ENHANCING YOUR INTELLIGENCE AGENCY INFORMATION RESOURCES IQ

PART 3: DEFENSE INTELLIGENCE AGENCY (DIA) AND NATIONAL SECURITY AGENCY (NSA)

Professor Bert Chapman
Purdue University Libraries
FDLP Academy
September 18, 2018

PURDUE UNIVERSITY
Libraries

Graphic design contributions by Aly Edmondson, Purdue University Libraries

DEFENSE INTELLIGENCE AGENCY

- Prior to 1960, there's a lot of duplication in U.S. military intelligence collection, analysis, and findings.
- Eisenhower orders CIA Inspector General Lyman Kirkpatrick to form a joint study group to find a solution.
- Dec. 20, 1960-This group issues report recommending a single unified military intelligence organization.
- Feb. 1961-New SECDEF Robert McNamara orders Joint Chiefs of Staff to devise a plan for a consolidated military intelligence organization. Formally established Aug. 1, 1961 by DOD Directive 5105.21
- Statutory authorities at 10 USC 1601, 1621 and 50 USC 3003 and DOD Directive 5105.21
- 1962 DIA Intelligence School chartered
- 1964 Scientific & Technical Intelligence Directorate established
- 1965 Defense Attaché system established.
- Mission: Producing, analyzing, and disseminating military intelligence information to combat and non-combat military missions. We serve as the Nation's primary manager and producer of foreign military intelligence and are a central intelligence producer and manager for the Secretary of Defense, the Joint Chiefs of Staff (JCS), and the Unified Combatant Command.
- Workforce is a mix of military employees including Army, Navy, Air Force, Marines and Department of Defense (DOD) civilians. Totals over 16,500 men and women work worldwide. Budget classified.

DIA ORGANIZATION

- Headquarters
- Director: Lieutenant General Robert P. Ashley, Jr., USA-Since Oct. 31, 2017-DIA director is a 3 star officer rotating among service branches every three years. Principal advisor to Secretary of Defense and Joint Chiefs of Staff on military intelligence matters.
- Deputy Director: Melissa A. Drisko

- J2 Directorate for Intelligence
- Joint Functional Component Command-Intelligence, Surveillance, & Reconnaissance
- Chief of Staff (COS)
- Chief Financial Officer (CFO)
- General Counsel (OGC)
- Inspector General (OIG)
- Command Senior Enlisted Leader (CSEL)
- Equal Opportunity & Diversity Office (EO)
- National Intelligence University (NIU)
- Executive Secretariat (CSES)
- Strategic Planning, Policy, & Performance Management Office (SPP)
- Office of Corporate Communications (OCC)

