepared by the “CyberCOP Product Manager”.

Eckert explained that although most of these documents were very interesting, not everything was newsworthy enough or in the public interest to publish. Also the opinions of various experts had to be asked, because journalists were not always able to judge what the context or the importance of particular pieces of information was.

CYBERCOP

The CYBERCOP presentation is from April 11, 2013 and contains several screenshots of a graphical user interface in which NSA analysts can see where cyber attacks occur. The map part seems very similar to a well-known flashy visualisation on the website of the Norwegian cyber security company Norse:
It was decided not to publish the full MONSTERMIND/CYBERCOP presentation, but the documentary Schlachtfeld Internet ("Battlefield Internet") did contain several slides, which showed that NSA is apparently powerful enough to trace such attacks and that therefore the agency must be present at numerous points on the internet. This was considered newsworthy enough to report about.

In the documentary itself it was explained that an analysis tool called CYBERCOP makes it possible for NSA to monitor "cyber war" in real time. The presentation described at least one specific attack: on April 10, 2012, the US federal banking system in New York was successfully attacked by Iran, not directly, but through thousands of computers around the world, controlled through internet servers in Germany.

Broadcaster NDR published three slides of the CYBERCOP presentation here (pdf). Two of them show the CYBERCOP interface in a high resolution:

Monstersmind

The MONSTERMIND system was first disclosed in a very long interview that James Bamford had with Edward Snowden in August 2014. There, Snowden said that MONSTERMIND is a frightening program that automated "the process of hunting for the beginnings of a foreign cyberattack".

It could also automatically prevent attacks from entering the country, but its unique capability is that "instead of simply detecting and killing the malware at the point of entry, MonsterMind would automatically fire back, with no human involvement" - with the risk of hitting the wrong one, as Snowden warned.

The "killing" capability was also described in Eckert’s documentary, but without mentioning the codename MONSTERMIND. It didn’t become clear whether this just...
came from Snowden's recollection or that it's mentioned in the CYBERCOP presentation (or other documents).

Eavesdropping on chancellor Merkel

The journalists from Der Spiegel also found interesting things purely by accident. The cache of documents for example contained an NSA presentation from the Center for Content Extraction (CCE, unit designator T1221) about a system to automatically sort out interesting and useful parts of intercepted phone calls.

One slide of this presentation shows an example list of some chiefs of state (cos), among which German chancellor Angela Merkel was listed. The presentation was not about actual interception operations, but did provide an indication that Merkel had been a target:

Der Spiegel published this slide on March 29, 2014 and the full presentation (pdf) was released online in June 2014. That chancellor Merkel had been a target of NSA had already been revealed in October 2013, based upon a database entry that allegedly did not came from the Snowden documents, but from another and yet unidentified second source.

So far, it seems that this example from the chiefs-of-state list is the only confirmation of NSA's targeting of chancellor Merkel that came from the Snowden documents. The intercepted content published by Wikileaks is also supposed to be from the second source.

> See also: New interpretations of NSA monitoring the German chancellor

Some other issues

During and after the interview, Stark, Rosenbach and Eckert were also asked about various aspects of working with Snowden Documents:

- Contrary to some claims made by the US government, there seemed to be little danger that these documents could endanger the lives of operatives or other people. The work that NSA does is highly technical and therefore the documents hardly contain any names. Most of the names they do contain are of authors, not of operative field agents.

- Eckert found it disappointing that the documents had almost no code or malware signatures in them, which could have been useful to identify hacking operations conducted by the NSA (Eckert said the XKEYSCORE rules were not included in the set she received). Again this was because the documents were often for management and training purposes and contained information on a meta level instead of actual operational details.
- The journalists were aware of the fact that these presentations had to be judged according to their intended purpose and audience and that the audio of these presentations was of course absent, although some presentations came with speaker's notes, which proved to be useful. Important was also to that presentations will often have presented things in a positive way.

Finally, when asked about the future of the Snowden documents, the journalists thought that it could be good to make them available for scientific research, but that it's not up to them to decide. They were not in favor of making all the documents publicly available, like in the way WikiLeaks used to do.

