

A look at the documents in No Place to Hide.

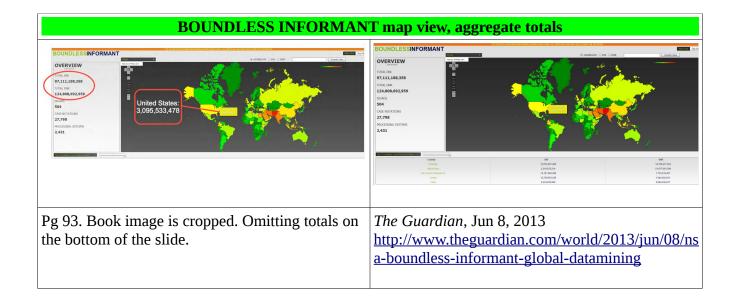
The left hand column lists documents in the book, the right hand column displays, if possible, the same slide from a previous release. This allows a side by side comparison with existing releases. As a general rule, the version in the book is more cropped than the online versions, probably due to space considerations. However, it is somewhat disappointing that the online reference materials do not show at least as much material in a given document as has already been published. In addition, it would make it more inconvenient for researchers if the supplemental material would put slides in context of their original deck. For example, to include a file with all of the released BOUNDLESINFORMANT slides.

One of the few valid criticisms of the Snowden reporting that comes from the Security State is that the reporting is presented in a somewhat scattered manner, providing a confusing picture. It is true that they themselves are responsible for much of the situation. They demand a high degree of redaction, provide misleading statements, or none at all, and then blame the reporter for getting it wrong.

In this book there are relatively few true surprises for the obsessive NSA-watchers, two of this book's main stories were known since the 30C3 conference at the end of last year. Jacob Appelbaum made much of Interdiction at his speech "To Protect and Infect," and Der Spiegel's release of the TAO ANT catalog showed many of the actual bugs installed by interdiction. Glenn Greenwald, in his speech at the same conference leaked the airline WiFi story to his audience.

However, this book provides in a single unit a comprehensive picture about the true scope and purpose of NSA and GCHQ operations and the danger they pose to civil liberties. While I do complain about the shortage of documents, it is also true that Greenwald has provided in his book, and in his journalism generally more original material than any other reporter working on the Snowden material. This record he continues by making the documents available online for free, and publishing his work in several languages.

By contrast Der Spiegel in their book, provided exactly zero new documents, and made their book available only in German, limiting its reach and utility.



FISC Order demanding that Verizon hand over all call metadata records to NSA

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Four page order is too large to fit in a table cell. Document is here:

http://www.theguardian.com/world/interactive/201 3/jun/06/verizon-telephone-data-court-order

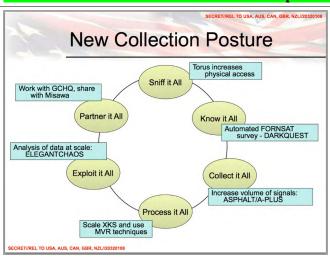
Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

Pg 93 & 94. Book only reproduces an excerpt from body of order.

The Guardian, Jun 5, 2013

http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

2011 top secret presentation



Pg 97. Previously unpublished.

2010 document presented to the Five Eyes conference by the GCHQ



Pg 97. Previously unpublished. Apparently cropped, only about half of a slide.

2009 memo from the technical director NSA's Mission operations in Misawa, Japan

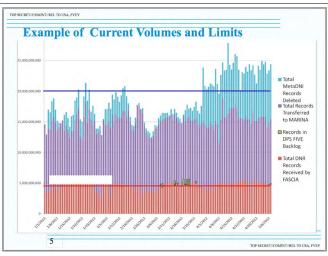
Future Plans (U)

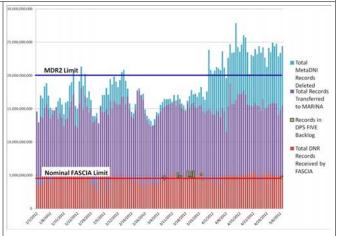
(TS//SII/REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

Pg 98. Previously unpublished. An excerpt of a larger memo.

Slide from a deck about Storage limits and optimization (source: Ashkan Soltani's tweet:





Pg 98. This version is identical to what the Washington Post intended to publish, however due to an error made by the Washington Post's technical staff, it was possible to de-redact this slide. The Washington Post also publishes an additional <u>slide</u>.

Washington Post, Dec 4, 2013

http://www.washingtonpost.com/world/nationalsecurity/nsa-tracking-cellphone-locationsworldwide-snowden-documentsshow/2013/12/04/5492873a-5cf2-11e3-bc56c6ca94801fac_story.html

BOUNDLESS INFORMANT slide about Poland



Slide not published but referenced. Quote from article. "In Poland, which is also under surveillance, the numbers varied between 2 million and 4 million in the first three weeks of December. "

Pg 99. Previously unpublished.

Der Spiegel, Jul 1, 2013

http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-2.html

2011 GCHQ document

Knowing what we have - Guiding Light

- GCHQ has massive access to international internet communications
- We receive upwards of 50 Billion events per day (...and growing)

Pg 100. Previously unpublished. Appears to be about one-half of a slide.

SHELLTRUMPET processes it's One Trillionth Metadata record.

(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes $it^{\prime}s$ One Trillionth Metadata Record

By NAME REDACTED ON 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO's DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.

Though not published, this message was quoted: "On December 31, 2012, an SSO official wrote that ShellTrumpet had just 'processed its One Trillionth metadata record' "

An additional published quote: "though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year"

Pg 100. Previously unpublished.

The Guardian, Jun 27, 2013. http://www.theguardian.com/world/2013/jun/27/ns a-online-metadata-collection



Pg 102. Previously unpublished.

Special Source Operations Corporate Partner Access





Pg 103. Previously unpublished, 2nd slide is cropped.

Undated slides about FAIRVIEW.



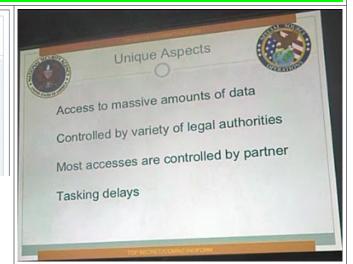
Unique Aspects



Access to massive amounts of data

Controlled by variety of legal authorities

Most accesses are controlled by partner



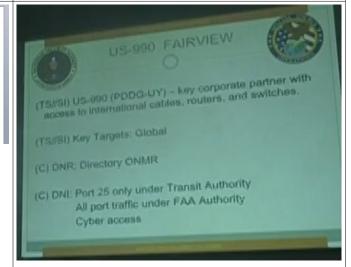


US-990 FAIRVIEW



(TS//SI) US-990 (PDDG-UY) – key corporate partner with access to international cables, routers, and switches.

(TS//SI) Key Targets: Global



Pg 104. Slide cropped.

Fantastico, Sept 8, 2013. Screengrab.

http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html

Undated Memo Excerpt relating to FAIRVIEW

FAIRVIEW — Corp partner since 1985 with access to int. cables, routers, switches. The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs. Aggressively involved in shaping traffic to run signals of interest past our monitors.

Pg 105. Previously unpublished



Pg 105. Previously unpublished.

Undated and Unnamed Memo about ORANGECRUSH

(TS//SI//NF) ORANGECRUSH, part of the OAKSTAR program under SSO's corporate portfolio, began forwarding metadata from a third party partner site (Poland) to NSA repositories as of 3 March and content as of 25 March. This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA Corporate Partner and a division of the Polish Government. ORANGECRUSH is only known to the Poles as BUFFALOGREEN. This multi-group partnership began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM and its DNR capability. The new access will provide SIGINT from commercial links managed by the NSA Corporate Partner and is anticipated to include Afghan National Army, Middle East, Limited Affican continent, and European communications. A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW.

