SPIEGEL ONLINE INTERNATIONAL

The NSA in Germany: Snowden's Documents Available for Download

In Edward Snowden's archive on NSA spying activities around the world, there are numerous documents pertaining to the agency's operations in Germany and its cooperation with German agencies. SPIEGEL is publishing 53 of them, available as PDF files.

June 18, 2014 – 04:21 PM

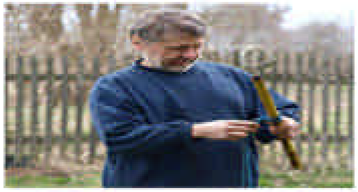
Print | E-Mail

Feedback

Tweet 39 Recommend 2 g+1

America's National Security Agency has been active in Germany for decades. During the Cold War, much of its focus was on targets beyond West Germany's eastern border. But even then, the NSA continued to monitor communications within, and originating in, West Germany. Since the terror attacks of Sept. 11, 2001, the NSA has increased its ability to monitor global communications -- and documents from the archive of whistleblower Edward Snowden show that Germany is the agency's most important base of operations in continental Europe.

The documents show that the NSA, while focusing on counter-terrorism and other areas of importance to national security, has also established systems that allow it to monitor vast amounts of digital and other forms of communications in Germany and elsewhere. The agency can intercept huge amounts of emails, text messages and phone conversations. The NSA even monitored the mobile phone of German Chancellor Angela Merkel.



When revelations of NSA spying in Germany first broke last year, German officials indicated they were unaware of the breadth of US intelligence activity in the country. For this week's cover story, SPIEGEL once again examined all of the documents from Snowden's archive pertaining to NSA activity in Germany. The story can be read here.

But Snowden documents also indicate that Germany's foreign intelligence agency, the BND, and its domestic intelligence agency, the BfV, work closely together with the NSA in sites around Germany. For SPIEGEL's story on that cooperation, click here.

Below are PDF files of the most important documents pertaining to that cooperation. SPIEGEL has redacted them to obscure the identification of BND and NSA agents, phone numbers, email addresses and other information that could put lives in danger. A glossary explaining many of the abbreviations found in the documents can be found here. SPIEGEL's editorial explaining why we have elected to publicize the documents can be read here.

Please note, in some of the documents, you may have to scroll down to get to the text.

Nostalgic recollections out of the NSA intranet from NSA workers formerly stationed in Bad Aibling

Document excerpt on the sharing of the NSA spy tool XKeyscore with the Federal Office for the Protection of the Constitution (BfV), Germany's domestic intelligence agency

Secret document on the cooperation between the NSA, BND and BfV in the fight against terrorism

Preliminary agenda of a meeting between high-ranking NSA and BND officials

Edward Snowden's Germany Files

(U) Analytics for Targets in Europe

The NSA in Germany: Snowden's Documents Available for Download

New NSA Revelations: Inside Snowden's Germany File

Spying Together: Germany's Deep Cooperation with the NSA

Abbreviations Explained: How to Read the NSA Documents

NSA in Germany: Why We Are Posting Secret Documents

Interview with Ex-Stasi Agent: 'The Scope of NSA Surveillance Surprised Me'

From DER SPIEGEL

The article you are reading originally appeared in German in issue 25/2014 (June 16, 2014) of DER SPIEGEL.

Click on the links below for more information about DER SPIEGEL's history, how to subscribe or purchase the latest issue of the German-language edition in print or digital form or how to obtain rights to reprint SPIEGEL articles.

Frequently Asked Questions: Everything You Need to Know about DER SPIEGEL

Six Decades of Quality Journalism: The History of DER SPIEGEL

A New Home in HafenCity: SPIEGEL's New Hamburg HQ

Reprints: How To License SPIEGEL Articles

NSA Spying Scandal

Edward Snowden

Related SPIEGEL ONLINE links

New NSA Revelations: Inside Snowden's Germany File (06/18/2014)

Spying Together: Germany's Deep Cooperation with the NSA (06/18/2014)

NSA in Germany: Why We Are Posting Secret Documents (06/18/2014)

Abbreviations Explained: How to Read the NSA Documents (06/18/2014)

Get Mobile with Our New App

Download It Today: 'DER SPIEGEL in English' Now Available for iPhone

Newsletter

SPIEGEL ONLINE

Sign up for Spiegel Online's daily newsletter - and get the best of Der Spiegel's and Spiegel Online's international coverage in your In-Box everyday.

Facebook

Briefing on the visit to the NSA of a high-ranking BND official

Final agenda of a meeting between high-ranking NSA and BND officials

Internal NSA presentation on the BND's organization

Internal NSA discussion guidelines relating to cooperation with the BND and BfV

Internal NSA discussion guidelines in preparation for a meeting with high-ranking BND officials

Comprehensive internal summary of the history and current state of cooperation between the NSA and BND

FAQs on the Boundless Informant program

Boundless Informant statistics on Germany

Boundless Informant overview (global)

Boundless Informant statistics for so-called Third Parties, which includes Germany

Boundless Informant statistics on data from "Foreign Partners"

Overview of the use of Boundless Informant (world map)

World map from the Boundless Informant program

Zoom of a Boundless Informant document, with project names

Agenda for the visit of BSI Vice President Andreas Könen to the NSA

Report on the beginnings of the European Security Center (ESC) in the Dagger Complex

Report on the changing of the ESC's name to European Security Operations Center (ESOC)

ESOC: Report on the experiences of one NSA worker

Report on the changing of the ESOC's name to European Cryptologic Center (ECC) including details on missions launched from there

Report on an XKeyscore training session at the ECC / Dagger Complex

Presentation on the spying program PRISM and ECC's participation

NSA/CSS presentation on technical surveillance in Europe and Africa

Report on an unexploded ordnance alarm at the European Technical Center in the Mainz-Kastel neighborhood of Wiesbaden

Report on an NSA SIGDEV training course for allied countries

Report on the technical expansion of the European Technical Center in the Mainz-Kastel neighborhood of Wiesbaden

Report on the NSA-BND cooperation known as Joint SIGINT Activity (JSA)

Report on the surveillance of African countries by JSA

Restrictions on the technical surveillance performed by JSA

Report on data exchange between the NSA and BND within the JSA framework

Merkel in the database: Presentation from the Center for Content Extraction

Report on the NSA's access to TEMPORA

Report on the work of NSA/CSS Europe, including the capture or killing of 40 terror suspects

Guidelines for the classification of NSA SIGINT details (1945-1967)

Slide: Worldwide locations of the Cryptologic Services Groups

Slide: Worldwide locations of NSA/CSS satellite surveillance

US sites with NSA personnel in Germany

Logo of NSA-BND cooperation

Explanation of Nymrod, a system for searching for people and places in databases and documents

NSA presentation on the work of Nymrod

Report on an NSA visit to the BND site in Schöningen and on data transfer from the BND to the NSA

Presentation on the NSA/CIA unit Special Collection Service (SCS), active in US embassies around the world

Report on the one-year anniversary of the NSA liaison unit SUSLAG at the new site in the Mangfall Kaserne in Bad Aibling

Guidelines for the classification of SUSLAG details and the NSA-BND cooperation

GCHQ report on the technical abilities of the powerful spying program TEMPORA, which allows for a "full take"

Report on a WHARPDRIVE incident in an SSO presentation

Details on XKeyscore from an internal GCHQ website

Boundless Informant statistics on Great Britain

European Technical Center: Report on the experiences of one NSA

NSA/CSS Europe: Report on the experiences of one NSA worker

(U//FOUO) A Little Bad Aibling Nostalgia

FROM: Some BA Veterans
Unknown
Run Date: 06/04/2004

(U//FOUO) Once the closure of Bad Aibling Station (located in southern Bavaria in Germany) became official with DIRgram-312 announcing the cessation of mission, we thought it appropriate to give those lucky enough to have been stationed there a chance to reminisce!?!

(U) You know you are a BA veteran if...

...driving eight hours to buy pottery is a day well spent.
...you get excited to see a "new release" that has been out in the States for almost a year.

...dreaming of honey wagons is anything but sweet.
...mixing lemon-lime soda with beer doesn't always seem like a bad idea.
...you have seen 10,000 people do the Macarena in a tent.
...you know that UPPER Bavaria is SOUTH of LOWER Bavaria.
...you've seen Neuschwanstein or the Glockenspiel in Munich 53 times, and never because YOU wanted to go.
...you've been to "town hall" meetings at which a final decision to close the site was announced in three different years.
...you attended both the final closing and re-opening of the AFRC facilities at Chiemsee.
...Derek the car registration guy has called you "mate".
...you bought a sea-van's worth of Windex, "just because it was in stock today".
...you have spent $200 worth of time to get $40 worth of Italian gas coupons.
...while dining, you consistently chose beer as your beverage because it was half the price of Coke!
...you missed a day of mission work to verify the slot machine take at the club.
...you've concluded that, as a general rule in restaurants, German dogs behave better than some American patrons.
...your windshield still has an Austrian Autobahn Toll Vignette on it.
...driving on the Autobahn at 120 mph seems far safer than traveling the Washington Beltway.
...you know that leberkaese is made neither of liver, nor cheese.
...you welcomed biergarten season because a non-smoking restaurant was never an option.
...you swapped free biers for free pizza at the 4th of July fest.
...you understand why perfectly normal people bang tiny bottles of schnapps on a fest table before drinking them.
...you purchased window screens and Velcro tape in order to keep mosquitoes from invading your house.
...you had a map of every ESSO gas station in Germany and planned your trips accordingly.
...you understood why you needed to have someone guard your vehicle when you went pottery shopping in Poland.
...you packed out to return to the States, but bought more stuff and had to ship it home with a friend who was leaving after you.
...you sought out the person with the schedule for working the beer booth at the 4th of July fest.
...you were a recipient of a "free bier at the club" email.

exchange.

(TS//SI//NF) **Germany:** Provision of XKEYSCORE software to the BfV will expand their ability to support NSA as we jointly prosecute CT targets. Technical support for XKEYSCORE will be provided by the BND as it involves CES equities that a non-technical partner could inadvertently place at risk. Based on our CA relationship with the BND, they are well aware of, and able to, protect those equities.

(U) Topic

(S//REL TO USA, DEU) NSA's Counterterrorism (CT) Relationship with the German Federal Intelligence Service (BND) and the German Federal Office for the Protection of the Constitution (BfV)

(U) Potential Landmines

- (TS//SI//NF) The Germans may bring up the subject of SKYPE. NSA's response has been that it has had some success working SKYPE via tailored access at the end point by gaining access to one or more of the computers involved in the session. When Hr. Klaus-Fritsche (State Secretary, Germany Ministry of Interior) sought NSA's assistance with intercepting SKYPE transmissions during a 10 January 2012 meeting with DIRNSA, DIRNSA suggested the DNI Representative Berlin take the lead in arranging an exchange to include CIA, FBI and NSA. Should the partner raise this issue again, recommend that NSA once again redirects them to FBI and CIA.
- (S//NF) The Germans have previously approached NSA about using information derived from SIGINT in open court. CT is concerned that exposing SIGINT capabilities in German court threatens the ability to maintain the desired and planned for level of SIGINT cooperation.

(U) Talking Points

(U) Director's Talking Points

- (S//REL TO USA, DEU) Ensure that the Germans understand the importance that NSA places on its robust CT sharing relationship with the BND and the BfV, as well as NSA's desire to continue to move forward in the ongoing analytic and technical exchanges.
- (S//REL TO USA, DEU) Acknowledge that NSA/CT now has a formal relationship with the BfV (approved 20 March 2013). CT expects to receive value from a closer NSA/BND/BfV partnership because it will generate a greater synergy to more effectively counter terrorist threats. CT is pleased that BND is taking a leadership role in implementing technical solutions when partnering with the BfV, and we expect this to continue.

(U) SIGINT Director's Talking Points

- (S//SI//REL TO USA, DEU) Discuss and emphasize NSA's commitment to continuing and increasing the exchange on discovery methodologies. The topic

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

and importance of using behavior detection techniques to identify unknown extremists was discussed several times in 2012 with both BND and BfV and CT sees great value in working closely with both German partners on these analytic tradecraft methodologies. The next meeting to further discuss behavior detection is scheduled for 10-11 April in Bad Aibling with the BND and BfV. These sessions are specifically focused on understanding, creating, and implementing discovery capabilities through XKEYSCORE. Ultimately, CT's goal is to gain benefit by collaborating on German extremists targets once the BfV has, and is optimally using, XKEYSCORE.

- [redacted]

(U) Background

(TS//REL TO USA, FVEY) NSA's CT collaborates with the BND (bilaterally and multilaterally) and with the BfV (bilaterally) on a variety of CT issues and targets. Engagement in the multilateral realm is via the SIGINT Seniors Europe (SSEUR) CT coalition (SISECT). NSA CT exchanges information with the BND and the BfV on the following topics:

- [redacted]

(TS//REL TO USA, FVEY) CT also provides information to the BND on the following topics:

- [redacted]

(TS//REL TO USA, FVEY) The primary stakeholders for CT exchanges with the Germans are the European Cryptologic Center (ECC) and the S2I Deployed Analyst (DA) in Berlin. NSA's CT meets with the BND and BfV quarterly and with the BND every six months at SISECT. The latest analytic exchange was on 4-5 December 2012 in Berlin. Although previous discussions focused on extremists traveling to Germany and Central Asia, this latest exchange focused heavily on North African CT topics, including key presentations from both sides on [redacted] CT European targets remain the focus of the relationship with BfV; however, it is likely that CT North African targets will have an expanded focus with BND and BfV as North Africa continues to serve as a magnet for aspiring jihadists from Europe. In addition, future discussions will likely expand to Europeans traveling to [redacted] to fight in the ongoing [redacted] and the threat they may pose upon return to Europe.

[redacted]

(TS//SI//NF) In addition, SSG has been working with the BND and BfV on collection as well as target discovery and development tradecraft. In October 2011, SSG partnered with SUSLAG and BND to conduct a demonstration of XKEYSCORE to the BfV using BfV domestic warranted collection. The BND XKEYSCORE system successfully processed DSL wiretap collection belonging to a German domestic CT target. As a result of this demonstration, the BfV Vice President formally requested the XKEYSCORE software from DIRNSA to further enable the BfV to achieve its mission goal of countering terrorist activities in Germany. By enhancing BfV's Internet analytic capabilities through the provision of XKEYSCORE, NSA will enable Germany to provide unique contributions in the form of collection, data summaries, and/or finished intelligence to the high-priority NSA CT mission. The SPF approving the provision of XKEYSCORE to the BfV was approved on 25 March 2013. The Terms of Reference related to this effort is currently with the Germans for signature, which is expected in mid-April.

(U) Date of Material

(U) 8 April 2013

(U) POCs

(U) Originator

(U//FOUO) [redacted] Foreign Partner Strategist, S2I, [redacted]

(U) Alternate POC

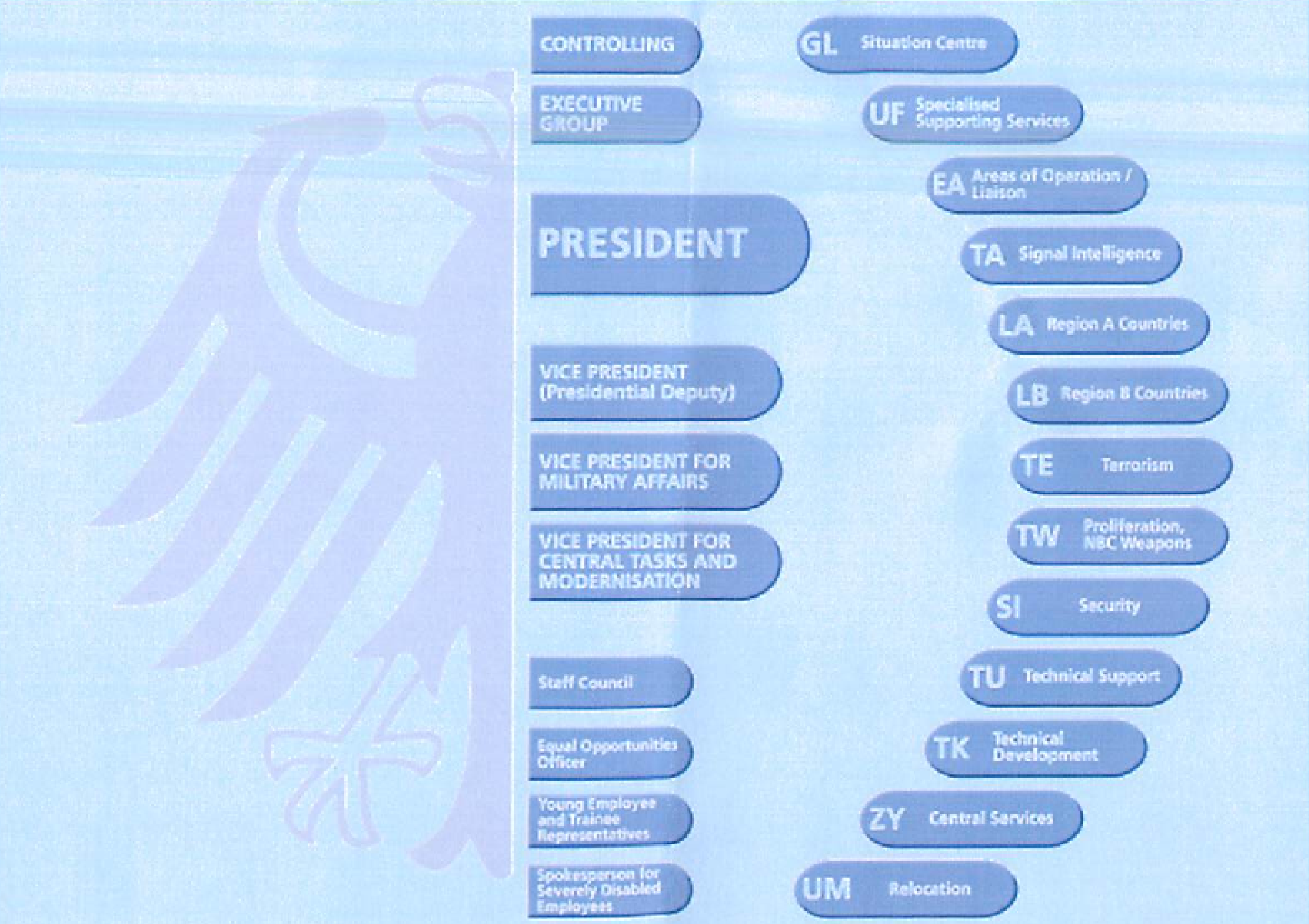
(U//FOUO)[redacted] Foreign Partner Strategist, ST, [redacted]

(U) Classification Review by

(U//FOUO)[redacted] Foreign Partner Strategist, ST, [redacted]

Bundesnachrichtendienst

Structure of the BND



CONTROLLING

EXECUTIVE GROUP

PRESIDENT

VICE PRESIDENT (Presidential Deputy)

VICE PRESIDENT FOR MILITARY AFFAIRS

VICE PRESIDENT FOR CENTRAL TASKS AND MODERNISATION

Staff Council

Equal Opportunities Officer

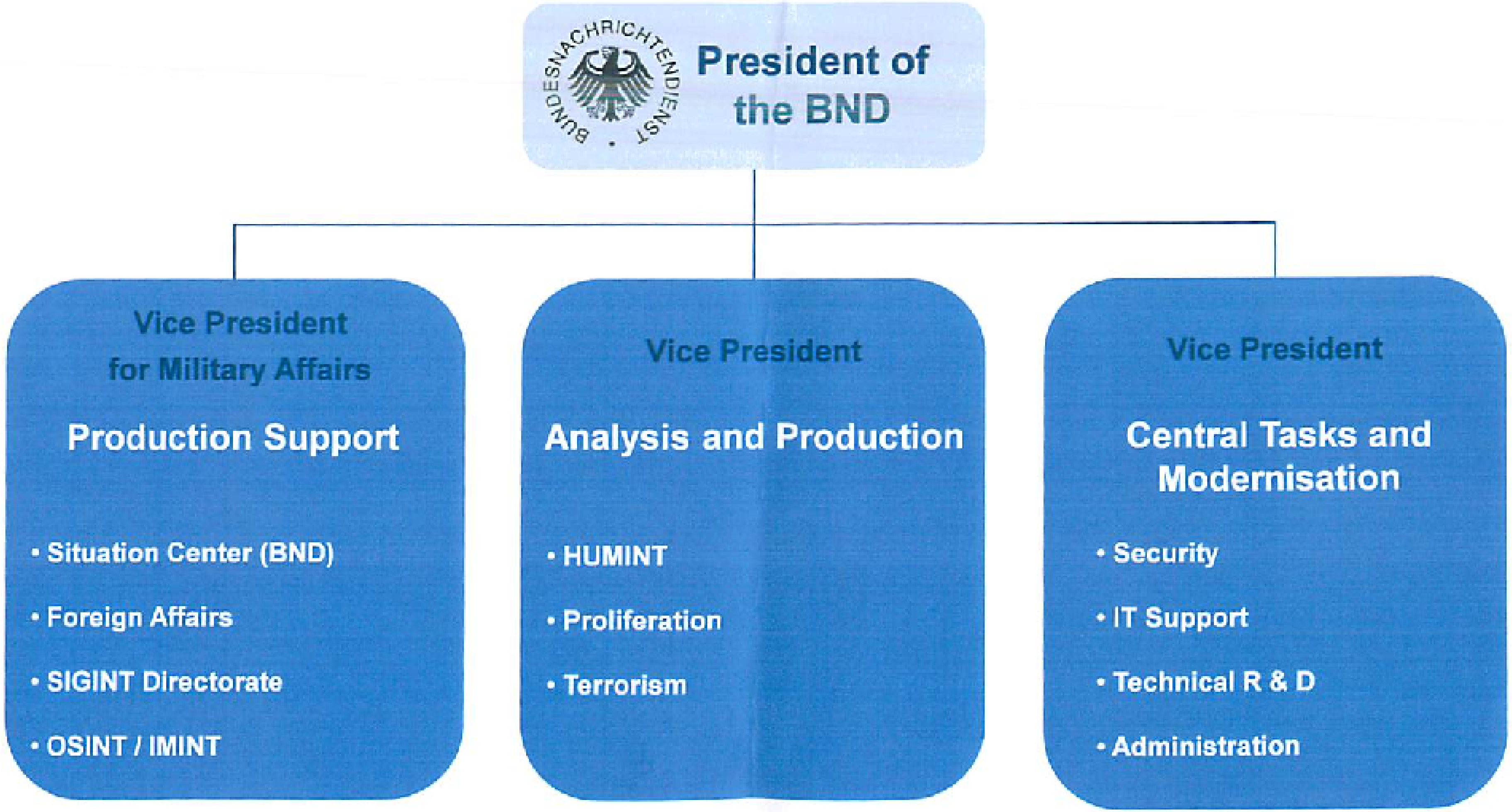
Young Employee and Trainee Representatives

Spokesperson for Severely Disabled Employees

GL	Situation Centre
UF	Specialised Supporting Services
EA	Areas of Operation / Liaison
TA	Signal Intelligence
LA	Region A Countries
LB	Region B Countries
TE	Terrorism
TW	Proliferation, NBC Weapons
SI	Security
TU	Technical Support
TK	Technical Development
ZY	Central Services
UM	Relocation

Abteilung Technische Aufklärung

Bundesnachrichtendienst



President of the BND

Vice President for Military Affairs

Production Support

- Situation Center (BND)
- Foreign Affairs
- SIGINT Directorate
- OSINT / IMINT

Vice President

Analysis and Production

- HUMINT
- Proliferation
- Terrorism

Vice President

Central Tasks and Modernisation

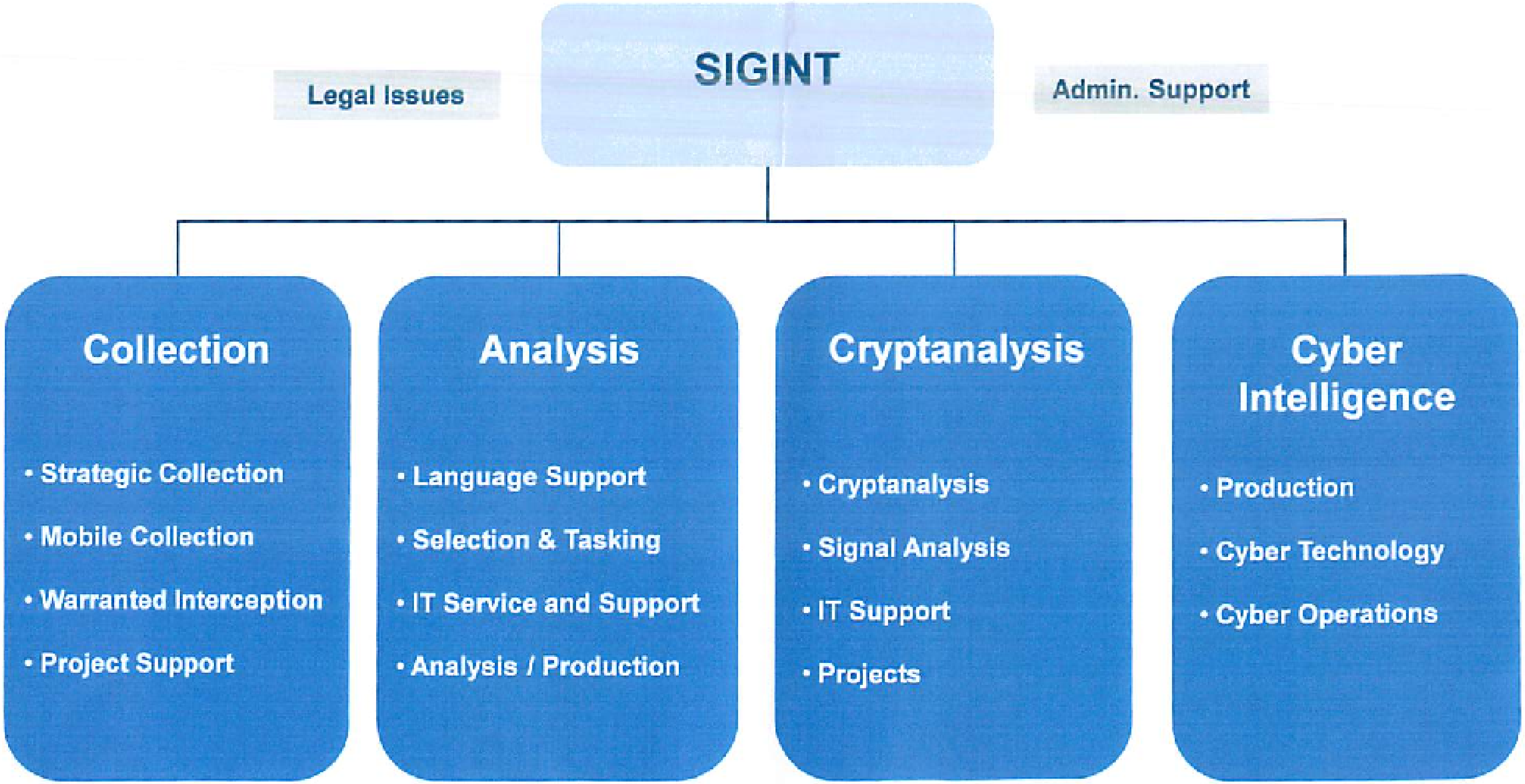
- Security
- IT Support
- Technical R & D
- Administration

Confidential

Bundesnachrichtendienst

Abteilung Technische Aufklärung

SIGINT Directorate



Legal Issues

SIGINT

Admin. Support

Collection

- Strategic Collection
- Mobile Collection
- Warranted Interception
- Project Support

Analysis

- Language Support
- Selection & Tasking
- IT Service and Support
- Analysis / Production

Cryptanalysis

- Cryptanalysis
- Signal Analysis
- IT Support
- Projects

Cyber Intelligence

- Production
- Cyber Technology
- Cyber Operations

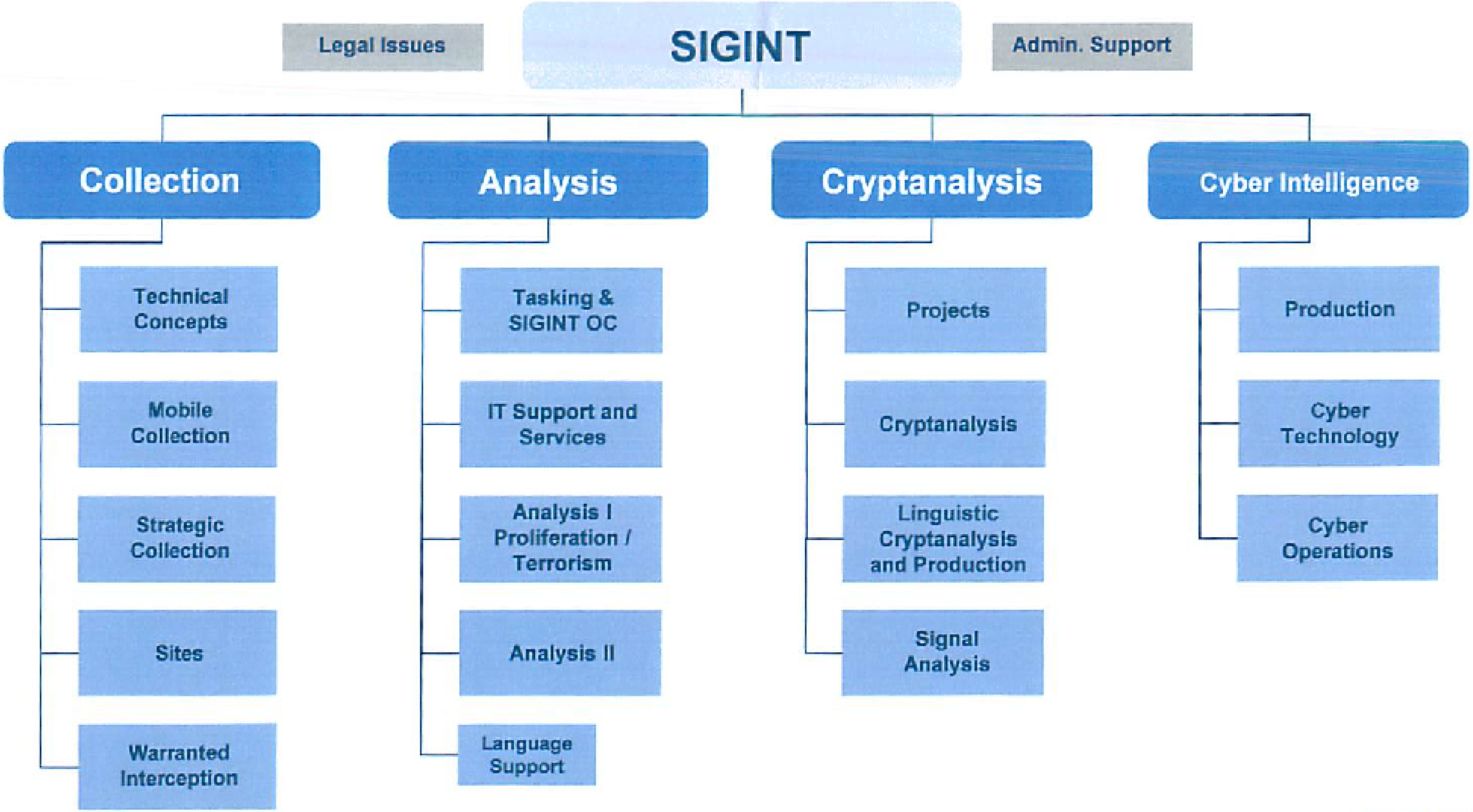
Stand Feb. 2013

Confidential

Bundesnachrichtendienst

Abteilung Technische Aufklärung

SIGINT Directorate / Branches



Legal Issues

SIGINT

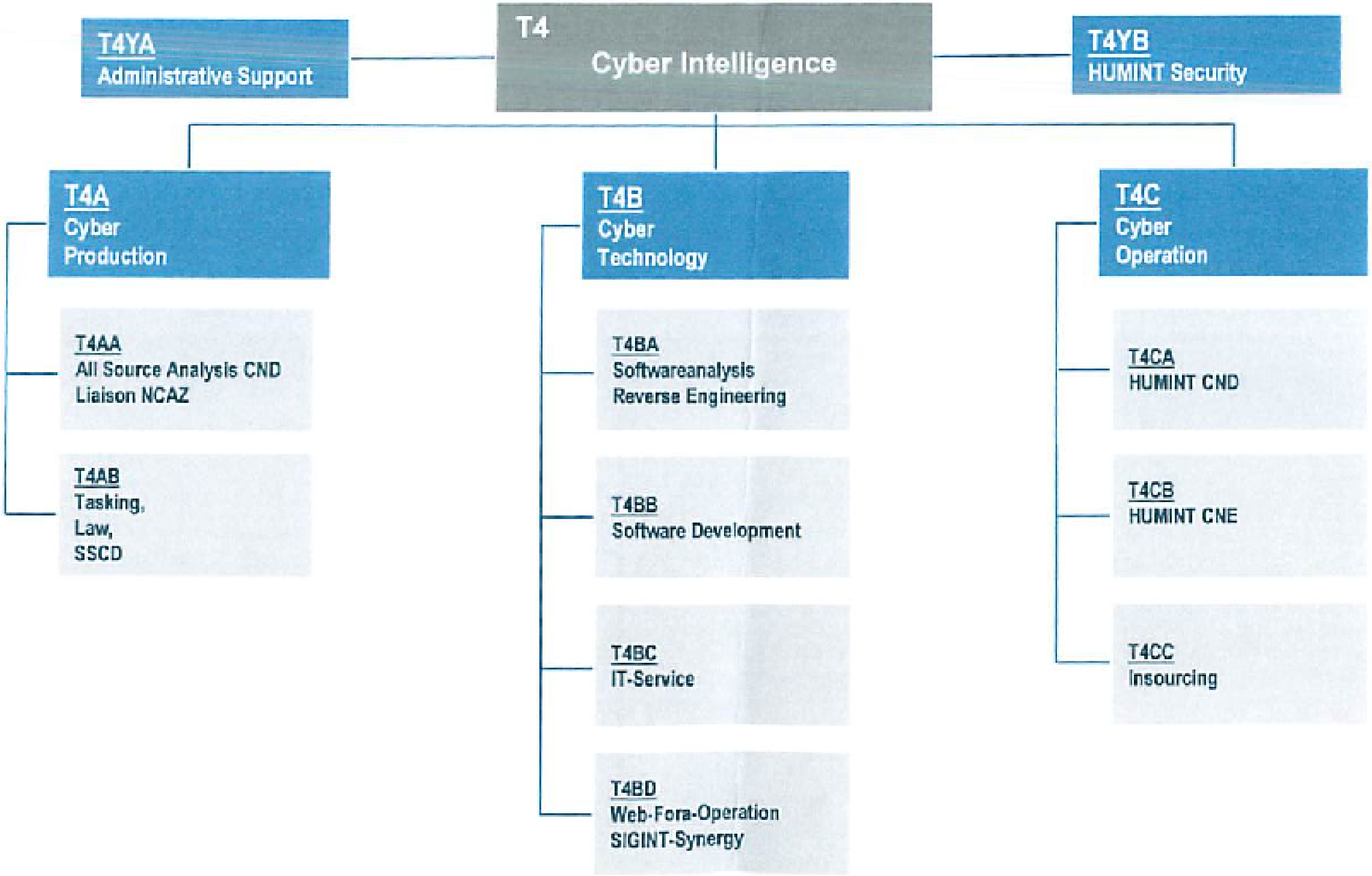
Admin. Support

- Collection
  - Technical Concepts
  - Mobile Collection
  - Strategic Collection
  - Sites
  - Warranted Interception
- Analysis
  - Tasking & SIGINT OC
  - IT Support and Services
  - Analysis I Proliferation / Terrorism
  - Analysis II
  - Language Support
- Cryptanalysis
  - Projects
  - Cryptanalysis
  - Linguistic Cryptanalysis and Production
  - Signal Analysis
- Cyber Intelligence
  - Production
  - Cyber Technology
  - Cyber Operations