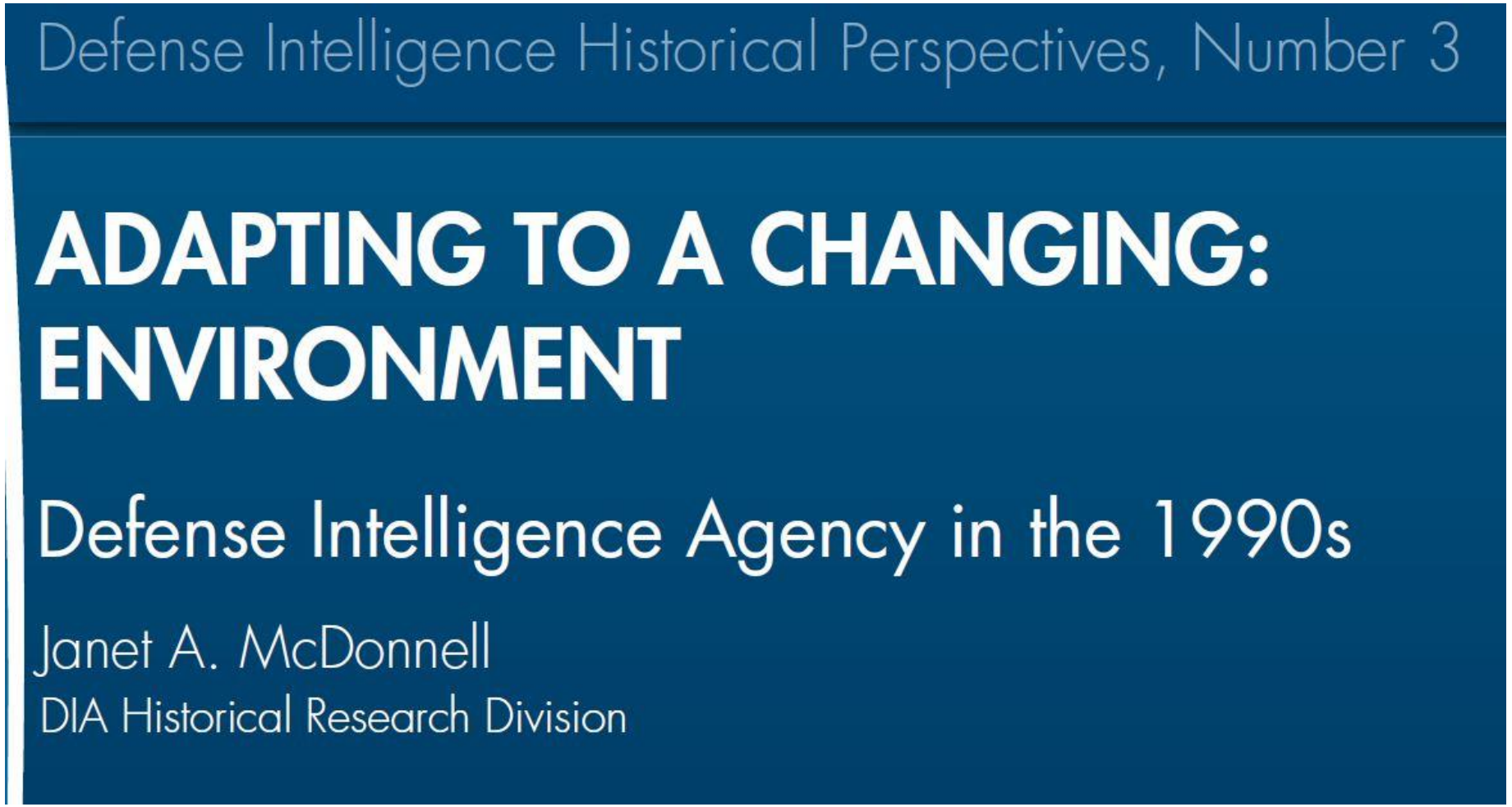
DIA ORGANIZATION

- Directorates
- Directorate for Analysis
- Directorate for Operations
- Directorate for Science & Technology
- Directorate for Mission Services

- Intelligence Centers
- Americas Center
- Asia/Pacific Center
- Europe/Eurasia Center
- Middle East/Africa Center

TRAINING

- Partners with other government entities to deploy trusted intelligence partnerships with combat missions including:
- Intelligence Community Centers for Academic Excellence
- Joint Military Attaché School-Graduates represent the U.S. in 140 countries globally
- Joint Military Intelligence Training Center
- National Intelligence University



DIA HEADQUARTERS – WASHINGTON DC

PURDUE UNIVERSITY
Libraries

Congress: National Defense Authorization Act for Fiscal Years 1992/1993

In the aftermath of the Persian Gulf War, Congress became more deeply involved in Defense department efforts to reform Defense intelligence. Hearings on the war convinced Congress that, despite better support to tactical operations by national intelligence assets than at any other time in our history, there was room for improvement. The Gulf War had revealed a lack of dedicated tactical reconnaissance assets, and severe problems disseminating information that made it difficult or impossible for tactical commanders to obtain critical intelligence. As Pentagon officials began implementing Secretary Cheney's plan for restructuring Defense intelligence, Congress drafted legislation that provided a strong mandate for change in Defense intelligence and would expand DIA's responsibilities. In December 1991 President Bush signed the National Defense Authorization Act for Fiscal Years 1992 and 1993, which acknowledged DIA's role as "the nation's preeminent producer of military intelligence."[29]

At the initiative of the Senate Armed Services Committee (SASC), the National Defense Authorization Act for Fiscal Year 1991 directed the secretary of defense together with the director of central intelligence to conduct a joint review of intelligence and intelligence-related activities in order to eliminate redundancy, strengthen joint intelligence support to combatant commanders, improve threat assessments for acquisition programs, ensure that intelligence priorities reflected the changed security environment, and improve the responsiveness and utility of national intelligence systems and organizations to the needs of

Defense Intelligence Historical Perspectives, Number 1

LEGACY OF ASHES, TRIAL BY FIRE:
The Origins of the Defense Intelligence Agency and the Cuban Missile Crisis Crucible

Michael B. Petersen
DIA Historical Research Support Branch

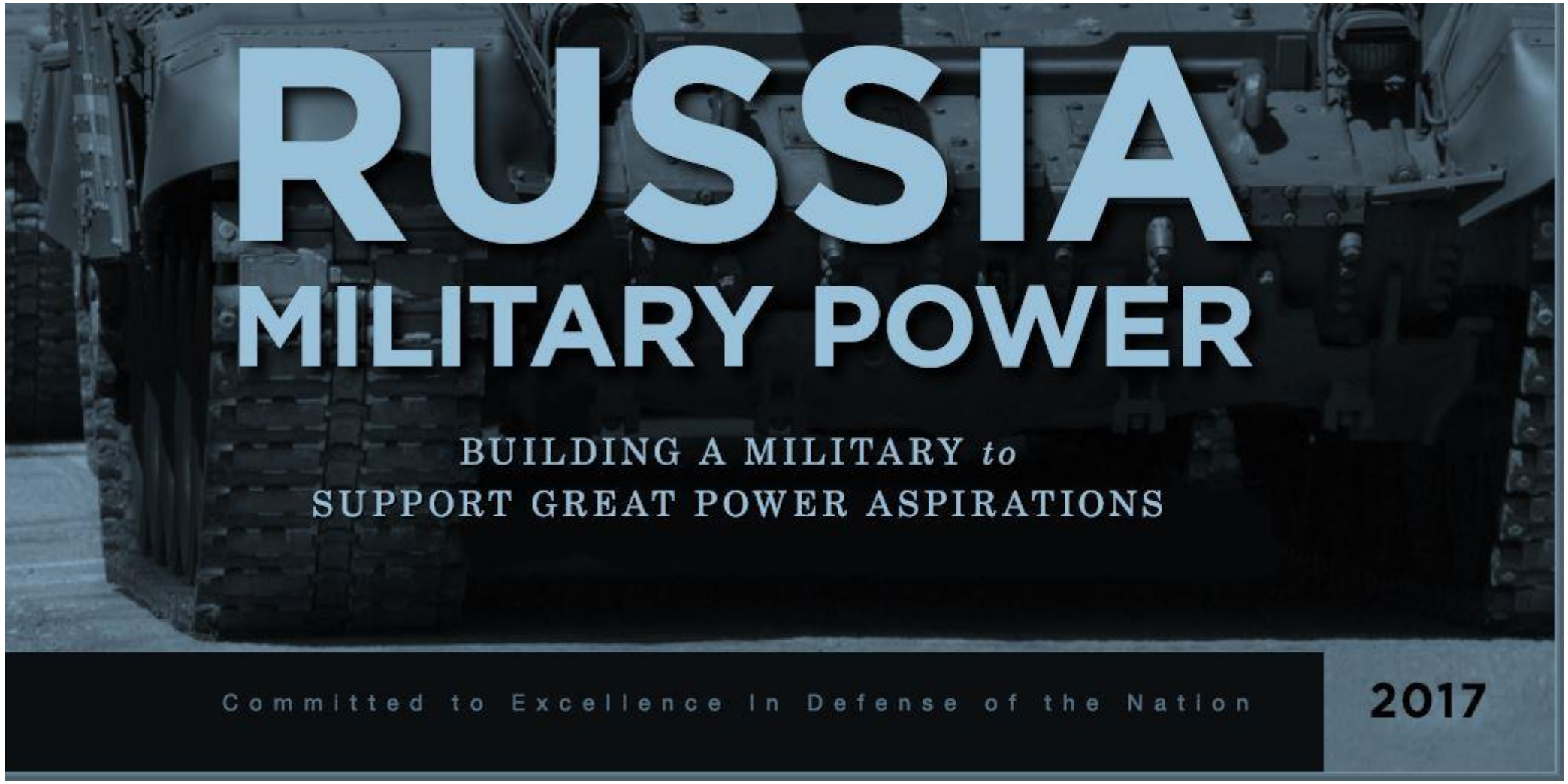
A week later, Carroll notified McNamara and Taylor that DIA analysts, using special crate analysis techniques ("crateology"), had detected the first hard evidence of Il-28/BEAGLE bombers in Cuba, which Carroll considered offensive weapons. At the same time, the accumulating evidence forced Rusk and Bundy to relent on their objections to U-2 overflights. Strategic Air Command, with McNamara's and Gilpatric's support, wrestled control of the flights away from CIA and received permission from Kennedy to conduct one "in and out" reconnaissance run. The selected path was a south to north pass over Piñar del Rio, through the center of the SA-2 triangle and the trapezoidal restricted area noted by Wright on September 21.[54]