The phones of US Director of National Intelligence James Clapper

One of the key players during the Snowden affair was Director of National Intelligence James Clapper. He is responsible for coordinating all 16 American intelligence agencies, a role which is reflected by the number and the types of telephone equipment in his office.

Clapper has six phones, more than for example the director of the NSA, or the Defense Secretary. Here we will take a close look at these telecommunication devices used by the US Director of National Intelligence.

The office of Director of National Intelligence (DNI) was created in 2004, after the 9/11 Commission Report recommended a stronger and separate leadership for the US intelligence community. Before, it was the director of the CIA who acted as Director of Central Intelligence (DCI) in order to coordinate the various intelligence agencies.
of the Office of the Director of National Intelligence (ODNI) at the Liberty Crossing compound near Tyson's Corner, Virginia, while he was visited by the Australian Minister for Foreign Affairs, Kevin Rudd.

When we take the high resolution version of the picture above, we can see that the displays and buttons of all the phones behind the DNI's desk are blurred by a censor. Apparently there's some rule for that, because from this distance it would be impossible to read anything.

**IST-2 phone**

The first phone on the left side is an Integrated Services Telephone version 2 (IST-2), which was designed by Raytheon and subsequently manufactured by Telecore, a small company that took over the production of these devices.

The IST is a so called "red phone", which means that it's connected to the Defense Red Switch Network (DRSN). This is the main secure telephone network for military command and control communications and connects all major US command centers and many other military facilities.

Like previous red phones made by Electrospace Systems Inc. (ESI), the IST-2 allows to make both secure and non-secure calls through this one single device. The phone itself has no encryption capability: any secure calls are encrypted in bulk before leaving the secure building, enclave or compound.

As part of a military telephone network, the IST-2 also has the distinctive 4 red buttons which are used to select the four levels of a system called Multilevel Precedence and Preemption (MLPP). This allows to make phone calls that get precedence over ones with a lower priority.

**VoIP phones**

Next, there are three Cisco 7975 unified IP phones, which belong to the most widely used high-end office phones. These phones have no encryption capability, but they can easily be used as part of dedicated and secure Voice-over-IP networks.

The first Cisco phone, next to the IST-2, seems to have a bright green label, indicating that it has to be used for unclassified phone calls. Probably this phone is part of the internal non-secure telephone network of the Office of the Director of National Intelligence (ODNI).

The second Cisco phone, right of the computer screen, has no recognizable label. It can be part of any secure or non-secure telephone network which DNI Clapper needs
to have access to. One option could be the National Secure Telephone System (NSTS), which is used by the signals intelligence community (i.e. NSA).

The third Cisco phone has a distinctive bright yellow faceplate instead of the standard silver one. This indicates that it's part of the highly secure Executive Voice over Secure IP-network, which connects the President with senior cabinet members and some other high-level government officials.

This top-level telephone network was set up in 2007-2008. Before, the President was connected to the general military DRSN, but during the attacks of 9/11, this network appeared to be not reliable enough.

It's this bright yellow Cisco phone that shows that the Director of National Intelligence has direct access to the President. As we have seen earlier, even the director of NSA doesn't have this kind of telephone, and therefore lacks a direct line to the President.

> See also: NSA director Alexander's phones - US State Department red phones

**STE phones**

The last type of telephone we see in Clapper's office are two big black phones called Secure Terminal Equipment (STE). These are made by the American defense contractor L3 Communications and are highly secure devices capable of encrypting calls up to the level of Top Secret/SCI.

STE phones can be used to make secure calls to anyone with a similar or compatible device and there are an estimated 400,000 STE users. STE is the successor of the almost legendary STU-III secure phone system from the late 1980s.

These STE phones can be used for secure communications with everyone working for the US government, the military, its contractors, and also foreign partners who can not be reached through a more select secure telephone network, like the DRSN or the NSTS.

**Videoteleconferencing**

Besides the six telephones, DNI Clapper also has two videoteleconferencing (VTC) screens behind his desk. In the first picture we saw a white videoconferencing screen at the far right, and another picture, from a different angle, shows another VTC screen standing at the far left side:
Both these VTC screens have a high-definition camera and are made by the Norwegian manufacturer Tandberg. In 2010 this company was bought by Cisco Systems, so their equipment can be safely used for classified US videoconferencing purposes.