Stand Feb. 2013

Confidential

T4 – Cyber Intelligence



T4
Cyber Intelligence

T4YA
Administrative Support

T4YB
HUMINT Security

T4A
Cyber
Production

T4AA
All Source Analysis CND
Liaison NCAZ

T4AB
Tasking,
Law,
SSCD

T4B
Cyber
Technology

T4BA
Softwareanalysis
Reverse Engineering

T4BB
Software Development

T4BC
IT-Service

T4BD
Web-Fora-Operation
SIGINT-Synergy

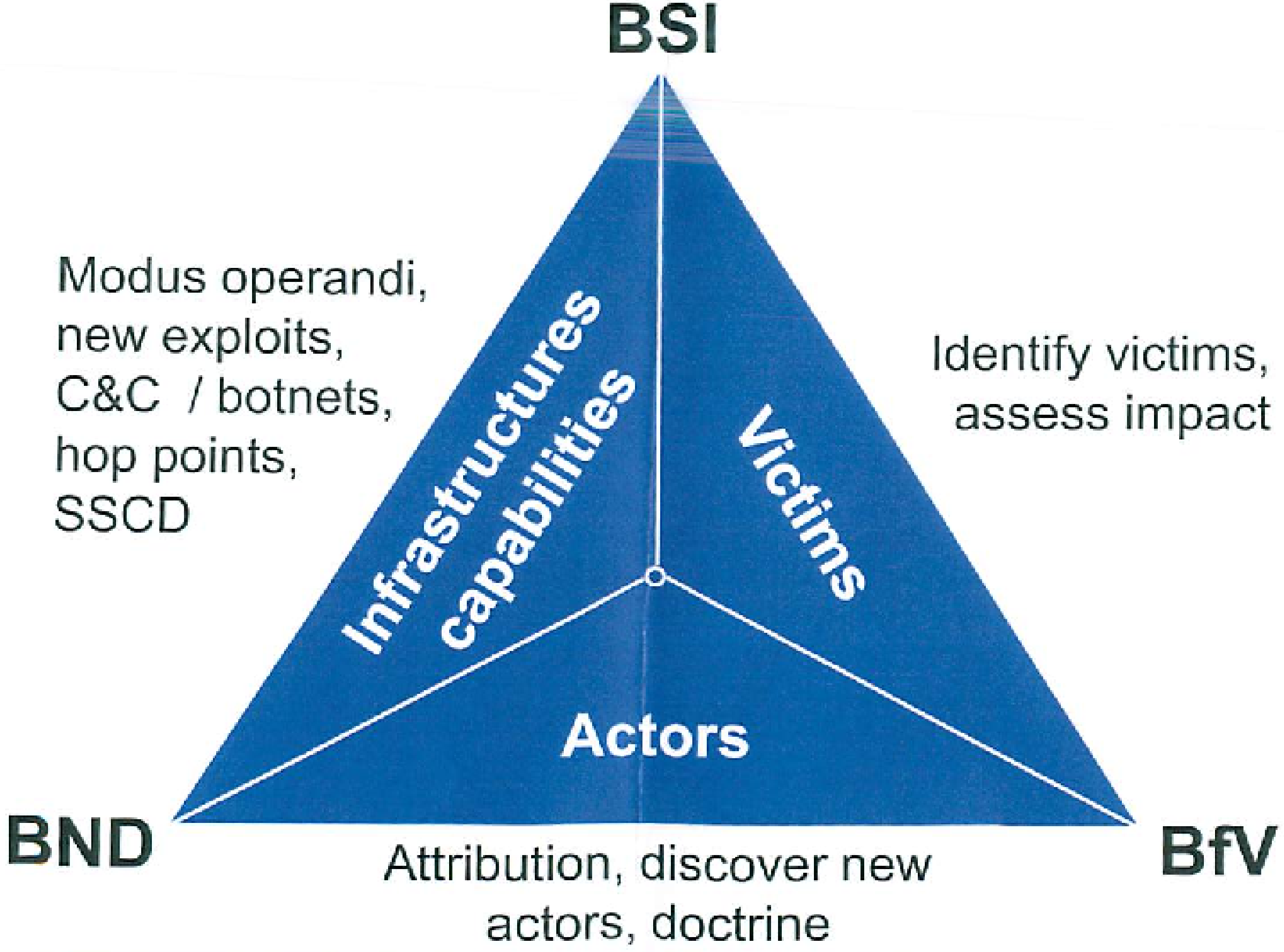
T4C
Cyber
Operation

T4CA
HUMINT CND

T4CB
HUMINT CNE

T4CC
Insourcing

Co-operation Model for Germany



BSI

Modus operandi,
new exploits,
C&C / botnets,
hop points,
SSCD

Infrastructures capabilities

Victims

Identify victims,
assess impact

Actors

BND

BfV

Attribution, discover new
actors, doctrine

(U) Topic

(S//REL TO USA, DEU) NSA's Counterterrorism (CT) Relationship with the German Federal Intelligence Service (BND) and the German Federal Office for the Protection of the Constitution (BfV)

(U) Potential Landmines

- (TS//SI//NF) The Germans may bring up the subject of SKYPE. NSA's response has been that it has had some success working SKYPE via tailored access at the end point by gaining access to one or more of the computers involved in the session. When Hr. Klaus-Fritsche (State Secretary, Germany Ministry of Interior) sought NSA's assistance with intercepting SKYPE transmissions during a 10 January 2012 meeting with DIRNSA, DIRNSA suggested the DNI Representative Berlin take the lead in arranging an exchange to include CIA, FBI and NSA. Should the partner raise this issue again, recommend that NSA once again redirects them to FBI and CIA.
- (S//NF) The Germans have previously approached NSA about using information derived from SIGINT in open court. CT is concerned that exposing SIGINT capabilities in German court threatens the ability to maintain the desired and planned for level of SIGINT cooperation.

(U) Talking Points

(U) Director's Talking Points

- (S//REL TO USA, DEU) Ensure that the Germans understand the importance that NSA places on its robust CT sharing relationship with the BND and the BfV, as well as NSA's desire to continue to move forward in the ongoing analytic and technical exchanges.
- (S//REL TO USA, DEU) Acknowledge that NSA/CT now has a formal relationship with the BfV (approved 20 March 2013). CT expects to receive value from a closer NSA/BND/BfV partnership because it will generate a greater synergy to more effectively counter terrorist threats. CT is pleased that BND is taking a leadership role in implementing technical solutions when partnering with the BfV, and we expect this to continue.

(U) SIGINT Director's Talking Points

- (S//SI//REL TO USA, DEU) Discuss and emphasize NSA's commitment to continuing and increasing the exchange on discovery methodologies. The topic

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

and importance of using behavior detection techniques to identify unknown extremists was discussed several times in 2012 with both BND and BfV and CT sees great value in working closely with both German partners on these analytic tradecraft methodologies. The next meeting to further discuss behavior detection is scheduled for 10-11 April in Bad Aibling with the BND and BfV. These sessions are specifically focused on understanding, creating, and implementing discovery capabilities through XKEYSCORE. Ultimately, CT's goal is to gain benefit by collaborating on German extremists targets once the BfV has, and is optimally using, XKEYSCORE.

- [redacted]

(U) Background

(TS//REL TO USA, FVEY) NSA's CT collaborates with the BND (bilaterally and multilaterally) and with the BfV (bilaterally) on a variety of CT issues and targets. Engagement in the multilateral realm is via the SIGINT Seniors Europe (SSEUR) CT coalition (SISECT). NSA CT exchanges information with the BND and the BfV on the following topics:

- [redacted]

(TS//REL TO USA, FVEY) CT also provides information to the BND on the following topics:

- [redacted]

(TS//REL TO USA, FVEY) The primary stakeholders for CT exchanges with the Germans are the European Cryptologic Center (ECC) and the S2I Deployed Analyst (DA) in Berlin. NSA's CT meets with the BND and BfV quarterly and with the BND every six months at SISECT. The latest analytic exchange was on 4-5 December 2012 in Berlin. Although previous discussions focused on [redacted] traveling to Germany and Central Asia, this latest exchange focused heavily on North African CT topics, including key presentations from both sides on [redacted]. CT European targets remain the focus of the relationship with BfV; however, it is likely that CT North African targets will have an expanded focus with BND and BfV as North Africa continues to serve as a magnet for [redacted] from Europe. In addition, future discussions will likely expand to Europeans traveling to [redacted] and the threat they may pose upon return to Europe.

[redacted]

(TS//SI//NF) In addition, SSG has been working with the BND and BfV on collection as well as target discovery and development tradecraft. In October 2011, SSG partnered with SUSLAG and BND to conduct a demonstration of XKEYSCORE to the BfV using BfV domestic warranted collection. The BND XKEYSCORE system successfully processed DSL wiretap collection belonging to a German domestic CT target. As a result of this demonstration, the BfV Vice President formally requested the XKEYSCORE software from DIRNSA to further enable the BfV to achieve its mission goal of countering terrorist activities in Germany. By enhancing BfV's Internet analytic capabilities through the provision of XKEYSCORE, NSA will enable Germany to provide unique contributions in the form of collection, data summaries, and/or finished intelligence to the high-priority NSA CT mission. The SPF approving the provision of XKEYSCORE to the BfV was approved on 25 March 2013. The Terms of Reference related to this effort is currently with the Germans for signature, which is expected in mid-April.

(U) Date of Material

(U) 8 April 2013

(U) POCs

(U) Originator

(U//FOUO) [redacted] Foreign Partner Strategist, S2[redacted]

(U) Alternate POC

(U//FOUO) [redacted] Foreign Partner Strategist, ST, [redacted]

(U) Classification Review by

(U//FOUO) [redacted] Foreign Partner Strategist, ST, [redacted]

National Security Agency/Central Security Service 17 January 2013

Information Paper

Subject: (S//REL TO USA, FVEY) NSA Intelligence Relationship with Germany – Bundesnachrichtendienst (BND)

(S//SI//REL TO USA, FVEY) **Introduction**: NSA established a relationship with its SIGINT counterpart in Germany, the BND-TA, in 1962, which includes extensive analytical, operational, and technical exchanges. In the past year, Germany displayed both eagerness and self-sufficiency in transforming its SIGINT activities and assumed greater risk in support of U.S. intelligence needs and efforts to improve information sharing within the German government, with coalition partners, and NSA. The BND supports NSA's emerging counterterrorism (CT) intelligence relationship with the German domestic services, taking steps to strengthen its SIGINT Development (SIGDEV) capabilities to perform a key technical advisory and support role within Germany. Both partners have agreed to maintain an intelligence focus on CT, transnational organized crime, [redacted], counternarcotics (CN), Special Interest Alien Smuggling (SIA), and U.S. and coalition support to Afghanistan (the Afghanistan SIGINT Coalition (AFSC)). In 2012, NSA welcomed BND President Schindler's eagerness to strengthen and expand bilateral cooperation and is exploring new analytic topics of mutual interest including Africa, [redacted] and counterproliferation (CP)-related activities. In U.S.-German cyber activity, NSA continues to encourage BND participation in foundational cyber defense discussions to demonstrate its potential to provide a technical platform.

(S//NF) Information Assurance and Computer Network Defense Relationship with Germany.

(S//NF) The Information Assurance Directorate (IAD) has a long-standing relationship with the Bundesamt für Sicherheit in der Informationstechnik (BSI) – the Federal Office of Information Security. After the German Government announced their Cybersecurity Strategy and identified BSI as the lead Agency for cyber defense, BSI expressed great interest in expanding the information assurance (IA) partnership to include computer network defense (CND) collaboration on cyber threats. Key Partners within the German Government along with BSI, are Bundesamt für Verfassungsschutz (BfV), Federal Office for Protection of the Constitution and BND. While BfV and BND have not been traditional IA partners, the expansion to include CND will open additional opportunities to develop relationships with the German agencies responsible for analysis and SIGINT. IAD and the NSA/CSS Threat Operations Center (NTOC) may be able to leverage the formal partnership the NSA Signals Intelligence Directorate (SID) is pursuing with BfV and its already strong relationship with BND (which is providing SIGINT Support to CND for

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360301

Germany's cyber defense efforts.) A draft IA and CND Memorandum of Understanding (MOU) for CND collaboration is in the coordination process at NSA, BSI and BND will both be signatories.

1. **(U) Key Issues**:

- Issue #1: (S//SI//NF) The BND has been working to influence the German Government to relax interpretation of the privacy laws over the long term to provide greater opportunity for intelligence sharing. In the near term, NSA decided to right-size its presence at the Joint SIGINT Activity (JSA) in Bad Aibling, Germany based on current mission needs and fiscal realities. In May 2012 NSA turned over full responsibility of the FORNSAT collection mission to the BND, allowing NSA's representational team to cultivate new cooperative opportunities with Germany.

- Issue #2: (S//SI//REL TO USA, FVEY) Chief, Special U.S. Liaison Activity Germany (SUSLAG), continues to work with DNI Representative Berlin on new CT initiatives between NSA and the BfV and with other German domestic agencies as appropriate. NSA has developed a significant level of trust and intelligence sharing with the BfV since the 2007 arrests of the Islamic Jihad Union members in Germany which resulted in regular U.S.-German analytic exchanges and closer cooperation in tracking both German and non-German extremist targets. NSA also has held several multilateral technical meetings with BND/BfV/NSA/CIA to introduce SIGDEV methodology and tradecraft to improve the BfV's ability to exploit, filter, and process domestic data accesses and potentially develop larger collection access points that could benefit both Germany and the U.S. The BND supports NSA's emerging CT intelligence relationship with the BfV, taking steps to strengthen its SIGDEV capabilities to perform a key technical advisory and support role within Germany. To facilitate cooperation, an NSA CT analyst, stationed in Berlin, occupies office space in BfV headquarters one day per week to nurture the relationship and facilitate U.S. requirements. Likewise, the Germans developed a communications link improving the connectivity between NSA and BfV/BND, as well as the timeliness of the intelligence exchange.

- Issue #3: (S//NF) NSA IAD, SID and NTOC are interested in leveraging Germany's accesses and capabilities to discover threats and vulnerabilities which provide timely warnings of attacks against U.S. Government and critical infrastructure networks. In December 2012, representatives from NTOC and FAD met with BSI and BND in Germany for bilateral CND discussions. As a result of the engagement, an analytical exchange was held in January 2013.

(U) Discussion:

- (S//NF) NSA's in-country representative is the Chief, SUSLAG, located on Mangfall Kaserne in Bad Aibling, Germany. SUSLAG has 18 personnel, consisting of 12 NSA civilians and six contractors. NSA has plans to reduce the SUSLAG workforce to approximately six personnel in FY 2013.

- (S//SI//REL TO USA, FVEY) What we provide to the partner: NSA has provided a significant amount of hardware and software at BND expense, as well as associated analytic expertise to help the BND independently maintain its FORNSAT capability. NSA also exchanges intelligence reporting on both military and non-military targets.

- (TS//SI//NF) What the partner provides to us: NSA is provided access to FORNSAT communications supporting CN, CT, [redacted] and Weapons of Mass Destruction (WMD) missions and is an important source of information on drug trafficking and force protection in Afghanistan. The BND provides Igbo language support by translating NSA collection of a high-value, time-sensitive [redacted] target. NSA is seeking the proper approvals to accept BND language support in [redacted] In addition to the day-to-day collection, the Germans have offered NSA unique accesses in high interest target areas.

(U) Success stories:

- (S//REL TO USA, FVEY) Germany has become an active participant in the AFSC, working closely with other member countries and embracing the new AFSC Division of Effort, under which each member country is responsible for covering a specific area of interest to the AFSC and then sharing reporting and metadata on that area with the other AFSC members. AFSC member countries include: the U.S, UK, Canada, Australia, New Zealand, Belgium, Denmark, France, Germany, Italy, Norway, the Netherlands, Spain and Sweden.

- (TS//SI//REL TO USA, FVEY) Having modernized its communications infrastructure in support of its unique FORNSAT GSM access in [redacted] the BND became the third largest contributor to the Real Time-Regional Gateway (RT-RG) analysis and processing tool.

- (S//REL TO USA, FVEY) The German government modified its interpretation of the G-10 Privacy Law, protecting the communications of German citizens, to afford the BND more flexibility in sharing protected information with foreign partners.

- (S//SI//RELTO USA, FVEY) The BND has provided unique sustained collection of targets such as [redacted] Ministry of Foreign Affairs (MFA), [redacted] MFA, [redacted] Global System for Mobile Communications (GSM), [redacted] GSM, and [redacted] Voice over Internet Protocol (VoIP).

- (TS//SI//NF) Problems/Challenges with the partner: Since 2008 NSA has started to foster other areas of cooperation with the BND to satisfy U.S. intelligence requirements at an appropriate level of investment. The BND's inability to successfully address German privacy law (G-10) issues has limited some operations, but NSA welcomed German willingness to take risks and to pursue new opportunities for cooperation with the U.S, particularly in the CT realm. NSA is open to holding a dialogue on topics to address mutual intelligence gaps, including [redacted] and CP-related activities.

(S//REL TO USA, FVEY) Prepared by: [redacted] Country Desk Officer (CDO)

Germany, DP11
[redacted] IA CDO, DP21

BOUNDLESSINFORMANT – Frequently Asked Questions___________ __09-06-2012_

(U/FOUO) Questions

1) What is ***BOUNDLESSINFORMANT***? What is its purpose?
2) Who are the intended users of the tool?
3) What are the different views?
4) Where do you get your data?
5) Do you have all the data? What data is missing?
6) Why are you showing metadata record counts versus content?
7) Do you distinguish between sustained collect and survey collect?
8) What is the technical architecture for the tool?
9) What are some upcoming features/enhancements?
10) How are new features or views requested and prioritized?
11) Why are record counts different from other tools like ASDF and What's On Cover?
12) Why is the tool NOFORN? Is there a releasable version?
13) How do you compile your record counts for each country?

Note: This document is a work-in-progress and will be updated frequently as additional questions and guidance are provided.

1) (U) What is *BOUNDLESSINFORMANT*? What is its purpose?

(U//FOUO) BOUNDLESSINFORMANT is a GAO prototype tool for a self-documenting SIGINT system. The purpose of the tool is to fundamentally shift the manner in which GAO describes its collection posture. ***BOUNDLESSINFORMANT*** provides the ability to dynamically describe GAO's collection capabilities (through metadata record counts) with no human intervention and graphically display the information in a map view, bar chart, or simple table. Prior to ***BOUNDLESSINFORMANT***, the method for understanding the collection capabilities of GAO's assets involved ad hoc surveying of repositories, sites, developers, and/or programs and offices. By extracting information from every DNI and DNR metadata record, the tool is able to create a near real-time snapshot of GAO's collection capability at any given moment. The tool allows users to select a country on a map and view the metadata volume and select details about the collection against that country. The tool also allows users to view high level metrics by organization and then drill down to a more actionable level - down to the program and cover term.

Sample Use Cases

- (U//FOUO) How many records are collected for an organizational unit (e.g. FORNSAT)?
- (U//FOUO) How many records (and what type) are collected against a particular country?
- (U//FOUO) Are there any visible trends for the collection?
- (U//FOUO) What assets collect against a specific country? What type of collection?
- (U//FOUO) What is the field of view for a specific site? What countriees does it collect against? What type of collection?

2) (U) Who are the intended users of the tool?

(U//FOUO) Mission and collection managers seeking to understand output characteristics of a site based on what is being ingested into downstream repositories.

(U//FOUO) Strategic Managers seeking to understand top level metrics at the organization/office level or seeking to answer data calls on NSA collection capability.

(U//FOUO) Analysts looking for additional sites to task for coverage of a particular technology within a specific country.

3) What are the different views?

(U//FOUO) Map View – The Map View is designed to allow users to view overall DNI, DNR, or aggregated collection posture of the agency or a site. Clicking on a country will show the collection posture (record counts, type of collection, and contributing SIGADs or sites) against that particular country in addition to providing a graphical display of record count trends. In order to bin the records into a country, a normalized phone number (DNR) or an administrative region atom (DNI) must be populated within the record. Clicking on a site (within the Site Specific view) will show the viewshed for that site – what countries the site collects against.

(U//FOUO) Org View – The Organization View is designed to allow users to view the metadata record counts by organizational structure (i.e. GAO – SSO – RAM-A – SPINNERET) all the way down to the cover term. Since it's not necessary to have a normalized number or administrative region populated, the numbers in the Org View will be higher than the numbers in the Map View.

(U//FOUO) Similarity View – The Similarity View is currently a placeholder view for an upcoming feature that will graphically display sites that are similar in nature. This can be used to identify areas for a de-duplication effort or to inform analysts of additional SIGADs to task for queries (similar to Amazon's "if you like this item, you'll also like these" feature).

4) (U) Where do you get your data?

(U//FOUO) BOUNDLESSINFORMANT extracts metadata records from GM-PLACE post-FALLOUT (DNI ingest processor) and post-TUSKATTIRE (DNR ingest processor). The records are enriched with organization information (e.g. SSO, FORNSAT) and cover term. Every valid DNI and DNR metadata record is aggregated to provide a count at the appropriate level. See the different views question above for additional information.

5) (U) Do you have all the data? What data is missing?

(U//FOUO) The tool resides on GM-PLACE which is only accredited up to TS//SI//NOFORN. Therefore, the tool does not contain ECI or FISA data.

(U//FOUO) The Map View only shows counts for records with a valid normalized number (DNR) or administrative region atom (DNI).

(U//FOUO) Only metadata records that are sent back to NSA-W through FASCIA or FALLOUT are counted. Therefore, programs with a distributed data distribution system (e.g. MUSCULAR and Terrestrial RF) are not currently counted.

(U//FOUO) Only SIGINT records are currently counted. There are no ELINT or other "INT" records included.

6) (U) Why are you showing metadata record counts versus content?

(U//FOUO)

7) (U) Do you distinguish between sustained collect and survey collect?

(U//FOUO) The tool currently makes no distinction between sustained collect and survey collect. This feature is on the roadmap.

8) What is the technical architecture for the tool?

- Click [redacted] for a graphical view of the tool's architecture
- (U//FOUO) DNI metadata (ASDF), DNR metadata (FASCIA) delivered to Hadoop Distributed File System (HDFS) on GM-PLACE
- (U//FOUO) Use Java MapReduce job to transform/filter and enrich FASCIA/ASDF data with business logic to assign organization rules to data
- (U//FOUO) Bulk import of DNI/DNR data (serialized Google Protobuf objects) into Cloudbase (enabled by custom aggregators)
- (U//FOUO) Use Java web app (hosted via Tomcat) on MachineShop (formerly TurkeyTower) to query Cloudbase
- (U//FOUO) GUI triggers queries to CloudBase – GXT (ExtGWT)

9) What are some upcoming features/enhancements?

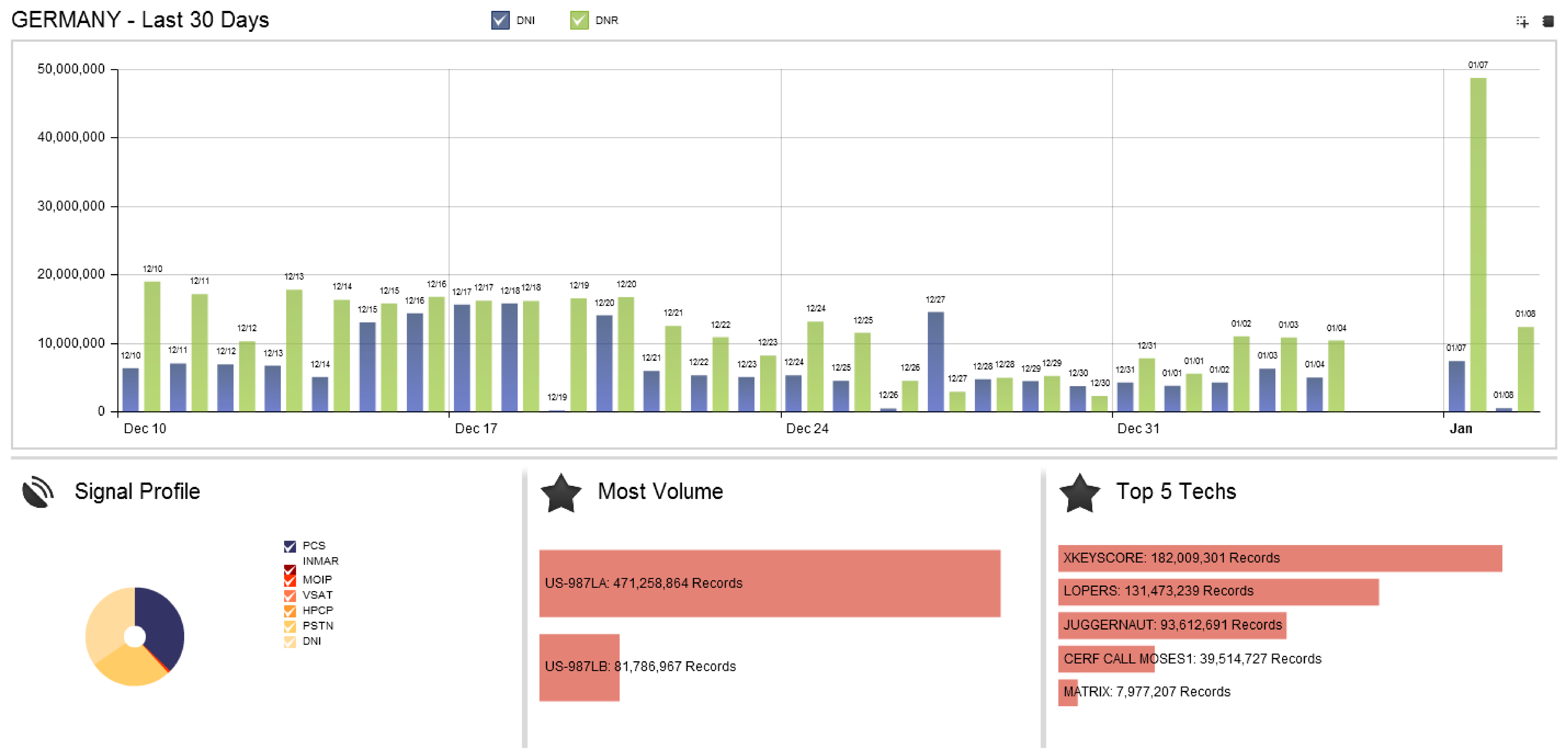
- (U//FOUO) Add technology type (e.g. JUGGERNAUT, LOPER) to provide additional granularity in the numbers
- (U//FOUO) Add additional details to the Differential view
- (U//FOUO) Refine the Site Specific view
- (U//FOUO) Include CASN information
- (U//FOUO) Add ability to export data behind any view (pddg,sigad,sysid,casn,tech,count)
- (U//FOUO) Add in selected (vs. unselected) data indicators
- (U//FOUO) Include filter for sustained versus survey collection

10) How are new features or views requested and prioritized?

(U//FOUO) The team uses [redacted] to accept user requests for additional functionality or enhancements. Users are also allowed to vote on which functionality or enhancements are most important to them (as well as add comments). The ***BOUNDLESSINFORMANT*** team will periodically review all requests and triage according to level of effort (Easy, Medium, Hard) and mission impact (High, Medium, Low). The team will review the queue with the project champion and government steering committee to be added onto the ***BOUNDLESSINFORMANT*** roadmap.

11) Why are record counts different from other tools like ASDF and What's On Cover?

(U//FOUO) There are a number of reasons why record counts may vary. The purpose of the tool is to provide



GERMANY - Last 30 Days

Signal Profile

Most Volume

US-987LA: 471,258,864 Records

US-987LB: 81,786,967 Records

Top 5 Techs

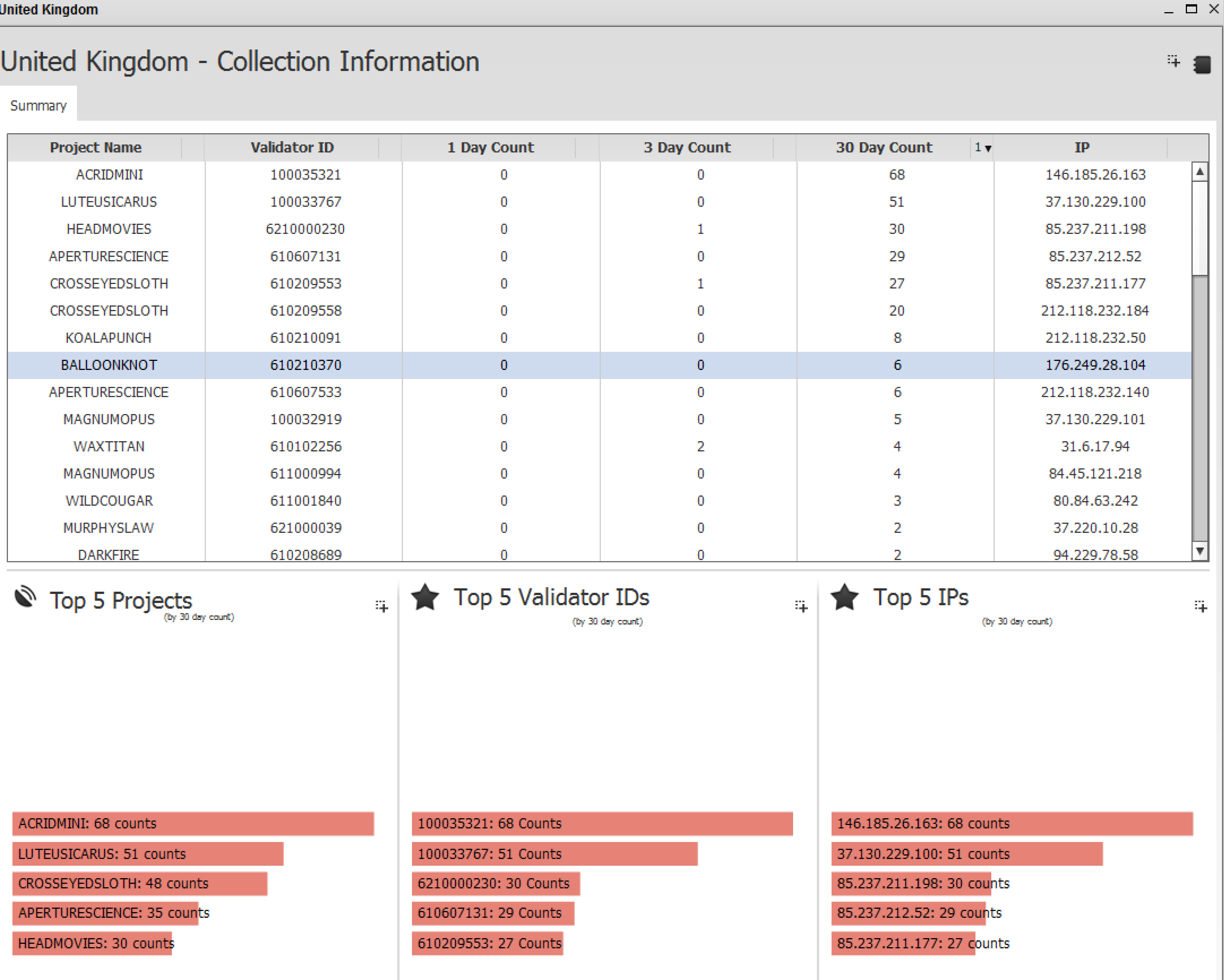
XKEYSCORE: 182,009,301 Records

LOPERS: 131,473,239 Records

JUGGERNAUT: 93,612,691 Records

CERF CALL MOSES1: 39,514,727 Records

MATRIX: 7,977,207 Records



United Kingdom

United Kingdom - Collection Information

Summary

Project Name	Validator ID	1 Day Count	3 Day Count	30 Day Count 1▼	IP
ACRIDMINI	100035321	0	0	68	146.185.26.163
LUTEUSICARUS	100033767	0	0	51	37.130.229.100
HEADMOVIES	6210000230	0	1	30	85.237.211.198
APERTURESCIENCE	610607131	0	0	29	85.237.212.52
CROSSEYEDSLOTH	610209553	0	1	27	85.237.211.177
CROSSEYEDSLOTH	610209558	0	0	20	212.118.232.184
KOALAPUNCH	610210091	0	0	8	212.118.232.50
BALLOONKNOT	610210370	0	0	6	176.249.28.104
APERTURESCIENCE	610607533	0	0	6	212.118.232.140
MAGNUMOPUS	100032919	0	0	5	37.130.229.101
WAXTITAN	610102256	0	2	4	31.6.17.94
MAGNUMOPUS	611000994	0	0	4	84.45.121.218
WILDCOUGAR	611001840	0	0	3	80.84.63.242
MURPHYSLAW	621000039	0	0	2	37.220.10.28
DARKFIRE	610208689	0	0	2	94.229.78.58

Top 5 Projects

(by 30 day count)

ACRIDMINI: 68 counts
LUTEUSICARUS: 51 counts
CROSSEYEDSLOTH: 48 counts
APERTURESCIENCE: 35 counts
HEADMOVIES: 30 counts

Top 5 Validator IDs

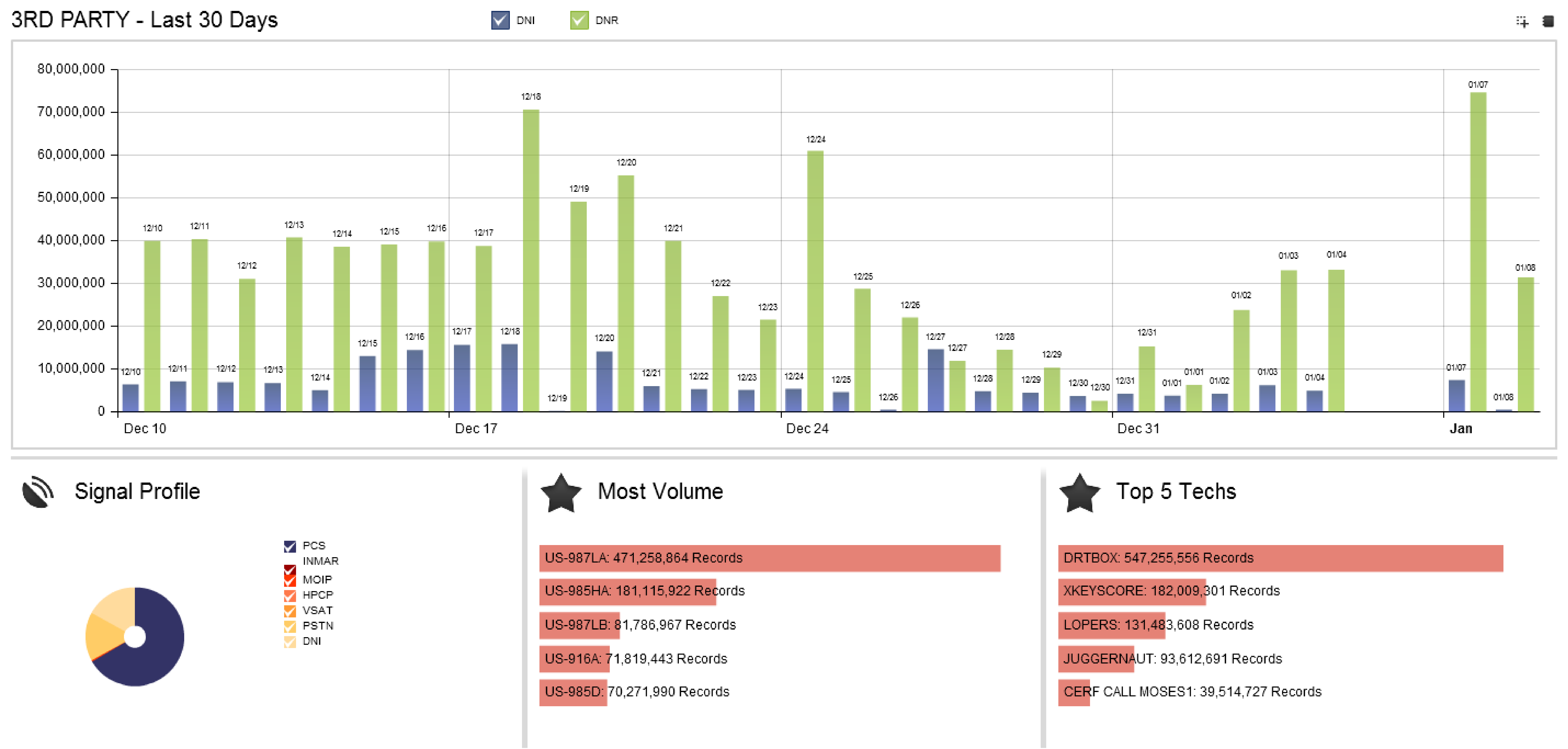
(by 30 day count)