Pg 106. Previously unpublished.

SILVERZEPHYR FAA DNI Access Initiated at NSAW

 ${\tt SILVERZEPHYR\ FAA\ DNI\ Access\ Initiated\ at\ NSAW\ (TS//SI//NF)}$

By NAME REDACTED on 2009-11-06 0918

(TS//SI//NF) On Thursday, 11/5/09, the SSO-OAKSTAR SILVERZEPHYR (SZ) access began forwarding FAA DNI records to NSAW via the FAA WealthyCluster2/Tellurian system installed at the partner's site. SSO coordinated with the Data Flow Office and forwarded numerous sample files to a test partition for validation, which was completely successful. SSO will continue to monitor the flow and collection to ensure a ny anomalies are identified and corrected as required. SILVERZEPHYR will continue to provide customers with authorized, transit DNR collection. SSO is working with the partner to gain access to an additional 80Gbs of DNI data on their peering network, bundled in 10 Gbs increments. The OAKSTAR team, along with support from NSAT and GNDA, just completed a 12 day SIGINT survey at site, which identified over 200 new links. During the survey, GNDA worked with the partner to test the output of their ACS system. OAKSTAR is also working with NSAT to examine snapshots taken by the partner in Brazil and Colombia, both of which may contain internal communications for those countries.

Pg 106. Previously Unpublished.



Pg 107. Previously Unpublished.

PRISM Slides





Motmail®

Pg 108. Identical to the *Washington Post's* version.

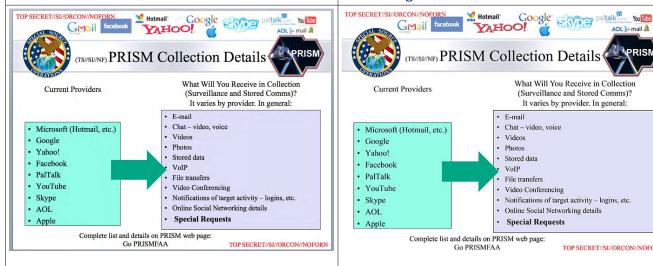
Washington Post Jun 10, 2013. http://www.washingtonpost.com/wpsrv/special/politics/prism-collection-documents/



Pg 110. Identical to *Le Monde's* version, aside from a PDF rendering issue.

Le Monde, Oct 25, 2013

http://www.lemonde.fr/technologies/article/2013/1 0/21/france-in-the-nsa-s-crosshair-wanadoo-andalcatel-targeted 3499739 651865.html



Pg 110. Identical to the version published by the Washington Post. The version published in the Guardian has a rendering bug.

Washington Post, Jun 6, 2013. http://articles.washingtonpost.com/2013-06-06/news/39784046 1 prism-nsa-u-s-servers

Guardian Jun 6, 2013. http://www.theguardian.com/world/2013/jun/06/us -tech-giants-nsa-data

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN Google paltalk on You Tube Motmail* GMail face (TS//SI/NF) Unique Selectors Tasked to PRISM PRISM (US-984XN) in FY2012 32% All Providers in FY12 ➤ Over 45,000 Selectors on Task at End of FY12 Strong Growth in FY12 Tasking: > Skype up 248% up 63%

Quote from article: "It boasts of what it calls "strong growth" in its use of the Prism program to obtain communications. The document highlights the number of obtained communications increased in 2012 by 248% for Skype – leading the notes to remark there was "exponential growth in Skype reporting; looks like the word is getting out about our capability against Skype". There was also a 131% increase in requests for Facebook data, and 63% for Google."

Pg 111. Previously unpublished.

The Guardian, Jul 11, 2013.

http://www.theguardian.com/world/2013/jul/11/mi crosoft-nsa-collaboration-user-data

Prism Expands Impact: FY2012 Metrics Dated Nov 19, 2012

TOP SECRET//SI//ORCON//NOFORN

PRISM Slides

(TS//SI//NF) PRISM (US-984XN) expanded its impact on NSA's reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:

PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall
Number of PRISM-based end-product reports issued in FY12: 24,096, up 27% from FY11
Single-source reporting reconstants.

27% from FY11
Single-source reporting percentage in FY12 and FY11: 74%
Number of product reports derived from PRISM collection and cited as
sources in articles in the President's Daily Brief in FY12: 1,477 (18% of
all SIGINT reports cited as sources in PDB articles – highest single SIGAD
for NSA); In FY11: 1,152 (15% of all SIGINT reports cited as sources in PDB
articles – highest single SIGAD for NSA)
Number of Essential Elements of Information contributed to in FY12:
4,186 (32% of all EEIs for all Information Needs); 220 EEIs addressed
solely by PRISM

4,180 (32% of all ELIS for all Information Needs); 220 ELIS addressed solely by PRISM
Tasking: The number of tasked selectors rose 32% in FY12 to 45,406 as of Sept 2012
Great success in Skype collection and processing; unique, high value targets acquired
Expanded PRISM taskable e-mail domains from only 40, to 22,000

Pg 111. Previously unpublished.

SSO Highlight – Microsoft Skydrive Collection Now Part of of PRISM Stored Communications Collection.

(TS//SI//NF) SSO HIGHLIGHT — Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this — a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

Quote from article: "The company worked with the FBI this year to allow the NSA easier access via Prism to its cloud storage service SkyDrive, which now has more than 250 million users worldwide"

Pg 113. Previously unpublished.

The Guardian, Jul 11, 2013.

http://www.theguardian.com/world/2013/jul/11/mi crosoft-nsa-collaboration-user-data

New Skype Stored Comms capability for PRISM

(TS//SI//NF) New Skype Stored Comms Capability For PRISM

By NAME REDACTED on 2013-04-03 0631

(TS//SI//NF) PRISM has a new collection capability: Skype stored communications. Skype stored communications will contain unique data which is not collected via normal real-time surveillance collection. S50 expects to receive buddy lists, credit card info, call data records, user account info, and other material. On 29 March 2013, S50 forwarded approximately 2000 Skype selectors for stored communications to be adjudicated in SV41 and the Electronic Communications Surveillance Unit (ECSU) at FBI. SV41 had been working on adjudication for the highest priority selectors shead of time and had about 100 ready for ECSU to evaluate. It could take several weeks for SV41 to work through all 2000 selectors to get them approved, and ECSU will likely take longer to grant the approvals. As of 2 April, ESCU had approved over 30 selectors to be sent to Skype for collection. PRISM Skype collection has carved out a vital niche in NSA reporting in less than two years with terrorism, Syrian opposition and regime, and exec/special series reports being the top topics. Over 2800 reports have been issued since April 2011 based on PRISM Skype collection, with 76% of them being single source.

Pg 114. Previously unpublished.

SSO Expands PRISM Skype Targeting Capability

(TS//SI//NF) SSO Expands PRISM Skype Targeting Capability

By NAME REDACTED on 2013-04-03 0629

(TS//SI//NF) On 15 March 2013, SSO's PRISM program began tasking all Microsoft PRISM selectors to Skype because Skype allows users to log in using account identifiers in addition to Skype usernames. Until now, PRISM would not collect any Skype data when a user logged in using anything other than the Skype username which resulted in missing collection; this action will mitigate that. In fact, a user can create a Skype account using any e-mail address with any domain in the world. UTT does not currently allow analysts to task these non-Microsoft e-mail addresses to PRISM, however, SSO intends to fix that this summer. In the meantime, NSA, FBI and Depti of Justice coordinated over the last six months to gain approval for PRINTAURA to send all current and future Microsoft PRISM selectors to Skype. This resulted in about 9800 selectors being sent to Skype and successful collection has been received which otherwise would have been missed.