On October 14, a U-2 piloted by Air Force Major Richard Heyser arrived over Cuba, where it

DIA Historical Research Support Branch

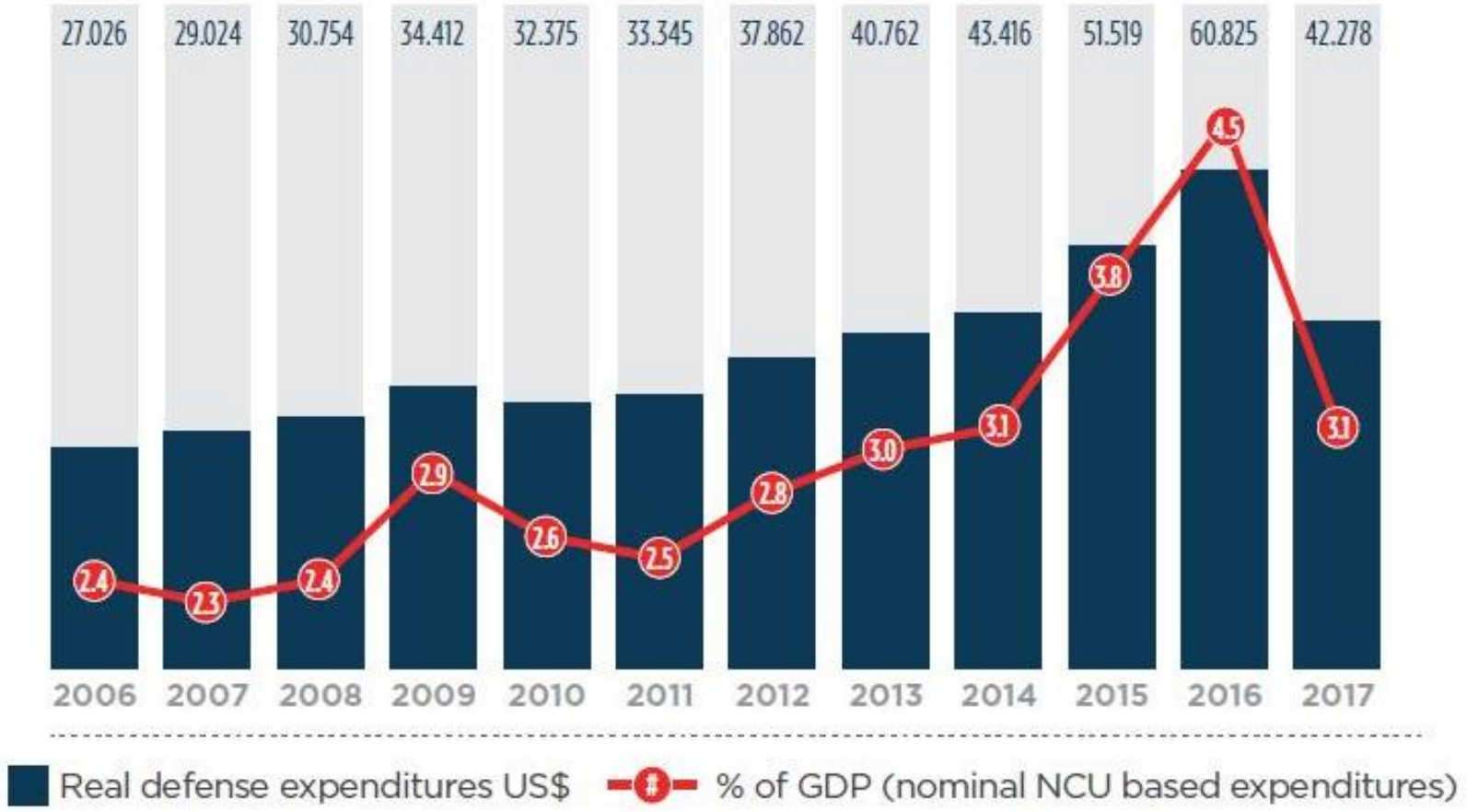
This photo, taken on October 14, revealed the presence of Soviet MRBMs in Cuba. The missiles are visible at the bottom-right of the photo.