100035321: 68 Counts
100033767: 51 Counts
6210000230: 30 Counts
610607131: 29 Counts
610209553: 27 Counts

Top 5 IPs

(by 30 day count)

146.185.26.163: 68 counts
37.130.229.100: 51 counts
85.237.211.198: 30 counts
85.237.212.52: 29 counts
85.237.211.177: 27 counts



3RD PARTY - Last 30 Days

☑ DNI ☑ DNR

Signal Profile

Most Volume

US-987LA: 471,258,864 Records

US-985HA: 181,115,922 Records

US-987LB: 81,786,967 Records

US-916A: 71,819,443 Records

US-985D: 70,271,990 Records

Top 5 Techs

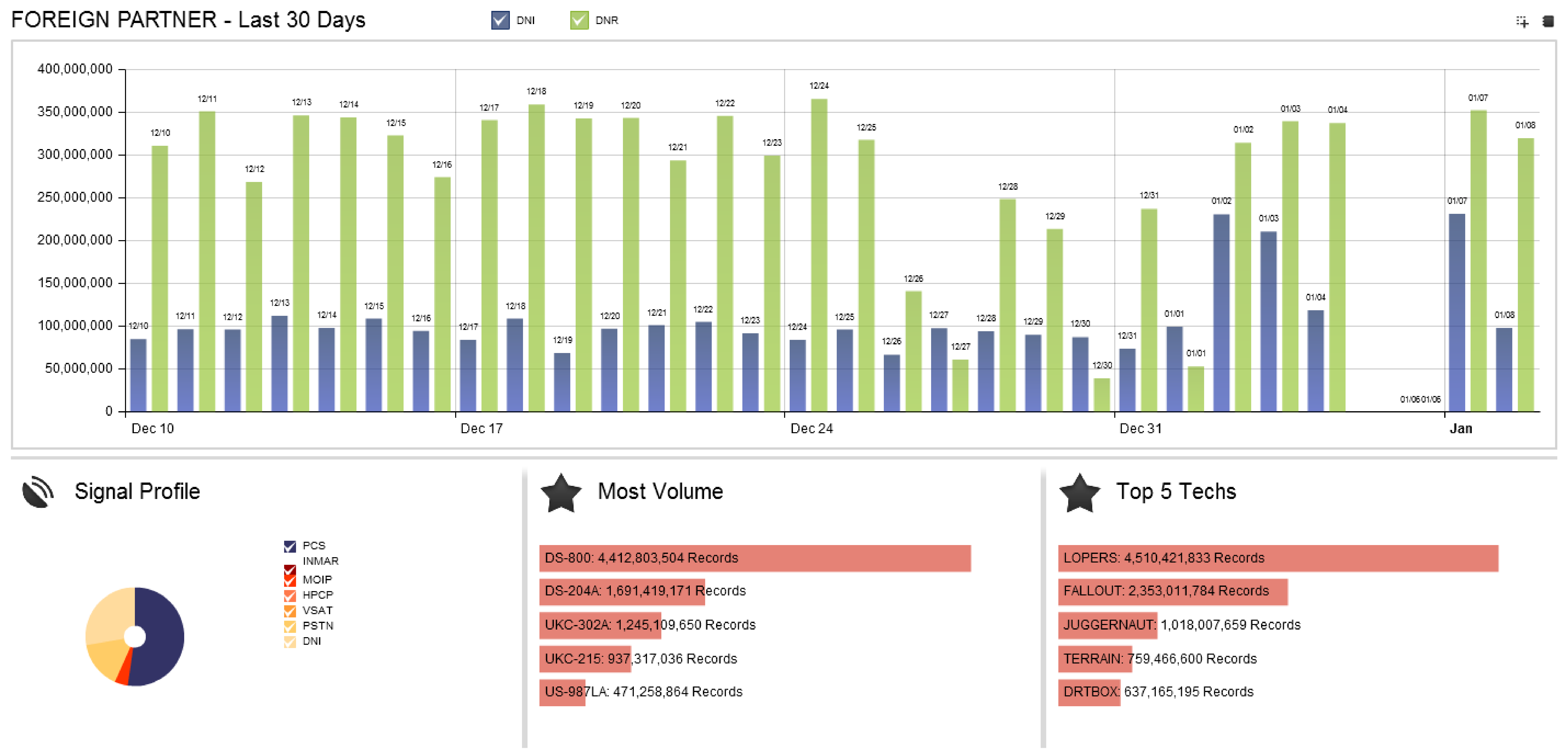
DRTBOX: 547,255,556 Records

XKEYSCORE: 182,009,301 Records

LOPERS: 131,483,608 Records

JUGGERNAUT: 93,612,691 Records

CERF CALL MOSES1: 39,514,727 Records



FOREIGN PARTNER - Last 30 Days

☑ DNI ☑ DNR

Signal Profile

☑ PCS
INMAR
☑ MOIP
☑ HPCP
☑ VSAT
☑ PSTN
☑ DNI

Most Volume

DS-800: 4,412,803,504 Records

DS-204A: 1,691,419,171 Records

UKC-302A: 1,245,109,650 Records

UKC-215: 937,317,036 Records

US-987LA: 471,258,864 Records

Top 5 Techs

LOPERS: 4,510,421,833 Records

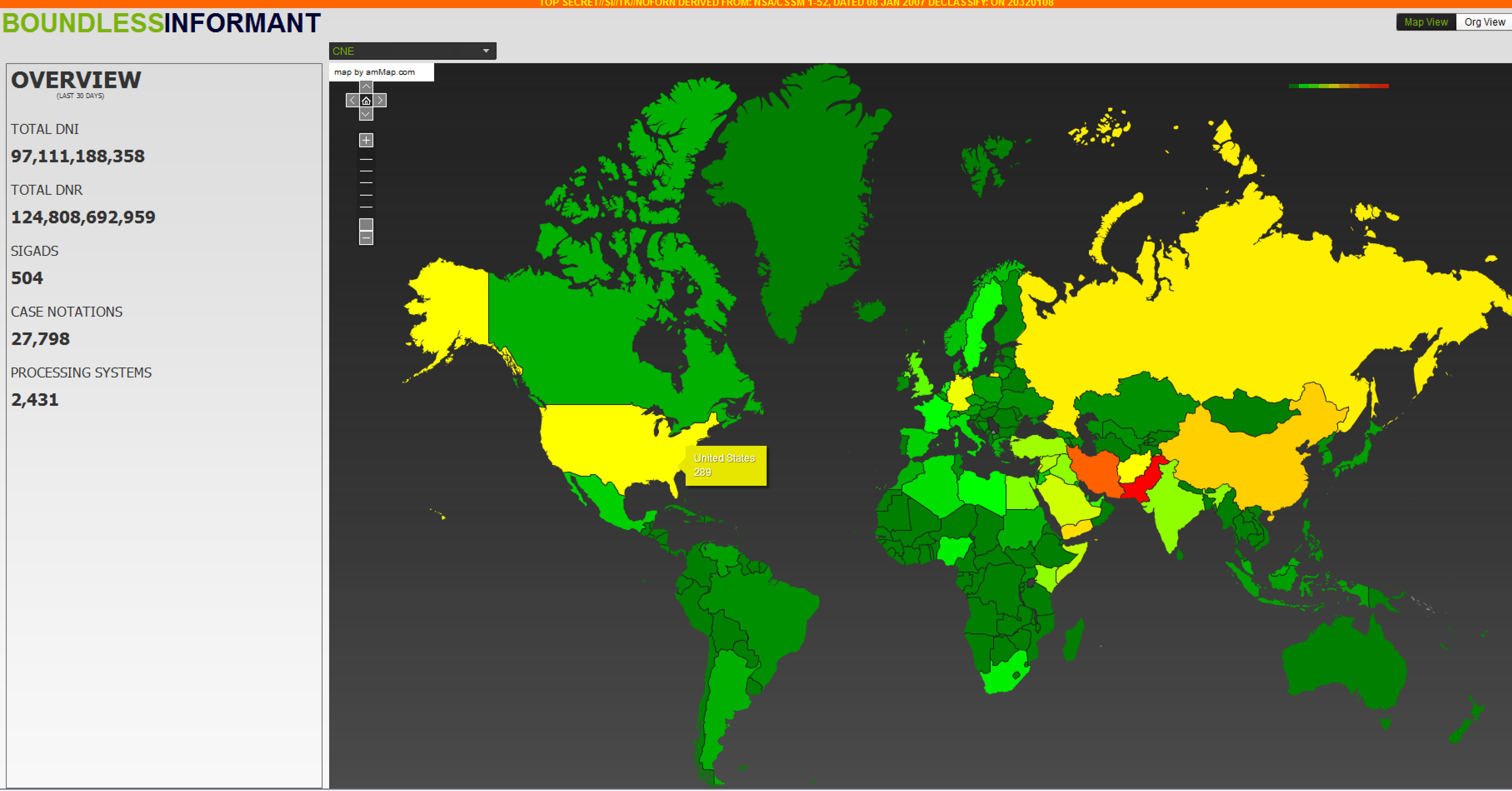
FALLOUT: 2,353,011,784 Records

JUGGERNAUT: 1,018,007,659 Records

TERRAIN: 759,466,600 Records

DRTBOX: 637,165,195 Records

TOP SECRET//SI//TK//NOFORN DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY: ON 20320108



OVERVIEW

(LAST 30 DAYS)

TOTAL DNI

97,111,188,358

TOTAL DNR

124,808,692,959

SIGADS

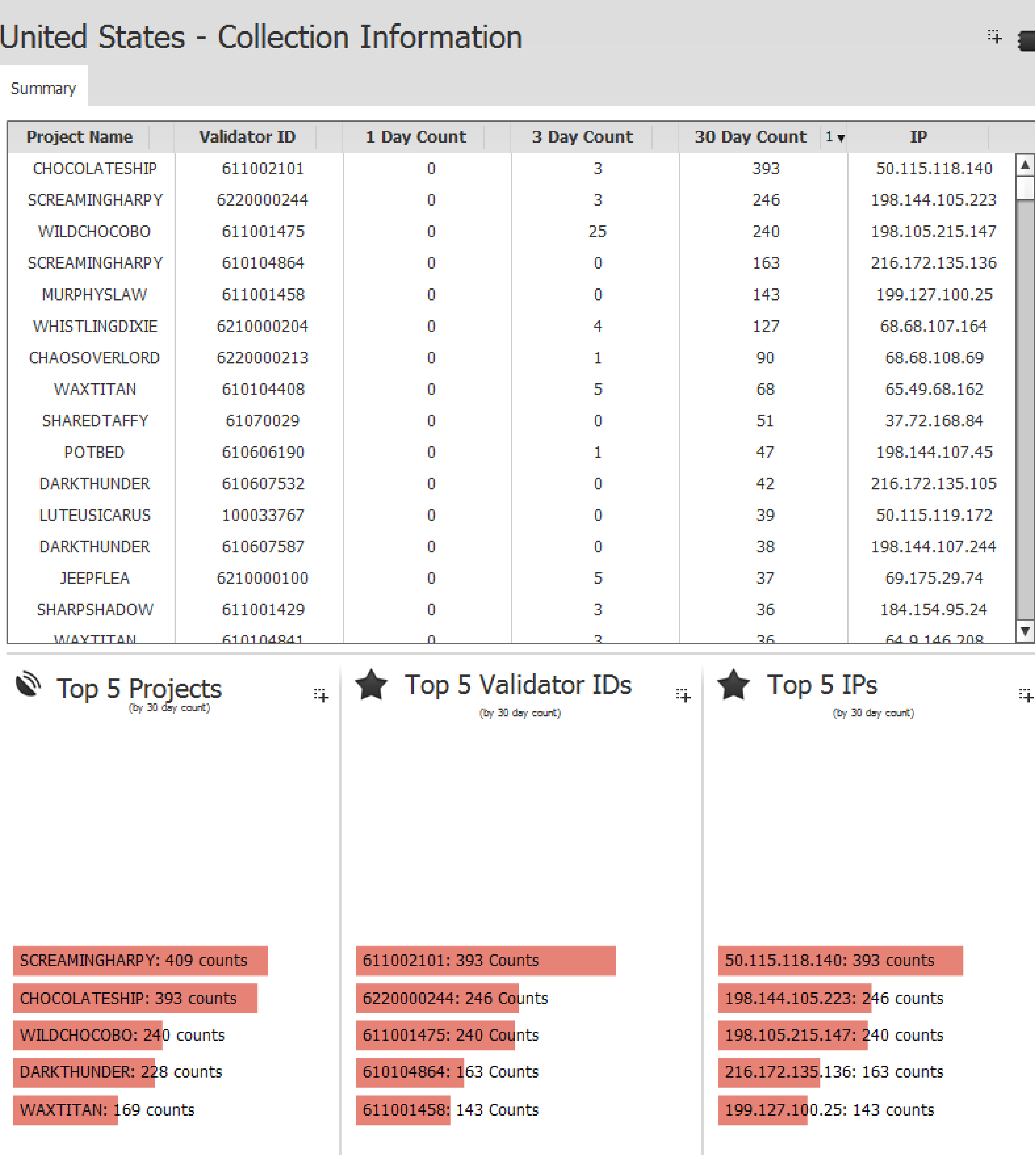
504

CASE NOTATIONS

27,798

PROCESSING SYSTEMS

2,431



United States - Collection Information

Summary

Project Name	Validator ID	1 Day Count	3 Day Count	30 Day Count 1 ▾	IP
CHOCOLATESHIP	611002101	0	3	393	50.115.118.140
SCREAMINGHARPY	6220000244	0	3	246	198.144.105.223
WILDCHOCOBO	611001475	0	25	240	198.105.215.147
SCREAMINGHARPY	610104864	0	0	163	216.172.135.136
MURPHYSLAW	611001458	0	0	143	199.127.100.25
WHISTLINGDIXIE	6210000204	0	4	127	68.68.107.164
CHAOSOVERLORD	6220000213	0	1	90	68.68.108.69
WAXTITAN	610104408	0	5	68	65.49.68.162
SHAREDTAFFY	61070029	0	0	51	37.72.168.84
POTBED	610606190	0	1	47	198.144.107.45
DARKTHUNDER	610607532	0	0	42	216.172.135.105
LUTEUSICARUS	100033767	0	0	39	50.115.119.172
DARKTHUNDER	610607587	0	0	38	198.144.107.244
JEEPFLEA	6210000100	0	5	37	69.175.29.74
SHARPSHADOW	611001429	0	3	36	184.154.95.24
WAXTITAN	610104841	0	3	36	64.9.146.208

Top 5 Projects

(by 30 day count)

SCREAMINGHARPY: 409 counts

CHOCOLATESHIP: 393 counts

WILDCHOCOBO: 240 counts

DARKTHUNDER: 228 counts

WAXTITAN: 169 counts

Top 5 Validator IDs

(by 30 day count)

611002101: 393 Counts

6220000244: 246 Counts

611001475: 240 Counts

610104864: 163 Counts

611001458: 143 Counts

Top 5 IPs

(by 30 day count)

50.115.118.140: 393 counts

198.144.105.223: 246 counts

198.105.215.147: 240 counts

216.172.135.136: 163 counts

199.127.100.25: 143 counts

As of: 22 April/0900 Hrs

Mr. Andreas Könen

e President, Federal Office of Information Security (BSI), Germany

23 Ap

Time	Presentation Title and Presenter	Location
1315	(U//FOUO) Welcome Mr. Andreas Könen [redacted] Met and escorted by Mr. [redacted], IA CDO Germany and [redacted] NSA/CSS Protocol Officer.	GH 1
1330-1400	(U//FOUO) NSA Information Assurance Directorate (IAD) Courtesy Call [redacted] DIR Information Assurance [redacted] D/DIR Information Assurance (*By Invitation Only*)	2C120
1400-1500	(U//FOUO) NSA Commercial Product Strategy and FISHBOWL [redacted] Technical Director, Mobility Mission Management Team (M3T)	2C120
1500-1530	(U//FOUO) National Information Assurance Partnership (NIAP) [redacted], Director, NIAP	2C120
1530	(U) Depart Met and escorted by [redacted] NSA/CSS Protocol Officer.	GH 1

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

(U//FOUO) European Security Center to Begin Operations

FROM: [redacted], USA
Chief, Operations Division, Army Cryptologic Operations (ACO)
Run Date: 03/29/2004

(S) A new tactical SIGINT producer will soon be up and running in Europe. On 10 March, MG [redacted] (SID) and MG [redacted] of the Army's Intelligence and Security Command (INSCOM) signed the Concept of Operations for the European Security

Center (ESC), setting the stage for an April start of formal SIGINT operations in Darmstadt, Germany. The ESC (USM-44) will perform SIGINT operations primarily in support of U.S. Army Europe and the European Command, but it will also conduct mutually beneficial, cooperative missions with various SID Product Lines.

(C) The ESC is a fixed site facility that will provide crisis support to military operations throughout the European Command theater, which includes not only Europe, but also much of Africa and parts of the Middle East. Working with a collocated INSCOM Theater SIGINT Battalion (TSB), the ESC will also provide an on-demand survey capability and deploy tailored front-end collection equipment. It will be a complete production facility, performing collection, processing, analysis and dissemination.

(C) The Center will also support theater SIGINT soldiers assigned at tactical echelons. It will serve both as a formal training center where those soldiers routinely train and maintain technical and language skills, and as a deployment center for soldiers who directly support contingency missions and combat operations.

(C) The ESC is initially staffed by SIGINT soldiers of INSCOM's 66th Military Intelligence Group, augmented by Army civilians and contractors. In the near term, they will be assisted by SID augmentees who possess critical skills, with the appropriate level of long-term SID support to be assessed as the ESC matures. Initially an "Army" organization, the ESC is a flexible construct that could potentially host personnel and missions from other Services and Agencies.

(C) The ESC is housed in two new SCIF** structures (over 10,000 square feet) adjacent to an existing Army Operations SCIF that houses other Army theater intelligence support missions, allowing an enhanced all-source effort against theater requirements. Current ESC systems and capabilities include 59 Distributed Common Ground Station - Army (DCGS-A) workstations, HIGHCASTLE (for voice processing and analysis and reporting), the TROJAN CLASSIC XXI collection, processing, analysis and reporting system, and an Emitter Mapping suite. Planned reconfiguration includes a "Linguarium", a novel construct to consolidate, focus and enhance voice analyst capabilities and productivity.

(U//FOUO) Army Points of Contact:
[redacted], Chief, Operations Division, Army Cryptologic Operations
[redacted]

[redacted] Chief, ACO Operations Field Support and European Desk Officer
[redacted]

(U//FOUO) SID Points of Contact:
[redacted] Chief Technical Support Program Management Office (TSPMO)
[redacted]

[redacted] Deputy Chief TSPMO [redacted]

**SCIF=Sensitive Compartmented Information Facility

(U//FOUO) The European Security Center to Become the 'ESOC'

FROM: [redacted]
A&P's Director, Enterprise Management (S2)
Run Date: 09/11/2006

(S//SI) NSA to help build up capabilities of the intelligence center in Darmstadt, Germany...

(S//SI) ***Good as it is, the ESC is about to get better.*** On 5 July 2006, the Director, NSA approved the "ESOC Concept" which transforms the European Security Center (ESC) into the European Security ***Operations*** Center (ESOC). With this move, NSA will help build up the Center's capabilities to allow it to assume even greater responsibilities within the worldwide SIGINT Enterprise. What will change, specifically?

(U) More Missions

(S//SI) Beginning in FY07 through FY13, the ESOC will evolve by expanding or adding more missions that will support national, theater and regional intelligence needs. ESOC's new or expanded missions include:

- additional select Counterterrorism targets,
- the African Union,
- Nigerian Energy Security,
- targets in Morocco, Algeria, Tunisia, and Libya, and
- complementary capabilities in SIGINT Development, Geospatial Analysis and Technical SIGINT.

(U) Changes in Manning

(S//SI) ...But that's not the only change. To ensure manning stability and to foster true national/tactical integration, a core of NSA civilians and multi-service Service Cryptologic Element military personnel* will work side-by-side with the (primarily) Army tactical SIGINT personnel who have manned the ESOC since its start-up.

(S) ESOC personnel at work

(U) Background: The ESC

(TS//SI) The European Security Center, primarily a theater SIGINT Center manned by Army Tactical SIGINT personnel from the 105th Military Intelligence Battalion in Darmstadt, Germany, was created over two years ago. It was the first center to use tactical resources -- augmented by a few NSA civilians -- to work both theater information needs as well as national missions.

(TS//SI) Today, the ESC is highly successful in producing intelligence for both national customers and the European Command. Its national mission focuses on select Counterterrorism targets, select Sub-Saharan Africa and North Africa target sets, SIGINT Development and Geospatial Analysis missions. Its theater missions include Force Protection, Global War on Terrorism support, Pan Sahel**, and targets in West Africa.

(TS//SI) The ESC's most recent SIGINT accomplishments include providing the majority of reporting and target tracking on the April 2006 coup attempt in Chad; providing linguistic and analytic support during the on-going Israeli-Lebanon crisis; and providing analytic and linguistic support which facilitated the arrests of terrorist facilitators operating in Italy.

(S//SI) The "ESOC Concept"

(S//SI) The decision to move forward with the creation of the ESOC was founded on the site's ability to...

- contribute to the national mission,
- plug into Theater all-source elements,
- optimize support to Theater operations,
- provide tactical over-watch (intelligence support to deployed troops), and
- maximize Second and Third party partnerships.

Under DIRNSA guidance, the US Army will retain its role as Executive Agent and Cryptologic Host for the new ESOC.

(S//SI) When fully realized, the "ESOC Concept" will be a model for future national/tactical integration, by providing an in-theater capability to produce high-impact analysis in support of all levels of national, tactical and Theater information needs.

(U//FOUO) POCs:

[redacted]

(U//FOUO) The ESOC

(U) Notes:

*(U//FOUO) The multi-service SCE military personnel are part of the Consolidated Cryptologic Program (CPE, also known as "P3"). Army tactical SIGINT personnel are known as "P2."

**(U) The Pan Sahel Initiative (PSI) is a State Department-led effort to assist Mali, Niger, Chad, and Mauritania in detecting and responding to suspicious movement of people and goods across and within their borders.

(S//SI//REL) Starting Up a New Mission at the European Security Operations Center: End-to-End SIGINT

FROM: [redacted]
Intelligence Analysis Intern
Run Date: 12/05/2007

(S//SI//REL) When considering possible TDY and deployment locations, many of my Intelligence Analysis Development Program (IADP) colleagues have opted for Iraq, Afghanistan, or an SCS site. At least for now, I chose to avoid the heat and sand and took advantage of a different opportunity for my fourth IADP tour. From May-September 2007, I completed a TDY from Ft. Meade to the European Security Operations Center (ESOC) in Darmstadt, Germany.

(U//FOUO) The ESOC

(S//SI//REL) ESOC, which stood up in April 2004 (see some background), is a joint Army/NSA SIGINT operations center and serves as the S2/Analysis & Production arm of NSA/CSS Europe (NCEUR). ESOC's personnel mix consists of 105th MI Battalion soldiers, a small Marine detachment, contractors, Department of the Army civilians, and NSA civilians in Darmstadt and Stuttgart in Germany as well as in Molesworth, England, and Mons, Belgium. ESOC's missions include African Regional Targets, North African and European Counter-Terrorism missions, Force Protection/Indications & Warning, and theatre SIGDEV.

(S//SI//REL) During my tour, I was assigned to the Africa Division and provided ESOC with target development support for the Gulf of Guinea Hydrocarbon Security mission, consisting primarily of Nigerian and Angolan targets. My particular focus was to launch the Africa Division's energy security mission covering Angola.

(S//SI//REL) Working African missions often present unique challenges, and both the Nigerian and Angolan energy sectors were certainly no different. While ESOC had worked the Nigerian energy security mission for over two years, due to resource constraints, relatively little development work had been done against the Angolan target. The larger Gulf of Guinea Hydrocarbon mission consisted of several analysts, a branch manager, and a technical leader, but it was largely up to me to do the bottom-up target development work in building the Angola mission.

(U) The Gulf of Guinea and surrounding region

(S//SI//REL) The task was somewhat daunting. Angola's state-owned oil firm, Sonangol, is a massive entity with its own airline, logistical service firms, and importantly, its own telecommunications subsidiary. Sonangol partners with several major Western and Chinese oil companies, and Chinese firms are heavily involved in the telecommunications sector. Our collection was minimal, and our day-to-day Angola team was essentially one deep: me.

(S//SI//REL) We compiled a detailed assessment and established good baseline knowledge of our current SIGINT posture in Angola. We reviewed existing SCS First Instance Reporting, and had several fruitful exchanges with SCS Luanda in Angola. We also worked closely both with ESOC's in-house SIGDEV elements and the European Technical Center to begin a target templating process and draft collection requirements. Through collaboration with CIA and EUCOM JAC*, Africa Division's understanding of our customer and partner requirements improved significantly.

(S//SI//REL) In order to gain a SIGINT window into Angola's telecom sector and energy industry, we chose to continue to chip away at Sonangol. Relying on skills and contacts acquired in previous IADP tours, I conducted intensive SIGINT research on Sonangol seed selectors using chaining, metadata analysis, and visualization tools such as Cmap and Renoir. My target development work spanned both the DNI and DNR realms. We were able to identify and unlock Sonangol target domains, locate and task e-mail selectors in CADENCE, and identify several new targets in the Angolan oil and telecommunications sectors.

(S//SI//REL) A key part of my tour at ESOC was identifying new potential collection accesses. Using open source, PINWALE, BLACKPEARL, NKB, ROADBED, and SURREY, I successfully located, identified, and submitted several new targets for FORNSAT and SCS collection. Partnering with ESOC SIGDEV, SCS, and FORNSAT collection staff at Ft. Meade and elsewhere, we were able to draft and submit the first collection requirement for the Angola energy mission. By the end of my tour ESOC had seen a significant increase in Angola energy traffic. We also were able to issue the first product of the Angola mission, a jointly issued report between the Africa division and ESOC SIGDEV.

(S//SI//REL) My tour at ESOC was an excellent exercise in end-to-end SIGINT to include initial research and target development, collection access discovery and tasking, and issuing products. My understanding of the SIGINT process improved greatly during my time at ESOC. The recent stand-up of the U.S. African Command (AFRICOM), co-located with EUCOM in Stuttgart, Germany is certain to create even more opportunities for analysts to support ESOC's missions in a dynamic environment.

(U) Notes:

* (U) EUCOM JAC = the European Command Joint Analysis Center

(U//FOUO) The ECC -- NSA's Newest Cryptologic Center

FROM: [redacted]
SIGINT Director
Run Dates: 06/10/2011 , 06/13/2011

[redacted]

(S//REL) On 9 May, NSA established the European Cryptologic Center (ECC) from what was formerly the European Security Operations Center (ESOC). The ECC will fall organizationally under NSA/CSS

[redacted]

Europe and Africa (NCEUR/AF). This is more than just a name change; it is furthering the commitment of the National Security Agency to a long-term mission presence in Germany. The name and accompanying organizational change reflect a recognition of the broader mission being supported from the ECC, as well as the strengthening of the analytic mission at the center.

(S//REL) In addition to the well-established SIGINT analytic and collection management missions, there is now an NSA/CSS Threat Operations Center (NTOC) and IT component to the center. ECC's enhanced analytic mission is a welcome development. The organization is a critical enterprise partner in the CT, Africa, and Middle East missions.

(S//REL) Since its beginnings in 2004 as the European Security Center (ESC), the ECC has been a success story in terms of SIGINT mission accomplishments and growth. In the last four years alone, the ECC's Analysis and Production mission set has increased from 5 to 26 distinct assigned missions, becoming the largest Analysis and Production activity in Europe. Complementing this rapid mission expansion has been an increased collaborative effort with foreign partners, with multiple IC members, and across the SIGINT Enterprise.

(S//REL) The quality and significance of ECC's SIGINT accomplishments speak for themselves. In the last month alone, ECC was a key contributor to the arrests of two key terrorist personalities, underscoring its refined collaborative environment. Overall, ECC products are included in the President's Daily Brief (PDB) on average twice a week. Further, for the second time in as many years, the ECC recently received an Honorable Mention citation in competition for the prestigious Travis Trophy award.

(S//REL) Located in Darmstadt, Germany, the ECC currently has a total of 240 personnel, a diverse mix of military service members, Department of the Army civilians, NSA civilians, and contractors. The ECC has responded to new intelligence priorities generated by the standup of AFRICOM, and has assumed new TOPI responsibilities in both the US European Command (EUCOM) and US Africa Command (AFRICOM) areas of responsibility.

(U//FOUO) Please join us in congratulating the ECC and its outstanding workforce on their accomplishments and welcoming them as NSA's newest cryptologic center.

(U/FOUO) View of the ESOC

(U//FOUO) Dragons, Shrimp, and XKEYSCORE: Tales from the Land of Brothers Grimm

FROM: [redacted]
European Cryptologic Center, SIGDEV (F22)
Run Date: 04/13/2012

(S//REL) The European Cryptologic Center (ECC) sits quietly nestled amongst vineyards and farmlands on

ECC

the outskirts of Darmstadt, Germany. To the passing motorist, the facility looks like many of the other random U.S. government facilities in the area, with one exception. One can almost hear a discernable buzz of activity from the analysts of the ECC executing queries, authoring fingerprints, and consuming metadata garnered from XKEYSCORE (XKS). In the past three months, the ECC has tripled, and even quadrupled in some cases, the number of queries performed, the number of items pushed to PINWALE, and the number of sessions viewed. And these numbers continue to grow.*

(S//REL) What has been the cause of this flurry of success? The ECC points to a recent ***XKS training blitz in support of the Analytic Modernization Outreach Campaign to encourage discovery.*** In early March, ECC SIGDEV analysts held an XKS Circuit Training event designed to expose analysts to five, 20-minute one-on-one sessions in a circuit-type environment. This "speed dating" for XKS consisted of five stations covering topics titled "Intro to the GUI and Basic Queries," "Metadata Setup and Manipulation," "Content and Manipulation of Results," "Introduction to Fingerprints," and "Introduction to Microplugins."

(S//REL) Over four days, 68 students were walked through these topics with five different instructors, able to ask specific questions and get more comfortable with the tool. "Everyone likes a new toy, and there was a lot of excitement about it. They will at least try it against their target and see what they will get out of it," said [redacted] one of the instructors and a SIGDEV Analyst embedded in Africa Division.

(S//SI//REL) With traditional targeting, analysts cast their nets wide into the murky waters of network traffic and haul in anything that gets caught in the net. We are like Forrest Gump on his shrimping boat off the coast of Alabama pulling in a boot, toilet seat, seaweed, and there they are... three shrimp! We burn up a lot of resources getting those shrimp, those reportable documents or metadata used to expand target knowledge, and we deal with tons of toilet seats, the spam and other junk. Then, we repeat the same process and hopefully catch enough "shrimp" to have ourselves a little cocktail. XKS has become so important because with it, analysts can downsize their gigantic shrimping nets to tiny, handheld goldfish-sized nets and merely dip them into the oceans of data, working smarter and scooping out exactly what they want.

(U//FOUO) And a short, two-hour class is an easy gamble of time for the hopes of being able to work smarter and more efficiently. ECC analysts have been trading in their old nets for new ones and are thrilled with their catches. Discovery can only occur if people are willing to try new things, and more of our analysts are getting comfortable with leaping into the relatively unknown world of XKS.

(U//FOUO) "The first time I saw XKS, I said, 'Whoa!!' It is intimidating because you open it up and you see all these queries and fields," said [redacted] "We took the students from that response to being able to approach it and navigate around in it. They see it differently now and know it's not a seven-headed dragon." This gentle introduction has definitely enabled analysts to ease into XKS and get more comfortable, and with that it has radically changed the overall mentality towards the tool.

(S//REL) ***Across the ECC, analysts wholeheartedly agree that the Circuit Training setup and content was a catalyst to give XKS a try or take existing users to the next level.*** The one-on-one setup provided a heavy injection of tool knowledge into each student. "Before the training, I was just happy to use it and not go to jail," said [redacted] a Circuit Training student and Arabic/French Language Analyst for CT (Counterterrorism). "Now, I feel comfortable in my ability to use it and NOT go to jail. I used to always ask someone to look over my query before I submitted it. Now, my hand doesn't need to be held."

(S//REL) That Circuit Training must be one tough training to pull off, you say? Not so, says [redacted] who spoke about the "off-the-shelf" nature of the training. "The framework was already developed by GCHQ, so it was simple for us to read over their notes, make it applicable to NSA, and conduct the training. We didn't have to spend time writing modules."

(TS//SI//REL) From the leadership level's perspective, the time invested sending analysts to the class had a tremendous return. [redacted], Tech Lead for the 50-person strong Africa Division, said, "The brevity of the class made it easy to send our people. Now we know exactly why we want to use it, and we have discovered new traffic and documents. Our analysts have been building hashes for document tracking and rolling them into fingerprints. We have been getting documents in XKS that we were not getting in our PINWALE queries. Just today analysts found reportable material from the Tunisian Ministry of Interior that was not from any selectors we were targeting. Now we know what we can do with XKS and exactly why we want to use it -- to make these discoveries."

(S//REL) These discoveries are igniting a trend of using XKS on a daily basis. "For daily pulls, analysts go through TransX, PINWALE, and now XKS to see what's new for the day," [redacted] said.

(U//FOUO) Combine these exciting finds with the introduction of XKS Skilz points, and you can see why McDonald's teamed up with Monopoly years ago: people buy more and even super size their orders just to get game pieces. With the brainchild of Skilz, where analysts can earn points and unlock achievements for performing tasks in XKS, people are willing to try new things within the tool. Analysts think to themselves, "Using the Pivot Data feature will earn 30 points... I'm going to try it and see what happens." Discovery! Points! We have been lured by our geeky desire to unlock achievements and earn points, and bragging rights are everything.

(U//FOUO) "Definitely a number of users have gotten into the Skilz points. We have several people at level six. They see what they need to do to earn more points and start trying out different things," said [redacted] In fact, ECC analysts now have the highest average of Skilz points compared to all of the S2 product lines and have written the most fingerprints per-capita! Some people say that the potent combination of Skilz points, the Circuit Training, and the team of easily-accessible, on-site instructors is the secret to ECC's successes with XKS.

(U//FOUO) Maybe XKS is a seven-headed dragon as [redacted] mentioned. Big and scary? Sure. Strong and powerful? Oh yeah. But, the ECC is taming it, and it is ours to do with whatever we like, including catching shrimp.

(U//FOUO) POC: [redacted]) ECC SIGDEV.