Pg 114. Previously unpublished.

The Guardian, Jul 11, 2013.

http://www.theguardian.com/world/2013/jul/11/mi crosoft-nsa-collaboration-user-data

Microsoft releases new service, affects FAA 702 collection.

(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

By NAME REDACTED on 2012-12-26 0811

(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements – no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.

Quote from article: A newsletter entry dated 26 December 2012 states: "MS [Microsoft], working with the FBI, developed a surveillance capability to deal" with the issue. "These solutions were successfully tested and went live 12 Dec 2012."

Pg 115. Previously unpublished.

The Guardian, Jul 11, 2013.

http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Expanding PRISM Sharing with the FBI and CIA

(TS//SI//NF) Expanding PRISM Sharing With FBI and CIA

By NAME REDACTED on 2012-08-31 0947

(TS//SII/NF) Special Source Operations (SSO) has recently expanded sharing with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) on PRISM operations via two projects. Through these efforts, SSO has created an environment of sharing and teaming across the Intelligence Community on PRISM operations. First, SSO's PRINTAURA team solved a problem for the Signals Intelligence Directorate (SID) by writing software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA. This enables our partners to see which selectors the National Security Agency (NSA) has tasked to PRISM. The FBI and CIA then can request a copy of PRISM collection from any selector, as allowed under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act law. Prior to PRINTAURA's work, SID had been providing the FBI and CIA with incomplete and inaccurate lists, preventing our partners from making full use of the PRISM program. PRINTAURA volunteered to gather the detailed data related to each selector from multiple locations and assemble it in a usable form. In the second project, the PRISM Mission Program Manager (MPM) recently began sending operational PRISM news and guidance to the FBI and CIA so that their analysts could task the PRISM system properly, be aware of outages and changes, and optimize their use of PRISM. The MPM coordinated an agreement from the SID Foreign Intelligence Surveillance Act Amendments Act (FAA) Team to share this information weekly, which has been well-received and appreciated. These two activities underscore the point that PRISM is a team sport!

Quote from article: "The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies.

The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that 'enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism'.

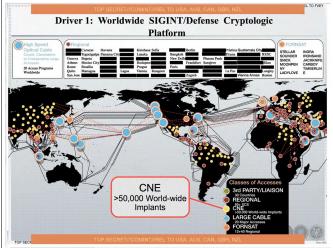
The document continues: 'The FBI and CIA then can request a copy of Prism collection of any selector...' As a result, the author notes: 'these two activities underscore the point that Prism is a team sport!'"

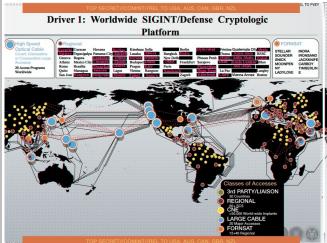
Pg 116. Previously unpublished.

The Guardian, Jul 11, 2013.

http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

SIGINT/Defense Cryptologic Platform Dated 2012





Pg 117. Identical to the version intended to be published by NRC, which redacted city names but did nothing about the red dots representing them. I have decensored much of this slide.

NRC, Nov 23, 2013.

http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/



Pg 120. Identical to slides previously published by *Fantastico* Oct 6, 2013 Fantastico in Brazil and CBC in Canada.

http://g1.globo.com/fantastico/noticia/2013/10/mi nisterio-das-minas-e-energia-esta-na-mira-deespioes-americanos-e-canadenses.html

CBC, Nov 30, 2013

http://www.theglobeandmail.com/news/politics/re ad-a-csec-document-on-brazil-that-was-firstacquired-by-edward-snowden/article15699941/

NSA's relationship with CSEC The full document does not fit in a table cell. It is TOP SECRET//SI//REL USA, FVEY published here: National Security Agency/ Central Security Service 3 April 2013 Information Paper http://www.cbc.ca/news2/pdf/nsa-canadaapril32013.pdf ect: (U//FOUO) NSA Intelligence Relationship with Canada munications Security Establishment Canada (CSEC) TOP SECRET//SI//REL TO USA, CAN (U) What NSA provides to the partner: (S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC coo developments, cryptologic capabilities, software and resources for state-of-this-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC coworldwide national and transnational targets. No Consolidated Cryptologic Plogram (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology coets on shared projects with CSEC. (U) What the partner provides to NSA: (TS//SI///REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increase its investment in R&D projects of mutual interest. Pg 121. extracts from a larger paper. CBC, Dec 9, 2013. http://www.cbc.ca/news/politics/snowdendocument-shows-canada-set-up-spv-posts-for-nsa-1.2456886 Letter from deputy director of Australia's DSD to NSA's SID **Dated Feb 21, 2011** While we have invested significant analytic and collection effort of our own to find and exploit these communications, the difficulties we face in obtaining regular and reliable access to such communications impacts on our ability to detect and prevent terrorist acts and diminishes our capacity to protect the life and safety of Australian citizens and those of our close friends and allies. We have enjoyed a long and very productive partnership with NSA in obtaining minimised access to United States warranted collection against our highest value terrorist targets in Indonesia. This access has been critical to DSD's efforts to disrupt and contain the operational capabilities of terrorists in our region as highlighted by the recent arrest of fugitive Bali bomber Umar Patek. We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities - in particular Australians involved with AQAP.

Pg 122. Previously unpublished.

Sharing computer network operations with cryptologic information foreign partners. Circa 2004

CONFIDENTIAL//NOFORN//20291123 Australia TIER A Canada **Comprehensive Cooperation** New Zealand United Kingdom Austria TIER B Belgium **Focused Cooperation** Czech Republic Denmark Germany Greece Hungary Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden

Switzerland Turkey



Pg 123. Extracted from a larger document.

El Mundo, Oct 30, 2013.

http://www.elmundo.es/espana/2013/10/30/52709 85d63fd3d7d778b4576.html

FY 2013 Foreign Partner review



Pg 123. Previously unpublished

FY 2012 Foreign Policy review



Pg 124. Previously unpublished

History of the US – Israel Sigint Relationship, Post-1992

(TS//SI//REL) There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner.

Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge. In the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner. Nevertheless, the survival of the state of Israel is a paramount goal of US Middle East policy. There is no doubt that the NSA-ISNU SIGINT relationship is built upon a solid foundation of trust and common purpose.

Pg 125. *The Guardian* also published additional excerpts of this document.