Hughes and McLaughlin immediately took the new intelligence to Carroll at his home on Bolling Air Force Base, located hard on the Potomac River in Washington, D.C. Carroll instructed both men to inform Roswell Gilpatric right away, and called the Deputy Secretary of



Russia's Official Defense Spending 2006-2017 (billions of 2017 dollars)[98, 99, 100]

1612-11108



Russian Perceptions of Modern Conflict

Since at least 1991, the Russian perception of the nature of modern conflict has evolved. Russia views wars as often undeclared, fought for relatively limited political objectives, and occurring across all domains, including outer space and the information space.[113] Russian leaders have noted the tendency for crises to arise quickly and develop impetuously, and to potentially escalate from local wars into global ones.[114,115] In addition, Moscow judges that modern conflicts are characterized by a destructive and rapid "initial period of war"—a subject on which Russian military leaders and theorists have written extensively since the 1920s—which is becoming more decisive than ever before. In modern cyber-enabled information and battlefield spaces, this destructive non-kinetic initial period can be reduced to milliseconds, and kinetically to hours.[116]

Moscow fears that the speed, accuracy, and quantity of non-nuclear strategic precision-guided weapons can achieve strategic effects on par with nuclear weapons,[117] one a conflict.[121,122] While most military theorists and leaders believe great-power conflict is unlikely, they nevertheless express concern about the usability of the information space to achieve state goals.[123] Russia has tied this decisive and shortened initial period to the idea that only more proactive or even preemptive action is required to counter it.[124,125,126] Russian developments in precision-guided munitions indicate a desire for "deep strike" capability to preempt attacks from an adversary.

Russia's Military Doctrine, last updated in December 2014, contained several new elements not in the 2010 Doctrine, which reflect Moscow's military focus and threat perceptions. First codified in the doctrine was the concept of non-nuclear deterrence, an idea that has been evolving since the Soviet period. The doctrine also underscored perceived threats to Russia's domestic security and described the military's requirement to inflict unacceptable damage on any adversary at any time. This requires the military to calculate or understand what level of damage

Major themes of Russian propaganda include:

The West's liberal world order is bankrupt and should be replaced by a Eurasian neo-conservative post-liberal world order, which defends tradition, conservative values, and true liberty.[296]

The West demonizes Russia, which is only trying to defend its interests and sovereignty and act as an indispensable nation in world affairs.

The United States is determined to interfere with and overthrow sovereign governments around the world.[297]

Russia uses a Troll Army to disseminate and overwhelm blogs and twitter communications.

The Internet Research Agency in St. Petersburg.

Russian Air Forces Air Bases[433]

1612-11135

Moscow maintains aviation units in Armenia and Kyrgyzstan, represented on the map by the two fighter base symbols outside Russia's borders.

DEFENSE INTELLIGENCE AGENCY

GLOBAL NUCLEAR LANDSCAPE 2018

Nuclear Capability/Stockpile

North Korea established a Strategic Force (previously known as the Strategic Rocket Forces) in 2012 and has described this organization as a nuclear-armed ballistic missile force. The Strategic Force includes units operating SRBMs, MRBMs, IRBMs, and ICBMs, each of which North Korea has stated represents a nuclear-capable system class. In 2016, the North claimed a Scud class SRBM launch had tested nuclear weapon components in a mock attack against a South Korean port.[136]

Infrastructure

North Korea has demonstrated the capability to produce kilogram quantities of plutonium for nuclear weapons and has claimed to possess the ability to produce enriched uranium for nuclear weapons.[137,138] North Korea also admitted in August 2016 that it has been producing highly enriched uranium for nuclear weapons. This put into context North Korea's revelation in 2010 of an enrichment facility at Yongbyon and the subsequent expansion of the facility, and raised concerns about its ability and intention to produce uranium-based nuclear weapons.[139,140]

North Korea has conducted six nuclear tests, one each in 2006, 2009, and 2013, two in 2016, and

missile development process—the first flight tests of a system capable of reaching the United States. Without additional flight tests, the ICBM's current reliability as a weapon system would be low. North Korea subsequently launched another new ICBM, Hwasong-15, in November 2017. North Korea also continues to develop the Taepo Dong 2 (TD-2), which could reach the continental United States if configured as an ICBM but has only been used as a space-launch vehicle (SLV). In April and December 2012 and again in February 2016, North Korea conducted launches of the TD-2 configured as an SLV, which used ballistic missile technology.[145,146]

North Korea has several hundred SRBMs and MRBMs available for use against targets on the Korean Peninsula and Japan. In the past 2 years, North Korea has diversified its ballistic missile force to include longer-range, solid-fueled systems. Solid-propellant missiles offer operational advantages over liquid-fueled systems, eliminating the time required to fuel a missile before firing it.[147] In 2017, North Korea test-launched a new solid-propellant MRBM from a tracked transporter-erector-launcher (TEL), describing this system as a land-based variant of its SLBM.[148] Following a successful flight test of its SLBM from a submerged submarine in September 2016,[149] and a second successful launch in May 2017, Kim approved deployment of the land-

North Korea Nuclear Weapon-Related Facilities

DIA FREEDOM OF INFORMATION ACT (FOIA) RECORDS BY COUNTRIES & SUBJECTS

Afghanistan
Africa
Argentina
ASEAN
Awards
Burma
China
Colombia
Congress
Contracts
Cuba
Defense Intelligence Agency - intelligence Summaries (DIAIS)
Denmark
Detainee Abuse
Detainee Recidivism Reports
Indonesia
Iran
Iraq
Latin America
Medical Reports
Mexico
Nicaragua
North Korea
Norway
Nuclear, Biological, and Chemical
Other Available Records
Pakistan
Peru
Russia
Thesis
Venezuela

PURDUE UNIVERSITY
Libraries

UNCLASSIFIED

DIA SEAL

Defense Intelligence Agency

Defense Intelligence Assessment

Home

Feedbac

Print

(U) Infectious Disease Risk Assessment: Afghanistan

August 2005
DI-1812-AFG-05
Information Cutoff Date: 19 August 2005

Key Judgments

- AFMIC assesses Afghanistan as **HIGH RISK** for infectious diseases. Without force health protection measures, mission effectiveness will be seriously jeopardized. See map for comparison of overall disease risk worldwide.