---

* (S//REL) Here are charts to illustrate the point:

(TS//SI/NF) PRISM (US-984XN) Based Reporting: June 2011 – May 2012

Sorted By # of PRISM-Based Reports Per OPI

OPI - Top Producers Issuing	PRISM-Based Reports	% Increase in PRISM-Based Reports Compared to June 2010-May2011	% Of All OPI Reporting Which is PRISM-Based	% Points Change from June 2010 - May 2011 period	All Reports By OPI	Single-Source to PRISM	% of PRISM-Based Reports Which are Single Source
SCS (F6*, US-96*, US-97*, US-3219)	3723	**Up 67%**	20	**+7 (up 54%)**	18640	3040	82
S2I - Counterterrorism	3493	**Up 5%**	42	**-2 (down 5%)**	8242	2074	60
S2E - Middle East & Africa	2574	**Up 47%**	16	**+2 (up 14%)**	16537	1959	76
S2G - Combating Prolif	2092	**Up 49%**	30	**+3 (up 11%)**	6872	1395	67
NSAT (USJ-783*)	1690	**Up 20%**	30	**+3 (up 11%)**	5713	1319	78
S2A - [redacted]	1389	**Up 8%**	11	**-1 (down 8%)**	12445	1196	86
NSAG (USJ-800*)	1255	**Down 8%**	11	**0 (no change)**	11741	883	70
ECC (ESOC) (USJ-753*, USM-44)	1147	**Up 6%**	52	**+2 (up 4%)**	2217	922	80
S2C - Intl Sec Issues	1147	**Up 75%**	13	**+5 (up 63%)**	8989	861	75
S2D - Countering Frgn Intel	862	**Up 40%**	12	**-5 (down 29%)**	7089	545	63
S2F - Intl Crime & Narc	666	**Up 41%**	16	**+2 (up 14%)**	4122	497	75
S2B - [redacted]	634	**Down 10%**	13	**-3 (down 19%)**	4842	452	71
NTOC (V*)	455	**Up 237%**	21	**+8 (up 62%)**	2195	355	78
DSD	310	**Down 15%**	4	**0 (no change)**	7511	296	95
NSAH (USJ-750*)	237	**Down 10%**	2	**+1 (up 50%)**	12023	155	65
S2J - Weapons and Space	225	**Up 221%**	33	**+11 (50%)**	692	186	83
GCHQ	197	**Up 137%**	2	**+1.9 (up 1900%)**	11257	170	86
S2H - [redacted]	**176**	**Up 159%**	**5**	**+3 (up 150%)**	**3353**	**155**	**88**
SSG	16	**Up 60%**	17	**-19 (down 52%)**	92	14	88
Utah Regional Ops Cntr (USJ-755)	12	**Up 20%**	6	**-17 (down 74%)**	207	12	100

Source: PLUS - 11-13 June 2012

(TS//SI//NF) PRISM (US-984XN) Based Reporting: June 2011 – May 2012

Sorted By % of PRISM-Based Reporting Per OPI

OPI - Top Producers Issuing	PRISM-Based Reports	% Increase in PRISM-Based Reports Compared to June 2010-May2011	% Of All OPI Reporting Which is PRISM-Based	% Points Change from June 2010 - May 2011 period	All Reports By OPI	Single-Source to PRISM	% of PRISM-Based Reports Which are Single Source
ECC (ESOC) (USJ-753*, USM-44)	1147	**Up 6%**	52	**+2 (up 4%)**	2217	922	80
S2I - Counterterrorism	3493	**Up 5%**	42	**-2 (down 5%)**	8242	2074	60
S2J - Weapons and Space	225	**Up 221%**	33	**+11 (50%)**	692	186	83
S2G - Combating Prolif	2092	**Up 49%**	30	**+3 (up 11%)**	6872	1395	67
NSAT (USJ-783*)	1690	**Up 20%**	30	**+3 (up 11%)**	5713	1319	78
NTOC (V*)	455	**Up 237%**	21	**+8 (up 62%)**	2195	355	78
SCS (F6*, US-96*, US-97*, US-3219)	3723	**Up 67%**	20	**+ 7 (up 54%)**	18640	3040	82
SSG	16	**Up 60%**	17	**-19 (down 52%)**	92	14	88
S2E - Middle East & Africa	2574	**Up 47%**	16	**+2 (up 14%)**	16537	1959	76
S2F - Intl Crime & Narc	666	**Up 41%**	16	**+2 (up 14%)**	4122	497	75
S2C - Intl Sec Issues	1147	**Up 75%**	13	**+5 (up 63%)**	8989	861	75
S2B - [redacted]	634	**Down 10%**	13	**-3 (down 19%)**	4842	452	71
S2D - Countering Frgn Intel	862	**Up 40%**	12	**-5 (down 29%)**	7089	545	63
S2A - [redacted]	1389	**Up 8%**	11	**-1 (down 8%)**	12445	1196	86
NSAG (USJ-800*)	1255	**Down 8%**	11	**0 (no change)**	11741	883	70
Utah Regional Ops Cntr (USJ-755)	12	**Up 20%**	6	**-17 (down 74%)**	207	12	100
S2H - [redacted]	**176**	**Up 159%**	**5**	**+3 (up 150%)**	**3353**	**155**	**88**
DSD	310	**Down 15%**	4	**0 (no change)**	7511	296	95
NSAH (USJ-750*)	237	**Down 10%**	2	**+1 (up 50%)**	12023	155	65
GCHQ	197	**Up 137%**	2	**+1.9 (up 1900%)**	11257	170	86

Source: PLUS - 11-13 June 2012

FAA702 UTT DNI Tasking

Snapshot on 30 Jan 2013

Product Line	All DNI Selectors Tasked	DNI Selectors Tasked to SSO_CT_N (FAA/PRISM)	% of DNI Selectors Tasked to FAA/PRISM	% Points Change From Dec 2011	Increase in number of selectors tasked to FAA/PRISM Compared to Dec2011
S2A	9650	987	10%	**-5**	**+232**
S2B	12872	2263	18%	**+6**	**+842**
S2C	8763	1059	12%	**+3**	**+468**
S2D	10846	3796	35%	**+11**	**+1872**
S2E	18061	6935	38%	**-4**	**+938**
S2F	3577	1011	28%	**+2**	**+423**
S2G	12788	4172	33%	**+2**	**+1019**
S2H	10497	828	8%	+6	+660
S2I	14945	11461	77%	**-1**	**+818**
S2J	1077	242	22%	**-2**	**-55**
ECC (F22)	4880	3523	72%	**-1**	**+715**
FTS	7194	2402	33%	**+9**	**+1126**
FTV	68	0	0%	--	0
FGS	6919	3114	45%	**-6**	**-17**
FGV	127	50	39%	**+21**	**+16**

Product Line	All DNI Selectors Tasked	DNI Selectors Tasked to SSO_CT_N (FAA/PRISM)	% of DNI Selectors Tasked to FAA/PRISM	% Points Change From Dec 2011	Increase in number of selectors tasked to FAA/PRISM Compared to Dec2011
FHS	6101	612	10%	**-7**	**+29**
FCS	592	55	9%	**+7**	**+52**
F6	29476	4007	14%	--	**+1650**
F1Z – CSG CENTCOM	105	3	3%	**-10**	**-46**
F74 - MOC	300	171	57%	**-7**	**-136**
F7A - AMOC	417	6	1%	**+1**	**+6**
F7U - UROC	926	27	3%	--	**-15**
NTOC – V24	278	0	0%	--	0
NTOC – V25	30	17	57%	**+39**	**+16**
NTOC – V26/V23	4237	2814	66%	**+4**	**+1490**
NTOC – V32	2388	12	1%	**+1**	**+11**
NTOC – V35	15	0	0	--	0
SSG	6609	0	0%	--	0
S32	1388	86	6%	**+1**	**+36**

DNR realms excluded from UTT query: IMEI, IMSI, ituE.164, Ki.

Source: UTT Team

(U) Running Strategic Analytics Affecting Europe and Africa

Region: Europe, Middle East (Israel), and Africa :
[redacted], ECC

The overall classification of this briefing is:

TOP SECRET//COMINT//REL USA, FVEYS//20291123

Outline

- (U) Background
- (U) Problem Definition & Challenge
- (U) Our AOR: Europe - Africa
- (U) Examples for Europe - Africa
- (U) Enrichment and Data Flow
- (U) Real-time, batch, XKEYSCORE
- (U) Conclusions

(U) Terrorists Transit via Europe

NCEUR Support to EUCOM

- (U) Communication
  - Transit Points
- (U) Partners
  - Second Party
  - Third Party
- (U) Relationships
  - EUCOM
  - AFRICOM
  - CENTCOM

North Sea
Baltic Sea
Neuendorf bei Wilster
Kiel Canal
Kiel
Rostock
Lübeck
Hamburg
Bremerhaven
Wilhelmshaven
Bremen
BERLIN
POL.
Hannover
Magdeburg
NETH.
Duisburg
Essen
Düsseldorf
Kassel
Leipzig
Elbe
Dresden
Cologne
Bonn
BEL.
Wiesbaden
Frankfurt
Rhine
Mannheim
CZECH REPUBLIC
LUX.
Saarbrücken
Karlsruhe
Nürnberg
Stuttgart
Danube
FRANCE
Munich
AUSTRIA
Zugspitze
0 50 100 km

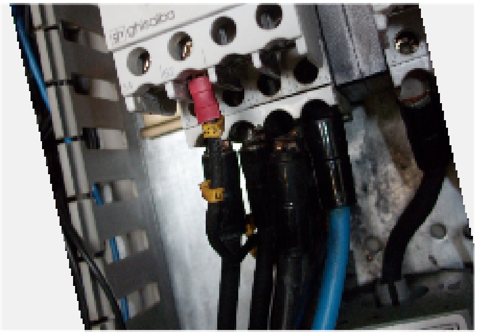
(U) US needs partners for data & to help capture, confine….

(U) Challenge: Integrating Tactical & National Collection

- (C//FVEY) Collection with HF/ VHF/UHF
  - Digital packets
  - Analog comms
  - Noise issues, lack of experience with these types of signals
- (C//FVEY) Tactical versus National (Strategic) Collection
  - RTRG
  - DISTILLERY

(U) Analytics for Targets in Europe

- (C//FVEY) OPSEC Savvy Targets
  - "…most terrorists stop thru Europe"
- (TS//FVEY) Use advanced techniques
  - Steganography
    - Forensics or Analytics on front end
  - Encryption
    - Takes time and has "black hole" issue
- (TS//SI//FVEY) Reliance on "special" collection
  - GCHQ and FAA
  - Problems processing w/r to TS



[redacted]

[redacted]

(U) Analytics for Identity Intelligence

(U) Human Trafficking	**(C//FVEY) Operations from Jordan to Syria in both directions; Sahel**	**Metadata for geolocation; content for confirmation**
(U) Weapons Smuggling	**(C//FVEY) From Libya to Sahel**	**Metadata for geolocation; content for confirmation**
(U) Drug Smuggling	**(C//FVEY) Sahel and financing of terrorism; Balkans into Europe**	**Metadata for geolocation; content for confirmation**
(U) Biometrics & Elections	**(C//FVEY) Used in Africa**	**Need collection assets**

(U) Enrichment Sources

- (U) Air Breather, HF & UHF/VHF
- (C//FVEY) Big Pipe & FORNSAT
- (U) Military SIGINT Services
- (U//FOUO) Forensics
- (U) Third Party Sources
- (C//FVEY) Second Party
  - GCHQ is critical for mission

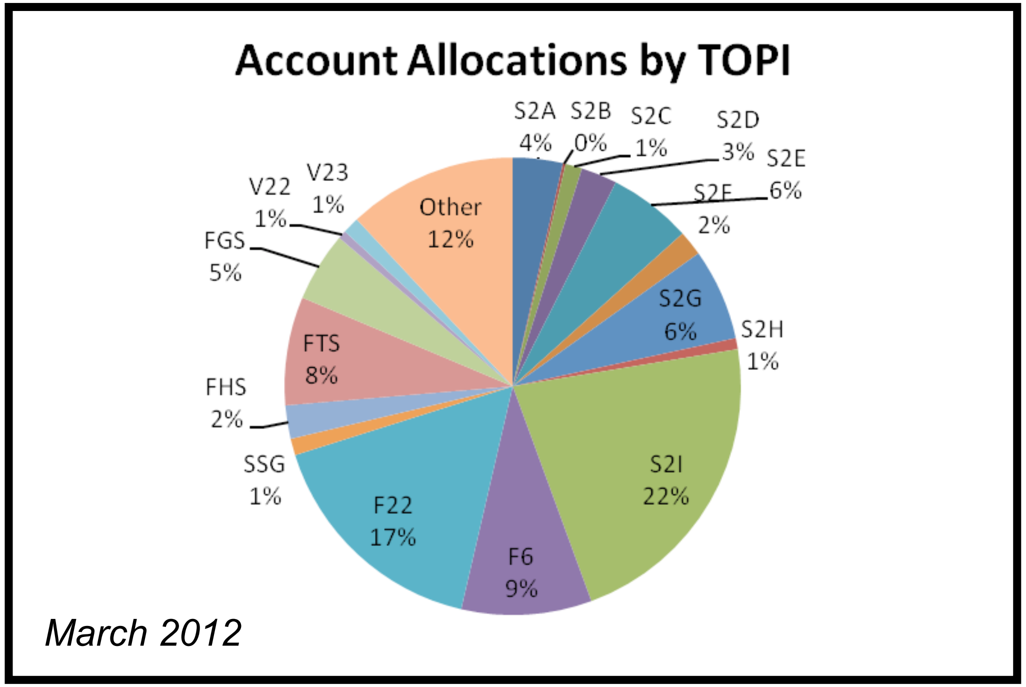
(C//FVEY) Key Idea: Low Priority of AFRICA may cause loss of metadata and content; makes "Discovery" more uncertain

QRC Package

3rd Party Partner Sharing

Computer Forensics

(U) Enrichment: SIGDEV & GCHQ QFDs



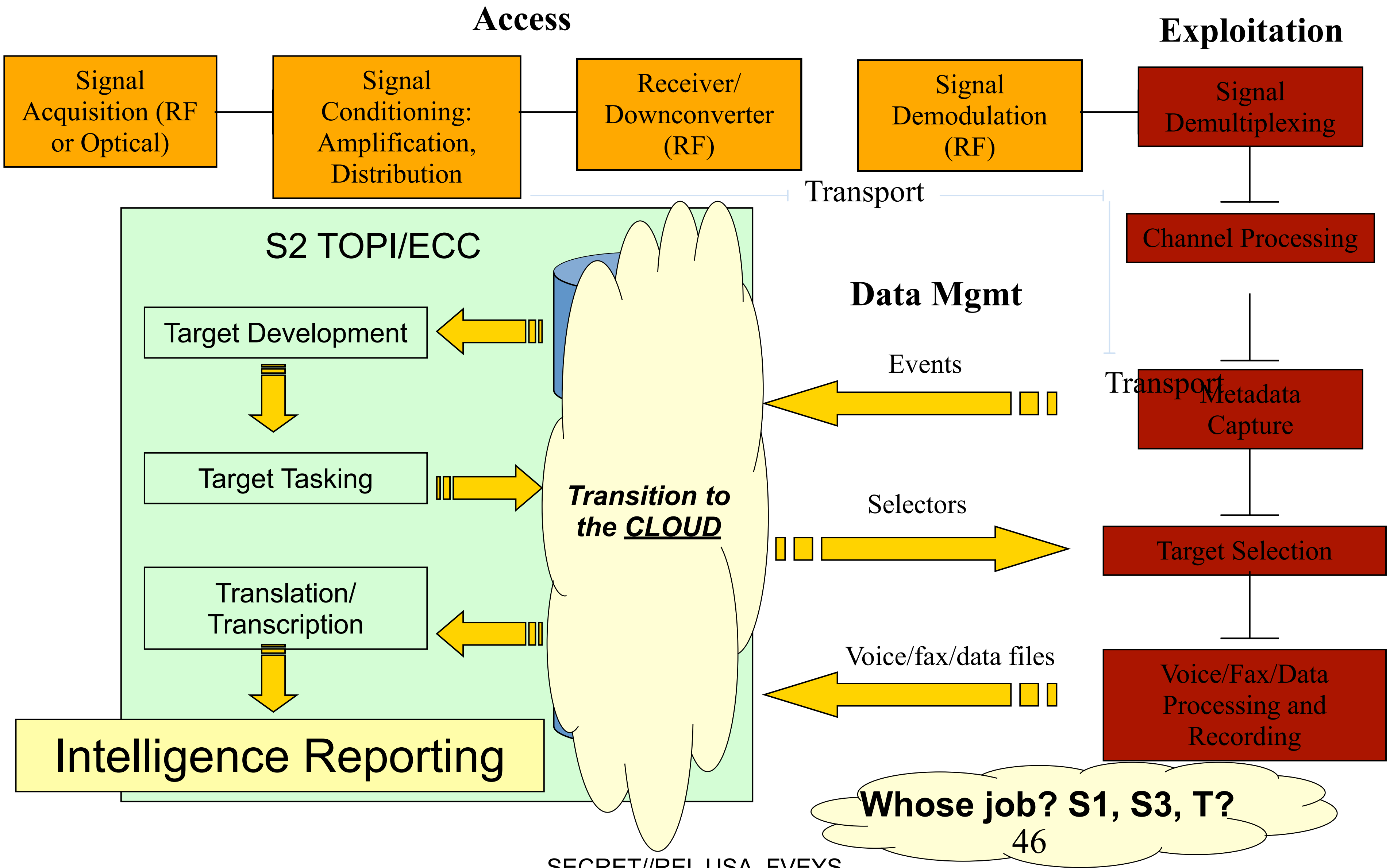
March 2012

- (S//FVEY) 54% of current ECC DNI tasking based on QFD data
- (S//FVEY) QFDs provide better access to metadata for European & North African targets than any other access at ECC due to poor passive collection
- (C//FVEY) Flexibility provided by the use of TDIs and the first stage query allows for better target discovery and development

Slide taken from ECC archives.

(C//FVEY) Much of ECC data comes from GCHQ QFDs

(U) Data Flow Integration is Constant Headache



SECRET//REL USA, FVEYS

(U) "Real Time" Analytics

- (U) Nascent Analytics with unclear definition of "real time"
  - How fast is alerting?
- (C//FVEY) DISTILLERY
  - Pulled from GHOSTMACHINE stack
- (U) NIAGARAFILES
  - File based
  - Starting to gain experience
- (C//FVEY) RTRG
  - Tools not integrated into ECC
  - Data Sets are sparse
  - Tactically oriented
  - Unregulated alerts can quickly spam user
- (C//FVEY) ECC Current Effort:
  - Focused on NTOC and Distributed Denial of Service attack alerting
  - Uses DISTILLERY

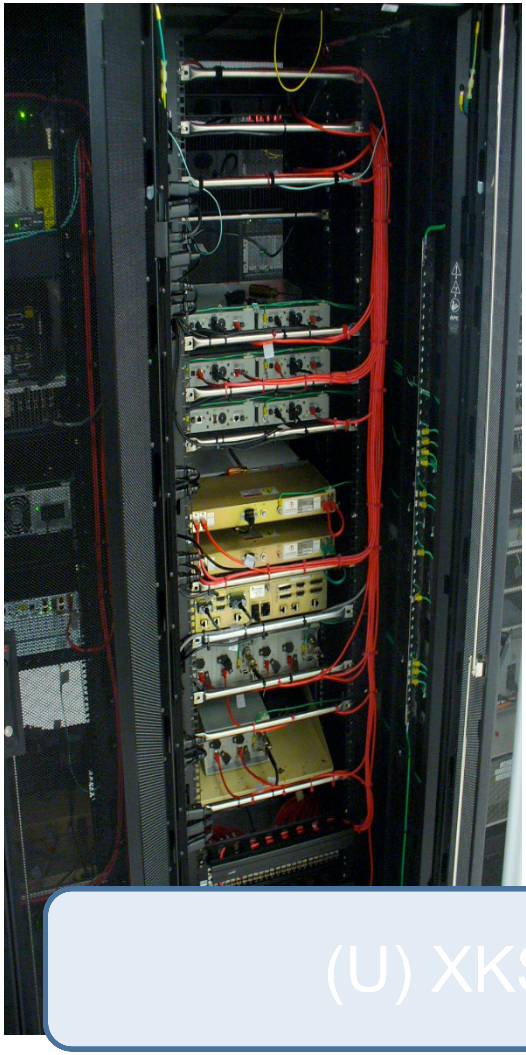
(U) How fast is real time?

(U) Batch: MapReduce Analytics

- (U) Batch oriented versus streaming
  - Run every 15 min to once a day or so
  - Not streaming
- (U) Good Data Storage
  - Good access outward to MDR-1, MDR-2
  - Days to years of storage
  - Promotion (?)
- (U) Complex Analytics like "Pattern of Life"
  - Reasonable amount of processing cycles at the front end collection system (not yet tested)
- (U) Session can be quite long and still captured (not yet tested)
- (U) UUID's (identifying sessions) are workable
- (U) No experience yet sharing with second and third party partners
- (U) Unknown level of entry training required
  - Menwith Hill has WHIZBANG

(C//FVEY) Batch gives you access to data 24 number hours ago

(U) Xkeyscore Fingerprints



- (C//FVEY) Streaming
  - Data available one hour later?
  - Most do pulls up to yesterday
- (U) Good Data Storage
  - RAW content: 3 days to a couple of weeks
  - Metadata: 90+ days
- (U) Complex Analytics like “Pattern of Life”
  - Reasonable amount of processing cycles at the front end collection system
- (U) Session can be quite long and still captured
- (U) UUID’s are workable
- (U) Good for sharing with second and third party
- (U) Relatively low level of entry training required

(U) XKS fingerprints great for streaming

(U) Key Take Aways

- (U//FOUO) Discovery in Africa is based on "we do not know what we do not see"
  - Unknown Unknown from url: https://wiki.nsa.ic.gov/wiki/NTOC-E_discovery_tradecraft
- (U) Europe has Opsec savvy CT targets
- (U) Analytics involve partners

  -- 3rd Party in future
- (U) Limited Resources: Processing Power & BW

NSA/CSS Europe & Africa

QUESTIONS?

(U//FOUO) SID Around the World: The Rheinland

FROM: [redacted]
Unknown
Run Date: 09/16/2003

(S//SI) Having served on one field tour at NCEUR, Stuttgart, Germany, in the mid-1990s, I was once again fortunate to get an offer for another field assignment in

Germany just two years later, at NSA's European Technical Center (ETC) in Wiesbaden. The position at ETC was as a Foreign Relations Staff Officer, responsible for coordinating technical support to NSA's Third Party partners in Europe and the Middle East. My wife served as NSA's liaison to the Army's 66th Military Intelligence Group in Darmstadt. We lived between Wiesbaden and Darmstadt, due south of Frankfurt, and our school-age children went to the DoDDs school in Darmstadt.

(S//SI) For a career Intelligence and Language Analyst, the most interesting and rewarding aspects of working at ETC were exposure to the engineering work that NSA does and to the superb group of people who carry it out. It was a pleasure, indeed, even an inspiration, to deal with the technical personnel who put SIGINT and related systems in place, to witness their expertise, and to gain greater awareness of technical support, maintenance, and logistics problems. The engineering and logistics friends I made in Wiesbaden are ones I would likely not have met in my regular career field back home, and I learned a lot from them. Supporting NSA's foreign partnerships and sometimes dealing directly with foreign partners was a particularly interesting experience as well.

(U) Outside of work, the most rewarding aspect of living in the Rheinland area of Germany is the opportunity to travel across Germany and much of Europe. France, the Benelux countries, and Switzerland are all within a few hours' drive, for a weekend or, for border destinations such as Strasbourg, even a day trip. For longer drives, Paris and Berlin are within six hours drive, the Alps are 3-7 hours away, depending on which mountain is being sought, and other destinations - in southern France, the Czech Republic, Austria, Hungary, Slovenia, Croatia, and Italy - are within reasonable long-distance reach for an extended vacation. Living near Frankfurt also puts one very close to rail and air connections to anywhere in Europe, including low-cost air travel to many European destinations. It was a thrill to be able to visit sites of historical and cultural significance during our tour, and living in Germany has marked our children with a considerable appreciation for European history and culture.

(U) The middle Rhein area between Mainz/Wiesbaden and Koblenz is quite scenic and offers many opportunities to sample aspects of German life, especially gastronomic pleasures, closer to home. You don't have to go far to find a really good white wine, for some very good Rieslings may well be just down the street. Wiesbaden is located within the Rheingau wine area; the Rheinhessen is just across the Rhein, and the Rheinpfaltz (Rheinland Palatinate) and Mosel-Saar-Ruwer regions, as well as the French province of Alsace, are close by. Even lesser-known wine regions, like Franconia, are within reach.

(U) As for cuisine, eating in Germany can be a real pleasure for all but the most conservative tastes. I have not had a bad German meal yet. Local specialties abound; in the Rhein/Main plain closer to Darmstadt, the Germans grow the sweet, white asparagus ("Spargel") that is harvested in May and enjoyed throughout Germany. The strawberry season follows immediately thereafter.

(U//FOUO) It might belabor the obvious that I enjoyed living in Germany to no end. Working and living in the field is a great experience, and working at ETC and living in Germany was no exception. I'd do it again.

(U//FOUO) First-Ever Formal SIGINT Development (SIGDEV) Training Is Provided to SIGINT Seniors Europe (SSEUR) Partners

FROM: SIGDEV Strategy and Governance, Governance & Community Engagement (SSG GCE),
Associate Directorate for Education and Training (ADET),
and NSA's Foreign Affairs Directorate (FAD)
Run Date: 10/25/2010

(U//FOUO) History has been made: for the first time ever SID, ADET, and FAD personnel collaborated to create an analytic course for NSA Third Party partners. "Introduction to SIGDEV" was held at the European Technical Center (ETC) in Wiesbaden, Germany, and taught to 26 students from SSEUR nations,* 14-16 September 2010.

(S//REL) The course provided the SSEUR partners with a common understanding of the importance of SIGINT Development (SIGDEV) as a discipline, and a common definition of SIGDEV efforts. This effort enhanced the opportunities for SSEUR partners to work together more effectively to tackle mission areas of mutual interest -- especially Afghanistan and Counterterrorism (CT) target sets.

(U//FOUO) The training was extremely successful, based on survey responses, and many of the partners plan to incorporate information from this course into training programs for their own new SIGINT analysts.

(U//FOUO) SID, ADET, and FAD are currently creating another more in-depth telephony analysis training course with the hopes of presenting this training to NSA Third Party partners in spring/summer 2011.

(U//FOUO) For more information on SSG Governance & Community Engagement, visit SSG Governance & Community Engagement Website (go ssg-gce).

(U//FOUO) For more information on the Associate Directorate for Education and Training, visit ADET Website ("go adet").

(U//FOUO) For more information on the Foreign Affairs Directorate, visit FAD Website ("go faks").

(U//FOUO) POC: [redacted]

(U) Notes:
* (S//SI//REL) SSEUR members are the Five Eyes nations (Australia, Canada, New Zealand, United Kingdom and United States) and the following Third Party partners: Belgium, Denmark, France, Germany, Italy, Netherlands, Norway, Spain, Sweden. All Third Party nations in SSEUR sent students to the training, as did the UK.

(C//REL) NSA Communications Hub in Europe Is Modernized

FROM: (U//FOUO [redacted]
Director, European Technical Center (F25)
Run Date: 10/20/2011

(C//REL) Introduction: The European Technical Center (ETC) in Wiesbaden, Germany, is NSA's primary communications hub in that part of the world, providing communications connectivity, SIGINT collection, and data-flow services to NSAers, warfighters and foreign partners in Europe, Africa and the Middle East. That's why it is essential that ETC's capabilities keep up with the demand...

(C//REL) On 19 September, NSA officials* proudly hosted a ribbon-cutting ceremony to officially mark the completion of GODLIKELESION -- ETC's Communications Center modernization project. The project initially began as a limited effort to address challenges in cooling, equipment configuration, cable management, and space in the room. Over time the effort grew into a much broader joint project to completely rebuild the room from the ground up into a state-of-the-art communications center.

ETC ribbon cutting

(C//REL) Many years of high operations tempo and expansion had resulted in incorrect rack configurations, poor airflow, insufficient rack size, installation shortcuts, substandard safety and security measures, inconsistent cable management, and lackluster documentation. In early 2010, over 150 power supplies failed over several months, spurring an agreement between NSA's I&L, Technology Directorate and ETC leadership to expand the scope of the GODLIKELESION project to include a new supporting power infrastructure.

(C//REL) The GODLIKELESION project was completed in seven phases, all without any interruption to the mission data flowing through ETC. Work alternated between Enterprise IT Services (T3) and I&L elements to replace legacy flooring and equipment racks; close partnering among the organizations allowed for timely completion of the various phased tasks. As an example, all equipment supporting communications for 27 Third Party partner dataflows was moved, re-installed and documented within 12 days.

(U//FOUO) The work completed by I&L included new Uninterrupted Power Supply (UPS), UPS distribution system, grounding system, raised access floor, rack power distribution elements (PDE), and computer room air-conditioner (CRAC) units and condensation piping. ETC partnered with T32 personnel to remove 81 legacy racks, install 89 new equipment racks, move 253 pieces of equipment, install 5,668 feet of new fiber, and create 1,076 pages of documentation. The new racks represent a 670% increase in available equipment space with cooling capacity doubled from 2009 conditions. The newly outfitted space will provide reliable and robust IT, communications, and data-transport services for the foreseeable future.

(U) Notes:

* (U//FOUO) Hosting the event were [redacted] Director of the European Technical Center, together with [redacted], Chief, NCEUR; [redacted] [redacted] Director, Technology Directorate; Mr. [redacted] Assistant Deputy Director for Data Acquisition; and [redacted] Chief, Installations and Facilities Services.

(U//FOUO) TEC Successfully Installs BOTANICREALTY at LADYLOVE (USJ-799)

[redacted]

(TS//SI//REL) In response to a request from S2B, MSOC System Development and Signals Development Lab personnel collaborated with the TEC to deploy a solution to collect a [redacted] video network. When first detected, the video was unencrypted. The video then became encrypted over a period of two months. The current demodulation solution from the TEC is called BOTANICREALTY. Originally, SALTYDOGS was used to find carrier acquisitions and discover signal characteristics. This provided the frequency range, carrier rates, and a rough time up and time down for channel activity.

(TS//SI//REL) In mid-April, the TEC installed BOTANICREALTY (formerly known as UNCANNY) at LADYLOVE in the hopes of locating, identifying, and collecting [redacted] clear and encrypted video signals found on the [redacted] of [redacted]. The collection of these signals, in support of [redacted] is important to the S2B [redacted], various special projects at the CIA, and in general product reporting [redacted]

(TS//SI//REL) Within minutes of the system coming on line, BOTANICREALTY successfully collected its first signal matching the parameters of the encrypted (HIGH PRIDE) video [redacted] signals. The hub control channels are session encrypted while the outstations are bulk encrypted video. Since proving the ability to automatically process these signals of interest at LADYLOVE, over 1000 collects, totaling hundreds of hours of raw data, have been made and forwarded to cryptanalytic personnel in CES for further investigation.

(U//FOUO) Joint SIGINT Activity Annual Report for 2007

[redacted]

(S//SI//REL) The Joint SIGINT Activity (JSA) experienced notable successes in its FORNSAT mission during 2007 for NSA and the German Federal Intelligence Service, or Bundesnachrichtendienst (BND). However, concurrent with the JSA mission changes, manpower requirements were re-evaluated and reductions to both civilian and contractor manning levels were approved with implementation to be carried out in FY08.

(S//SI//REL) The past year also saw an expansion of JSA's partnerships with SSO, TOPIs, and ESOC, with plans to expand these further and increase support on various operations in 2008. JSA will continue to build on its successes and improve its mission contribution in collection and SIGINT development to both NSA and BND.

(U//FOUO) Highlights for 2007:

(S//SI//REL) JSA engineers developed various analysis tools and an automated selector sanitizing tool. The selector sanitization tool can be used at other sites, including those working special projects.

(S//SI//REL) The expansion of site capabilities through the installation and integration of U.S. and German systems significantly improved collection and development of high-priority targets. New or improved capabilities include an automated survey system, VoIP processing and metadata collection capabilities, a high speed filtering system, GSM metadata collection capabilities, and new data flows to NSA for DNI, VoIP and GSM metadata.

(S//SI//REL) A closer relationship between ESOC, JSA and BND resulted in new exploitation of targets in Algeria as well as other African targets. New TROPICPUMA fax processing capabilities deployed in December immediately began to provide unique and valuable intelligence to ESOC and BND on [redacted]

(S//SI//REL) The BND used JSA [redacted] GSM collection to identify, track, alert, and [redacted]

(S//SI//REL) JSA continues to provide critical collection of the [redacted] network, providing unique insights into [redacted]

(S//SI//REL) NSA personnel continued to improve BND's skills through both classroom and on-the-job training allowing BND personnel to take on greater roles in DNI processing and analysis.

(S//SI//REL) Joint SIGINT Activity-Developed VoIPSum and AutoNorm Tools Used in Local Analysis, Create Agency-wide Interest

[redacted]

(S//SI//REL) JSA has developed and is now using two new number normalization tools – a VoIP Summarization (VoIPSum) tool and an Automated Normalization (AutoNorm) tool.

(S//SI//REL) Voice-over-IP (VoIP) traffic is prevalent at many collection sites, including JSA. Site engineers have developed a simple tool, called VoIPSum, to extract, parse, and organize VoIP metadata for analysis by Intelligence Analysts, Signals Analysts, and developers. VoIPSum provides the user with several outputs: a summary file of cities/countries on each case notation seen in its run, also viewable by web browser; a file containing URIs (Uniform Resource Indicators) and their associated IP addresses; a file of normalized numbers and location information; and a file of normalization suggestions for non-normalized numbers, generated with help from AutoNorm.

(S//SI//REL) Generating normalization rules for NORMALRUN can be very difficult without adequate knowledge of a region's Country Code (CC), National Destination Code (NDC), Local Exchange Office Code (LEOC), and Subscriber Number (SN). JSA has found their in-house developed tool, AutoNorm, a great time saver for generating NORMALRUN rules. AutoNorm works by matching substring combinations of the raw number against the Global Numbering Database flat file. It provides several input options: generic, which tries to find an exact match; prelist, which appends a given set of digits to domestic calls before attempting matches; and sort, which sorts its output into groups that share the same digits stripped or pre-pended.

(S//SI//REL) These two tools have been used by JSA analysts to aid in generating reports and number normalizations and target research. Additionally, representatives from the NAC, Misawa, SSG, S2C, and SSO have expressed interest in receiving and using VoIPSum and AutoNorm.

(S//SI//REL) VoIPSum and AutoNorm are now available for download! For more information, including user manuals, output examples, and a downloadable tarball, please visit JSA's website. You may also contact the POCs listed above.

(S//SI//REL) Joint SIGINT Activity Begins New SMS and Call Event Dataflows for NSA Analysts

[redacted]

(S//SI//REL) JSA initiated two new SMS dataflows for NSA analysts in April. These new dataflows are from USD-1079's AST128B and AST128C DNR collection platforms. The SMS data is flowing into DISHFIRE, and the corresponding call event data into FASCIA. A cursory look at dialing showed [redacted] Poland and others. Preliminary data shows that JSA is sending over 330,000 SMS events to DISHFIRE daily. So, let the hunt begin! One can isolate this new SMS data by querying in DISHFIRE on JSA's PDDG (IQ) and collection box (RA, L1). This SMS collection is being processed on multiple case notations from INTELSAT-902 (G2), YAMAL-202 (E9), and EUTELSAT-W6 (KL) with forward and reverse gateways with [redacted] (primarily). However, we also have Tajikistan, Russia, Monaco, Lebanon and UAE gateways represented. As a reminder, JSA has been forwarding SMS data from its JUGGERNAUT GSM collection platform since 2007.

Der Zeitgeist

(C) Joint SIGINT Activity (JSA)

(S//SI//REL) US, German SIGINTers Increase Cooperation on African Targets

FROM: (S//SI//REL) [redacted]
SIGDEV Analyst, Joint SIGINT Activity (H52G1)
Run Date: 12/13/2007

(S//SI//REL) The JSA* is a joint US-German SIGDEV operation conducted from a German SIGINT facility. It has been filling collection gaps for the US-run European

Security Operations Center's (ESOC) counterterrorism effort, as well as other African missions, for over a year now**. So far in 2007, NSA has produced thirteen Africa-related SIGINT reports from JSA collection, a success which has opened the door to greater cooperation at JSA on the African target set.

(S//SI//REL) Mangfall Kaserne in Bavaria, home to JSA.

(S//SI//REL) **ESOC and JSA: A Logical Match**

(S//SI//REL) Due to higher priority ongoing tasks for Iraq and Afghanistan, ESOC (see background) has had difficulty in getting collection resources to survey for African signals. As a result, ESOC has been investigating possible Third Party relationships to leverage partner accesses and linguistic capabilities. BND is both a trusted partner and a very modern and capable SIGINT service, which lessens concerns about sharing capabilities and SIGINT selectors with this partner as opposed to other potential African partners. JSA's collection resources, as well as BND's overlapping requirements regarding North Africa, made JSA an obvious choice to quickly respond to ESOC's SIGDEV requirements.

(S//SI//REL) **JSA Collects Against Africa**

(S//SI//REL) In fall of 2006, JSA began collecting email traffic related to [redacted] GSM infrastructure, producing a number of SIGDEV-related reports. Then in the summer of 2007, ESOC requested that JSA perform a survey of six satellites in search of specific North African communications. During the course of the survey, JSA located and initiated collection on [redacted] GSM signals carrying [redacted] communications. In October 2007, ESOC issued its first CT SIGINT report from JSA's GSM (Global System for Mobile communications) collection. In addition to supporting ESOC, JSA is now collecting [redacted] signals in support of NSAW's CT mission.