The Guardian Sept 11, 2013

http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents

Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807) During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance. Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part. Pg 129. Previously unpublished. **Communications metadata fields in ICREACH Communications Metadata Fields in ICREACH** (S//NF) NSA populates these fields in PROTON: Called & calling numbers, date, time & duration of call (S//SI//REL) ICREACH users will see telephony metadata* in the following fields: IMEI - International Mobile Equipment DURATION – Length of Call CALLED NUMBER CALLING NUMBER Identifier MSISDN - Mobile Subscriber Integrated CALLING NUMBER **Services Digital Network** CALLED FAX (CSI) – Called Subscriber MDN – Mobile Dialed Number CLI - Call Line Identifier (Caller ID) CLI – Call Line Identifier (Caller ID) DSME – Destination Short Message TRANSMITTING FAX (TSI) – Transmitting Subscriber ID IMSI – International Mobile Subscriber OSME – Originating Short Message

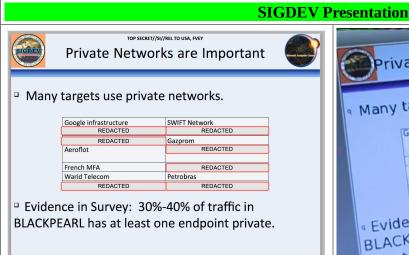
Pg 132. Previously unpublished

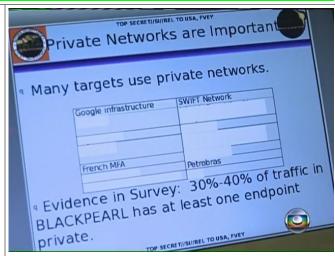
VLR - Visitor Location Register

SECRET//COMINT//NOFORN//20320108

TMSI – Temporary Mobile Subscriber

Identifier





Pg 135. In this case, the book version shows a few more companies.

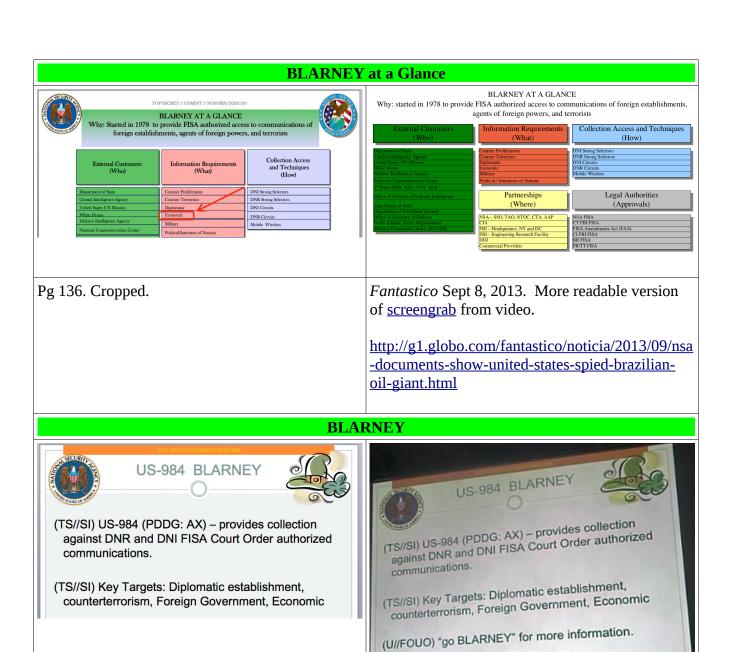
Fantastico Sept 8, 2013. Screengrab from video.

http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html

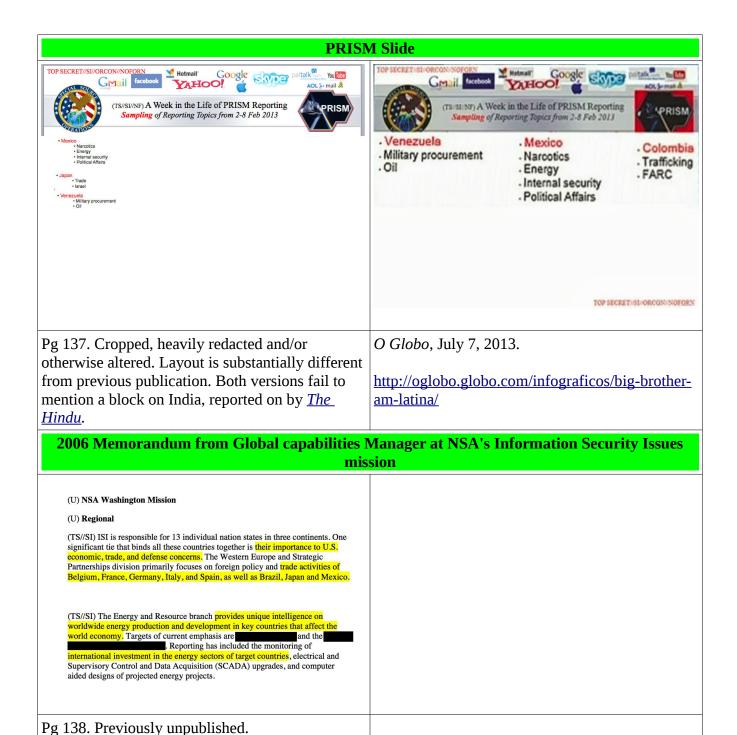
Serving Our Customers



Pg 136. Previously unpublished.







Letter from Ambassador Thomas Shannon to Kieth Alexander

The more than 100

reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.

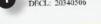


United States Department of State

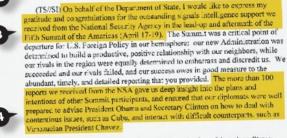
Washington, D.C. 20520

May 17, 2009



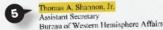






(TS//SI) Our work is far from done—the Organization of American States General Assembly meeting next month will probably feature renewed discussion of Culia, and such countries as Venezuels, and Bolivia remain intent on challenging our interests in the short term—but I are confident but NSA reporting will continue to give us the edge that our diplomacy needs.





TOP SECRET//COMINT
Classified by: John Dinger, INR A/8, Acting
REASON FOR CLASSIFICATION: E.O. 12958 1.4(c) and (d)
DECL ON: 20340506

Pg 139. Small excerpt from larger letter published in full by Epoca.

Epoca Aug 2, 2013

http://epoca.globo.com/tempo/noticia/2013/08/car ta-em-que-o-atual-bembaixadorb-americano-nobrasil-bagradece-o-apoio-da-nsab.html

Intelligently Filtering Your Data: Brazil and Mexico Case studies

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZ

(U//FOUO) S2C42 surge effort (U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZI

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort (U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Intelligently Filtering Your Data: Brazil and Mexico Case studies

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZ

(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

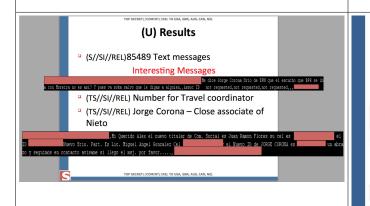
TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZ

(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a twoweek target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZI



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U) Results

(S//SI//REL)85489 Text messages

Interesting Messages

le dice longe forma frio de EVI que el escuebo que EVI se di con Boreira no es asil/T pues va soba salvo que le digue a alquien, Assoc D — not requested, not respected, no

, Ti (perión blen el meno titular de Con. Social es Juan Ranon Flores su cel es Un servicio Part. Es Lic. Mignel Angel Gonzaler Cel el Bero 10 de JORE CORNU es un abra o y seguinos en contexto arisane si llego el maj, por fanor.....,

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Intelligently Filtering Your Data: Brazil and Mexico Case studies

(U) Conclusion

- (S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery
- (TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.

(U) Conclusion

□(S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery a(TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against highprofile, OPSEC-savvy Brazilian and Mexican targets.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZI

Pages 139 – 141. Published fewer slides, but reproduced the "results" slide in full.

Fantastico, Sept 1, 2013

http://g1.globo.com/fantastico/noticia/2013/09/vej a-os-documentos-ultrassecretos-que-comprovamespionagem-dilma.html

April 2013 briefing from SSO

TOP SECRET//SI//NOFORN



(U) OPERATIONAL HIGHLIGHT



(TS//SI//NF) BLARNEY Team assists S2C52 analysts in implementing **Xkeyscore fingerprints that yield** access to U.N. Secretary General talking points prior to meeting with POTUS.