Maybe one of the sets in Clapper's office is used for unclassified, and the other for classified videoconferencing, but it's also possible that both are used for secure video connections but at different classification levels.

At least one of the VTC screens will be used for Top Secret/SCI Videoconferencing, which is for users within the intelligence community. From within secured locations (SCI enclaves), this video feed goes over the JWICS-network, which is secured by stream-based Type 1 bulk encryption devices.

Computer

Finally, there's also one computer screen standing in the midst of the telephones. Below is a keyboard and likely there's also a KVM-switch to enable access to multiple physically separated networks through a single "Keyboard, Video and Mouse" set.

For US intelligence officials, such a KVM-switch usually provides access to NIPRNet or DNI-U (Unclassified, for general purposes), SIPRNet (Secret, for military and intelligence purposes) and JWICS (Top Secret/SCI, for intelligence purposes).

> See also: US military and intelligence computer networks
numbers, e-mail addresses and a whole range of similar groups of characters that can be used to identify a particular target.

However, very little was revealed about how exactly these selectors are used in order to pick out communications of interest. But meanwhile, declassified documents about NSA, German parliamentary commission hearings and an intelligence oversight report from The Netherlands give some details about that.

It came out that the signals intelligence agencies of these three countries (and likely many other countries too) group all selectors that belong to a certain target into sets called correlations or equations.

Wrapping individual selectors into equations makes sense, as one of the most important requirements for signals intelligence is of course knowing which phone numbers, e-mail addresses etc. a particular target uses, as often they will use many of them and change them regularly.

United States

In two recent postings on this weblog, the NSA’s storage and analysis of domestic phone records under the Section 215 (or BR FISA) program was analysed. Information about this program comes almost solely from a large number of documents that have been declassified by the US government.

Among those documents is a BR FISA Review (.pdf) from 2009, in which, probably for the first time, we find the term "correlation". The report says that NSA uses correlated selectors to query the BR FISA metadata. The function of such a set of selectors is described as follows:

"If there was a successful RAS determination made on any one of the selectors in the correlation, all were considered RAS-approved for purpose of the query because they were all associated with the same [target redacted]"

RAS stands for Reasonable Articulable Suspicion, which must be determined for a certain selector, before it can be used to query the domestic telephone metadata. So, when one selector was RAS-approved, the analyst was allowed to also use all other selectors that were correlated to the same target.

This practice of what can be described as "one approved selector approves the whole correlation set" was ended when on February 20, 2009, the Emphatic Access Restriction (EAR) tool was implemented. Since then, each selector has to be individually RAS-approved before it can be used to query the metadata database.

Note that this only applied to selectors used for querying domestic phone records. As we learned from the German situation described below, NSA continued to use correlations for its foreign collection efforts overseas.

Correlation database

According to the BR FISA Review, NSA has a database that holds correlations between selectors of interest and which provides automated correlation results to analysts. So when an analyst wants to know which (other) identifiers a certain target uses to communicate, he can look that up in this database.

The name of this database was redacted, but according to its position in the review’s glossary, it starts with A. The correlation database is therefore different from the OCTAVE tasking tool, which is used to activate telephony selectors on the various collection systems. Analysts can therefore decide by themselves which of the correlated selectors they actually want to task.

It’s not clear though whether these correlations include both phone and internet selectors, but obviously it’s useful to collect and group all kinds of identifiers used by a particular target.
The way NSA uses correlations immediately reminds of a practice that was revealed during hearings of the German parliamentary commission that investigates NSA spying practices. On May 20, 2015, BND employee W.O. explained that until 2012, the NSA sent its selectors to BND in the form of a so-called "equation".