- **High Risk Diseases**: The main force health protection emphasis should be on these diseases, which are the most likely to degrade operations by affecting a large percentage of personnel, or by causing severe illness in a smaller percentage. High risk diseases are grouped into transmission categories that are prioritized in descending order of risk.

Foodborne And Waterborne Diseases	Diarrhea - bacterial, Hepatitis A, Diarrhea - protozoal, Typhoid / paratyphoid fever
Vector-borne Diseases	Malaria
Animal-contact Diseases	Rabies

Overview:

Sanitation is extremely poor throughout the country, including major urban areas. Local food and water sources (including ice) are heavily contaminated with pathogenic bacteria, parasites, and viruses to which most US service members have little or no natural immunity.

Effective disease surveillance does not exist within the country. Only a small fraction of diseases are identified or reported.

Diarrheal diseases can be expected to temporarily incapacitate a very high percentage of personnel within days if local food, water, or ice is consumed. Hepatitis A and typhoid fever can cause prolonged illness in a smaller percentage.

In addition, though not specifically assessed in this document, viral gastroenteritis (e.g., norovirus) and food poisoning (e.g., Bacillus cereus, Clostridium perfringens, Staphylococcus) may cause significant outbreaks.

The diseases of high risk are listed first, in descending order of expected impact. Diseases of intermediate risk, with a lower or unknown likelihood to degrade operations, are listed alphabetically in tabular form.

Diarrhea - bacterial

8. ~~(C/NF)~~ VENEZUELA: A CONTROVERSY OVER THE MATTER OF JURISDICTION IN A NAVY CORRUPTION SCANDAL HIGHLIGHTS THE COUNTRY'S CONTINUING CIVIL-MILITARY TENSION. TENSION REPORTEDLY ESCALATED LATE LAST WEEK FOLLOWING THE ISSUANCE OF CIVILIAN ARREST WARRANTS FOR FOUR SENIOR NAVAL OFFICIALS BELIEVED INVOLVED IN CONTRACTING
/****** BEGINNING OF SECTION 004 ******/
IRREGULARITIES. UNDER NORMAL CONDITIONS, MILITARY AUTHORITIES MAINTAIN JURISDICTION OVER ACTIVE DUTY PERSONNEL. RESOLVING THIS CASE, HOWEVER, COULD TAKE MONTHS, AND PRESIDENT PEREZ WILL PROBABLY PROCEED CAUTIOUSLY TO AVOID WORSENING THE ARMED FORCES' DISCONTENT THAT HAS LINGERED SINCE THE 4 FEBRUARY COUP ATTEMPT. IN ADDITION, GOVERNMENTAL OFFICIALS WORRY THAT PROLONGED NEWS MEDIA ATTENTION TO THE SCANDAL WILL INCREASE THE PUBLIC'S DEMANDS FOR WIDE-SCALE CORRUPTION INVESTIGATIONS THAT COULD IMPLICATE PEREZ. IN ANY EVENT, THE JURISDICTIONAL CONTROVERSY SURFACED ONLY HOURS BEFORE PEREZ ORDERED THE MILITARY COURT TO PROHIBIT THE AIRING OF A POTENTIALLY DESTABILIZING INTERVIEW WITH LT COL **HUGO CHAVEZ**, THE JAILED LEADER OF THE FEBRUARY **COUP** ATTEMPT. THE SENIOR LEADERSHIP HAS CONTINUALLY PLAYED DOWN THE POSSIBILITY OF ANOTHER COUP ATTEMPT. ACCORDING TO (b)(3):10 USC 424 HOWEVER, CONSIDERABLE PRO-CHAVEZ SENTIMENT REMAINS ENTRENCHED IN THE NCO RANKS. (b)(3):10 USC 424

[redacted]

SOURCE: A. (U) DAILY NEWSPAPER, "EL NUEVO DIARIO", MANAGUA, NICARAGUA, 20010417 (U), SPANISH. THE PAPER IS KNOWN FOR ITS LEFTIST VIEWS AND IS CONSIDERED SENSATIONALISTIC IN BOTH EDITORIALS AND IN REPORTING. WIDELY READ AND CONSIDERED INFLUENTIAL.

[redacted]

SUMMARY: (U) MEDIA PORTRAY US INVOLVEMENT IN EVENTS SURROUNDING VENEZUELAN PRESIDENT CHAVEZ COUP AND COUNTER-COUP - US POSITION AND HANDLING OF EVENTS SEEN AS DIPLOMATIC FAILURE.