TOP SECRET//SI//NOFORN

Pg 142. Previously unpublished.

BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection

(S//SI) BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection $% \left(1\right) =\left(1\right) \left(1$

By NAME REDACTED

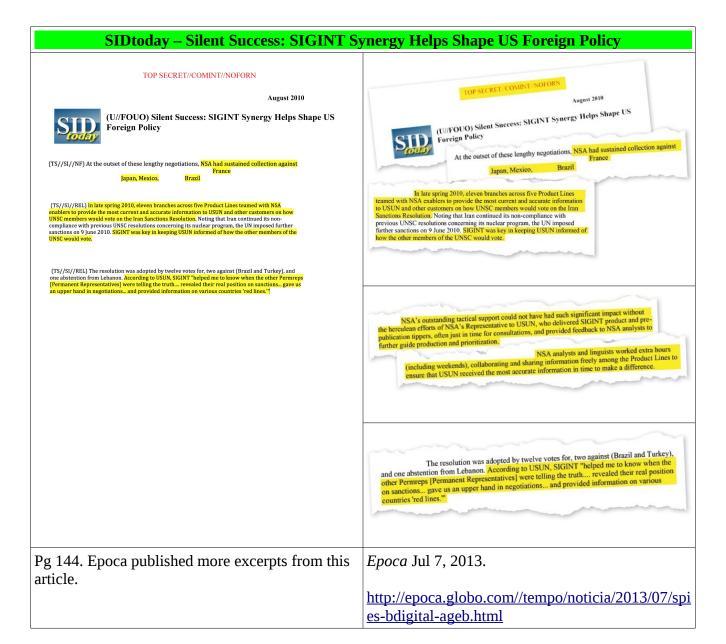
on 2010-05-28 1430

(TS//SI//NF) With the UN vote on sanctions against Iran approaching and several countries riding the fence on making a decision, Ambassador Rice reached out to NSA requesting SIGINT on those countries so that she could develop a strategy. With the requirement that this be done rapidly and within our legal authorities, the BLARNEY team jumped in to work with organizations and partners both internal and external to NSA.

(TS//SI/NF) As OGC, SV and the TOPIs aggressively worked through the legal paperwork to expedite four new NSA FISA court orders for Gabon, Uganda, Nigeria and Bosnia, BLARNEY Operations Division personnel were behind the scenes gathering data determining what survey information was available or could be obtained via their long standing FBI contacts. As they worked to obtain information on both the UN Missions in NY and the Embassies in DC, the target development team greased the skids with appropriate data flow personnel and all preparations were made to ensure data could flow to the TOPIs as soon as possible. Several personnel, one from legal team and one from target development team were called in on Saturday 22 May to support the 24 hour drill legal paperwork exercise doing their part to ensure the orders were ready for the NSA Director's signature early Monday morning 24 May.

(S//SI) With OGC and SV pushing hard to expedite these four orders, they went from the NSA Director for signature to DOD for SECDEF signature and then to DOJ for signature by the FISC judge in record time. All four orders were signed by the judge on Wednesday 26 May! Once the orders were received by the BLARNEY legal team, they sprung into action parsing these four orders plus another "normal" renewal in one day. Parsing five court orders in one day — a BLARNEY record! As the BLARNEY legal team was busily parsing court orders the BLARNEY access management team was working with the FBI to pass tasking information and coordinate the engagement with telecommunications partners.

| - | 4 40 | T • 1 | | 1 ' | |
|----|-------|--------------|----------|-----|--------|
| שמ | 1/1/ | Previous ! | 37 11DD1 | ıh | lichad |
| ГΥ | 14.). | FIEVIOUS | v unin | 11, | naneu. |
| | | | | | |



Close Access Sigads

Document is too large for a table cell. See

http://nsa.gov1.info/dni/2014/no-place-to-hide/spying/1.jpg

| Т | SIGAD | US-3136 | | | | |
|-----|---------------------|---------------------|----------------|----------------------|---|---|
| ш | Suffix | Target/Country | | Location | Coverterm | Mission |
| 1.3 | SI | Brazi/Emb | | Wash, DC | KATEEL | HIGHLANDS |
| | BE | Brazi/Emb | | Wash, DC | KATEEL | UFESAVER |
| 11 | VO | Braz MUN | | New York | POCOMOKE | HIGH ANDS |
| ш | 13 | Brazi/UN | | New York | POCOMOKE | LIFESAVER |
| ш | HN | Brazil/UN | | New York | POCOMOKE | VAGRANT |
| П | | EWEnt | | Wash, DC | MAGGTHY | DROPMIRE |
| Ш | | EWEmb | | Wash, DC | MAGOTHY | HGHLANDS |
| ш | | EWEmb | | Wash, DC | MAGOTHY | MINERALIZE |
| П | | EWUN | | New York | APALATCHEE/PERDIDO | |
| 11 | | EU/UN | | New York | APALATCHEE/PERDIDO | |
| П | uc | France/Emb | | Wash, DC | WARASH | HIGH ANDS |
| ш | LO | France/Emb | | Wash, DC | WABASH | PBK |
| ш | OF. | France/UN | | New York | BLACKFOOT | HIGHLANDS |
| П | vc | France/UN | | New York | BLACKFOOT | VAGRANT |
| Ш | | Greece/Emb | | Wash, DC | KLONDYKE | |
| Ш | | Greece/UN | | New York | POWELL | |
| П | | India/Emb Annex | | Wash, DC | | HIGHLANDS |
| П | | India/Emb Arnex | | Wash, DC | | VAGRAIT |
| н. | | India/Emb | | Wash, DC | | LIFESAVER |
| Ι. | | IndiaEmb | : | Wash, DC | | MAGNETIC |
| н | | Inda/Emb Inda/UN | | Wash, DC New York | | VAGRAIT HIGHLANDS |
| 1.3 | | IndiaUN | | New York | | HESSAVER |
| П | | IndiaUN | | New York | | MAGNETIC |
| 11 | | India/UN | | New York | | VAGRANT |
| ш | SU | Italy/Emb | | Wash, DC | BRUNEAU | LIVESAVER |
| | | ttaty/Emp. | | Wish, DC | HEMLOCK | HOH ANDS |
| П | | Japan | | | | |
| П | | Mexico | | | | |
| ш | | South Korea | | | | |
| П | | Turkey | | | | |
| Ш | PD | Clase Access | | New York | | COOP |
| Ι. | | | | | | |
| | SICAD | US-3137 | | Location | | Mission |
| н | Sumox | Target/Country | | | Coverterm | MISSION |
| н | | Austria/IAEA | | Vienna | | |
| н | | | | | | |
| П | US-3138 - STAR | RUBY (trastint) | | | | |
| Ш | | | | | | |
| | General Term De | scriptions | | | | |
| | HIGHLANDS | | Collection fro | | | |
| | VAGRANT MAGNETIC | | | computer Scr | eens atic Emanations | |
| | MINERALIZE | | | im LAN Implai | | |
| | OCEAN | | | | n. For Raster-Based Computer | Screens |
| | LIFESAVER | | Imaging of th | | to reason bases componer | |
| | GENIE | | Multi-stage o | peration; jump | ing the sirgap etc. | |
| | BLACKHEART | | Collection fro | m an FBI imp | lant | |
| | PBX | | | h Exchange S | | |
| | CRYPTO ENABL | ED | | | s efforts to enable Crypto | |
| 1 | DROPMIRE | | | | ations using an antenna | |
| 1 | CUSTOMS DROPMIRE | | | | : LIFESAVER) rely proximal access (**NOT | W to a local control of |
| | DEWSWEEPER | | | | | "implamady." ides COVERT link over USB link into a target network. Operates wRF relay subsystem to provide wireless Bridge into target network. |
| | RADON | | | | | onto the same target. Allows Bi-directional exploitation of Denied networks using standard on-net tools. |
| 1 | | | or prietorna | | con rights continue province | the or same argue, rame or account expression is overea (2001to 300g station) with 000s. |
| 1 | | | | | | |
| 1 | | | | | | |
| | | | | | | |

Pg 145-147. Adds Bulgaria, Columbia, Georgia, Slovakia, Taiwan, Venezuela, Vietnam. Omits Turkey and a few still-unnamed countries.