(U) **Overlapping Requirements**

(S//SI//REL) NSA and BND have similar SIGINT requirements regarding Africa. BND has standing intelligence requirements for various political and humanitarian issues throughout Africa. BND's current priorities in Africa are Sudan, Algeria, and Somalia. In Sudan, BND is collecting two different GSM networks at another FORNSAT facility, and using the metadata to track targets. Germany is very interested in the peace process in Darfur and southern Sudan. Regarding Algeria, BND has been processing border guard communications from JSA collection, but these signals appear to be migrating to a new data network, requiring a new processing capability. BND HQs analysts are eagerly awaiting a processing solution in order to more fully exploit these internal Algerian communications. For Somalia, Germany has forces in the Horn of Africa region supporting Operation Enduring Freedom, and is very interested in the political and humanitarian issues surrounding Somalia.

(U) **Future**

(S//SI//REL) NSA analysts at JSA are working with CSRC (Collection Strategies and Requirements Center)-Europe and NSA/CSS Representative AFRICOM to explore new areas where JSA can support overlapping African SIGINT requirements from

NSA and BND.

(U) Notes:

* (S//SI//REL) "JSA" stands for "Joint SIGINT Activity." It is operated by NSA and the Bundesnachrichtendienst (BND - German Foreign Intelligence Service) at the German SIGINT facility Mangfall Kaserne in Bavaria. Any association of NSA with Mangfall Kaserne is SECRET//COMINT//REL TO USA, FVEY.

** (U) GSM = Global System for Mobile Communication; [redacted]

[redacted]

JSA Restrictions

ACLogoRed.png

Access Central: Targeting

Targeting and selector management are services that Access Central offers. This incorporates the configuration, delivery, and exchange of targeting as well its optimisation, assurance, and enrichment. For more about the services that Access Central offers visit Services

[edit] General

JSA is a US/German COMSAT Site which although provides a unique access has several restrictions on what can be targeted. The broad restrictions can be defined as:

1. No German or 5 Eyes nationality or location
2. No European Economic Targeting

3. 5 Eyes/No Eyes Only
4. No Unknown Nationality/Location

[edit] Domains

We have been advised that the following domains are not accepted at JSA to avoid any sensitive nationality selectors being targeted, a full list of country codes is available here

- .as
- .at
- .au
- .ca
- .de
- .gu
- .mp
- .nz
- .pr
- .uk
- .us
- .vi

[edit] Companies/Entities

This is a list that we received from JSA stating address that should not be targeted due to them being German companies or entities

- BASF.COM
- BAUMARKTFORSCHUNG.COM
- BOEHRINGER-INGELHEIM.COM
- BRANDSTIFTER.COM
- BUNDESWEHR.ORG
- CLEARSTREAM.COM
- DEBITEL.NET
- DEUTSCHE-BANK
- DHL.COM
- EADS.NET
- EUROCOPTER.COM
- FEUERWEHR-INGOLSTADT.ORG
- HANAFOS.COM
- HERRENKNECHT
- KLIMAWANDEL.COM
- MERCEDES-BENZ.COM
- MTU-NET.RU
- MUNICH.ORG
- NDSATCOM.COM

- NEUE-EINHEIT.COM
- ORGELBAU.COM
- PAETZOLD.COM
- ROHDE-SCHWARZ.COM
- SACHERGMBH.COM
- SENIORENHEIM.COM
- SIEMENS.COM
- SIEMENS-AFGHANISTAN.COM
- TESSAGIRAN.COM
- VS-HYDRO.COM
- WACKER
- [redacted]@HOTMAIL.COM

(S//SI) German, NSA SIGINTers Share DNI Processing Knowledge

FROM: [redacted]
SUSLAG (Special US Liaison Activity Germany)
Run Date: 05/22/2006

(S//SI) A BND* delegation responsible for building BND's next generation DNI (Digital Network Intelligence)- processing architecture visited the Joint SIGINT Activity (JSA) in late February for two days of discussions to learn more about

NSA's DNI architecture. The JSA, an operational element of the Special US Liaison Activity Germany (SUSLAG), is a joint SIGINT development, collection, and exploitation site manned by German and US personnel.

(S//SI) BND analysts discussed their processing architecture, which is largely based on NSA's old P25 and P26 GRANDMASTER prototypes. Their focus is primarily e-mail processing, specifically SMTP e-mail. Spam filters are used to manage large data volumes. Selected traffic is passed through an automated privacy protection system, ensuring that analysts cannot view German-protected traffic. On-site BND analysts then manually assess all selected traffic to determine potential intelligence value.

(S//SI) In conducting this evaluation, they do not prioritize the selected traffic by target or keyword. Instead they focus on e-mails carrying attachments with the goal to scan e-mails as quickly as possible to increase their throughput. E-mails that are determined to be of potential intelligence value are then forwarded to BND HQS for follow-on evaluation and reporting.

(S//SI) NSA intelligence analysts discussed NSA's SIGINT Development model, NSA's "Hunt versus Gather" philosophy, our multi-stage selection and filtering process, and the evolution of DNI processing systems from GRANDMASTER to WEALTHYCLUSTER and, in the future, TURMOIL. The BND appeared especially interested in the TURMOIL approach of scanning and making judgments at the packet level prior to any sessionizing.

(S//SI) In summary, **NSA and BND use opposite selection and filtering approaches.** Where NSA primarily relies on equipment for selection (e.g. BLACKNIGHT) and analyst minimization for privacy protection, the BND relies on analysts to manually scan traffic for selection, and then equipment to filter data for privacy protection. Full use of current NSA DNI processing systems and analysis methodologies at JSA will be key to influencing the BND to alter their strategic DNI processing approach.

*(U) Note: BND = Germany's Bundesnachrichtendienst (the Federal Intelligence Service)

(U) This article is reprinted from the *Foreign Affairs Digest*, April edition.

Der Zeitgeist

Human Language Technology

Center for Content Extraction

Content Extraction Analytics

SIGDEV *End-to-End* Demo

[redacted]

21 May 2009

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20330108

Introduction to Content Extraction

- New technologies can find Essential Elements of Information in documents
- The Center for Content Extraction provides “one stop shopping” for these technologies at NSA

Extraction can benefit SIGDEV from end to end

- Selection
- Translation & Transliteration
- Analysis
- Interpretation/Enrichment
- Retrieval
- Storage & Distribution

STAIRS Partners

S (Marina, CEA)

T (Cybertrans)

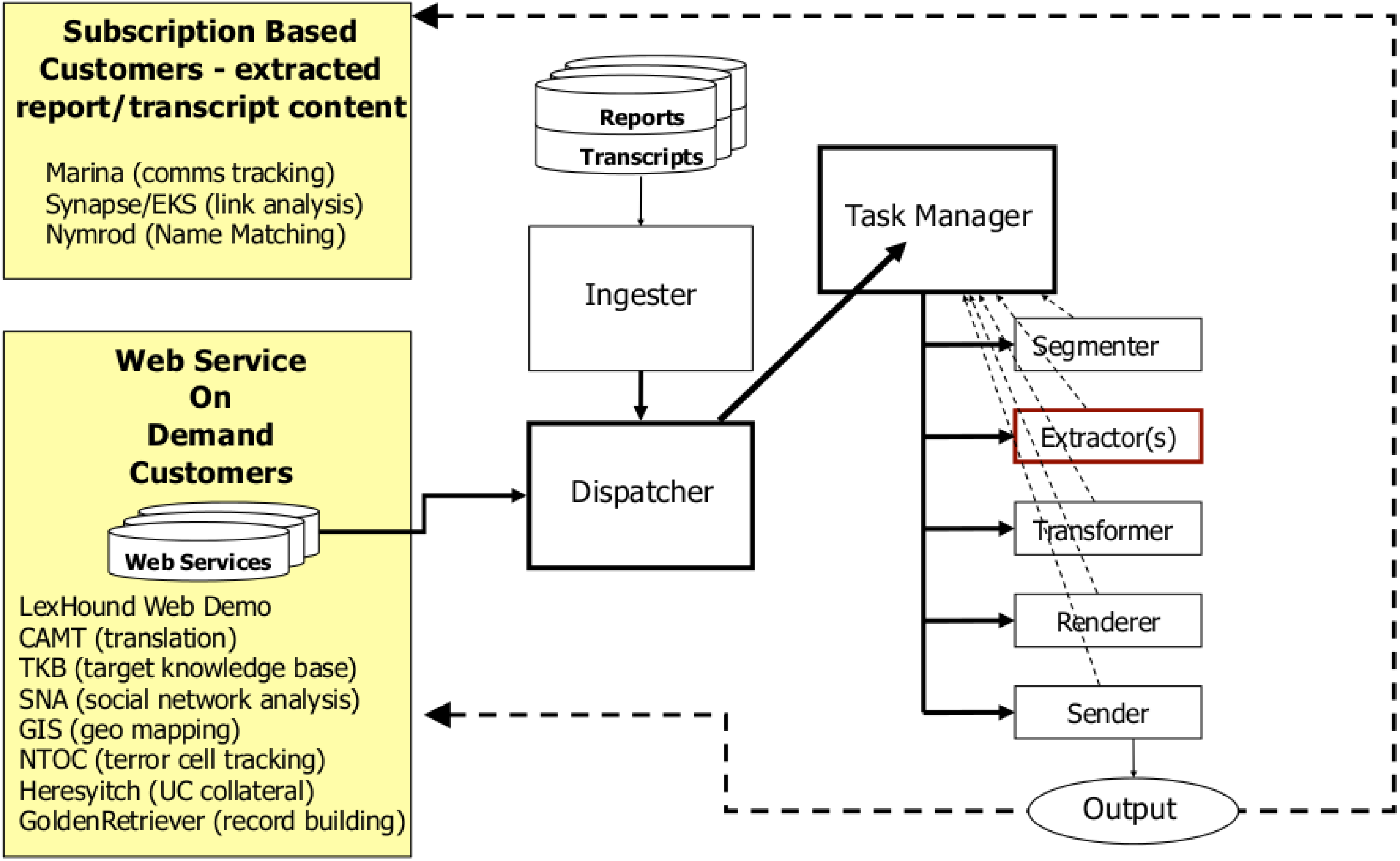
A (SNA/Paintball, Synapse)

I (Nymrod,Thundercloud)

R (Journeyman/CPE)

S (GoldenRetriever, SocioPath)

Implementation: CCE Extraction Architecture (LexHound)



Subscription Based Customers - extracted report/transcript content

Marina (comms tracking)
Synapse/EKS (link analysis)
Nymrod (Name Matching)

Web Service On Demand Customers

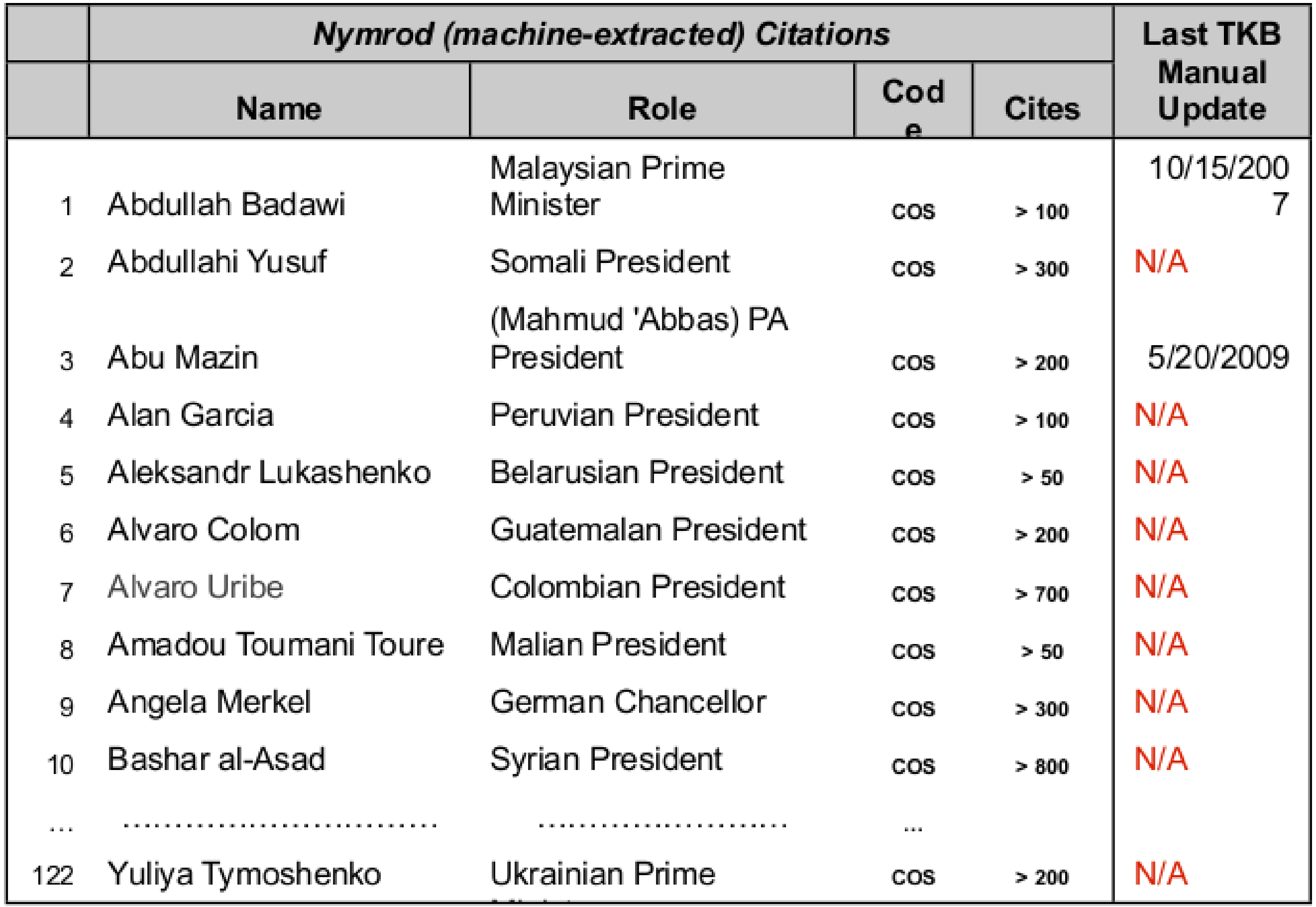
Web Services

LexHound Web Demo
CAMT (translation)
TKB (target knowledge base)
SNA (social network analysis)
GIS (geo mapping)
NTOC (terror cell tracking)
Heresyitch (UC collateral)
GoldenRetriever (record building)

Elaboration: *The Central Importance of Storage*

- Each of the STAIRS Steps exploits stored information
  - Selection Dictionaries (“get it”)
  - Linguistic Glossaries for Translation
  - Wikis etc for enrichment (“know it”)
- Manual record-formation is slow, prone to omissions and inconsistencies
  - <200K Person Targets in TKB
  - Growth ~= 20K/year
- Automatic extraction accelerates storage
  - >3000K Citation Records in ***Nymrod*** Entity DB
  - Growth ~= 1000K/year

Machine vs. Manual Chief-of-State Citations



	Nymrod (machine-extracted) Citations				Last TKB Manual Update
	Name	Role	Code	Cites	
1	Abdullah Badawi	Malaysian Prime Minister	COS	> 100	10/15/2007
2	Abdullahi Yusuf	Somali President	COS	> 300	N/A
3	Abu Mazin	(Mahmud 'Abbas) PA President	COS	> 200	5/20/2009
4	Alan Garcia	Peruvian President	COS	> 100	N/A
5	Aleksandr Lukashenko	Belarusian President	COS	> 50	N/A
6	Alvaro Colom	Guatemalan President	COS	> 200	N/A
7	Alvaro Uribe	Colombian President	COS	> 700	N/A
8	Amadou Toumani Toure	Malian President	COS	> 50	N/A
9	Angela Merkel	German Chancellor	COS	> 300	N/A
10	Bashar al-Asad	Syrian President	COS	> 800	N/A
...	....	....	...		
122	Yuliya Tymoshenko	Ukrainian Prime	COS	> 200	N/A

(C//REL) TEMPORA -- "The World's Largest XKEYSCORE" -- Is Now Available to Qualified NSA Users

FROM: (U//FOUO) [redacted]
NSA Integree at GCHQ
Run Date: 09/19/2012

(U//FOUO) SIGINT analysts: We have all heard about Big Data; now you can get **Big Access** to Big Data.

(TS//SI//REL) What happens when one site contains more data than all other XKEYSCOREs combined? At more than 10 times larger than the next biggest XKEYSCORE,* **TEMPORA at GCHQ** is the world's largest XKEYSCORE and the NSA workforce is now getting greater access to it. This massive site uses over 1000 machines to process and make available to analysts more than 40 billion pieces of content a day. And starting today, skilled NSA XKEYSCORE users can get access to the TEMPORA database via the XKS-Central interface.

(TS//SI//REL) **What is TEMPORA?** TEMPORA is GCHQ's XKEYSCORE "Internet buffer" which exploits the most valuable Internet links available to GCHQ. TEMPORA provides a powerful discovery capability against Middle East, North African and European target sets (among others). Analysts who have benefited from GCHQ Special Source accesses like INCENSER or MUSCULAR will almost certainly benefit from TEMPORA.

(TS//SI//REL) **How valuable is TEMPORA?** The value and utility of TEMPORA were proven early into a 5-month evaluation that began this past March. With a limited user base of 300 analysts, TEMPORA became the second most valuable XKEYSCORE access for discovery. Additionally, this small group of analysts produced over 200 end-product reports and provided critical support to SIGINT, defensive, and cyber mission elements.

(TS//SI//REL) **Why TEMPORA?** TEMPORA provides the ability to do content-based discovery and development across a large array of high-priority signals. Similar to other XKEYSCORE deployments, TEMPORA effectively "slows down" a large chunk of Internet data, providing analysts with three working days to use the surgical toolkit of the GENESIS language to discover data that otherwise would have been missed. This tradecraft of ***content-based discovery*** using the GENESIS language is a critical tool in the analyst's discovery tool kit, and nicely complements the existing and well-known tradecrafts of strong selection targeting and bulk meta-data analysis.

(TS//SI//REL) **How do I get an account?** To comply with GCHQ policy and to ensure users are successful in such a large-scale environment, TEMPORA access requires users to be proficient with XKEYSCORE. At NSA this is achieved via the completion of various XKS Skilz achievements. Beginning today, users will see a new "TEMPORA" achievement, which requires users to have remained current with their UK Legalities training (OVSC1700), be a level 3 or higher XKS Skilz user, and have used GENESIS by either querying or authoring fingerprints. Users who meet those criteria will automatically be given TEMPORA access in their XKS Central account.

(S//SI//REL) **What do I need to know about using TEMPORA?** Although TEMPORA will appear as an additional database in XKS Central, there are some important items analysts need to be aware of when they search this database. Analysts are asked to pay close attention to details concerning the UK Legality requirements on the TEMPORA user-guidance wiki page. TEMPORA queries must comply with both UK and U.S. legal requirements, and the analytic community must ensure we are using this access wisely and compliantly.

(S//SI//REL) **How can I learn more about using XKEYSCORE?** If you'd like to get TEMPORA access but need some help fulfilling the proficiency requirements, the XKEYSCORE Outreach Team is ready to help. The team recently added an additional round of XKEYSCORE training sessions on ERS, which users can sign up for via this link. Also, analysts can find great tradecraft and training tips via the XKEYBLOG, or they can contact the team directly at DL XKS_Mentoring.

(U//FOUO) For more information **"go TEMPORA"** or contact [redacted]

(U) Notes:

* (S//SI/REL) XKEYSCORE is a computer-network exploitation system that combines high-speed filtering with SIGDEV. XKEYSCORE performs filtering and selection to enable analysts to quickly find information they need based on what they already know, but it also performs SIGDEV functions such as target development to allow analysts to discover new sources of information.

(S//SI) Forward Production at NCEUR -- Inside the Customers' Decision Space

FROM: [redacted] Customer Account Manager for EUCOM (S112) and NCEUR staff
Unknown
Run Date: 01/14/2005

Analytic team working at NSA/CSS Europe; success story with Global War on

Terrorism (GWOT) (S//SI)

(S//SI) In early 2003, NSA/CSS Europe (NCEUR) and the Geospatial Exploitation and Counterterrorism Product Lines initiated a Forward Production effort (at NCEUR) to support our national goals and strategy in North Africa. Among those goals was to enable African governments to police their own borders, sustain or enhance stability, and make it clear that their countries were an environment hostile to terrorist organizations and their supporters.

(S//SI) This small investment of five-to-six analysts has provided a significant return: Forward Production and headquarters analysts* were able to report the predicted movement of [redacted] EUCOM Senior Staff and U.S. Ambassadors in the region used this information to engage and enable regional governments to conduct successful counterterrorism operations. Intelligence generated by this Forward Production-NSAW partnership has been responsible for the **capture or kill of over 40 terrorists** and has helped achieve GWOT and regional policy successes in Africa.

(S//SI) While based on the skills of the forward-deployed analysts as supported by NSA HQ, two other overarching factors contributed to the effort's success. These factors are:

- collocation with the primary regional implementer or action arm of the US Government as well as supporting elements, and
- an aggressive effort to release SIGINT to foreign governments supporting truly non-traditional customers (e.g., governments in Algeria, Mali, and Mauritania).

(S//SI) Forward Production's effectiveness is based on collocation and integration with operational planners and teaming with all-source customers and partners. This allows Forward Production analysts to better anticipate requirements, to provide better-tailored products and services, to better operate in the customers' decision cycle, and to better understand customer needs.

(S//SI) As the title of DIRgram-337 states "It's About Relating, Not Disseminating" and NCEUR forward-deployed analysts as "our expeditionary force inside our customers' information space..." are better enabling CT operations and reaching analytic conclusions not otherwise possible. The Forward Production cell at NCEUR is serving as a model for operational partnering and analytic collaboration within the customer's environment.

(S//SI) This Forward Production model will be implemented on an industrial scale when the European Security Center (ESC) in Darmstadt, Germany, becomes fully operational. The ESC is the realization of a significant investment by US Army Europe (USAREUR) and Intelligence and Security Command (INSCOM) to perform SIGINT analysis and production against national, theater, and tactical requirements within the customer domain. (See related story.)

Notes:
* (S//SI) Extended enterprise and HQ communities of the GEO, CT, Regional Targets, and Middle East North Africa product lines collaborated on this target.

(U//FOUO) On the Road Again: SID Team Visits Germany

FROM: [redacted]
Assistant Deputy Director for Analysis & Production (S2)
Run Date: 02/01/2006

(U//FOUO) After staying around headquarters for the last quarter, it was time for me to get out and about into the extended enterprise! In early January I joined a SID team on a trip to Germany to gain insight into the operations there and to update the NSA/CSS Europe workforce on Agency, SID and S2 initiatives. Our team consisted of:

- [redacted] SID Chief of Staff;
- [redacted] SID CoS Executive Assistant;
- [redacted] A&P Deputy Technical Director;
- [redacted] A/DDAP Executive Assistant; and
- [redacted], A/DDAP and Senior Intelligence Authority).

(U//FOUO) We visited elements of the European Command (EUCOM) headquarters and NSA/CSS Europe (NCEUR) near Stuttgart, Germany; the European Security Center (ESC) in Darmstadt; and the European Technical Center (ETC) in Wiesbaden. (See a map of NCEUR locations.) Chief, NCEUR, [redacted] accompanied us throughout.

Stuttgart: European Command HQ and NSA/CSS Europe (U//FOUO)

(U//FOUO) We arrived in Stuttgart on Monday, 9 January. To stave off the jet lag, we walked around downtown Stuttgart until meeting up with a group of NCEUR folks for a dinner of good German food.

(C) On Tuesday morning we were treated to several briefings on EUCOM and NCEUR operations and met with the EUCOM J3 (Director of Operations), Rear Admiral [redacted] and EUCOM J2 (Director of Intelligence), Brigadier General [redacted] coming away with a better understanding of their perspectives. We used the opportunity to explain to them how NSA's distributed analytic enterprise can be engaged in efforts to meet their information needs.

(U//FOUO) Our session with the J3 was very positive and he appreciated the value of analysis. Rear Admiral [redacted] feels strongly that intelligence sharing needs a systematic approach to enable transparency. He recognizes that we are integrated and connected and therefore can't afford to operate independently.

(U//FOUO) We next met with the J2, BG [redacted] The JAC (EUCOM's Joint Analysis Center in Molesworth, England) joined us virtually, giving us the chance to hear their concerns. We discussed the Mission Build-out, governance, resource challenges and mission management of a distributed enterprise. A key area of concern is "less commonly taught languages" and what we're doing to meet that challenge. We made sure they knew that A&P is at the forefront by leveraging language resources in Utah (see a related message), the National Virtual Translation Center (NVTC), and our 2nd party partners. We intend to leverage those opportunities enterprise-wide. We also discussed the new "lane structure" and the Strategic Mission List. BG [redacted] is interested in results from an all-source perspective and asked that we keep our capabilities relevant to EUCOM. He was glad we were there and hoped we would gain an appreciation of their ops during the rest of our visit.

(U//FOUO) We also held a town meeting with NCEUR personnel to cover current events relating to resources and the structure of the Agency, as well as strategic planning initiatives. Major points included:

- Future trends and challenges in A & P,
- Future roles for the extended enterprise in A & P

- Changes in IT infrastructure due to new tools and techniques
- S2 Assessment Cell
- Senior Intelligence Authority issues

(U//FOUO) We need to ensure we take advantage of their forward presence. As a forward-deployed function they are empowered leaders and strategists. We need to keep doing forward what's best done forward! Following a busy and productive day, we went to a great little restaurant "Waldheim" - or "home in the woods."

(U//FOUO) Patch Barracks, near Stuttgart: home to EUCOM HQ and NCEUR.

Darmstadt: The European Security Center (U//FOUO)

(U//FOUO) On the morning of Wednesday, 11 January, we traveled to Darmstadt Army Base to visit with the 66th MI Group and European Security Center. COL [redacted] 66th MI GP Commander; LTC [redacted] ESC Director [redacted], ESC Deputy Director; and their energetic team provided an outstanding overview of their organizational structure, operations, successes and challenges.

(U//FOUO) The ESC** is a functioning part of the enterprise. They've made great strides in their analytic expertise. The analytic support received from SID/S2/SSG is great and continues to expand. S2 elements, in particular GEO, CT, RT, and CP, were lauded for their outstanding support. The ESC, as an A&P-forward function gives them many advantages. Their state-of-the-art operations area allows them quick, deployable, and operational partnerships. Weekly VTCs with virtual teams for targets relevant to the EUCOM theater help them maintain perspective.

Wiesbaden: The European Technical Center (U//FOUO)

(U//FOUO) We drove on to Wiesbaden that evening. We met up with folks from the ETC for dinner (at a great restaurant - The Winkger (yes, the Vikinger)) to get to know a bit about each other and to help set the stage for Thursday's visit. Through a series of briefings we gained a good perspective on the critical role ETC plays in the enterprise and gained an appreciation of how we can work together to benefit the enterprise. We also held a town meeting with the ETC team where I reiterated what a great job they are doing with customers, partners, and Third Party relationships.

Impressions (U)

(U//FOUO) Throughout the visit, the knowledge and insights our personnel gain by being "forward" in the customer's domain was evident. Even more impressive was how their knowledge of other operations centers, such as NSA HQ, the Cryptologic Centers, SCS, mission ground stations - just to name a few - was being leveraged to respond to the needs of the EUCOM customer. By knowing how the cryptologic system operates, and knowing how to insert requirements, our personnel are able to make significant contributions to the cryptologic enterprise. In addition, they grow professionally and personally - by seeing our Agency from a different perspective, gaining a broader understanding of how we're viewed, and by experiencing life in a different culture.

(U//FOUO) For more details about NCEUR type "go nceur" on your web browser!

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

(U) CLASSIFICATION GUIDE FOR SIGINT Material Dating from 16 August 1945 - 31 December 1967

Effective Date: 21 December 2011

Revised Date(s): 24 February 2012, 13 April 2012
25 April 2012

CLASSIFIED BY: [redacted]
Intelligence Director

REASON FOR CLASSIFICATION:
1.4(c), 1.4 (d)

DECLASSIFY ON: *75 years from date of material or event, as indicated

ENDORSED BY: [redacted]
Deputy Associate Director for Policy and Records

(U) Change Register

Change No.	Change	Date Made mm/dd/yy	By (initials)
1	Numerous administrative changes were made to clarify certain guidance, correct some errors in dates, revise the proposed exemption categories, and correct typos.	02/24/12	SLS
2	Entry 24 was amended to account for two specific exceptions.	4/13/12	SLS
3	Entry 3 was amended to bring it in line with previous guidance regarding intercept or reference to specific intercept of belligerent or non-belligerent communications through 31 December 1946	4/25/12	SLS

(U) Classification Guide for SIGINT Material Dating Prior to 1 January 1968

(U) PUBLICATION DATE:

(U) OFFICE OF ORIGIN: SID

(U//FOUO) POC: [redacted] S02

(U) PHONE: [redacted]

(U) ORIGINAL CLASSIFICATION AUTHORITY:
SIGINT Director, [redacted]

(U) This classification guide describes the SIGINT material that is dated from 16 August 1945 – 31 December 1967 and warrants protection for more than 50 years. It supersedes all prior guidance relating to material originating during this timeframe. This guidance pertains to NSA/CSS as well as to its predecessor organizations.

Description of Information	Classification/Markings	Reason	Declass	Remarks
1. (U) All sources- and methods-related metadata added to SIGINT product reports by NSA/CSS or included in NSA/CSS metrics reports	CONFIDENTIAL//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U//FOUO) This includes information such as SIGINT addresses (SIGADs), Producer Designator Digraphs (PDDGs), Case Notations (CASNs), *RASIN* Manual designators, intercept designators, SRIs, Crypt *System Title*s, Intelligence Source Indicators (ISIs), Time of Intercept (TOI), Communications Lanes (foreign FROM/TO entities), Message Telex numbers assigned by foreign target, number of messages collected for a specific target, number of messages decrypted for a specific target, etc. (U) Exceptions: For the period of the Vietnam conflict (through 31 December 1967) – all metadata for otherwise releasable reports in which the targeted entity was a participant in the Vietnam conflict is UNCLASSIFIED. (U//FOUO) The methodologies used by

				NSA/CSS to log, track, account for, and analyze collection prior to 1968 are still used today. Revealing this "who," "when," "where," and "how" could provide an adversary with a great deal of insight into NSA's targets, collection sites, and other collection- and analysis-related information that is still being used today. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
2. (S//NF) Information revealing the fact of NSA/CSS targeting, collecting, or processing the communications of these specific foreign countries/international organizations: - Algeria after 31 Dec 1946 - Belgium after 31 Dec 1946 - France after 31 Dec 1946 - Germany (i.e., West Germany) after 31 Dec 1946 - Netherlands after 31 Dec 1946 - Norway after 31 Dec 1946 - Saudi Arabia after 31 Dec 1946 - Sweden after 31 Dec 1946 - Tunisia after 31 Dec 1946 - Turkey after 31 Dec 1946 - Taiwan (Formosa) after 31 Dec 1949 - Italy after 31 Dec 1947 - Jordan after 31 Dec 1947 - Denmark after 31 Dec 1953 - South Korea after 31 Dec 1953 - Japan after 31 Dec 1954 - Austria after 31 Dec 1955 - Israel for any timeframe (see	SECRET//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U) The fact of NSA/CSS targeting, collecting, or processing against any nation not listed as classified ***through 1967*** is UNCLASSIFIED. (U) Revealing these specific targets will enable adversaries to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the communications systems used then and those used today, the targets can adopt blanket denial practices not currently used because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS. In addition, certain historical targets are also (and were in the timeframe covered by this guide) SIGINT partners, and revealing that NSA/CSS targeted nations that are current partners could have an immediate negative effect on those relationships. (U) The fact that NSA/CSS processed intercepted Israeli communications during the USS Liberty incident (24

remark for specific exception) - Pakistan for any timeframe - Singapore for any timeframe - all international organizations				May – 8 June 1967) is UNCLASSIFIED. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
3. (S//NF) Information revealing the fact of NSA/CSS targeting, collecting, or processing the communications of a Second Party country	SECRET//NOFORN	75X1 75X3 75X6 75X9	*75 years from either the date of material or the end of the partnership, whichever is longer	(S//NF) Second Party partnerships are among NSA/CSS's strongest, oldest, and most important. Revealing the fact that NSA/CSS targeted their communications at any time would most likely have serious implications for, and could cause irreparable damage to, the partnerships. (U) Serious damage to national security can be expected if this material were to be declassified.
4. (U) The identities of specific NSA/CSS Third Party SIGINT partners	SECRET//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) NSA/CSS's Third Party partners provide NSA with unique and valuable insights on counterterrorism, combating proliferation, and regional stability issues. They also often provide NSA/CSS information about each other. Although they may suspect they were targets prior to 1968, their level of cooperation with NSA is expected to diminish if it became a known fact. Conversely, if information that NSA/CSS has relating to these countries that is outside the scope of the partnerships were to be released, the countries could gain insight into NSA's other SIGINT capabilities, and could also become aware of information that NSA/CSS has not been sharing. The future of NSA/CSS's Third Party SIGINT foreign partnerships would be at stake.

				(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
5. (U) The fact that NSA/CSS shared particular SIGINT material with a specific Second Party partner, when the partner is identifiable	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6 75X9	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement, signed in 1946, mandates that the Second Parties respect each others' preferences in these cases. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
6. (U) The fact that NSA/CSS shared particular SIGINT material with a specific Third Party partner, when the partner is identifiable	SECRET//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) NSA/CSS's Third Party partners provide NSA with unique and valuable insights on counterterrorism, combating proliferation, and regional stability issues. If it were revealed that NSA/CSS shared particular information with specific Third Party partners (essentially revealing the countries with which it had Third Party SIGINT partnerships prior to 1968), the future of its Third Party SIGINT foreign partnerships would be at stake. (U) Serious or exceptionally grave damage to national security can be expected if

				this material were to be declassified, depending on the particular information being revealed.
7. (U) Information revealing NSA/CSS targeting, collecting, or processing diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual (post 31 December 1946)	SECRET//REL TO USA, FVEY at a minimum	50X1 50X3 50X7	*75 years from date of material	(U) Exceptions: - (U) diplomatic/leadership communications collected *during* ***and*** *related to* the Cuban Missile Crisis (1 January 1959-31 December 1963) are UNCLASSIFIED - (U) North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications related to the Vietnam conflict and collected between 1 January 1960 and 31 December 1975 are UNCLASSIFIED (U//FOUO) Indicating whose diplomatic/leadership communications NSA/CSS targeted, collected, and/or processed prior to 1968 would cause diplomatic challenges for the U.S., and could also enable a targeted country that is still using similar communications systems to change their systems, thereby denying NSA/CSS valuable intelligence. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
8. (U//FOUO) Information revealing NSA/CSS targeting, collecting, or processing of specific international commercial (ILC) communications (post 31 December 1946)	SECRET//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	(U//FOUO) Indicating whose ILC communications NSA/CSS targeted, collected, and/or processed prior to 1968 could also enable a target that is still using similar communications systems to change its systems, thereby denying NSA/CSS valuable intelligence.

				(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
9. (U) Information that contains or reveals foreign SIGINT partner equities	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6 75X9	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) This includes the basic "fact of" specific Third Party partnerships, names of personnel associated with partner organizations (Second or Third Party), indications of projects that were worked with specific foreign partners (Second or Third Party), collection locations in partner nations (Second or Third Party), etc. (U//FOUO) NSA/CSS's foreign partners provide NSA with unique and valuable insights on a wide variety of issues that are critical to U.S. national security (e.g., counterterrorism, combating proliferation, and regional stability). It is a given that they need to protect their equities as vehemently as NSA/CSS protects its own. If NSA/CSS were to release information that revealed the equities of its foreign partners (Second as well as Third Parties), the future of its SIGINT foreign partnerships would be at stake. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
10. (U//FOUO) Information revealing specific overseas collection and High-Frequency Direction Finding (HFDF) locations that remain open today	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or closure of site, whichever is longer	(U//FOUO) Revealing specific overseas collection and HFDF locations could adversely affect Third Party SIGINT partnerships and reveal NSA/CSS's HFDF capability strengths and weaknesses. Such revelations

				would identify NSA/CSS's Third Party partners and enable its adversaries to develop countermeasures against its strengths and exploit its weaknesses. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
11. (S//SI//REL TO USA, FVEY) The fact that NSA/CSS conducted/conducts covert SIGINT operations at unspecified officially flagged U.S. facilities abroad	SECRET//SI//REL TO USA, FVEY	75X1 75X3 75X6 75X7	*75 years from either the date of material or end of overall activity, whichever is longer	(S//SI//REL TO USA, FVEY) Revealing the fact that NSA/CSS conducted covert SIGINT operations from officially flagged U.S. facilities abroad would impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President).
12. (S//REL TO USA, FVEY) The association of a specific location with an SCS site, the existence of which is releasable to Second Party partners	TOP SECRET//SI//REL TO USA, FVEY	75X1 75X3 75X6 75X7	*75 years from either the date of material or end of overall activity, whichever is longer	(S//SI//REL TO USA, FVEY) Revealing that NSA/CSS conducted covert SIGINT operations from specific officially flagged U.S. facilities abroad would impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S.; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President).