TEXT: 1. (U) SOURCE A REPORTS THAT ACCORDING TO VENEZUELAN AMBASSADOR IN NICARAGUA, MIGUEL ((GOMEZ)) NUNEZ, THAT CARACAS IS TEACHING WASHINGTON THE ABC'S OF DEMOCRACY. ACCORDING TO GOMEZ THE UNITED STATES CANNOT BEHAVE AS IF DEMOCRACY IS A GOOD THING WHEN IT IS TO THEIR (USG) ADVANTAGE AND THAT DEMOCRACY IS A BAD THING WHEN IT IS TO THEIR DISADVANTAGE. GOMEZ REMARKED THAT DEMOCRACY MUST BE A SINGULAR AND INDIVISIBLE CONSTRUCT. VENEZUELAN AMBASSADOR GOMEZ WHO CLAIMS TO BE OVERSHADOWED BY EVERY PUBLIC PRONOUNCEMENT MADE BY THE U.S. AMBASSADOR NOW HAS THE MEDIA LIMELIGHT THRUST ON HIM. ACCORDING TO AMBASSADOR GOMEZ, THE RETURN TO POWER OF HUGO CHAVEZ DEMONSTRATES THE GREAT POLITICAL FAILURE OF THE MIGHTY UNITED STATES THAT SEEKS TO

R 240953Z MAY 91
FM (b)(3):10 USC 424
TO RUEKJCS/DIA WASHDC
INFO RUSNNOA/USCINCEUR VAIHINGEN GE/(b)(3):50 USC 403-1(G)
RUSNAAA/USEUCOM (b)(3):50 USC 403-1 VAIHINGEN GE
BT

NTROLS:
[redacted] (b)(3):10 USC 424

[redacted]

-
SERIAL: (U) IIR (b)(3):10 USC 424

DY:

-
COUNTRY: (U) IRAN (IR); CHINA (CH); SOVIET
- UNION (UR); PAKISTAN (PK).
-
SUBJ: IIR (b)(3):10 USC 424 /IRAN IN THE MARKET FOR TANKS,
- FIGHTERS AND SSM'S FROM CHINA AND SOVIET UNION (U)

SUMMARY: [redacted] IRAN HAS RECENTLY CONDUCTED EXPLORATORY DISCUSSIONS WITH CHINA TO ACQUIRE M-11 MISSILES AND T-69 TANKS. AGREEMENT REACHED ON SALE OF F-7 AIRCRAFT TO IR.

-

TEXT: 1. [redacted] IN DISCUSSIONS 910500 WITH CH TO ACQUIRE SSM'S, IRAN WAS OFFERED AN UNDISCLOSED NUMBER OF M-9 MISSILES. IR INDICATED IT WAS INTERESTED IN CONVENTIONAL SRBM WITH A RANGE OF AT LEAST 1,000 MILES SUCH AS THE M-11. CH DID AGREE IN PRINCIPLE TO SELL THE M-11, BUT THE DETAILS ARE YET TO BE FINALIZED.

-

2. [redacted] IR IS ALSO INTERESTED IN PURCHASING 1,000 MAIN BATTLE TANKS OVER A TWO TO THREE YEAR PERIOD. CH OFFERED TO PROVIDE T-69 TANKS TO IR AT 750,000 USD EACH. IR WOULD PREFER TO PURCHASE THE MORE ADVANCED MT-2000, AND IR IS INTERESTED IN CO-PRODUCTION OF THE MT-2000 IN IR. CH HAS ALREADY AGREED TO CO-PRODUCE THE MT-2000 WITH PAKISTAN, BUT INITIAL PRODUCTION MAY BE AS MUCH AS TWO YEARS IN THE FUTURE. IR MAY AGREE TO PURCHASE SOME T-69'S NOW IF AN AGREEMENT ON MT-2000 CO-PRODUCTION IN IR CAN BE REACHED. (b)(3):10 USC 424 -- IR HAS ALSO DISCUSSED THE SALE OF UP TO 1,000X T-72M1 TANKS FROM THE SOVIETS.

(b)(1),(b)(3):10 USC 424,1.4 (c)

NATIONAL SECURITY AGENCY (NSA)-CENTRAL SECURITY SERVICE

PURDUE UNIVERSITY
Libraries

NSA MISSIONS AND OBJECTIVES

- Saving lives
- Defending vital networks
- Advancing U.S. goals and alliances
- Protecting privacy rights
- Enabling national decision-makers to know what adversaries are doing and what their capabilities are so we can make decisions & plans & execute policies & operations.
- Be able to communicate and exchange information securely, so that our adversaries can't undermine our plans.
- Must be able to outmaneuver those who would do us harm in cyberspace.

- NSA is the world leader in cryptology-the art & science of making codes.
- Cyber threats to U.S. national and economic security increase each year in frequency, scope and severity of impact. Cyber criminals, hackers and foreign adversaries are becoming more sophisticated and capable every day in their ability to use the Internet for nefarious purposes.
- Our information networks and technology are constantly at risk from a variety of bad actors using a multitude of techniques – remote hacking intrusions, the placement of malware, spearphishing and other means of gaining access to networks and information.

Paul M. Nakasone
General U.S. Army
Commander, U.S. Cyber Command
Director, National Security Agency
Chief, Central Security Service

George C. Barnes
Deputy Director, National Security Agency

Rachel "Rach" J. Velasco-Lind
Captain, U.S. Navy
Acting Deputy Chief, Central Security Service

Harry Coker, Jr.
Executive Director, National Security Agency

Earnest 'Earnie' Green
Chief of Staff, National Security Agency

NSA HEADQUARTERS-FORT MEADE, MD

PURDUE UNIVERSITY
Libraries

NSA ESTABLISHED BY PRESIDENT TRUMAN NOV. 4, 1952

MEMORANDUM FOR: The Secretary of State
The Secretary of Defense

SUBJECT: Communications Intelligence Activities.

The communications intelligence (COMINT) activities of the United States are a national responsibility. They must be so organized and managed as to exploit to the maximum the available resources in all participating departments end agencies 2nd to satisfy the legitimate intelligence requirements of all such departments and agencies.