Earlier reconstruction of document based on multiple sources. (own work)

SIDtoday: Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

TOP SECRET//COMINT//NOFORN

June 2010



(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) NAME REDACTED , Chief, Access and Target Development (S3261)

(TS//SI/NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away... In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are intercepted. Next, they are redirected to a secret location where Tailored Access Operations (AO = \$320 employees, with the support of the Remote Operations Center (\$321), enable the installation of beacon implants directly into our targets' electronic devices. These devices are then re-packaged and placed back into transit to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.





(TS//SI/NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supplychain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.

Pg 149. Previously unpublished.

Report generated Apr 11, 2013 TOP SECRET//COMINT//REL TO USA, FVEY Active ECP Count: 1 ECP Lead: NAME REDACTED Update Software on all Cisco ONS Nodes Title of Change: Update Software on all Cisco ONS Nodes AMDERIA REDACTED APPLET : CLEVERDEVICE : HOMEMAKER: DOGHUT : OUARTERFOUNDER: OUERSIAND: SCALLION SUBSTRATUM: HITAN POINTE: SUBSTRATUM: BIRCHWOOD: MAYTAG: EAGLE: EDEN: Comms/Network: Comms/Ne Approval Priority: C-Routine No Project(s) Entered Site(s): SubSystem(s): System(s): Description of Change: Udate software on all Cisco Optical Network Switches All of our Cisco ONS SONET multiplexers are experiencing a software bug that causes them to intermittently drop out. The mission impact is unknown. While the existing bug doesn't appear to affect traffic, applying the new software update could. Unfortunately, there is now way to be sure. We cart simulate the bug in our lab and so it's impossible to predict exactly what will happen when we apply the software update. We propose to update one of the nodes in NBP-320 first to determine if the update goes smoothly. Mission Impact: Recently we tried to reset the standby manager card in the HOMEMAKER node. When that failed, we attempted to physically reseal it. Since it was the standby card, we did not expect that would cause any problems. However, upon reseating the card, the entire ONS crashed and we lost all traffic through the box. It took more than an hour to recover from this failure. The worst case scenario is that we have to blow away the entire configuration and start from scratch. Prior to starting our upgrade, we will save the configuration to that if we have to configure the box from scratch, we can simply uploade the saved configuration. We estimate that we will be down for no more than an hour for each node in the system. We have tested the upgrade in our lab and it works well. However, we can't repeat the bug in our lab, so we don't know if we will encounter problems when we attempt to upgrade a node that is affected by the bug. 04/10/13 16:00-11 [NME REDACTE] 09 Apr Blamey CCB - Blamey ECP board approved ECP lead [NME REDACTE] Blamey Fairview Oakstar Stormbrew Additional Info: Last CCB Entry: Programs Affected: No Related Work Tasks Pg 150. Previously unpublished. NSA document prepared for 5 eyes SigDev conference. The Challenge Collection is outpacing our ability to ingest, process and store to the "norms" to which we have become accustomed.

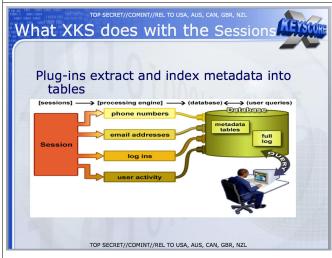
Pg 151. Previously unpublished. However, it may

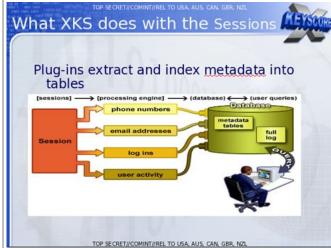
be part of a previously published <u>deck</u>.

Large Scale Expansion of NSA Metadata Sharing Large Scale Expansion of NSA Metadata Sharing (S//SI//REL) Increases NSA communications metadata sharing from 50 billion records to 850+ billion records (grows by 1-2 billion records per day) Yearly Growth ■ Projected DNI ■ DNI ☐ Projected PSTN ■ PSTN 204 205 205 204 205 206 201 *(C//REL) Includes Call Events from 2nd Party SIGINT Partners (est. 126 Billion records) (S//NF) Call Events in PROTON* •Total Call Events in NSA PROTON* est. 149 Billion •Total Call Events Non-NSA est. 101 Billion •Total Call Events Non-NSA, est. 92,000 Non-NOFORN, Non-HCS Non-NSA Events NOT Shareabl with 5 Eyes (NOFORN / HCS) $\ensuremath{^{\star}}$ For date range 2000-2006, as of early July 2006; some data has been aged off system SECRET//NOFORN//20320108

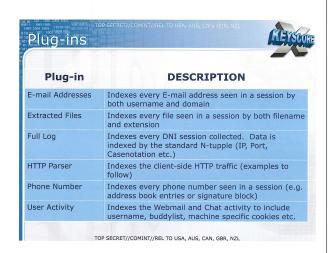
Pg 152. Previously unpublished.

XKEYSCORE slides





| Plug-ins Top secret//comint//rel to usa, aus, can, gbr, nzl | | | | | |
|--|---|--|--|--|--|
| Plug-in | DESCRIPTION | | | | |
| E-mail Addresses | Indexes every E-mail address seen in a session by both username and domain | | | | |
| Extracted Files | Indexes every file seen in a session by both filename and extension | | | | |
| Full Log | Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.) | | | | |
| HTTP Parser | Indexes the client-side HTTP traffic (examples to follow) | | | | |
| Phone Number | Indexes every phone number seen in a session (e.g. address book entries or signature block) | | | | |
| User Activity | Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. | | | | |
| тс | OP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL | | | | |



Pg 154.

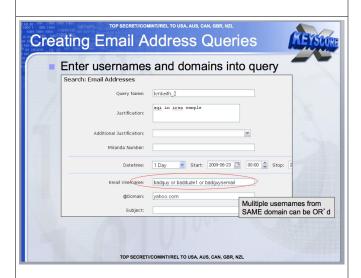
The Guardian, Jul 31, 2013.



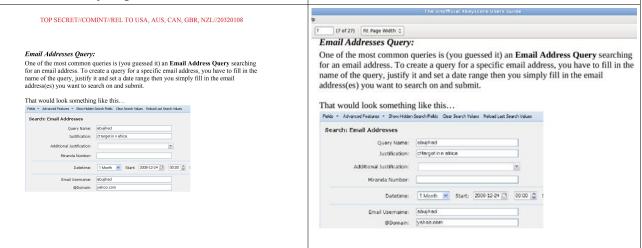
Pg 155. Previously unpublished. Cropped.



XKS HTTP Activity Search For example let's say we want to see all traffic from IP Address 1.2.3.4 to the website www.website.com While we can just put the IP address and the "host" into the search form, remember what we saw before about the various host names for a given website

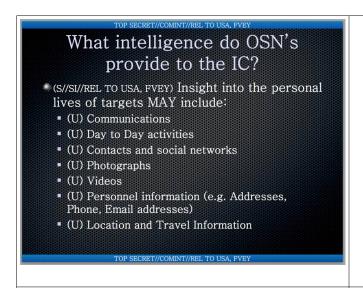


Pg 157. Previously unpublished.