				(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
13. (S//REL TO USA, FVEY) The association of a specific location with an SCS site that is NOFORN	TOP SECRET//SI//NOFORN	75X1 75X3 75X6 75X7	*75 years from either the date of material or end of overall activity, whichever is longer	(S//SI//REL TO USA, FVEY) Revealing that NSA/CSS conducted covert SIGINT operations from specific officially flagged U.S. facilities abroad would immediately impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President). (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
14. (U) Information revealing specific sources and methods used by NSA/CSS to target, collect, and/or process SIGINT and that are currently used today	CONFIDENTIAL//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U//FOUO) NSA/CSS uses the same sources and methods to obtain SIGINT today as it did prior to 1968. Revealing the specific sources and methods used by NSA/CSS to target, collect, and/or process SIGINT would enable targets to adopt blanket denial practices not used today because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS. (U) See Entry 31 for additional information.
15. (TS//SI//REL TO USA, FVEY) Information revealing the fact of, as well as details relating to, NSA/CSS conducting covert	TOP SECRET//SI//NOFORN	50X1 50X3 50X6	*75 years from date of material	(TS//SI//REL TO USA, FVEY) NSA/CSS's covert SIGINT activities, such as SIGINT enabling and the use

SIGINT activities, including material dealing with SIGINT enabling; cover plans, programs, and mechanisms; and/or clandestine SIGINT				of particular cover mechanisms, are much the same today as they were prior to 1968. Revealing the specific covert activities would nullify the particular programs where they are successfully used today. Targets would adopt blanket denial practices not used today because they simply do not appreciate how NSA/CSS's covert activities support SIGINT successes. (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
16. (U) *TICOM* documents dated prior to 31 December 1967 where the acquired document was originally created by the U.S. or a Second Party partner and was in the possession of an "enemy" organization.	CONFIDENTIAL//REL TO USA, FVEY at a minimum	50X1 50X3 50X6 50X9	*75 years from date of material	(U) *TICOM* documents should only be released if they would have been released by the U.S. or Second Party directly. (U) *TICOM* documents that may be declassified and released include acquired code books and the description of applications of techniques to cryptographic systems. (U//FOUO) *TICOM* was a joint Five Eyes effort. NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement mandates that the Second Parties respect each others' preferences in these cases.

				(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
17. (U) *TICOM* interrogation reports	CONFIDENTIAL//REL TO USA, FVEY, at a minimum	50X1 50X3 50X6 50X9	*75 years from date of material	(U) *TICOM* documents should only be released if they would have been released by the U.S. or Second Party directly. (U) In some cases, *TICOM* interrogation reports remain not releasable due to *BRUSA* agreements to protect personal information whose release could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person. (U//FOUO) *TICOM* was a joint Five Eyes effort. NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement mandates that the Second Parties respect each others' preferences in these cases. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
18. (U) ELINT material related to radar/weapons systems that are still used today	S//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	(U//FOUO) Many of the collection and exploitation methods used prior to 1968 continue to be employed in the Intelligence Community.

				Declassifying ELINT material that is 50 years old (and older) would enable adversaries, who do not appreciate how well their signals are currently being exploited by NSA, to ascertain those collection and analysis techniques and subsequently adopt denial practices that could preclude further intelligence exploitation. Such denial would hamper intelligence of the modification of old systems as well as the newest ones. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
19. (U//FOUO) A single ELNOT or list of ELNOTs or designators that equate to specific radars, including those from weapons systems, or similar non-communications signal devices weapons system when associated with amplifying data that identifies the emitter radar, weapon system, country of origin, or ELINT signal acquisition method.	CONFIDENTIAL//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	(U//FOUO) This category includes information equating a specific ELNOT with a specific radar nickname, such as a NATO nickname, or a radar model number. (U//FOUO) A single ELNOT or list of ELNOTs or designators, e.g., B329A, 1222Z, T6090, 123MZ, when used **without** amplifying data that identifies the emitter radar, weapon system, or country of origin, or ELINT signal acquisition method is UNCLASSIFIED (C//REL TO USA, FVEY) Examples: - the fact that P307Z and P334A emanate from the Crotale surface-to-air missile is classified CONFIDENTIAL//REL TO USA, AUS, CAN, GBR, NZL - the fact that A427B emanates from SLOT BACK radar is

				CONFIDENTIAL//REL TO USA, AUS, CAN, GBR, NZL (U//FOUO) Many of the collection and exploitation methods used prior to 1968 continue to be employed today. Declassifying ELINT material that is 50 years old (and older) would enable adversaries, who do not appreciate how well their signals are currently being exploited by NSA, to ascertain those collection and analysis techniques and subsequently adopt denial practices that could preclude further intelligence exploitation. Such denial would hamper intelligence of the modification of old systems as well as the newest ones. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
20. (U//FOUO) FISINT-related material (i.e., information related to collection, processing, and analysis of telemetry and beacons, command uplinks, video data links, tracking, and arming/fusing/command signals as well as reporting based on said data types)	SECRET//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	(U) Exceptions: - Refer to the following Information Management Instructions (IMIs) for guidance on specific UNCLASSIFIED FISINT-related information: - DEFSMAC IMI ([redacted]) - Soviet Deep Space Telemetry Collection IMI ([redacted]) (U//FOUO) FISINT activity began in 1956, and amounts to information that weapons designers use to verify weapon system performance capabilities. The exact

				collection and exploitation methods used from that time are still being used successfully today. (U//FOUO) Declassification of FISINT-related material that is 50 years old and older would show NSA/CSS's ability to fully exploit the data, even with the lack of an identification key and poor signal quality, and likely lead to widespread data denial practices among target countries who do not currently appreciate how well their signals are currently being exploited by NSA. This would deprive the U. S. of vital knowledge of foreign weapons and space systems, which in turn would ultimately lead to policy decisions being made on faulty/incomplete data and to increased loss of life and mission failure during future military operation. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
21. (U//FOUO) SIGINT material pertaining to counterespionage efforts that reveal NSA/CSS knowledge, exploitation, and analysis of adversaries' tradecraft that is still being used today	TOP SECRET//SI//NOFORN	50X1 50X3 50X6	*75 years from date of material	(C//REL TO USA, FVEY) Foreign intelligence services' tradecraft is unique to the individual service. Declassifying information indicating that NSA/CSS has successfully exploited their activities, or that it understands their methodologies, would enable the adversaries to refine or alter their practices to the point where it might be denied the information/access entirely (an example would be cover names of agents of an adversary's intelligence service). Adversaries'

				underlying tradecraft (including communications methods and patterns, and all aspects of recruitment and handling of agents) generally remains the same over time, and must be protected in order to maintain NSA/CSS's ability to exploit it. In addition, such material may reveal the identities of a person, or the cooperation of a still-living person, who was the source of information for evidence that was compiled against spies who were later arrested, causing that person's life to be in jeopardy. (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
22. [redacted]	[redacted]	[redacted]	[redacted]	[redacted]

				declassified, depending on the particular information being revealed.
23. [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
24. [redacted]	[redacted]	[redacted]	[redacted]	[redacted]

				[redacted]
25. (U) SIGINT serialized Product Reports that contain *cryptologic information*	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologics used then and those used today, a straightforward interpolation would allow the target who builds and uses *indigenous logics* to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation. When NSA/CSS releases a selected target's decrypts, it has already seen substantive changes in that target's use of cryptography.

				(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
26. (U) SIGINT serialized Product Reports consisting of or containing decrypts for the *Soviet Bloc* or People's Republic of China for the period 1 January 1951 through 31 December 1967	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(S//SI//REL TO USA, FVEY) SIGINT serialized product reports for the *Soviet Bloc* or People's Republic of China consisting of or containing decrypts for the period 16 August 1945 through 31 December 1950 are UNCLASSIFIED, as long as all relevant sources- and methods-related metadata has been redacted. (U//FOUO) Relevant sources- and methods-related metadata includes post-*BRUSA system title*s, which did not exist until 1946 and comprised a combination of four or more letters and/or numbers. In addition, it includes case notations, *RASIN* Manual designators, and intercept designators, which are not strictly cryptanalytic, but have relevance to cryptanalytic equities. (U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual **- for any timeframe -** remain classified, **except** for those decrypted using techniques declassified in the versions of Military Cryptanalytics I and II, written by [redacted]

				released by NSA, that were collected during **and** related to the Cuban Missile Crisis (1 January 1959-31 December 1963), and North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications collected prior to 31 December 1975, which are UNCLASSIFIED. (C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologics used then and those used today, a straightforward interpolation would allow the target who builds and uses *indigenous logics* to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
27. (U) SIGINT serialized Product Reports consisting of or containing decrypts for North Korea for the period 1 July 1951 through 31 December 1967	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(S//SI//REL TO USA, FVEY) SIGINT serialized product reports for North Korea consisting of or containing decrypts for the period 16 August 1945

				through 30 June 1951 are UNCLASSIFIED, as long as all relevant metadata, including sources- and methods-related information, has been redacted. (U//FOUO) Relevant sources- and methods-related metadata includes post-*BRUSA system title*s, which did not exist until 1946 and comprise a combination of four or more letters and/or numbers. In addition, it includes case notations, *RASIN* Manual designators, and intercept designators, which are not strictly cryptanalytic, but have relevance to cryptanalytic equities. (U) All reports by Korea-based field units based on the exploitation of manual codes and ciphers, provided they make no connection to encrypted communications, during and related to the Korean War, 25 June 1950 – 31 December 1953 are UNCLASSIFIED. (U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual - **for any timeframe** - remain classified, **except** for those decrypted using techniques declassified in the versions of Military Cryptanalytics I and II, written by [redacted] and officially released by NSA, that were

				collected during **and** related to the Cuban Missile Crisis (1 January 1959-31 December 1963), and North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications collected prior to 31 December 1975, which are UNCLASSIFIED. (C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologics used then and those used today, a straightforward interpolation would allow the target who builds and uses *indigenous logics* to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
28. (U) SIGINT serialized Product Reports consisting of or containing decrypts for any other target (i.e., not *Soviet Bloc* or People's Republic of China from 1 Jan 1951-31 Dec 1967, not North Korea from 1 July 1951-31 Dec 1967) for the	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or

				target's decrypts, it has already seen substantive changes in that target's use of cryptography. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
29. (U) *Alphabet Generators*: Documents that demonstrate or include the application of any cryptanalytic technique relating to *Alphabet Generator* systems that became operational *after* 15 August 1945	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U) A document that demonstrates or includes the application of any cryptanalytic technique to an electromechanical cipher system that is an *alphabet generator* is UNCLASSIFIED only if the system is UNCLASSIFIED in accordance with the WWII Guidance. (U) This guidance pertains to documents relating to: • Wired wheels (such as ENIGMA), • Telephone selectors (such as PURPLE, RED, JADE, and CORAL), and Hagelin *alphabet generators*. (C//REL TO USA, FVEY) In this time frame, commercial companies and nation states developed and deployed cryptographies which have many features still in use in cryptosystems NSA/CSS exploits today. Documents that detail the application of cryptanalytic techniques to these earlier systems will reveal capabilities still in use today against operational target cipher systems. (U) Various levels of harm to national security can be expected if this material were

				to be declassified, depending on the particular information being revealed.
30. (U) Cryptosystems Other Than *Alphabet Generator*s: Documents that demonstrate or include the application of a cryptanalytic technique to any cipher system other than an *alphabet generator*	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U) This guidance includes documents relating to any electromechanical systems that are *key generator*s, to include Hagelin *key generators* and TUNNY. (U) **Exception:** When a document only contains specific previously declassified techniques applied to a *low-grade* or *medium-grade* cryptographic system, the document will be UNCLASSIFIED unless it deals with the application of *depth reading* or *depth-reading* techniques. Previously declassified techniques are those declassified in the versions of Military Cryptanalytics I and II, written by [redacted], officially released by NSA. (U) *Cryptanalytic worksheets* remain classified if they: – are for *key generators*, and/or – indicate *depth* or *depth-reading* techniques (e.g., have different cipher texts associated with the same key) – are associated with a specific operational target (C//REL TO USA, FVEY) In this time frame, commercial companies and nation states developed and deployed cryptographies which have many features

				still in use in cryptosystems NSA/CSS exploits today. Documents that detail the application of cryptanalytic techniques to these earlier systems will reveal capabilities still in use today against operational target cipher systems. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
31. (TS//SI//REL TO USA, FVEY) Commercial Cryptanalytic Relationships: Documents that contain information that implies that commercial companies cooperate with NSA/CSS or Second Party partners to render their products exploitable from a cryptanalytic standpoint	TOP SECRET//SI//REL TO USA, FVEY	75X1 75X3 75X6 75X9	*75 years from either the date of material or end of the relation-ship, whichever is longer	(U) Such documents may also be compartmented. (TS//SI//REL TO USA, FVEY) Exposure of any company's commercial cryptanalytic relationship with NSA/CSS, even for a company no longer in existence, will damage NSA/CSS's credibility with current companies who are approached for assistance. Exposure of even decades-old commercial cryptanalytic relationships may cause significant harm to the company's reputation and financial status. (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
32. (C//REL TO USA, FVEY) Commercial Information Security Devices: Documents containing details of commercially available cryptographic algorithms, information security devices, or systems that identify an actual vulnerability not currently publicly known, or details relating to NSA/CSS exploitation of a publicly known vulnerability	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(C//REL TO USA, FVEY) Disclosing details of vulnerabilities or NSA/CSS's methods of choice for exploitation will allow commercial companies to fix those weaknesses in existing systems and avoid implementing them in future systems. Frequently, commercial companies make the same or similar mistakes through several generations of their products.

				(U) Information Security Devices provided to other countries by the U.S. Government are considered Commercial Information Security Devices. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
33. (U) *Indigenous* Information Security Devices: Documents containing details of *indigenous* cryptographic algorithms, information security devices or systems	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(C//REL TO USA, FVEY) For *indigenous* security devices or systems, any documents revealing NSA/CSS's knowledge of the cryptography of those devices will risk its ability to diagnose and exploit these devices, and in some cases, knowledge it received from sensitive HUMINT sources. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
34. (U//FOUO) Signal designators when combined with <u>any</u> details that would reveal a target user/country or when associated with cryptanalytically relevant information, such as UKUSA nicknames, coverterms, or any targeting, collection, or exploitation details	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U//FOUO) Examples of signal designators include *RASIN* Manual designators and *TEXSIG*s. (U//FOUO) Signal designators with no indication of target user or country are UNCLASSIFIED. (U) This information is directly linked to NSA/CSS sources and methods for collection and processing. The Second Party standards and notation developed under UKUSA are still in use today. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending

				on the particular information being revealed.
35. (U//FOUO) Documents dated after December 31, 1956 that demonstrate or include the application of a signals analytic technique to any digital or digitized system	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	[redacted]
36. (S//REL TO USA, FVEY) Information identifying specific organizations or government agencies that facilitated NSA/CSS *close access* operations	SECRET// REL TO USA, FVEY	50X1 50X3	*75 years from date of material	(U) These organizations may be U.S. companies, specific units within a U.S. government agency, U.S. national laboratories, or U.S. academic institutions. (S//REL TO USA, FVEY) Revealing the organizations that facilitated *close access* operations would have a high probability of causing harm to current operations in which those organizations continue to have a role or had a role in the past (even if the organization is now defunct). (U) Serious damage to national security can be expected if this material were to be declassified.
37. (S//REL TO USA, FVEY) The fact that NSA/CSS has successfully conducted and has an organization devoted to *close access* operations	SECRET// REL TO USA, FVEY	50X3	*75 years from date of material	(S//REL TO USA, FVEY) The exact collection and exploitation methods used prior to 1968 are still being used successfully today. Declassifying *close access*

				material that is 50 years old (and older) will enable targets to adopt blanket denial practices not used today because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS. (U) Serious damage to national security can be expected if this material were to be declassified.
38. [redacted]	[redacted]	[redacted]	[redacted]	[redacted]

				magnetometers, accelerometers, and commercial microphones. This includes information dealing with receivers and the use of radar systems against mechanical or electromechanical office equipment, as well as tools/techniques no longer being used (such as magnetometers, accelerometers, audio signals, power and/or signal line clamps) and that have little chance of future use. (S//REL TO USA, FVEY) Indications that NSA has knowledge of specific and/or unusual parameters, or of NSA's capabilities, could provide information that could be used to understand and counter the collection capability. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
39. (S//REL TO USA, FVEY) Information describing concealment /camouflage techniques for sensors/systems used in NSA/CSS *close access* operations	SECRET//SI// REL TO USA, FVEY at a minimum	50X3 50X6	*75 years from date of material	(U) While removal of such sensors/systems is desired once a facility is no longer of interest, is not always feasible. Inadvertent discovery of such systems/sensors could jeopardize future operations and/or raise questions about or point to NSA's involvement. (U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
40. (S//REL TO USA, FVEY) Information that identifies a	TOP SECRET//SI// REL TO USA, FVEY at a minimum	50X3 50X6	*75 years from date	(S//REL TO USA, FVEY) Covert or clandestine

specific target, contains details or parameters relating to specific targets, and/or contains details that could possibly identify a covert or clandestine listening post used by NSA/CSS			of material	Listening Posts (LPs) are physical locations that are close to the target facility and serve as a collection point for the signals of interest. Identification of a LP could result in the identification of information such as the identities of cooperating parties/people. Exposure of such information could adversely impact current and future operations by revealing information about partner relationships. (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
41. (S//SI//REL TO USA, FVEY) Details, including the "fact of," regarding NSA/CSS collection capability against Short Duration Signals (SDS)	SECRET//SI//REL TO USA, FVEY	50X3 50X6	*75 years from date of material	(S//SI//REL TO USA, FVEY) The methods used to exploit SDS signals and radio fingerprinting are basically the same today as they have been during the period of interest. Specific details regarding how NSA/CSS exploits such signals, as well as the physical locations where it may access them, would provide adversaries information they need to deny them to NSA/CSS. Targets of interest could develop countermeasures that would render NSA/CSS's current capability to collect SDS ineffective. (U) Serious damage to national security can be expected if this material were to be declassified.
42. (U//FOUO) Details regarding NSA/CSS ability to perform radio fingerprinting	SECRET//SI//REL TO USA, FVEY	50X3 50X6	*75 years from date of material	(S//REL TO USA, FVEY) The methods used to perform radio fingerprinting are basically the same today as they have been during the period of interest. Specific details regarding how NSA/CSS exploits such signals, as well as the physical locations where it

				may access them, would provide adversaries information they need to deny them to NSA/CSS. Exception: The fact of, and details regarding, U.S. and South Vietnamese use of radio fingerprinting during the Vietnam Conflict (1 January 1960-31 December 1975) , as outlined in the Vietnam is UNCLASSIFIED. (U) Serious damage to national security can be expected if this material were to be declassified.

[redacted]

				[redacted]
45. (S//SI//REL TO USA, FVEY) Information regarding NSA/CSS ability to collect and process International Commercial (ILC), non-Second Party government agencies, non-government organizations, and proprietary communications in the radio frequency spectrum via FORNSAT or Terrestrial means	SECRET//SI//REL	50X3 50X6	*75 years from date of material	(S//SI//REL TO USA, FVEY) Fundamental targets have not changed over time and they continue to use the same basic method of communication. If the fact that NSA targeted these entities is released, the commercial providers, government, non-government, and proprietary entities can implement countermeasures that would degrade NSA/CSS's ability to collect and process these communications. (U) Serious damage to national security can be expected if this material were to be declassified.

***75 years from date of material or event, as indicated**: (U) This indicates that the information is classified for *75 years from date a document is created or until the end of the specified event.

ACRONYMS/DEFINITIONS:

Acoustic – (U) Signals related to the production and transmission of sound. Sound is not restricted to audio range signals

Alphabet Generator - (U) A cipher machine that generates a multiplicity of cipher alphabets from the interaction of two or more components. Compare to *key generator,* below.

BRUSA - (U) The 1946 agreement, now known as UKUSA. In Appendix B (of the 26 February 1946 version) the section on standardization describes the functional system to be used for the nomenclature of foreign cryptographic systems. This common system of nomenclature is now called UKUSA *system title*s.

Close Access - (S//REL TO USA, FVEY) Refers to the targeting, collection, and/or processing of unintentional emanations from information processing equipment, as well as a program to develop special unique sensors and systems to collect unintentional (compromising) *emanations* and/or signals from information processing equipment to exploit TEMPEST vulnerabilities. Keywords that could identify *close access* equities include (but are not limited to) transducer, radiation, conductance, BOOKLET, magnetic probe, *acoustic* probe, magnetometer, accelerometer, microphone, transmitted over copper wire, *emanations*, and unintentional *emanations*.

Cryptologic Information - (U) Information that describes the target's use of cryptographic techniques and processes or of cryptographic systems, equipment, and software and their functions and capabilities, and all cryptographic material.

Cryptanalytic Worksheets - (U) Any records that show methods of analysis of encrypted and/or enciphered information/data. This includes reports, working aids and papers, instructions, informal technical notes, manuals, technical exchange letters, handbooks, listings, collateral documents, procedure files, evaluation plans, specific documentation or records portraying steps, processes, tables, devices, and/or others means employed in cryptanalysis of target communications.

Depth - (U) Texts are said to be in a *depth* relationship when the texts were produced by encrypting two or more different sequences of plain text with the same sequence of key. Related terms include *depth reading/stripping*, flush depth, near *depth*, offset *depth*, partial *depth*, and slid *depth*.

Depth Reading/Stripping - (U) Recovery of plain text and key from messages in *depth*.

Electromagnetic - (U) Signals that are produced as a result of the use of electrical power

Emanations - (U) Unintentional signals, that, if intercepted and analyzed could disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. These signals may be *acoustic*, *electromagnetic*, or optical in nature

Generic - (U) Describes *emanations* and sensors in broad general categories e.g. magnetic, *acoustic*, power line/signal line conductance, electric field emissions or other naturally occurring phenomena. Sensors are transducers which convert physical or electromechanical signals into an electrical signal which can be collected and analyzed.

Indigenous Algorithm, Device, Logic, or System - (U//FOUO) Non-commercial cryptographic information security system, device or component developed by a SIGINT target for their use. *Indigenous* will include target modifications to commercial products and algorithms. If a target-developed version of a commercially available product is cryptographically indistinguishable from the commercial product, it will be considered commercial.

Key Generator - (U) A cipher machine that generates key from the interaction of two or more components. Compare to *alphabet generator*, above.

Listening Post - (U) Physical locations that are close to the target facility and serves as a collection point for the signals of interest

Low-Grade - (U) Pertaining to a cryptosystem which offers only slight resistance to cryptanalysis; for example:
(1) Playfair ciphers,
(2) Single transposition,
(3) Unenciphered one-part codes

Medium-Grade - (U) Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example:
(1) Strip ciphers,
(2) Double transposition,
(3) Unenciphered two-part codes

RASIN – (U) **Radio SIgnal Notation (RASIN)** – A notation assigned permanently and jointly by DIRNSA and second Party headquarters to a signal after basic signal characteristics have been verified by NSA/CSS or Second Party signals analysts

Soviet Bloc – (U) Cold War adversaries (Soviet Bloc) up to and including 1950:
Albania, Bulgaria, Czechoslovakia (after February 1948), East Germany (though the German Democratic Republic was

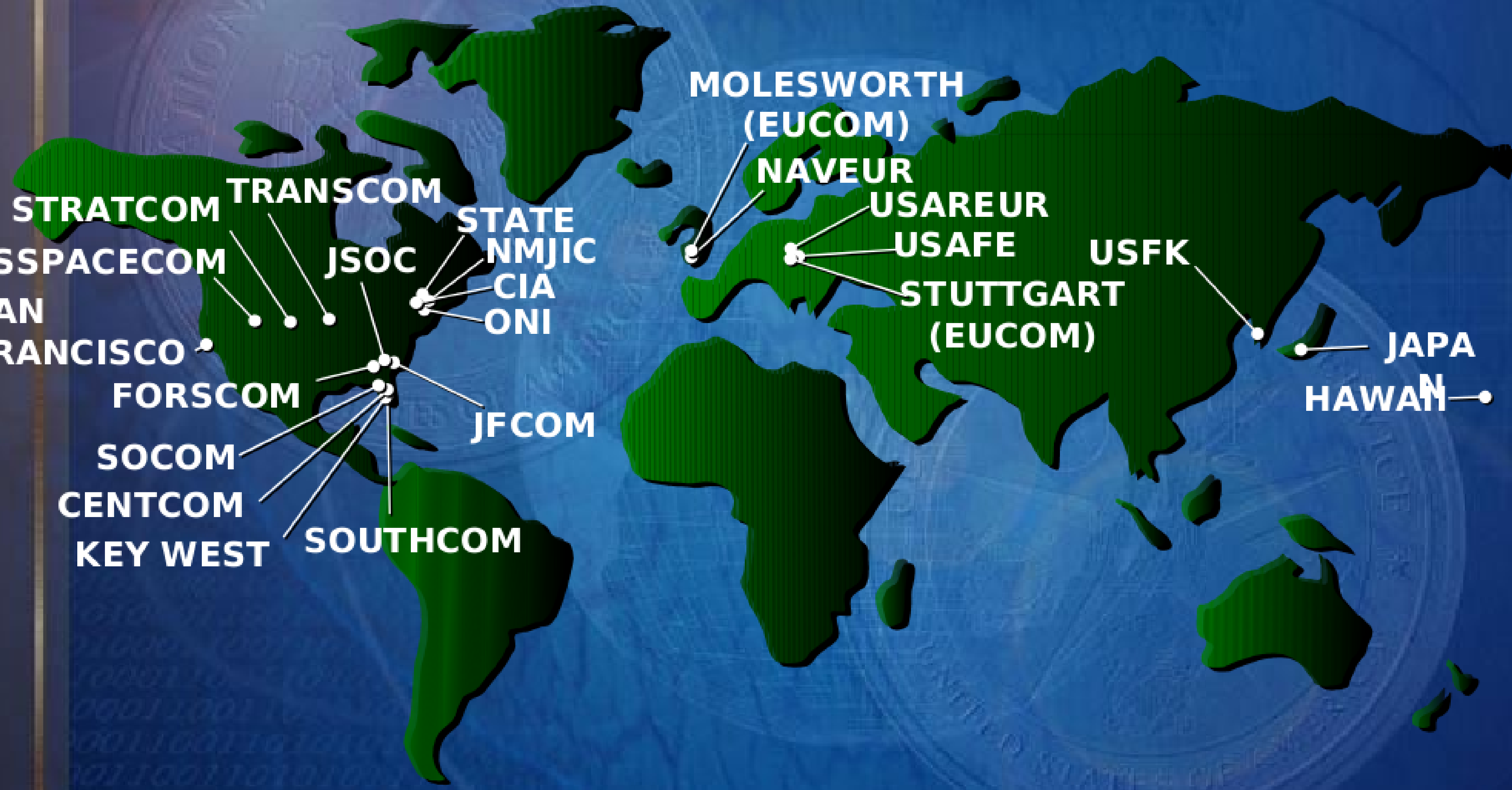
only established on October 1949, any prior German activities in the Soviet Zone should be considered as East German and within this definition), Hungary, Poland, Romania, USSR, Yugoslavia

System Title - (U//FOUO) Cryptographic system titles are short identification labels used to create a logical reference mechanism for all cryptographic systems and which identifies the users. Cryptographic system titles are assigned on the basis of cryptography, target country, and entity.

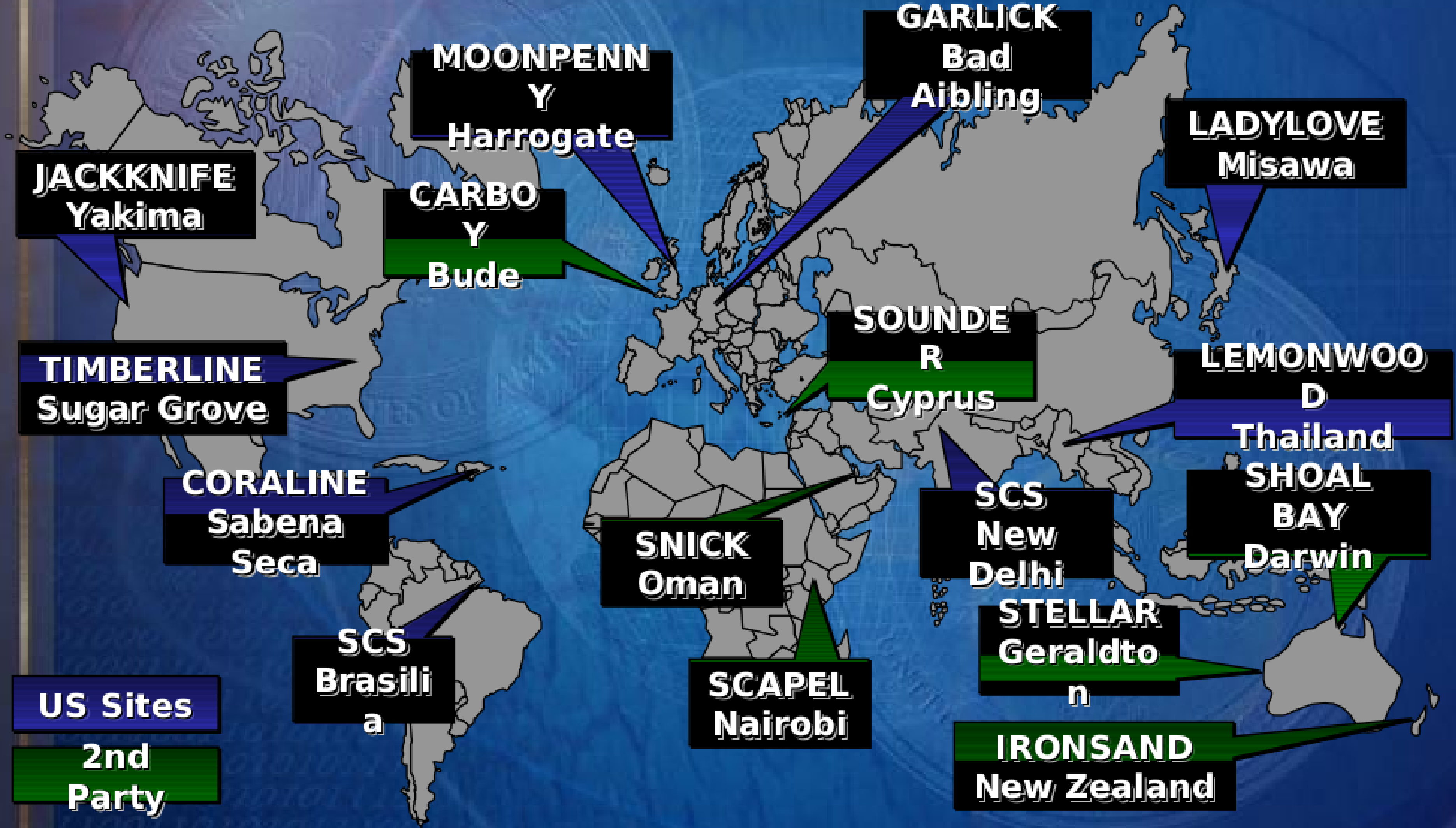
TEXSIG – (U//FOUO) **Technical EXtracts of SIGnals (TEXSIG)** – A unique designator assigned to a new signal by a SIGINT field element (USSS or Second Party) or to a signal under analysis or cryptanalytic development by the headquarters of NSA/CSS and Second Parties (jointly assigned)

TICOM - (U) **Target Intelligence Committee (TICOM)** - TICOM was formed in London in October 1944 as a joint U.S./UK activity to interrogate captured enemy COMINT personnel and to acquire enemy COMINT records and equipment.

CRYPTOLOGIC SERVICES GROUPS (CSGs)



PRIMARY FORNSAT COLLECTION OPERATIONS



GARLICK
Bad Aibling

MOONPENNY
Harrogate

LADYLOVE
Misawa

JACKKNIFE
Yakima

CARBOY
Bude

SOUNDER
Cyprus

TIMBERLINE
Sugar Grove

LEMONWOOD
Thailand

SHOAL BAY
Darwin

CORALINE
Sabena Seca

SNICK
Oman

SCS
New Delhi

STELLAR
Geraldton

SCS
Brasilia

SCAPEL
Nairobi

IRONSAND
New Zealand

🟦 US Sites

🟩 2nd Party

K. (S//SI//REL) NSA Presence - For the following locations, the fact of NSA personnel assigned to these sites/activities is UNCLASSIFIED. It is therefore UNCLASSIFIED, for example, to display plaques from these organization/locations. However, the fact that SIGINT may have been performed at these sites or that they may have been former A5 sites is CLASSIFIED.

(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremerhaven, Germany (Freedom through Vigilance USAF Security Service)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]

(U) [redacted] (A Remote Operations Facility)
(U) [redacted]
(U) Herzogenaurach, Germany ((Strength through knowledge) 16th USASA Field Station)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) NSA Europe, Frankfurt, Germany
(U) NSA Europe, Stuttgart
(U) [redacted]
(U) Naval Security Group Activities (NSGAs) at Bremerhaven, Germany; [redacted] and [redacted]
(U) Rothwesten, Germany
(U) [redacted]

(S//SI//REL) Trying to Find Potential Matches for a Garbled or Misspelled Name? Get Help from NYMROD

FROM: [redacted]
Project Director, Center for Content Extraction (T1221)
Run Date: 06/11/2008

(S//SI//REL) Have you ever had trouble finding out more about a SIGINT target with a garbled or misspelled name? The NYMROD system was invented to help with just that problem. The NYMROD name-matching system, developed by the Center for Content Extraction (CCE), can accept queries consisting of personal names, perform a "fuzzy" match of the input name to one or more sets of stored names, and return a list of potential matches for presentation to the user. NYMROD finds potential name matches without wildcards and can match across scripts (for example, between Arabic and Roman scripts).

(S//SI//REL) NYMROD's first sets of names stored for matching have all been taken from intelligence reports from NSA, CIA, and DoD databases, with CREST (transcript database) names coming on-line soon. Since its initial release in January 2008, analysts have been using NYMROD to find information relating to targets that would otherwise be tough to track down. The user interface is very simple: you just type in the name you are looking for, set a matching threshold from 0.1 (very tolerant of differences) to 1.0 (exact match), select the datase(s) you want to search within, and submit the query. The results presentation will allow you to browse the snippets of text that contained the matched name. You can try out this capability for yourself if you "go NYMROD" in your web browser.

(S//SI//REL) "But I don't want yet another tool!", many of you have said, and the CCE has taken this to heart. NYMROD also offers a web service that other systems can use to create their own datasets and perform matching queries. We are working with partners such as the Target Knowledge Base, the Unified Targeting Tool, and FASTSCOPE to begin integrating the service into those systems so that its operation is available to their users without anyone having to leave their normal work environment. Developers can find more information about NYMROD's web service, including an Interface Control Document, on the CCE's documentation web page.

(U//FOUO) NYMROD's performance is monitored using a quality-assurance process. We work closely with our commercial and R6 technology suppliers to continuously improve the underlying matching software so that we can offer performance enhancements with each quarterly release of NYMROD. Our April 2008 release made large strides in performance on Arabic names, while the upcoming release in July will offer greatly improved Chinese name matching. The CCE welcomes your feedback and inquiries. Please contact us at any time using the CCE_HELP e-mail alias.