I therefore designate the Secretaries of State and Defense as a Special Committee of the National Security Council for COMINT, which Committee shall,

KEY NSA HISTORICAL EVENTS

- 50 USC 3601 et. seq. legal authority.
- Director is presidentially appointed and subject to Senate confirmation.
- 1952 Venona Project uncovers massive Soviet espionage effort to threaten national security. Declassified in 1990s.
- 1957 NSA moves to Fort Meade, MD
- 1959 P.L. 86-36 gives NSA greater statutory authority.
- 1962 Cuban Missile Crisis-Signals Intelligence (SIGINT) plays critical role in defusing this crisis.
- 1964 P.L. 88-290 Covers NSA Personnel Security Procedures
- June 1967-U.S.S. Liberty accidentally sunk by Israel during Six Day War
- Jan. 1968-North Korea seizes U.S.S. Pueblo and holds crew for one year. Ship remains in N. Korea
- 1972 Central Security Service establishes full partnership between NSA and armed forces cryptologic elements
- Ca. 1975 NSA target of Church Committee inquiries into intelligence community activities.
- Jan. 22, 1980-Guidance given for Tactical Cryptologic Program
- 1983 Korean Air Lines Flight 007 shot down by Soviet Union. NSA intercepts of Soviet jet fighter pilot conversation publicly released.
- 1985 Former NSA employee Ronald Pelton & John Walker convicted of espionage for Soviet Union.
- 1987 Computer Security Act (ongoing concern for NSA)

KEY NSA HISTORICAL EVENTS

- 1991 NSA provides key SIGINT support during Operation Desert Storm
- 1993-National Cryptologic Museum Opens
- 2001 9/11 Attacks
- 2003-present NSA assists in wars in Afghanistan and Iraq.
- 2010 NSA Director General Keith Alexander also appointed Cybercom Director.
- 2013 Former NSA Contractor Edward Snowden leaks information on surveillance programs affecting multiple countries to various media outlets flees to Russia.
- 2016 House Intelligence Committee executive summary report reveals Snowden removed over 1.5 million classified documents from "secure" NSA network; caused tremendous national security damage; stolen documents did not deal with individual privacy, but had defense, military, & intelligence interest of great interest to U.S. adversaries, Snowden was not a whistleblower and did not notify intelligence officials of concerns about propriety of intelligence programs; was reprimanded for a workplace dispute with NSA managers prior to beginning downloads; remains a serial exaggerator and fabricator, House Intel Committee remains concerned that the Intelligence Community and NSA have not done enough to minimize risk of another massive unauthorized disclosure.

What is Signals Intelligence?

- SIGINT involves collecting foreign intelligence from communications and information systems and providing it to customers across the U.S. government, such as senior civilian and military officials. They then use the information to help protect our troops, support our allies, fight terrorism, combat international crime and narcotics, support diplomatic negotiations, and advance many other important national objectives.
- NSA/CSS collects SIGINT from various sources, including foreign communications, radar and other electronic systems. This information is frequently in foreign languages and dialects, is protected by codes and other security measures, and involves complex technical characteristics. NSA/CSS needs to collect and understand the information, interpret it, and get it to our customers in time for them to take action. Our workforce is deeply skilled in a wide range of highly technical fields that allow them to this work, and they develop and employ state-of-the-art tools and systems that are essential to success in today's fast-changing communications and information environment. Our researchers are working constantly to help us anticipate and prepare for future developments.

2. HOW ARE THE ACTIVITIES OF THE NSA/CSS REGULATED AND WHO MONITORS THEM?

The U.S. Constitution, federal law, executive order, and regulations of the Executive Branch govern NSA's activities. As a defense agency, NSA operates under the authority of the Department of Defense. As a member of the Intelligence Community, NSA also operates under the Office of the Director of National Intelligence. NSA/CSS activities are subject to strict scrutiny and oversight both from the outside and from within. External bodies such as the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), the President's Intelligence Oversight Board, the Foreign Intelligence Surveillance Court, the Department of Defense, and the Department of Justice provide oversight to ensure the Agency's adherence to U.S. laws and regulations. Internally, the Office of the Inspector General conducts inspections, audits, and investigations to make certain that NSA/CSS operates with integrity, efficiency, and effectiveness, while the Office of the General Counsel provides legal advice. Most importantly, each NSA/CSS employee is charged with knowing, understanding, and obeying to the fullest the laws of the nation.

WHAT IS NSA'S ROLE IN U.S. CYBERSECURITY?

NSA's role in U.S. cybersecurity includes its primary information assurance mission: serving as the National Manager for National Security Systems. National Security Systems include U.S. systems that contain classified information or are otherwise critical to U.S. military or intelligence missions.

What does NSA do as the National Manager for National Security Systems? NSA performs a number of functions that help the Government protect and defend those systems, such as approving standards, techniques, systems, and equipment related to the security of National Security Systems.

Additionally, NSA is uniquely positioned to contribute to U.S. cybersecurity because it also has a foreign signals intelligence mission. The two missions complement one another, enhancing the agency's ability to detect and prevent cyber threats. NSA employs experts in signals intelligence, information security, and computer network defense and exploitation. Their work gives NSA end-to-end insights into malicious cyber activity, the activities of hostile foreign powers, and cyber best practices. This expertise is often called on by partners across the Department of Defense and the Intelligence Community to help the government mitigate threats and secure networks.

Finally, NSA works to advance the state of cybersecurity by partnering with industry and academia through research efforts such as the NSA Technology Transfer Program, and the Science of Security Initiative. NSA also helps develop the skills of the next generation of cyber professionals through programs like the NSA Cyber Exercise (NCX), and the Centers of Academic Excellence in Cybersecurity. For more, see NSA's Information Assurance, and Research pages.