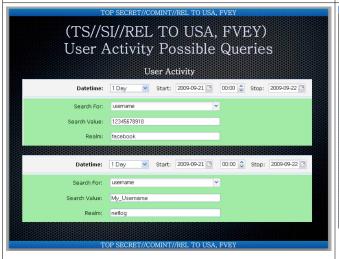


Pg 158. *The Guardian's* version is shown within a reader.

The Guardian, Jul 31, 2013.



Pg 158. Previously unpublished.





Pg 159. *The Guardian's* version cropped the bottom classification bar.

The Guardian, Jul 31, 2013.

SSO - Last 30 Days Signal Profile Most Volume Most Vol

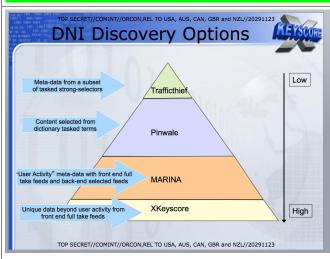


Pg 159. *The Guardian* published a small snippet of this side at a nearly illegible resolution.

The Guardian, Jul 31, 2013.

http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

XKEYSCORE slide





Pg 160. *The Guardian* cropped the bottom classification bar.

The Guardian, Jul 31, 2013.

BLARNEY Exploits the Social Network via Expanded Facebook Collection.

(TS//SI//NF) BLARNEY Exploits the Social Network via Expanded Facebook Collection

By NAME REDACTED ON 2011-03-14 0737

(TS//SI//NF) SSO HIGHLIGHT – BLARNEY Exploits the Social Network via Expanded Facebook Collection

(TS//SI//NF) On 11 March 2011, BLARNEY began delivery of substantially improved and more complete Facebook content. This is a major leap forward in NSA's ability to exploit Facebook using FISA and FAA authorities. This effort was initiated in partnership with the FBI six months ago to address an unreliable and incomplete Facebook collection system. NSA is now able to access a broad range of Facebook data via surveillance and search activities. OPIs are excited about receiving many content fields, such as chat, on a sustained basis that had previously only been occasionally available. Some content will be completely new including subscriber videos. Taken together, the new Facebook collection will provide a robust SIGINT opportunity against our targets — from geolocation based on their IP addresses and user agent, to collection of all of their private messages and profile information. Multiple elements across NSA partnered to ensure the successful delivery of this data. An NSA representative at FBI coordinated the rapid development of the collection system; SSO's PRINTAURA team wrote new software and made configuration changes; CES modified their protocol exploitation systems and the Technology Directorate fast-tracked upgrades to their data presentation tools so that OPIs could view the data properly.

Pg 160. Previously unpublished.

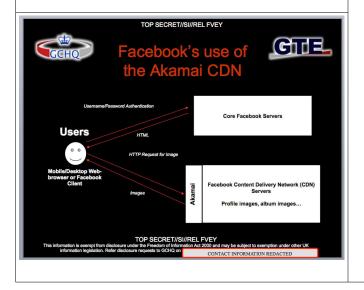
Exploiting Facebook traffic in the passive environment to obtain specific information Dated 2011



Exploiting Facebook traffic in the passive environment to obtain specific information Dated 2011

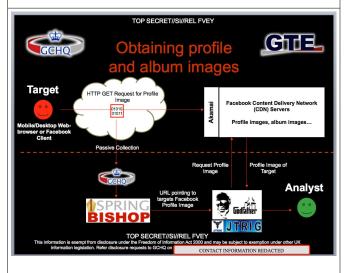






Exploiting Facebook traffic in the passive environment to obtain specific information Dated 2011





Pg 161 – 163. Previously unpublished

THIEVING MAGPIE presentation dated 2012



THIEVING MAGPIE presentation dated 2012



On board GSM Services



- •Many airlines are offering on-board mobile phone services, particularly for long haul and business class (list is growing)
- •At least British Airways are restricting the service to data and SMS only no voice

TOP SECRET//COMINT//REL TO USA, FVEY STRAP!
This information is exampt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK





GPRS Events



- •Currently able to produce events for at least Blackberry phones in flight
- •Able to identify Blackberry PIN and associated Email addresses
- •Tasked content into datastores, unselected to Xkeyscore, further details of usage available

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1
n is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK

This information is exempt from disclosure under the Freedom of Information Act information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTE



Pg 161 – 165. Previously unpublished.

HOMING PIGEON Dated 2012

TOP SECRET//COMINT//REL TO USA, FVEY

(U) ANALYTIC DRIVER (CONT.)

- ☐(S//SI//REL FVEY) Analytic Question

 Given a GSM handset detected on a known aircraft flight, what is the likely identity (or identities) of the handset subscriber (and viceversa)?
- ☐(TS//SI//REL FVEY) Proposed Process
 Auto correlation of GSM handsets to subscribers observed on two or more flights.

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA EVEY

(U) GOING FORWARD

- ☐ (TS//SI//REL FVEY) SATC will complete development once a reliable THIEVING MAGPIE data feed has been established
- ☐ (TS//SI//REL FVEY) Once the QFD is complete, it will be available to FVEY users as a RESTful web service, JEMA component, and a light weight web page
- □ (TS//SI//REL FVEY) If the S2 QFD Review Panel elects to ask for HOMING PIGEON to be made persistent, its natural home would be incorporation into FASTSCOPE

TOP SECRET//COMINT//REL TO USA, FVEY

Pg 166. Previously unpublished.

The Role of National Interests, Money, and Egos



Oh Yeah...

Put Money, National Interest, and Ego together, and now you' re talking about shaping the world writ large.

What country doesn't want to make the world a better place... for itself?

U//FOUO



What's the Threat?

- Let's be blunt the Western World (especially the US) gained influence and made a lot of money via the drafting of earlier standards.
 - □The US was the major player in shaping today's Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by US entities.

Pg 167. Previously unpublished.

National Security Agency: Overview Briefing



Pg 168. Previously unpublished.

Letter from the Director of the NSA **dated Oct 3, 2012**

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these publicabilities in the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- · Viewing sexually explicit material online or using sexually explicit persuasive
- language when communicating with inexperienced young girls;

 Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;

 Charging an exorbitant amount of money for their speaking fees and being
- singularly attracted by opportunities to increase their stature; or

 Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.

BACKGROUND (U)

(TS/SI/REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particle nerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, we link question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these

(TS/SI/REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting valuerabilities of character, credibility, or both, of the radiculture and his message could be enhanced by an understanding or the vehicles he uses to discentable this message to the susceptible pool of people and where he is valuerable in terms of access.