Human Language Technology

Center for Content Extraction

Chartered to distribute multi-lingual *Content Extraction Services* to NSA enterprise applications supporting and enhancing 6 analytic functions:

- Selection
- Translation
- Analysis
- Investigative Research
- Retrieval
- Storage

Project Director: [redacted]

Technical Leader: [redacted]

T1221
July 2008

Nymrod Mission

What analytic problems is Nymrod trying to address?

- We need to search for the target behind what's been extracted (find reported information about targeted persons)
- HUMAN beings are central to most targets
- We need to cope with linguistic variation among entity names (esp Person names)
- We need to resolve Entity "coreference" problems using contextual information ("Evidence")

Top 10

Most Frequent Mentions in Anchory Reports for the Previous Week

[redacted] [redacted]
(TS) 33 reports

[redacted]
(TS) 18 reports

[redacted] [redacted]
(TS) 13 reports

[redacted] [redacted]
(TS) 12 reports

[redacted]
(TS) 11 reports

BAN KI-MOON
U.N. Secretary General
(TS) 11 reports

[redacted] [redacted]
(TS) 11 reports

[redacted]
(TS) 11 reports

[redacted] [redacted]
(TS) 10 reports

[redacted]
(TS) 10 reports

[redacted]
(TS) 10 reports

[redacted] [redacted]
(TS) 10 reports

(S//SI//REL) NSAers Make First-Ever Visit to FORNSAT Collection Site in Schöningen, Germany

FROM: [redacted]
Joint SIGINT Activity (H52G)
Run Date: 10/31/2006

(U) Visitors impressed with software demos.

(S//SI//REL) This summer Special United States Liaison Activity Germany (SUSLAG) and Joint SIGINT Activity (JSA) representatives, along with Counterterrorism analysts from S2I, became the first US visitors at Schöningen, a Bundesnachrichtendienst* (BND) FORNSAT collection site located in northern Germany.

(S//SI//REL) During these visits, BND senior site managers and analysts provided briefings on their mission, site manning, technical capabilities, as well as current and advanced analytic tools and techniques. These visits in June and July provided insights into the BND's collection, processing, and analytic capabilities, and promoted the close technical partnership between JSA and the BND.

(S//SI//REL) Before the reunification of Germany, Schöningen (located on the former East-West German border) collected East German radar, radio, and microwave communications. When Germany reunified in 1990, BND personnel at Schöningen were forced to recreate their role and mission. Schöningen did so proudly, and now plays a key role in the BND's Counterterrorism (CT) and Force Protection efforts by collecting mobile communication systems (specifically Thuraya, INMARSAT, and GSM).

(S//SI//REL) Today, Schöningen is manned with approximately 100 personnel. There [redacted]

(S//SI//REL) Schöningen personnel focus on development and production of voice and facsimile traffic collected from Thuraya, INMARSAT and GSM. Schöningen collects over 400,000 Thuraya cuts per day, 14,000 INMARSAT cuts and 6,000 GSM cuts from both the [redacted] network. E-mail is also collected at site, with an average of 62,000 collects per day. NSA benefits from this collection, especially the Thuraya intercepts from [redacted] which the BND shares on a daily basis.

(S//SI//REL) Site analysts and linguists are responsible for evaluating collected traffic, transcribing voice cuts and forwarding raw cuts on to their HQS for further evaluation and reporting. To improve their collection and SIGDEV capabilities, site engineers have developed several systems to improve BND call-chaining capabilities, data-viewing of voice and fax data, and data-forwarding to BND HQS. Development efforts at a field site are unusual for BND, and it was interesting to learn about these on-site efforts.

(S//SI//REL) The second visit by JSA and NSA Headquarters analysts represented the first technical exchange with BND Schöningen. US analysts were shown several BND analytic tool suites, some of which were under development. BND contract software developers and analysts sought regular feedback on the utility of these tools and techniques. These tool suites, such as MIRA 4, integrate multiple database analytic functions (such as viewing voice and listening to fax), much like NSA Headquarters has UIS (User Integrated Services). In some ways, these tools have features that surpass US SIGINT capabilities. Among a series of interesting items, NSA analysts noted that BND analysts could seamlessly move from VERAS (call-chaining software) to the associated voice cuts. BND Schöningen also performed geolocational selection of mobile communicants. For instance, they could define any particular geographical area, like [redacted], and select any communicant that dwelled in that area for several minutes.

(S//SI//REL) BND Schöningen developers also demonstrated a software prototype that uses Social Network Analysis algorithms against metadata to discover and assess target groups among other things, looking for information flow. The goal (at least in part) was to monitor these targets in the background within analyst-set parameters, with alerts to notify the analyst when any anomalous measurement appeared, and potentially to steer front-end collection. They claimed to have some successes on small groups on which they had good collection.

(S//SI//REL) They seemed interested in also characterizing movement patterns on geocoordinates to find persons such as couriers (terrorist or otherwise), then using that characterization for SIGDEV discovery purposes and predictive (trend) analysis. BND also showed us that they are interested not only in selection based on movement patterns or network structures, but also in hardware changes. They used a variety of algorithms (such as fuzzy logic) to discover these patterns. The BND responded positively to NSA's request for a copy of MIRA4 and VERAS software, and made several requests from NSA concerning target and tool development and data.

(S//SI//REL) This first series of meetings represents a new level of engagement for NSA and its German partner. We hope that this dialogue continues, and makes each partner more capable of satisfying common SIGINT requirements.

(U) Notes:
* BND = Federal Intelligence Service

(U//FOUO) This article is reprinted from the *Foreign Affairs Digest*, September edition.

Special Collection Service

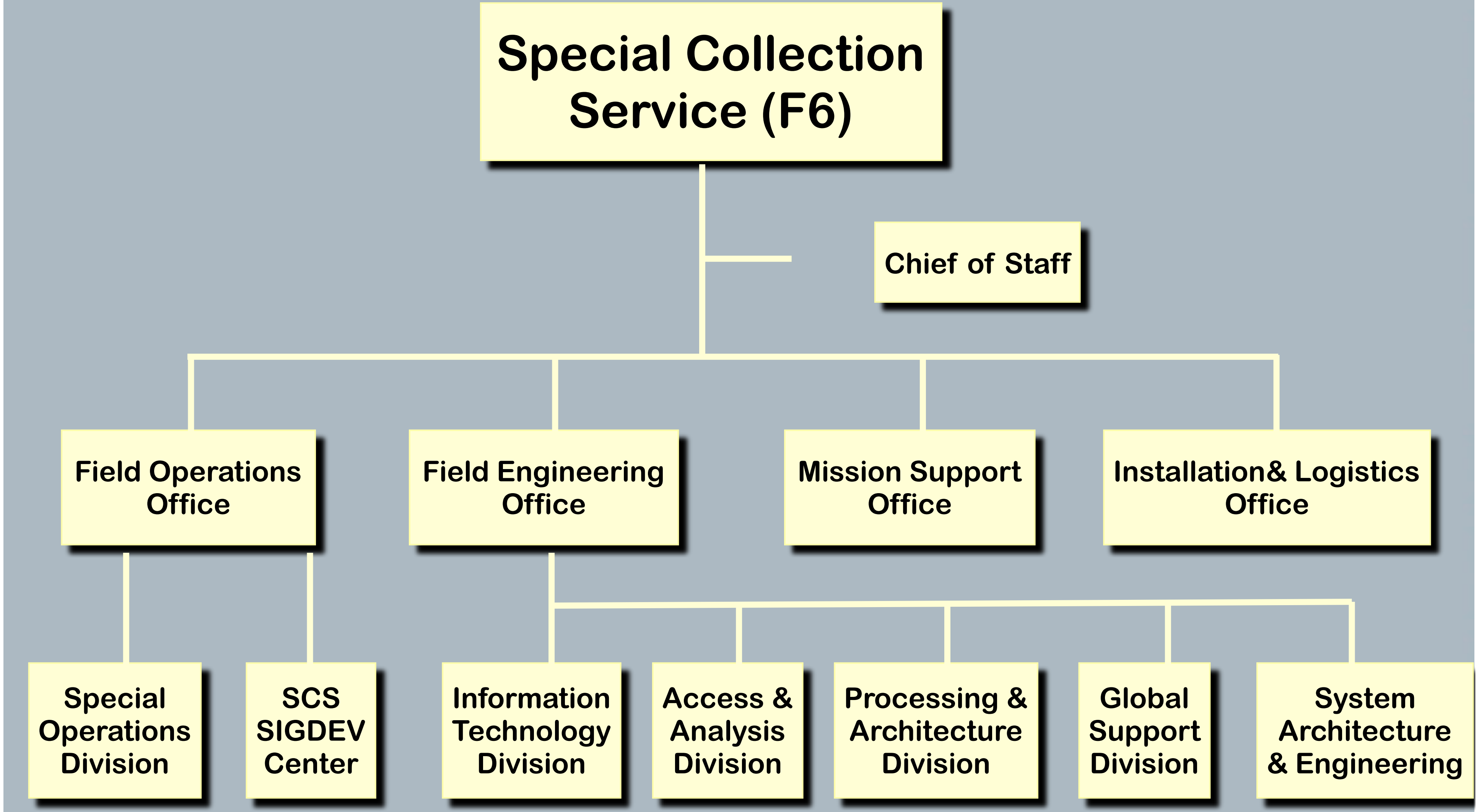
Pacific SIGDEV Conference
March 2011

The Overall Classification of this Briefing:

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

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360301

SCS Organization



Special Collection Service (F6)

Chief of Staff

Field Operations Office

Field Engineering Office

Mission Support Office

Installation& Logistics Office

Special Operations Division

SCS SIGDEV Center

Information Technology Division

Access & Analysis Division

Processing & Architecture Division

Global Support Division

System Architecture & Engineering

Special Collection Service

Strategic Partnerships

SIGINT Enabling HUMINT

HUMINT Enabling SIGINT

DEA

DIA

NRO

SSO

FBI

State

Secret Service

Law Enforcement

Homeland Security

Tailored Access

COVCOM

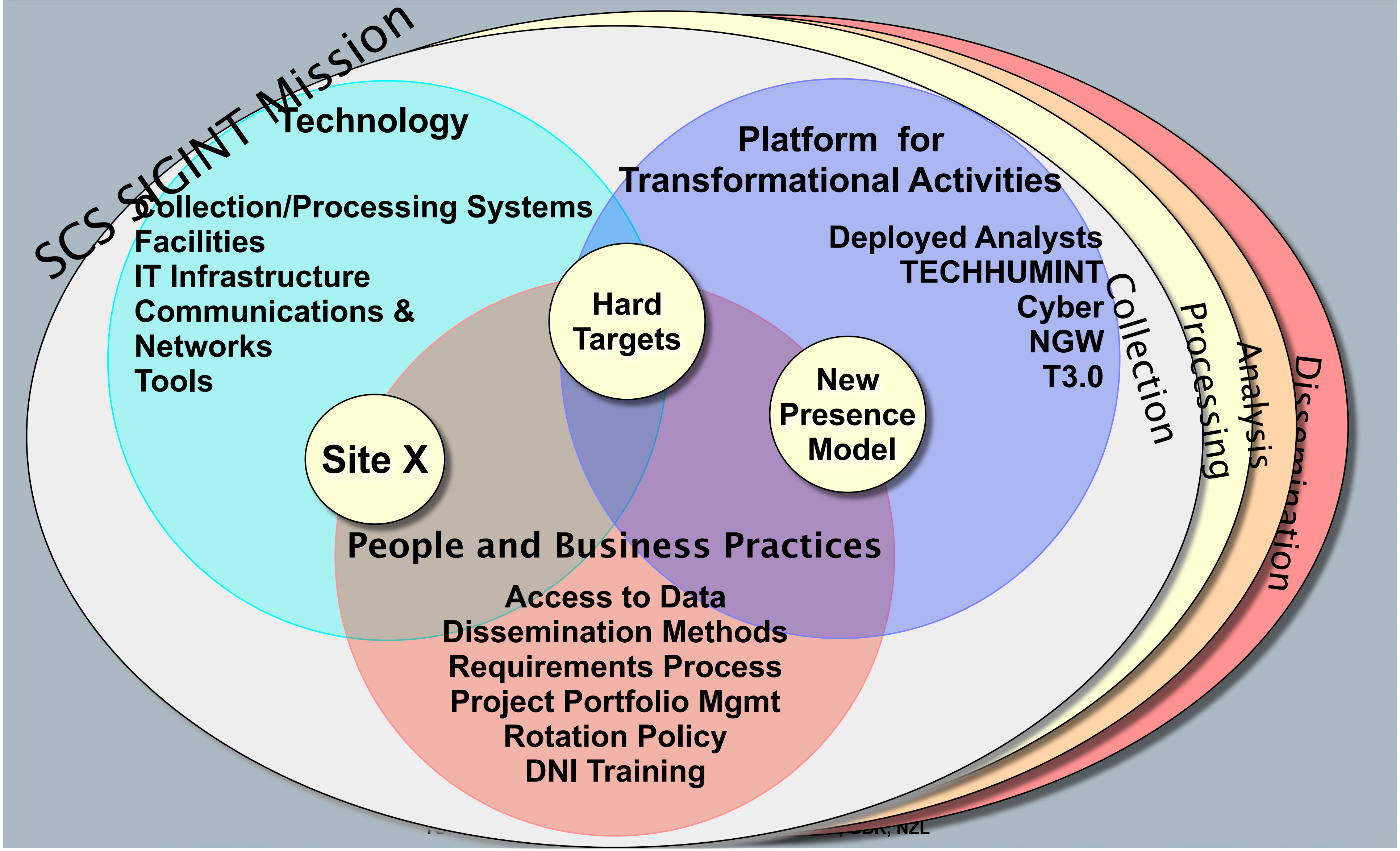
Military

CLANSIG

Second Party

Special Collection Service

SCS Modernization



SCS SIGINT Mission

Technology

Collection/Processing Systems
Facilities
IT Infrastructure
Communications & Networks
Tools

Platform for Transformational Activities

Deployed Analysts
TECHHUMINT
Cyber
NGW
T3.0

Hard Targets

Site X

New Presence Model

People and Business Practices

Access to Data
Dissemination Methods
Requirements Process
Project Portfolio Mgmt
Rotation Policy
DNI Training

Collection

Processing

Analysis

Dissemination

Overview

- Unified IT Core and Virtualization
- Cloud Computing
- Global Situational Awareness
- Beyond Traditional Accesses
- Coherent Digital Access
- Empowering Automation
- The SCS Cyber Advantage

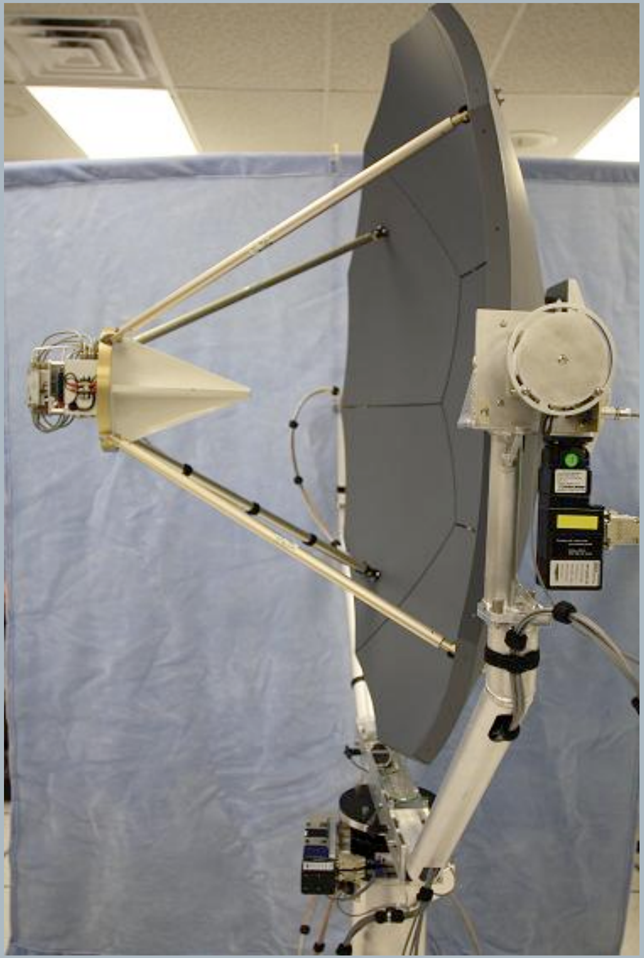
Special Collection Service

Unified IT Core

IT Services, IT Infrastructure

- **Capability Improvements:**
  - Modern IT services and infrastructure to support a net-centric operational model and enhance maintenance and security
- **Capability Change:**
  - Rapid response SIGINT presence
  - Next generation virtual infrastructure
  - Diversified WAN topology, enhanced LAN
  - Enhanced interoperable desktop
  - Improved email service
  - Workforce mobility
  - Robust collaboration environment
  - Site destruct enabler

EINSTEIN/CASTANET



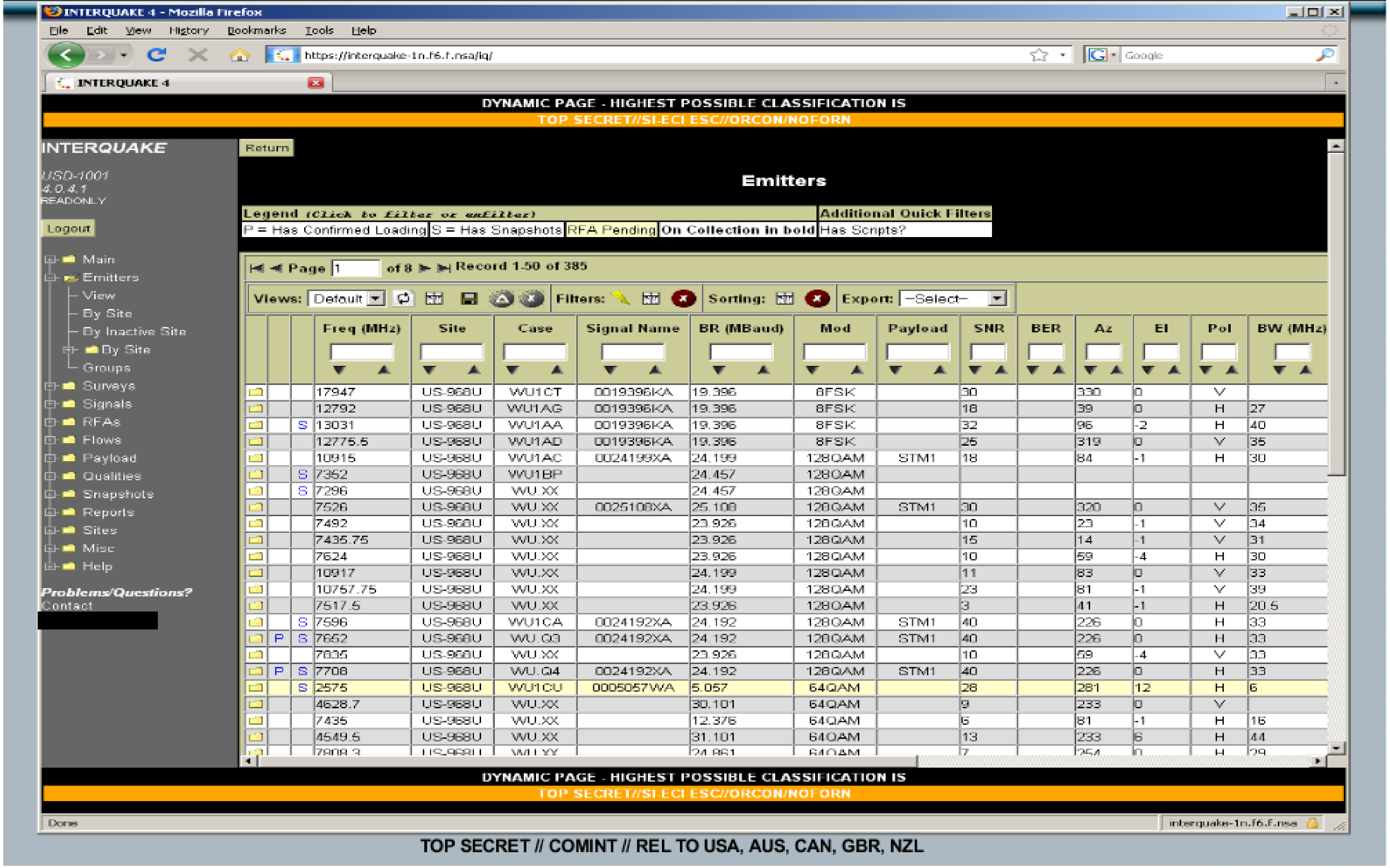
Special Collection Service

INTERQUAKE

- Terrestrial Environmental Knowledge Base
  - Available to all NSA analysts and partners
- PANOPLY populates IQ with Emitter information and reports including:
  - Signal Externals
  - Radio and Payload information
  - LACs and Cell ID's
  - Protocol Stacks

Special Collection Service

INTERQUAKE



https://interquake-1n.f6.f.nsa/iq/

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//SI-ECI ESC//ORCON/NOFORN

INTERQUAKE

USD-1001
4.0.4.1
READONLY

Problems/Questions?
Contact
[redacted]

Emitters

Legend *(Click to filter or unfilter)*				Additional Quick Filters
P = Has Confirmed Loading	S = Has Snapshots	RFA Pending	On Collection in bold	Has Scripts?

Page 1 of 8 Record 1-50 of 385

			Freq (MHz)	Site	Case	Signal Name	BR (MBaud)	Mod	Payload	SNR	BER	Az	El	Pol	BW (MHz)
			17947	US-968U	WU1CT	0019396KA	19.396	8FSK		30		330	0	V	
			12792	US-968U	WU1AG	0019396KA	19.396	8FSK		18		39	0	H	27
		S	13031	US-968U	WU1AA	0019396KA	19.396	8FSK		32		96	-2	H	40
			12775.5	US-968U	WU1AD	0019396KA	19.396	8FSK		25		319	0	V	35
			10915	US-968U	WU1AC	0024199XA	24.199	128QAM	STM1	18		84	-1	H	30
		S	7352	US-968U	WU1BP		24.457	128QAM							
		S	7296	US-968U	WU.XX		24.457	128QAM							
			7526	US-968U	WU.XX	0025108XA	25.108	128QAM	STM1	30		320	0	V	35
			7492	US-968U	WU.XX		23.926	128QAM		10		23	-1	V	34
			7435.75	US-968U	WU.XX		23.926	128QAM		15		14	-1	V	31
			7624	US-968U	WU.XX		23.926	128QAM		10		59	-4	H	30
			10917	US-968U	WU.XX		24.199	128QAM		11		83	0	V	33
			10757.75	US-968U	WU.XX		24.199	128QAM		23		81	-1	V	39
			7517.5	US-968U	WU.XX		23.926	128QAM		3		41	-1	H	20.5
		S	7596	US-968U	WU1CA	0024192XA	24.192	128QAM	STM1	40		226	0	H	33
	P	S	7652	US-968U	WU.Q3	0024192XA	24.192	128QAM	STM1	40		226	0	H	33
			7835	US-968U	WU.XX		23.926	128QAM		10		59	-4	V	33
	P	S	7708	US-968U	WU.Q4	0024192XA	24.192	128QAM	STM1	40		226	0	H	33
		S	2575	US-968U	WU1CU	0005057WA	5.057	64QAM		28		281	12	H	6
			4628.7	US-968U	WU.XX		30.101	64QAM		9		233	0	V	
			7435	US-968U	WU.XX		12.376	64QAM		6		81	-1	H	16
			4549.5	US-968U	WU.XX		31.101	64QAM		13		233	6	H	44
			7808.3	US-968U	WU.XX		24.861	64QAM		7		254	0	H	29

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//SI-ECI ESC//ORCON/NOFORN

interquake-1n.f6.f.nsa

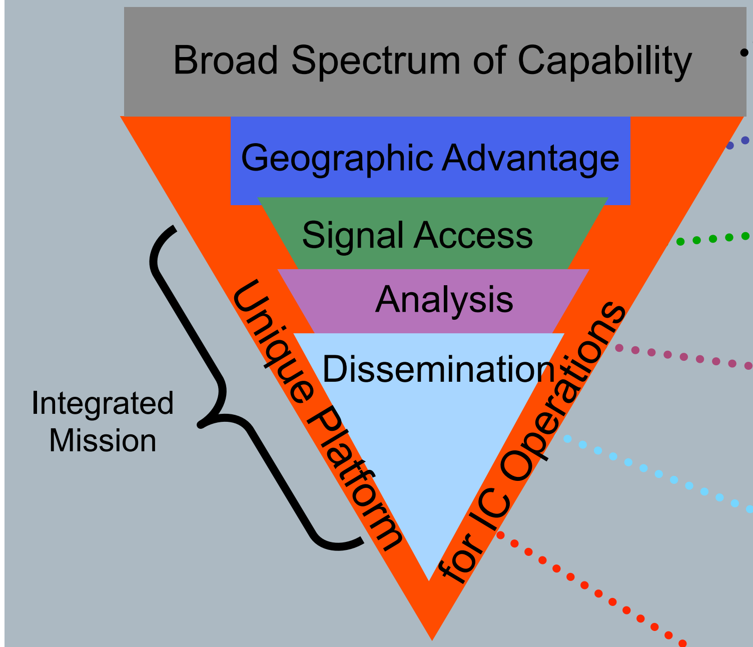
Special Collection Service

CES/SSC/AAD VPN “Surge”

- Main Goal:
  - To evaluate SCS VPN access and analysis to determine better methods of identifying and exploiting networks of interest.
- Two Focuses:
  - What can we do with VPN data that is already ingested into the system?
    - Find better methods of reporting VPN stats and exploitation determinations from CES back to SSC and site.
  - Are there methods to better identify and survey VPN’s to provide CES the data they need?
    - Can we leverage MIRROR, DARKQUEST, PANOPLY survey information to quickly identify and report the presence of VPN’s in surveyed signals?
    - Can we use BIRDWATCHER or other means to automatically resurvey for key exchanges and obtain paired collect?

Special Collection Service

The SCS Cyber Advantage



SIGINT prowess provides cyber advantage

Unified operations provides holistic approach
The right intelligence delivered to the right customer

Home field advantage in adversary's space

Where our customers want us and our adversaries do not
Capitalizing on the "element of surprise"

Signal access for collection, exfil,and infil

Microwave, WiFi, WiMAX, GSM, CDMA, Satellite, etc.

Living in the environment

Insights on infrastructure and configurations
Discovery of targets, signatures, and behavior

Tailored intelligence products

Diverse products driven by national objectives and local needs through formal reporting, target packages, analytic insights, situational awareness, threat warning

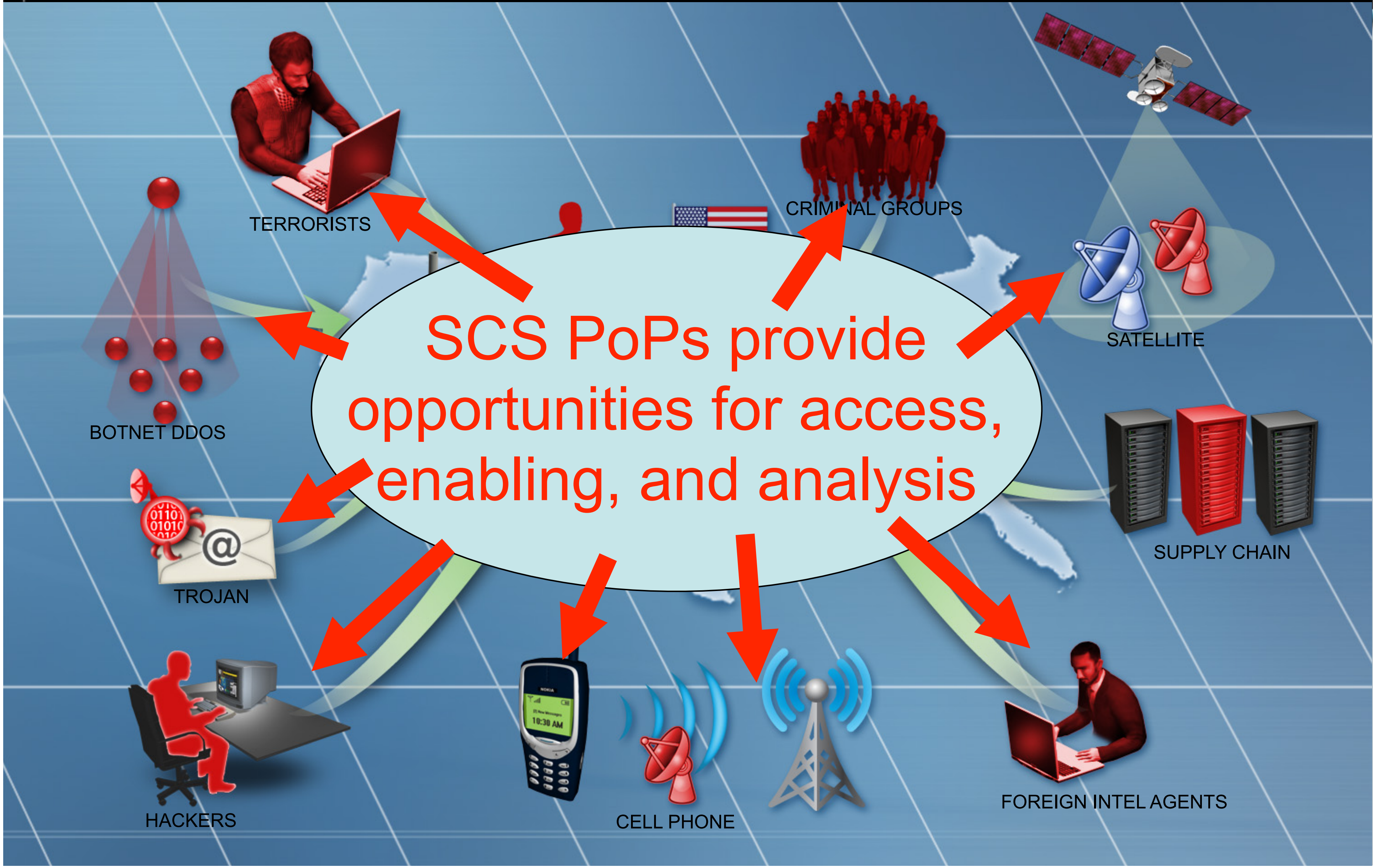
Unique platform for conducting and enabling IC operations

Fully leveraging 30-years of experience within the NSA and CIA enterprises and using existing authorities

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

Special Collection Service

SCS Opportunities



SCS PoPs provide opportunities for access, enabling, and analysis

(S//SI) One-Year Anniversary for SUSLAG

FROM: (S//SI)
SUSLAG (F28)
Run Date: 06/10/2005

Special US Liaison Activity Germany has spent a year in a "tin can." (It's better than it sounds -- it's the nickname for their new facility!) (S//SI)

(S//SI) In April, the Special US Liaison Activity Germany (SUSLAG) celebrated one year in their purpose-built facility on the German Ministry of Defense facility Mangfall Kaserne in Bad Aibling, Germany. SUSLAG (formerly known as Combined Group Germany) was compelled to find a new home by the closure of its previous host, Bad Aibling Station.

(S//SI) [redacted] first Chief SUSLAG, helps [redacted] (Chief of Engineering and Maintenance/KE-60) plant a tree in front of the new SUSLAG building on Mangfall Kaserne. Also participating are, from left to right, [redacted] (RF Engineering), and [redacted] (Chief of Station, Mangfall Kaserne/LA-60).

(S//SI) Thanks to the combined efforts of the Bad Aibling Transition Team, the Technical Support Program Management Office, Bundesnachrichtendienst (BND, the German intelligence service and our German partner), the European Technical Center (ETC), ITD, NCEUR, I&L**, and others too numerous to mention, the building was completed in just 4½ months, from groundbreaking to move-in, all during the depths of winter. (SUSLAG's BND colleagues affectionately refer to the new SUSLAG building as "Die Blechdose" or "the Tin Can," owing to its difference in appearance from the other buildings on Mangfall Kaserne -- it has no windows, is made of metal and is shelter-like in appearance). SUSLAG went off NSANET at Bad Aibling Station on Friday, 3 April 2004, and reappeared on NSANET in the new facility on the following Monday, thanks to an outstanding team of IT professionals working through the weekend.

(S//SI) In addition to SUSLAG's long-standing role as liaison to the German intelligence service, **it is parent to two exciting joint ventures, the Joint Analysis Center (JAC) and the Joint SIGINT Activity (JSA).** The Joint Analysis Center (JAC) comprises five NSA civilian analysts who are integrated into the BND [redacted]

(S//SI) JSA, the JAC's younger sibling, was declared operational last year and continues to build toward full operating capability, which is expected by the end of 2005. The JSA is the outcome of an agreement between the Director, NSA, and the President of the BND to launch a strategic cooperation initiative in the mutual pursuit of intelligence related to counterterrorism, counterproliferation, and other transnational targets.

(S//SI) With the establishment of a US-only communications center in the new SUSLAG facility, it became possible to provide secure connectivity for JSA, piggy-backing on SUSLAG's connection to ETC, at which point the JSA comms pass through ETC's Third-Party guard device subsystem onto NSANET. This provided for the first time an electronic connection from NSA to JSA for tasking to flow in one direction, and SIGINT in the other. JSA is primarily a SIGDEV asset from NSA's point of view, but is an essential component of BND's collection architecture. JSA is unique as a jointly manned, jointly tasked DNI site.

(S//SI) Following DIRNSA's dictum that making our foreign partners more capable also makes NSA more capable, NSA personnel assigned to JSA are teaching their BND counterparts new tools and techniques in advanced signals and protocol analysis and DNI exploitation. But this is far more than an academic exercise -- training is being conducted in the course of executing tasked mission, currently one NSA and two BND tasks. BND senior leadership recently commended JSA for their efforts, particularly the contribution that JSA's Afghan GSM** task has made to one of BND's highest priority task, Force Protection in Afghanistan. FORNSAT /SCS Mission Management has assigned primary responsibility to JSA for 10 beams on seven satellites, and JSA is continually surveying these beams and feeding the resulting metadata to NSA systems.

(S//SI) **SUSLAG continues in its traditional role as SIGINT liaison** to the Federal Republic of Germany. This role has been greatly facilitated by SUSLAG's new location on Mangfall Kaserne. NSA personnel interact daily with BND counterparts, coordinating policy, conducting technical exchanges, expanding the range of cooperation in SIGINT, and deepening the partnership in many ways. The availability of SUSLAG's secure VTC facility on Mangfall Kaserne allows for a close and continuing exchange with our partner based on an unprecedented series of VTCs. Additionally, visiting NSA technical experts have immediate access to BND counterparts, providing for an unmatched exchange of expertise.

(S//SI) SUSLAG is now established on a solid foundation for years to come. In the past year, DIRNSA, SID's Deputy Director, and the Principal Director of Foreign Affairs have visited to add emphasis to their charge to Chief, SUSLAG to broaden and deepen the SIGINT relationship with the German partner, moving in new and exciting directions. These efforts have already begun to bear fruit, and the future of this productive partnership seems assured.

**(U) Notes:
ITD = Information Technology Directorate
NCEUR = NSA/CSS Europe
I&L = Installations & Logistics
GSM = a type of digital cellular comms (Global System for Mobile Communications)

(U//FOUO) This article is reprinted from May's *Foreign Affairs Digest*

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

FOREIGN AFFAIRS DIRECTORATE

A WORLD OF OPPORTUNITIES

(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Special U.S. Liaison Activity Germany (SUSLAG)/ Joint SIGINT Activity (JSA)/ Defense Communications Interoperability Group (DCIG), CLASSIFICATION GUIDE

Guide Number (10-03)

Effective Date: ***16 February 2005***

[redacted]

REASON FOR CLASSIFICATION: 1.4 *(c), (d)*

DECLASSIFY ON: 20291123

[redacted]

CLASSIFICATION GUIDE TITLE/NUMBER: (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Special U.S. Liaison Activity Germany (SUSLAG)/ Joint SIGINT Activity (JSA)/ Defense Communications Interoperability Group (DCIG), 10-03

PUBLICATION DATE: (U) 16 February 2005

OFFICE OF ORIGIN: (U) Foreign Affairs Directorate, European Affairs Office (DP12)

POC: (U//FOUO) [redacted]

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: (U) [redacted] Principal Director, Foreign Affairs

(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) BND – Bundesnachrictendienst – German Federal Intelligence Service. The fact that the BND has a SIGINT mission is UNCLASSIFIED. The fact that the BND has a presence at Mangfall Kaserne and the fact that the BND conducts SIGINT at Mangfall Kaserne are both classified.