According to the witness, an equation was a record that could contain up to one hundred selectors used by or related to a particular target. This large number of selectors is because the equation contains all different ways of spelling and technical encoding permutations of a selector. For one e-mail address this could for example be:

- mustermann@internet.org
- mustermann%40internet%2Eorg (HTML-Hex)
- mustermann\#37;2540internet.org (multiple encodings)
- mustermann\U0040internet.org (UTF-16)

The explanation given by witness W.O. of how BND managed these NSA equations was rather confusing, but an important element seemed to be that such a whole set of selectors could be prevented from being activated, when BND rejected just one selector when using it would violate German law or German interests.

Especially for internet identifiers (like chat handles or nicknames) it can be very difficult if not impossible to attribute them to a particular country. But when an equation contains just one identifier that is easier to attribute (like an e-mail address), the whole set of selectors can be either approved or disapproved based upon the identifiable selector.

Witness W.O. contradicted himself on whether an equation contains only internet selectors, or also telephone numbers (with wildcards and blanks), but on September 24, 2015, witness D.B. said that equations were only used NSA internet selectors.

Splitting up

W.O. also explained that until 2012, the NSA sent its selectors in the form of equations. When BND rejected one selector from such an equation set, BND employees in Bad Aibling had to ask NSA to remove that number from their equation, or else the other selectors in that equation were rejected too.

Since 2011, these equations were split up and phone and internet selectors were each put in separate databases, which apparently made it possible to reject individual selectors. Afterwards, the computer system reassembles the selectors into their proper equations again, which can now have for example a rejected phone number
alongside an approved e-mail address. But if one of them is disapproved, the whole equation will not be forwarded to the collection system.

This explanation by witness W.O. is rather puzzling because the situation before and after 2011/2012, and before and after splitting up the equations seems to be the same: in both cases all selectors from an equation are rejected when just one of them was disapproved.

It seems therefore that splitting up the equations had another purpose, but that didn't become clear from the commission hearings. The commission members often had difficulties in understanding these technical issues and were then hardly able to ask the witnesses the questions that could bring clarity.

Maybe the splitting up only meant separating telephone and internet selectors, as from the report of a special independent government investigator it did become clear that NSA provided a description or a justification for every single telephone selector, but that justifications for internet selectors weren't available for BND personnel.

Investigation

There's similar confusion about the internal BND investigation into the selectors provided by the NSA. Witness D.B. explained that when in August 2015, Dr. T. investigated suspicious NSA internet selectors, he was not given them in the form of equations, but as separate, individual ones.

Apparently D.B. suggested that this was the reason that Dr. T. found so many selectors that could not be identified: they were separated from correlated ones that could have made them easier to identify. But why separate these selectors when that rips them from elements that attributes them to a certain target and/or a particular country?

BND selectors

What is said before is only about the selectors that were provided by NSA, in order to be tasked on the satellite collection system operated by BND in Bad Aibling. Besides these, BND of course also has its own selectors.

During the hearing from January 28, 2016, witness D.B. was asked whether BND's own selectors were also grouped into equations. D.B. explained that BND doesn't use the term equation, but that in its central tasking database system PBDB, there are multiple selectors for a certain target (with for each selector (German: Telekommunikationsmerkmal or TKM) multiple permutations).

The Netherlands

In the Netherlands, a report (.pdf) from last February by the intelligence oversight
commission CTIVD advised the General Intelligence and Security Service AIVD to consider using some kind of correlations or equations for its bulk collection efforts too.

The report reveals that currently, the AIVD uses a list (Dutch: kenmerkenlijst) containing all selectors, like phone numbers, e-mail addresses and keywords, used for specific operations. For most of these selectors, the list contains a short justification for why it was put on this list, with a reference to an underlying document. Earlier, the commission found that too often, these justifications were too short, not related enough to the target, or even absent.

According to the commission, it would be better when the AIVD would provide a justification for each targeted person or organisation, instead of for every single selector. Often, one target will use multiple phone numbers and e-mail addresses. Grouping them by target and providing a justification for that target would therefore also reduce the length of the list.

This approach is already used by AIVD when it comes to targeted interception.

Geplaatst door P/K op 22:12 1 comment:

Labels: Germany, Netherlands, NSA

Home Older Posts

Subscribe to: Posts (Atom)

Awesome Inc. template. Powered by Blogger.