Pg 187. The Huffington Post publishes additional; | Huffington Post, Nov 26, 2013 excerpts.

http://www.huffingtonpost.com/2013/11/26/nsaporn-muslims n 4346128.html

Manhunting Timeline Read Edit Page history 🗘 🔻 Search (U) Manhunting Timeline 2010 (U) Manhunting Timeline 2010 TOP SECRET//SI/TK//NOFORN See also: Manhunting Timeline 2011 See also: Manhunting Timeline 2009 See also: Manhunting Timeline 2008 Main article: Manhunting See also: Manhunting Timeline 2011 See also: Manhunting Timeline 2009 See also: Manhunting Timeline 2008 (U) The following manhunting operations took place in Calendar Year 2010: (U) November (U) The following manhunting operations took place in Calendar Year 2010: [edit] (U) November Contents (U) United States, Australia, Great Britain, Germany, Iceland [edit] (U) United States, Australia, Great Britain, Germany, Iceland (U) The United States on 10 August urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider filing criminal charges against Julian Assange, founder of the rogue Wikileaks Internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war and Afghanistan. The documents may have been provided to Wikileaks by Army Private First Class Bradley Manning. The appeal exemplifies the start of an international effort to focus the legal element of national power upon non-state actor. Assange, and the human network that supports Wikileaks, London and the human network that supports Wikileaks. The Intercept, Feb 18 2014 Pg 188 https://firstlook.org/theintercept/article/2014/02/1 8/snowden-docs-reveal-covert-surveillance-andpressure-tactics-aimed-at-wikileaks-and-itssupporters/

Discovery SIGINT Targeting Scenarios and Compliance

[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

[edit] (TS//SI//REL) Unknowingly targeting a US person

I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report... but it's nothing to worry about', (Source #001)

Document is too large to fit in a table cell. See:

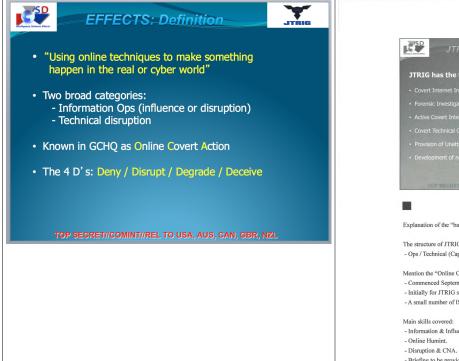
https://firstlook.org/theintercept/document/2014/0 2/18/discovery-sigint-targeting-scenarioscompliance/

Pg 189. Published small excerpts of a much larger document.

The Intercept, Feb 18, 2014

https://firstlook.org/theintercept/document/2014/0 2/18/discovery-sigint-targeting-scenarioscompliance/

Cyber Integration: the Art of the Possible Dated 2012



JTRIG - Core Femetions

JTRIG has the following core functions:

Covert Internet Investigations

Forensic Investigation and Analysis

Active Covert Internet Operations, (including online Humint and Effects)

Covert Technical Operations

Provision of Unattributable Internet Access

Development of new capability

TOP SECRETICOMINITIES TO USA AUS, CAN, GBR, NZL

Explanation of the "base-line" for JTRIG-related work and make-up:

The structure of JTRIG:

Ops / Technical (Cap Dev) / JBOS.

Mention the "Online Covert Action Accreditation" Programme.

Commenced September 2011.

Initially for JTRIG staff.

A small number of ISD analysts now being accepted on courses.

Main skills covered:

Information & Influence Operations.

Online Humint.

Disruption & CNA.

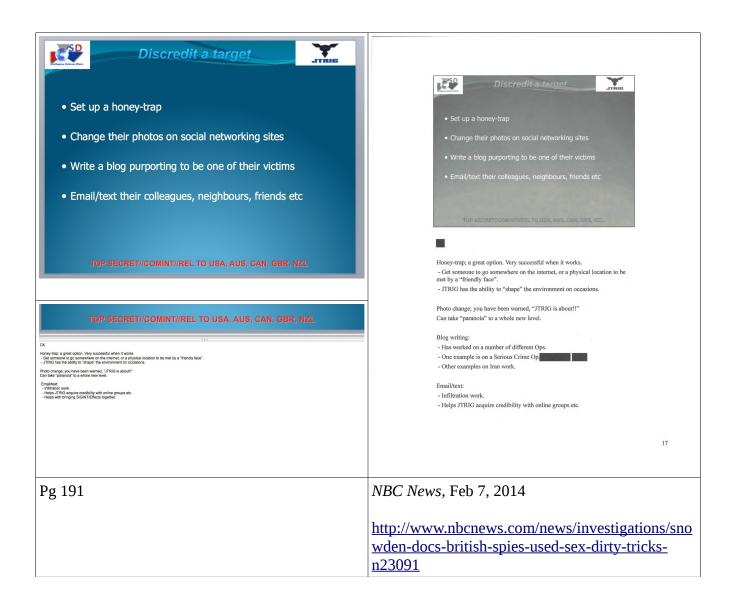
Briefing to be provided by

13

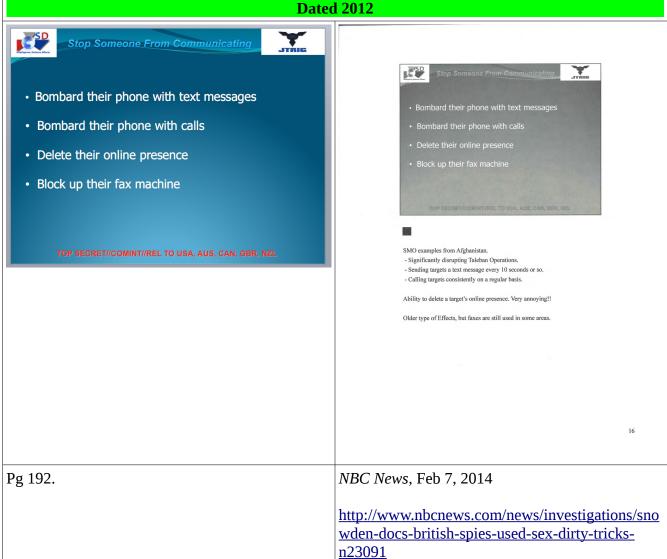
Pg 190

NBC News, Feb 7, 2014

http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091



Cyber Integration: the Art of the Possible Dated 2012



Cyber Integration: the Art of the Possible Dated 2012



Stop someone's computer from working

Send them a virus:

AMBASSADORS RECEPTION – encrypt itself, delete all emails, encrypt all files, make screen shake, no more log on

Conduct a Denial of Service attack on their computer

Virus sending:

- Use of various JTRIG tools, including AMBASSADORS RECEPTION.
- Has been used in a variety of different areas, very effective.

Pg 192.

NBC News, Feb 7, 2014

http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

Cyber Offensive Session: Pushing the Boundaries Against Hactivism

Why do an Effects Operation?

- Disruption v Traditional Law Enforcement
- SIGINT discovered the targets
- Disruption techniques could save time and money

TOP SECRET//COMINT//REL AUS/CAN/NZ/UK/US

Pg 193. Previously unpublished.

Cyber Offensive Session: Pushing the Boundaries Against Hactivism NBC NEWS INVESTIGATIONS investigations.nbcnews.com Effects on Hacktivisim Effects on Hacktivisim Op WEALTH – Summer 2011 • Intel support to Law Enforcement – identification of top • Op WEALTH - Summer 2011 targets • Intel support to Law Enforcement - identification of top Denial of Service on Key Communications outlets targets Information Operations · Denial of Service on Key Communications outlets Information Operations Pg 193. NBC News, Feb 4, 2014 http://www.nbcnews.com/news/investigations/war -anonymous-british-spies-attacked-hackerssnowden-docs-show-n21361 SECRET//SI//REL TO USA, FVEY DISRUPTION **DISRUPTION** Operational Operational Playbook Playbook • Infiltration Operation • Ruse Operation · Infiltration Operation • Set Piece Operation Ruse Operation • False Flag Operation • Set Piece Operation • False Rescue Operation • False Flag Operation Disruption Operation • False Rescue Operation Sting Operation · Disruption Operation Sting Operation SECRET//SI//REL TO USA, FVEY

Pg 194

The Intercept, Feb 24, 2014

manipulation/

https://firstlook.org/theintercept/2014/02/24/jtrig-