(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) DCIG – Defense Communications Interoperability Group – DCIG is a cover designator used to represent the SUSLAG organization in UNCLASSIFIED fora. DCIG should not be used in UNCLASSIFIEDIED fora in association with NSA.

(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) FIFTYEXCLAIM - FIFTYEXCLAIM is the coverterm representing NSA's contract with Computer Sciences Corporation (CSC) for mission support. All publicly available information regarding work on this contract at Mangfall Kaserne will be sanitized so that no association with NSA will be made. This will entail removal of references to Maryland Procurement Office/MPO, NSA-related DODAICs, NSA civilian/military affiliate names, NSA phone numbers, etc. (This is not an all-inclusive list.)

(S/SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) JSA – Joint SIGINT Activity – JSA is the joint NSA/BND organization that performs SIGINT collection at Mangfall Kaserne. The title JSA should only be used in classified fora.

(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) SUSLAG – Special U.S. Liaison Activity Germany – SUSLAG is the NSA organization at Mangfall Kaserne that conducts foreign liaison with the BND. JSA falls under SUSLAG for administrative actions. The title SUSLAG should only be used in classified fora.

Description of Information	Classification/Markings	Reason	Declass	Remarks
A. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) NSA PRESENCE AT MANGFALL KASERNE				
1. (U) The fact of the presence of U.S. personnel at Mangfall Kaserne.	UNCLASSIFIED	N/A	N/A	(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) No association with NSA, SIGINT, intelligence, or the BND.
2. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact of an NSA presence at Mangfall Kaserne.	SECRET//COMINT REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Mention of a SIGINT mission at Mangfall Kaserne is classified SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR and NZL.
3. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact of a SUSLAG presence at Mangfall Kaserne.	SECRET//COMINT REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Mention of a SIGINT mission at Mangfall Kaserne is classified SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR and NZL.
4. (U) The fact of the DCIG presence at Mangfall Kaserne.	UNCLASSIFIED	N/A	N/A	(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) No association with NSA, SIGINT, intelligence, or the BND.
5. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact of the JSA presence at Mangfall Kaserne.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
B. (U) ASSOCIATIONS **(U) Note that if an entity's association with NSA is classified, that entity's association with other NSA organizations is also classified.**				
1. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of NSA with SUSLAG.	SECRET//COMINT REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
2. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of NSA with the DCIG.	SECRET//COMINT REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
3. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of SUSLAG with the DCIG.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	

4. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of SUSLAG with the BND.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
5. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of the DCIG with the BND.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR and NZL	1.4 (c) (d)	20291123	
6. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of NSA with the JSA.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
7. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of SUSLAG with the JSA.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
8. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of the DCIG with the JSA.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
9. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of the JSA with the BND.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
C. (S//SI//REL TO USA, AUS, CAN, DEU, GBR and NZL) NSA/BND RELATIONSHIP				
1. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of NSA with the BND.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR and NZL	1.4 (c) (d)	20291123	
2. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact that the BND is one of NSA's Third Party partners.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
3. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Details regarding the NSA/BND SIGINT relationship.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL (at a minimum)	1.4 (c) (d)	20291123	(U) Consult the Country Desk Officer for Germany for additional information.
D. (U) CONTRACT IT SUPPORT				
1. (U) The association of NSA with the FIFTYEXCLAIM contract.	UNCLASSIFIED	N/A	N/A	
2. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of SUSLAG with the FIFTYEXCLAIM contract.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
3. (S//SI/REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of DCIG with the FIFTYEXCLAIM contract.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
4. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of JSA with the FIFTYEXCLAIM contract.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	

5. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of the BND with the FIFTYEXCLAIM contract.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
E. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) SUSLAG/DCIG MISSION				
1. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The identification of the SUSLAG mission as follows: "SUSLAG is DIRNSA's in-theater foreign liaison representative to the BND SIGINT organization."	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, and NZL	1.4 (c) (d)	20291123	
2. (U) The identification of the DCIG mission as follows: "DCIG is an organization of DoD technicians and U.S. contractors that provide operations and maintenance support for antennas and high-performance communications equipment at Mangfall Kaserne."	UNCLASSIFIED	N/A	N/A	(S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The association of the DCIG with its true SIGINT mission is classified SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR and NZL at a minimum, depending on the level of detail provided.
F. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) JSA MISSION				
1. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The identification of the JSA mission as follows: "The JSA is a joint NSA/BND organization whose mission is SIGINT development and collection of digital network communications and international telecommunications traffic."	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, and NZL	1.4 (c) (d)	20291123	
2. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact that NSA and BND jointly, as JSA, perform SIGINT collection at Mangfall Kaserne.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
3. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) Details regarding SIGINT collection performed by JSA at Mangfall Kaserne.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL (at a minimum)	1.4 (c) (d)	20291123	

4. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The identification of entities or communications technologies targeted and/or collected by JSA.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL (at a minimum)	1.4 (c) (d)	20291123	
5. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact that JSA targets and collects satellite communications (FORNSAT).	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
7. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact that JSA has a SIGINT development mission.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	
8. (S//SI//REL TO USA, AUS, CAN, DEU, GBR, NZL) The fact that JSA forwards selected target communications to NSA.	SECRET//COMINT// REL TO USA, AUS, CAN, DEU, GBR, NZL	1.4 (c) (d)	20291123	

[edit] News

BREAKING NEWS (May 2012) - The second tranche of 'deep dive' processing capability at RPC has gone live. In addition 2 extra 10G's are being processed at OPC. This brings the current 'deep dive' capability to:

- CPC with 16 x 10g,
- OPC with 7 x 10g
- RPC1 with 23 x 10g.

This gives over 300 GCHQ and ~250 NSA analysts access to huge amounts of data to support the target discovery mission.

The MTI programme would like to say a big thanks to everyone who has made this possible (Which includes MTI [redacted], TGA, TEA, SSMG, SSOS, GTE, ACD, OPP-LEG, IT Services, R1 at NSA, AHS and) - a true collaborative effort!

TEMPORA was delivered by the MTI Enhanced Discovery swimlane, led by [redacted] is part of the MTI SIGINT Apps theme led by [redacted] ([redacted] PM) and [redacted] ([redacted])

[edit] TEMPORA

TEMPORA is an Internet Buffer capability being delivered by MTI, IPP and GTE for joint mission benefit. It builds upon the key success of the TINT experiment and will provide a vital unique capability to MISD/MCE communities.

- TEMPORA is the codeword for GCHQs internet buffer business capability as a whole – which is the ability to loosely promote a % of traffic across GCHQs SSE access into a repository which will keep the content (and its associated metadata) for periods of time (approximately 3 days for content and up to 30 days for metadata) to allow retrospective analysis and forwarding to follow on systems.
- TEMPORA as a capability is *agnostic* of the technologies used to promote that traffic and to store that traffic and so should not be used as a codeword for the individual components (e.g XKS, MVR etc).
- At the moment the components include, amongst others, GCHQ SSE Access, POKERFACE sanitisation, XKS (in various configurations) and it will include MVR in the very near future.
- TEMPORA also covers the management of the rules used to promote traffic into the internet buffer capability.
- TEMPORA is not processing centre specific. At the moment there are instances of TEMPORA at all xPC (Namely CPC, OPC and RPC1). These should be referred to, when required, as OPC/CPC/RPC1 TEMPORA

[edit] A bit more detail

TEMPORA are GCHQ's large-scale, Deep Dive deployments on Special Source access (SSE). Deep Dive XKeyscores work by promoting loose categories of traffic (e.g., all web, email, social, chat, EA, VPN, VoIP...) from the bearers feeding the system and block all the high-volume, low value traffic (e.g., P2P downloads). This usually equates to ~30% of the traffic on the bearer. We keep the full sessions for 3 working days and the metadata for 30 days for you to query, using all the functionality that Keyscore offers to slice and dice the data. The aim is to put the best 7.5% of our access into TEMPORA's, comprising a mix of Deep Dive Keyscores and promotion of data based on IP subnet or technology type from across the entire MVR. At the moment, users are able to access 46x10Gs of data via existing Internet Buffers.. This is a lot of data! Not only that, but the long-running TINT program and our initial 3-month operational trial of the CPC Internet Buffer (the first operational Internet Buffer to be deployed) show that every area of ops can get real benefit from this capability, especially for target discovery and target development. Internet Buffers are different from TINT in that the latter is purely an experimental, research environment whereas Internet Buffers can be used operationally for EPR, Effects, enabling CNE etc.

For a more detailed depiction of how TEMPORA and TINT differs please see here.

[edit] Contacts

Name	Role
[redacted]	GTE XKS Senior User
[redacted]	MTI SIGINT apps theme lead
[redacted]	Enhanced Discovery Project Manager
[redacted]	Enhanced Discovery XKS SME

14 MARCH 2013

Special Source Operations Weekly

(U//FOUO) OPERATIONAL HIGHLIGHT WHARPDRIVE

(TS//SI//NF) SSO was informed on 12 March 2013 that the access point for WHARPDRIVE was discovered by commercial consortium personnel. Witting partner personnel have removed the evidence and a plausible cover story was provided. All collection has ceased.

(TS//SI//NF) SSO was planning to conduct a week of training in April and support a deployment in June, however, the partner has requested to delay both training and shipping.

XKeyscoreTabs XKS Development

Jump to: navigation, search

News | Getting an Account | Using XKeyscore | Training | XKS Development | XKS Contacts | Requirements | News Archive

Quick Links

- XKEYSCORE Main Page
- XKS @ scale on SSE
- Getting Strong-Selected Content into XKS
- Getting an XKS Account
- Using XKEYSCORE
- XKEYSCORE Training
- **XKEYSCORE Development**
- XKEYSCORE Contacts
- XKS News Archive
- XKS Requirements
- XKS Searches user guide
- XKS Results user guide
- XKS Approval process
- NFV in XKS
- Promotion from XKS
- Automatic Promotion from XKS
- XKS for CNE
- NSA XKeyscore Using XKS for CNE
- XKS Tech Dictionaries

Useful Links

- Mastering The Internet
- Transforming Analysis
- TINT
- GTE
- SD Home

v · d · e

Contents

[edit] XKS Upgrades

XKS is upgraded fortnightly on Thursday mornings between 0900-1100. If you can't log on or use the tool during this period, its because of this.

[edit] Guidance on microplugins

As you know, you can create microplugins to do different things: some perform advanced detection techniques to find types of traffic which can't be detected by keywords or regular expressions alone. Others identify and extract data fields into XKS's metadata table.

In the latter case, the extracted content fragments are stored in the metadata table for 30 days. It will depend on the precision and nature of the search criteria you have used as to how strongly – or weakly – selected that content will be.

If you are going to use search criteria that will extract data about people and store that in the metadata table, please consult OPPLEG before doing so. They will wish to understand the nature and scope of any data being stored in case it includes at least the names of individuals and the majority of the data is not believed to relate to probable intelligence targets. This would make this data particularly sensitive.

In addition, a quarterly check is now being made on all new microplugins which add data to the metadata table to ensure they meet UK legal and policy requirements.

Please also be aware that usually microplugins are automatically shared with at least NSA and may also get deployed to other 2P XKS. By mid-2011 a new version of XKS should have been deployed where individual microplugins will still be deployed to every XKS, but they can be tagged not to run on certain XKS. The only exception is where you deploy a microplugin only to GTE's XKS fleet: these will not be visible to 2P partners.

[edit] Types of XKEYSCORE

There are currently three different types of XKS:

- **Traditional**
- **Stage 2**
- **Deep Dive**

They differ principally on where in the processing chain they sit, whether the data they receive has already been sessionised or not and whether they ingest all of the data they receive or whether they apply rules to only ingest some data.

[edit] Traditional

When XKS was first developed it was used to receive data from low data rate signals being processed through WEALTHYCLUSTER (WC). WC sessionised all the data on the link and presented it all to XKS. All data was ingested into XKS.

GCHQ has traditional XKS at many of our sites, including all of our Comsat, Terrestrial and SMO sites. The EREPO XKS is also a traditional XKS, though in that case data has been softly selected at the implant and sessionisation takes place in TERRAIN, rather than WC.

[edit] Stage 2

For higher data rates, a “Stage 2” XKS was developed to ingest data from TURMOIL. TURMOIL passes 5% of the packets to XKS which XKS then sessionizes. TURMOIL decides which 5% of packets to pass based on the following criteria:

- strong selection
- subnet promotion
- technology promotion
- e-mail domains
- persona session promotion (where if a strong selector is seen, 10 minutes’ or 10 MB of data is collected)
- persona session collection (where the data is collected and forwarded to NSA’s PINWALE but is also passed to the XKS)

This data is then sent to the Stage 2 XKS. All other data is lost.

Only JPC (MUSCULAR) at GCHQ uses a Stage 2 XKS.

[edit] Deep Dive

Deep Dive XKS was developed to prove that sessionisation at 10G data rates was possible. First it sessionises all data on a link. Then it promotes data using the GENESIS selection language to identify data types where we assess there is potential intelligence value and ingests those. The promotion process can make one of three decisions:

- Block data that is legally not allowed to be in the system – ie UK-UK traffic
- Allow data that is known to be wanted through use of promotion rules
- And then to drop any data that doesn’t meet either of these

One of the experiments in TINT is seeking to identify where the best balance lies between what is kept and what is not. A factor in deciding how much data to keep is the scale of storage capacity that can be provided.

GCHQ already operates a number of Deep Dive XKS:

DRAFT AGENDA

As of: 22 April 2013

HR DIETMAR B[redacted]
Director SIGINT Analysis and Production
German Federal Intelligence Service
30 April – 1 May 2013

30 April 2013

Time	Presentation Title and Presenter	Location
0850	(U//FOUO) Welcome **Hr. Dietmar B[redacted]** Director, SIGINT Analysis and Production, BND **Hr. Wilfried K[redacted]** Director, Data Acquisition, BND **Hr. Andreas I[redacted]** Director, BND Cyber Defense Center [redacted] Chief, Tasking and Customer Relations [redacted] Liaison Officer [redacted] Senior Analyst, Counterproliferation [redacted] Senior Analyst, Political/Economic Issues, Pakistan [redacted] Chief SIGDEV [redacted] Senior Analyst, Counterterrorism [redacted] Senior Analyst, Africa [redacted] BND Liaison Officer, Washington [redacted] SUSLAG Liaison Officer Met and escorted by Mr. [redacted], DIRFA; [redacted], CDO; [redacted], CH SUSLAG Designee; and Mrs.[redacted] NSA/CSS Protocol Officer.	GH 2B
0900-0920	Foreign Affairs Directorate (FAD) Courtesy Call Mr. [redacted] DIRFA	2B4118-5

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371201

0930-0945	(U//FOUO) Directorate Courtesy Call (9) GEN Keith B. Alexander, U.S. Army, DIRNSA/CHCSS Hr. Dietmar B[redacted] Hr. Wilfried K[redacted] [redacted] [redacted], DIRFA [redacted], CH SUSLAG Designee [redacted] SUSLAG [redacted], CDO Germany NOTE: A memento will not be presented. A photographer will not be present.	2B8036 GEN A's Ofc.
1000-1045	(U//FOUO) Discussions with the Office of South Asia [redacted] Global Capabilities Manager (GCM)	
1100-1130	(U//FOUO) Office Call with Signals Intelligence Director [redacted] SIGINT Director	2W102
1145-1230	(U//FOUO) SID-Hosted Lunch [redacted] GCM International Crime and Narcotics (ICN) (Host) (by invitation)	Canine Annex
1230-1300	(U//FOUO) Discussions with the Office of ICN [redacted], GCM/ICN	2B4118-5
1300-1330	(U//FOUO) Office Call with Data Acquisition [redacted], DIR for Data Acquisition [redacted], D/DIR for Data Acquisition	2B4118-5
1345-1430	(U//FOUO) Special Project Discussions with Data Acquisition [redacted] Chief S352 [redacted], Chief S352S [redacted], Chief, SSO [redacted] Special Source Operations	2B4118-5
1430-1500	(U//FOUO) Discussions with the Office of China and Korea [redacted], Office of China and Korea [redacted], Foreign Affairs Officer	2B4118-5
1500-1530	(U//FOUO) CIED Discussions with the Office of Combatting Proliferation [redacted] S2G6	2B4118-5
1530-1600	Discussions with the Office of Middle East and Africa (MEA) on	2B4118-5

	Africa [redacted] GCM for MEA	
1600-1630	Discussions with the Office of Middle East and Africa (MEA) on Iran [redacted], GCM for MEA	2B4118-5
1630-1645	Wrap-up	
1645	Depart	
1800-2030	(U//FOUO) SID Hosted Dinner [redacted] Associate Deputy Director (ADD) for Counterterrorism (CT) (Host) *(by invitation)*	Clyde's
1 May 2013		
0850	Met and escorted by Ms. [redacted], CDO; Ms. [redacted] CH SUSLAG Designee; and Mrs. [redacted] NSA/CSS Protocol Officer.	GH2
0900-1015	Discussions with the Office of Counterterrorism [redacted] ADD/CT [redacted] GCM/CT	2B4118-5
1015-1100	Discussions with the Office of SIGINT Development Strategy & Governance (SSG) [redacted] Chief SSG [redacted] Technical Director, SSG [redacted] Deputy GCM/SIGDEV	2B4118-5
1115-1145	Courtesy Call with Ms. [redacted], Group CH Mission Management Integration	2B4118-5
1200-1245	Foreign Affairs Hosted Lunch [redacted] Director, FAD	Canine Suite
1300-1400	Discussions with the National Threat Operations Center [redacted] NTOC Special Program Office	2B4118-5
1415-1500	Discussions with the Office of International Secuirty Issues (ISI) [redacted] GCM/ISI [redacted] Chief, CT Branch, NSA Texas	2B4118-5
1500-1600	Wrap Up	2B4118-5
1600	Depart	

VISIT PRÉCIS

Hr. Dietmar B[redacted]
Director SIGINT Analysis and Production
German Federal Intelligence Service (BND)
30 April – 1 May 2013

SID DIR Courtesy Call: 30 April 2013, 1100 – 1130
Participants: Mr. [redacted] SUSLOL Designee; Mr. [redacted], D/DA; Mr. [redacted] D/A&P; Mr. [redacted] Chief SSG; Ms. [redacted], SUSLAG Designee; Ms. [redacted] CDO Germany

(U) BACKGROUND:

- (S//REL TO USA, FVEY) Hr. B[redacted] assumed his current position in 2011 and is marking his second visit to NSA. He is rumored to be under consideration to become the next SIGINT Director, succeeding MG Hartmut P[redacted]. He will be accompanied by Hr. Wilfried K[redacted] Director of SIGINT Collection, and the following BND leadership:

  Hr. Andreas H[redacted] Director, BND Cyber Defense Center
  [redacted] Chief, Tasking and Customer Relations
  [redacted] BND Liaison Officer, Washington, D.C.

(U) PURPOSE OF THE VISIT:

- (S//REL TO USA, FVEY) Discussions during the third Strategic Planning Conference (SPC) will focus on topics of mutual interest and future areas of collaboration. With NSA's encouragement, the Germans are coming prepared to define specific capabilities in potential new areas of analytic and Computer Network Defense (CND) collaboration. This SPC will present an opportunity for NSA/CSS leadership to assess the BND's contributions and reiterate their commitment to the German partnership. SID DIR's discussions will set the tone for a productive conference.

(U) VISITOR R EQUESTED:

- (TS//SI//REL TO USA, DEU) The BND is eager to present its SIGINT capabilities and gaps on the targets of [redacted] and [redacted] with the goal of expanding the partnership. Their delegation includes several senior analysts, who are prepared to engage NSA leadership in identifying areas of mutual cooperation. The BND also is prepared to discuss progress of the new BND Cyber Defense Center and the policies and authorities governing the mission, while seeking lessons learned from NSA.

(U) NSA/CSS REQUESTED: (TS//SI//NF) Status of BND-NSA bilateral initiatives, highlighting:

- Identify mutual intelligence gaps on [redacted] and [redacted] target areas

- Enhanced CT analytic and SIGDEV technical cooperation with BND and BfV (Federal Office for the Protection of the Constitution) given the formalization of the NSA-BfV SIGINT partnership in March 2013.
- Discussion of German policies/authorities of the new BND Cyber Defense Center and collaboration with the defensive mission; NTOC will brief TUTELAGE
- Status of [redacted] and Special Source access programs
- Germany's support to the [redacted] SIGINT Coalition ([redacted]) and continued support in [redacted] for the SIGINT Counter-IED mission and global IED threat.

(U) CYBERCOM REQUESTED: N/A.

(U) COMMON THREADS: (TS//SI//REL TO USA, DEU)

- NSA welcomes the BND's eagerness to strengthen and expand cooperation with NSA
- Investing in BND's technical expertise to support the BfV and other German services could bolster Germany's effectiveness against terrorism and cyber threats

(U) KEY TOPICS

- (S//REL TO USA, DEU) Thank Hr. B[redacted] for the close partnership that NSA enjoys with the BND
- (S//SI//REL TO USA, FVEY) Enhancing the technical and analytical capabilities of our German intelligence partners will better-equip Germany to counter terrorists; NSA's desire to partner closely with both BND and BfV
- (TS//SI//REL TO USA, DEU) NSA's willingness to explore new areas of cooperation that fill mutual intelligence gaps

(U) KEY TAKEAWAYS:

1. (TS//SI/REL TO USA, DEU) **<u>Expanding the Scope of Bilateral Cooperation</u>**: During recent meetings with BND leadership, DIRNSA, DDIR, and SID encouraged the BND to define specific capabilities on [redacted] and [redacted] for discussion at the SPC. Thank the BND for coming so well prepared to discuss its potential contribution in these area and to give NSA the opportunity to evaluate where a formal bilateral partnership at the TS//SI level has the most promise.

2. (S//SI//REL TO USA, DEU) **<u>Counterterrorism</u>:** Share that NSA received ODNI approval in March 2013 to *establish a formal CT relationship with the BfV* and anticipates increasing synergy against the target with BND/BfV/NSA collaboration; *NSA also has signed the Terms of Reference to provision XKEYSCORE technology* to the BfV. Thank the BND for its leadership in providing technical solutions/support to the BfV.

3. (TS//SI//REL TO USA, DEU) **<u>Computer Network Defense</u>**: Commend Germany for establishing the BND Cyber Defense Center in Berlin and the National Cyber Defense Centre in Bonn. Encourage BND/ BfV/ BSI (Information Assurance Service) collaboration to leverage SIGINT support to CND. Share that NSA is eager to learn more about German cyber authorities and is prepared to offer lessons learned and technical presentations, including TUTELAGE, to aid in the development of German SIGINT support to CND.

4. (TS//SI//NF) **Demonstrate the value of NSA-BND collaboration on [redacted] and Special Source access programs**.

- [redacted]
- (TS//SI //REL TO USA, DEU) **BND Collaboration with Special Source Operations (SSO): WHARPDRIVE (EMERALD)**: Thank the BND for their assistance with the trilateral program, acknowledging recent delays due to funding constraints by both partners. Reassure that the BND is the program lead with NSA playing a technical support role. *For background only, WHARPDRIVE has been identified for possible termination due to fiscal constraints, but the partners have not been informed.*

5. (TS//SI//REL TO USA, DEU) **Middle East & Africa**: Thank the BND for providing West African [redacted] language assistance used by high-level [redacted] officials; State that NSA is looking forward to learning more about the BND's capabilities in [redacted]

6. (TS//SI//REL TO USA, DEU) **AFSC:** Commend the Germans for their support and leadership in RC-North Multinational SIGINT Cell and their efforts to contribute to Division -of-Effort Reporting on governance targets. Explain that German support in [redacted] will be critical in maintaining necessary threat warning and force protection in 2013/14 as MES becomes a logistical hub and potential egress route into [redacted] *Regarding the post-2014 disposition of U.S. forces, state that the coalition partners will discuss this topic at the early May 2013 AFSC conference in Denmark.*

7. (S//SI//REL TO USA, DEU) **Counter-IED:** Thank the BND for supporting the Counter-IED mission in RC-North and for engaging the CIED SIGINT Seniors Europe (SSEUR) venues. NSA looks forward to continued cooperation in the post [redacted] 2014 environment on a global basis.

8. (S//REL TO USA, DEU) **NSA Manning at Bad Aibling Post-Summer 2013:** At the DDIR's request in January 2013, SID re-evaluated the technical presence at SUSLAG. Convey that NSA has difficult choices to make in this challenging fiscal climate and will continue to keep the BND's request for consideration. Reference the availability of VTC, the European Technical Center (ETC), and the CHATTERII communications tool to provide assistance.

(U) VISIT FORMAT:

- (TS//SI//REL TO USA, DEU) The BND will provide briefings on [redacted] and [redacted] as well as on Germany's posture on CND.
- (TS//SI//REL TO USA, DEU) NSA Participants: SID DIR, D/DIRFA, ADD/Acquisition; ADD/CT; GCM South Asia; GCM International Crime & Narcotics;

GCM Middle East & Africa; D/GCM CT; D/GCM International Security Issues; Chief SIGDEV; D/CH NTOC

(U) PREVIOUS VISITS AND RESPECTIVE TOPICS: Hr. B[redacted]first visited NSA in December 2011 for familiarization with NSA's mission and discussions with SID leadership.

(TS//SI//NF) POTENTIAL LANDMINES:

- (TS//SI//NF) **SKYPE:** The Germans may bring up the subject of SKYPE. NSA's response has been that it has had some success working SKYPE via tailored access at the end point by gaining access to one or more of the computers involved in the session. When Hr. Klaus-Fritsche (State Secretary, Germany Ministry of Interior) sought NSA's assistance with intercepting SKYPE transmissions during a 10 January 2012 meeting with DIRNSA, DIRNSA suggested the DNI Representative Berlin take the lead in arranging an exchange to include CIA, FBI and NSA. Should the partner raise this issue again, recommend that NSA once again redirects them to FBI and CIA.

(U) OTHER INFORMATION:

- (S//NF) BIOs: B[redacted] and K[redacted]
- (TS//SI//NF) Talking Point Papers: S2A, S2E, S2G, S2I, S3, and NTOC

(U//FOUO) POC: [redacted] CDO Germany, [redacted]

FINAL AGENDA

As of: 29 April 2013//1417

Protocol Rep: [redacted]
Visit manager:

Date/Time of Visit: (U) 30 April - 1 May 2013
30 April 2013//0930-1645
1 May 2013//0850-1600

Visitor: **(U) HR. DIETMAR B**[redacted]

Title: (U//FOUO) Director, SIGINT Analysis and Production

Country/Organization: (U//FOUO) Germany/German Federal Intelligence Service (BND) SIGINT Directorate

Equivalency: (U//FOUO) Deputy Director Analyis & Production

Accompanied by: **(U//FOUO) HR. WILFRIED K**[redacted]
Director, Data Acquisition, BND
HR. ANDREAS H[redacted]
Director, BND Cyber Defense Center
[redacted]
Chief, Tasking and Customer Relations
[redacted]
Liaison Officer
[redacted]
Senior Analyst, Counterproliferation
[redacted]
Senior Analyst, Political/Economic Issues [redacted]
[redacted]
Chief SIGDEV
[redacted]
Senior Analyst, Counterterrorism
[redacted]
Senior Analyst, Africa
[redacted]
BND Liaison Officer, Washington, D.C.
[redacted]
Liaison Officer, SUSLAG

Interpreter: (U//FOUO) None.

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

Previous visits:	(S//REL) Hr. B[redacted] last visited the Directorate in December 2011.
Clearances:	(U) TS//SI
Accompanying NSA/CSS Senior:	**(U//FOUO)** [redacted] Deputy Director Foreign Affairs (D/DIRFA)
Photographer:	(U) No.
Memento Presented:	(U) No.
Uniform of the Day:	(U) GEN A: Class B; D/DIR and Guests: Business Attire
Purpose of Visit:	(S//REL) Hr. B[redacted] will be leading the German delegation for the Strategic Planning Conference (SPC).
Justification for Directorate Involvement:	(S//NF) Germany is an active, valued partner and Directorate-level involvement in the SPC will underscore, for the Germans, the value of the partnership between NSA/CSS and BND.
Expected Outcome:	(S//NF) To explore topics of mutual interest to both partners in an effort to move the relationship forward over the next year.

[redacted]
Chief of Protocol
and Corporate Events
NSA/CSS Protocol Office

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

HR. DIETMAR B[redacted]
Director, SIGINT Analysis and Production
German Federal Intelligence Service (BND)

30 April 2013

Time	Presentation Title and Presenter	Location
0930	(U//FOUO) Welcome Hr. Dietmar B[redacted] Liaison Officer, SUSLAG Met and escorted by [redacted], D/DIRFA; [redacted], CDO; [redacted], CH SUSLAG Designee; and [redacted], NSA/CSS SID Protocol Officer.	GH1
0940-1000	Foreign Affairs Directorate (FAD) Courtesy Call [redacted] D/DIRFA	2B4118-5
1000-1045	(U//FOUO) Discussions with the Office of South Asia [redacted], Global Capabilities Manager (GCM), Office of South Asia	2B4118-5
1100-1130	(U//FOUO) Signals Intelligence Directorate (SID) Courtesy Call (12) [redacted] Hr. Dietmar B[redacted]	2W102
1145-1230	(U//FOUO) SID Hosted Lunch [redacted] Global Capabilities Manager (GCM)	Canine Annex

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

	International Crime and Narcotics (ICN) (Host) *(By Invitation Only)*	
1230-1300	(U//FOUO) ICN Discussions [redacted], GCM ICN [redacted], Chief of Operations, ICN [redacted] Foreign Affairs Officer	2B4118-5
1300-1330	(U//FOUO) Data Acquisition Directorate Courtesy Call [redacted] D/DIR for Data Acquisition [redacted] Assistant D/DIR for Data Acquisition	2B4118-5
1330-1345	(U) Break	
1345-1430	(U//FOUO) Data Acquisition Special Project Discussions [redacted], CH Radio Frequency Targeted Operations Office (RFTO) [redacted] CH RFTO Special Projects Office [redacted], CH Special Source Operations (SSO) [redacted], SSO	2B4118-5
1430-1500	(U//FOUO) Combating Proliferation Counter-Improvised Explosives Device (CIED) Discussions [redacted] CH CIED Division	2B4118-5
1500-1530	(U//FOUO) Office of China and Korea (OCK) Discussions [redacted] OCK Analyst [redacted] Foreign Affairs Office	2B4118-5
1530-1630	(U//FOUO) Office of Middle East and Africa (MEA) and Iran Discussions [redacted] GCM MEA	2B4118-5
1630-1645	(U//FOUO) Wrap-up Discussions [redacted] CDO	2B4118-5
1645	(U) Depart	GH 2B
1800	(U//FOUO) SID Hosted Dinner [redacted] Associate D/DIR for Counterterrorism (ADD/CT) (Host) *(By Invitation Only)*	Clyde's Columbia, MD

HR. DIETMAR B[redacted]
Director, SIGINT Analysis and Production
German Federal Intelligence Service (BND)

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

1 May 2013

Time	Presentation Title and Presenter	Location
0850	(U) Arrive	GH 2B
0900-1015	(U//FOUO) Office of Counterterrorism Discussions [redacted], ADD/CT [redacted] D/GCM CT-SIGDEV [redacted], CT Subject Matter Expert (SME)	2B4118-5
1015-1100	(U//FOUO) Office of SIGINT Development Strategy and Governance (SSG) Discussions [redacted] ADD/SSG [redacted], Tech DIR SSG [redacted] D/GCM CT-SIGDEV	2B4118-5
1105-1155	(U//FOUO) NSA/CSS Threat Operations Center (NTOC) Discussions [redacted] D/DIR NTOC	2B4118-5
1200-1245	(U//FOUO) Foreign Affairs Directorate Hosted Lunch [redacted], DIRFA (Host) *(By Invitation Only)*	Canine Suite
1300-1400	(U//FOUO) TUTELAGE Presentation [redacted] D/DIR NTOC [redacted], Assoc. DIR Special Projects, NTOC	2B4118-5
1415-1500	(U//FOUO) Office of International Security Issues (ISI) Discussions [redacted], D/GCM ISI [redacted] CH CT Branch, NSA-Texas (NSAT)	2B4118-5
1500-1600	(U) Wrap-up Discussions [redacted] CH SUSLAG Designee [redacted] CDO	2B4118-5
1600	(U) Depart Met and escorted by [redacted] NSA/CSS SID Protocol Officer.	GH 2B

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

Talking Point Topics Proposal

Name and Title of Visitor: (U//FOUO) Hr. Dietmar B[redacted] Chief Analysis and Production, German Federal Intelligence Service (BND) and Hr. Wilfried K[redacted] Chief of Collection, BND,

Accompanied by: Hr. Dietmar B[redacted] Chief Analysis & Production, German Federal Intelligence Service (BND); [redacted] Chief of Station, German Embassy; [redacted] BND Liaison Officer, Washington; [redacted] DNI Representative, Berlin

Date of Visit: (U) 30 APR – 1 MAY 2013

Visit Background: (TS//SI//REL TO USA, FVEY) Hr. B[redacted] and Hr. K[redacted] will be attending the Strategic Planning Conference, the goal of which is to do planning for the German partnership with NSA.

NTOC Topic(s): Computer Network Defense (CND) - Germany:
(S//REL TO USA, FVEY) Both German President Schindler, and BND SIGINT Director, BG P[redacted] continue to express a desire to increase CND engagement with the NSA. In addition, they have already expanded their cyber collaboration with the Federal Office of Information Security (BSI) and BfV by establishing the T4 (Cyber Intelligence) organization.

(S//REL TO USA, FVEY) As CND continues to be the focus of much discussion with NSA's 3rd Party Partners, Germany is no exception. They continue to seek guidance and advice regarding their CND effort. The T4 organization, although not expected to be fully staffed for almost one year, is almost fully staffed. Of the ~150 positions within this new organization, more than 130 are already filled and the remaining billets are to be filled by 'hackers', who are still being recruited.

(C//REL TO USA, FVEY) In preparation for the 8 May visit by Dr. Maassen, Director BfV, Dr. Massen's office asked for NSA's general assessment of the Mandiant Report and our comments on the structure and responsibilities. No answer was returned to BfV as this is supposed to be a discussion topic during his visit. Regarding the Mandiant Report, NSA was aware of it prior to its release, but NSA did not request its public release nor contribute to it. Notification of this report to our SSEUR partners was given via SIGDASYS, prior to the release of the report.

(S//REL TO USA, FVEY) During a VTC held in early February with personnel from NTOC, FAD, SUSLAG, BND, BSI and BfV, several observations were made:

(S//NF)

- BND/BSI/BfV's CND capability is unclear;
- NSA's Defense Industrial Base (DIB) partnerships and how NTOC gained cooperation was of interest to BSI;

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

- German law currently prohibits BND/BSI/BfV from doing 'near real time' cyber defense activities;
- NTOC provided a summary of TUTELAGE and how it is utilized on the NIPRNet within the .mil space, and
- NTOC requested follow on information on Germany's unique apertures for SIGINT, their ability to consume NSA reporting/data, feedback on the reporting/data being provided and defense and national level network technical information/architectures.

LANDMINE: (S//NF) The potential analytic and operational mission cost for engaging with the Germans appears to be much greater than the value gained by NTOC. NSA should continue to track the Germans' progress and commitment before investing heavily in analytic and operational exchanges.

WAY AHEAD: (S//NF)

- Continue to encourage BND/BSI/BfV to collaborate regarding CND;
- Continue to assess BND/BSI/BfV's capability for collection, analysis, and/or attribution of cyber threat;
- Continue to encourage BND/BSI/BfV to leverage SIGINT to support CND;
- Explore options for providing Lessons Learned on cyber technical, process, and training topics that aid in the development of German SIGINT support to CND, and
- Offer selected briefings/lessons learned discussions via a VTC later this year. Potential topics include: TUTELAGE/DECS implementation, ESF program overview and administration, methodologies for building intrusion sets (Diamond Model, etc.), and lessons learned on operations/intrusion set development

NTOC Point of Contact: (S//REL TO USA, FVEY) [redacted]
19 April 2013.