News & Stories

2018

07/23/2018	NSA Police K9 Unit Celebrates 140 Dog Years!
07/09/2018	Mission Critical: Engaging Schools and Students for Tomorrow's Workforce
06/07/2018	Near Record Crowds Honor America's Sons & Daughters at National Cryptologic Museum
06/06/2018	Cyber on I-C-E
05/30/2018	Memorial Wall Observance Honors Soldier and His Family's Sacrifice
05/21/2018	NSA Colorado Welcomes Students from University of Colorado Boulder
05/18/2018	Armed Services Week Viewpoint: Q&A With A Veteran Who Continues to Serve
05/07/2018	National Cryptologic Museum To Celebrate "America's Sons & Daughters" at Armed Forces and National Police Celebration
05/04/2018	NSA Welcomes General Paul Nakasone as Agency Director
04/20/2018	NSA's Innovative Cyber Tool: "Unfetter" Makes Cyber Better
04/18/2018	New NSA-funded "Lablets" to Advance the Science of Security and Privacy
04/05/2018	NSA's Cybersecurity Operations Mission in the Public Eye
03/28/2018	U.S. Naval Academy wins the inaugural NSA Cyber Exercise
03/28/2018	Smithsonian National Air and Space: WWII Women Cracking The Code
03/27/2018	Women of NSA Champion Leadership
03/14/2018	The Inaugural NSA Cyber Exercise, former Cyber Defense Exercise, brings new cyber competition to U.S. Service Academy Cadets and Midshipmen.

Speeches and Congressional Testimonies

Speeches | Congressional Testimonies

Speeches

05/23/2018	*Failing to Keep Pace: The Cyber Threat and Its Implications for Our Privacy Laws* by Glenn S. Gerstell, NSA General Counsel, at the Georgetown Cybersecurity Law Institute in Washington, D.C. on May 23, 2018
04/09/2018	*How We Need to Prepare for a Global Cyber Pandemic* by Glenn S. Gerstell, NSA General Counsel, at The Cipher Brief Threat Conference, Sea Island, Georgia, on April 9, 2018
9/14/2017	*Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act* by Glenn S. Gerstell, NSA General Counsel, at The Robert S. Strauss Center for International Security and Law and The University of Texas School of Law, on September 14, 2017
2/25/2017	*Confronting the Cybersecurity Challenge* Keynote Address by Glenn S. Gerstell, NSA General Counsel, at the 2017 Law, Ethics and National Security Conference, Duke Law School, on February 25, 2017
2/23/2015	Remarks by Admiral Michael S. Rogers at the New America Foundation Conference on Cybersecurity, Washington, D.C., on February 23, 2015
1/8/2015	Remarks by Admiral Michael S. Rogers at Fordham University's Fifth International Conference on Cyber Security (ICCS 2015), New York, New York, on January 8, 2015

Failing to Keep Pace: The Cyber Threat and Its Implications for Our Privacy Laws by Glenn S. Gerstell, NSA General Counsel

Georgetown Cybersecurity Law Institute, Washington, DC

May 23, 2018

Imagine walking through the front doors of your office on a Thursday morning and immediately receiving a note instructing you not to turn on your work computer for an indefinite period of time. On March 22, this very scenario played out in Atlanta's City Hall, as employees were handed printed instructions that stated, in bold, "Until further notice, please do not log on to your computer." At 5:40 that morning, city officials had been made aware that a particular strain of SamSam ransomware had brought municipal services in Atlanta to a halt. This type of ransomware is known for locking up its victims' files with encryption, temporarily changing those file names to "I'm sorry," and giving victims a week to pay a ransom.

Residents couldn't pay for things like water or parking fines. The municipal courts couldn't validate warrants. Police resorted to writing reports by hand. The city stopped taking employment applications. One city council member lost 16 years of data.

Officials announced that the ransom demand amounted to about $51,000, but have not indicated whether the city paid the ransom. Reports suggest, however, that the city has already spent over $2 million on cybersecurity firms who are helping to restore municipal systems. Atlanta also called in local law enforcement, the FBI, DHS, the Secret Service, and independent forensic experts to help assess what occurred and to protect the city's networks in the future.

Taking a somewhat relaxed approach to cybersecurity, as the situation in Atlanta seems to have demonstrated, is clearly risky, but unfortunately, it is not uncommon. As our reliance on digital technology has increased, both private companies and public sector entities have experienced crippling cyberattacks that brought down essential services. Atlanta is but one example of the pervasiveness of connected technologies and the widespread impact on our lives when those technologies no longer function correctly.

We've reached an inflection point: we now depend upon connected technology to accomplish most of our daily tasks, in both our personal and business lives. At least one forecast predicted that over 20 billion connected devices will be in use by 2020. I hardly need tell the audience at a cybersecurity conference about the nature and scope of our cyber vulnerabilities. What's surprising is not the extent of this vulnerability, but that it has manifested itself in ways that haven't yet had dramatic, society-wide effects, although the Atlanta example is

NSA's Puzzle Periodical

Intelligence. It's the ability to think abstractly. Challenge the unknown. Solve the impossible. NSA employees work on some of the world's most demanding and exhilarating high-tech engineering challenges. Applying complex algorithms and expressing difficult cryptographic problems in terms of mathematics is part of the w NSA employees do every day.

Try your hand at this month's problem written by a member of our expert workforce.

2018 ▾ Jan Feb Mar Apr May Jun Jul

2018 Puzzles

- July Puzzle Periodical
- June Puzzle Periodical
- May Puzzle Periodical
- April Puzzle Periodical
- March Puzzle Periodical
- February Puzzle Periodical
- January Puzzle Periodical

The Puzzle Periodical

Puzzle created by:
Dr. Benjamin E., NSA Research Mathematician
Dr. Sean W., NSA's Super Genius Extraordinaire (ala Wile E. Coyote), NSA Research Computer Scientist

Problem

1. (*Easy Difficulty*) You are given two bags of marbles, one contains only white marbles and the other contains only black marbles. You decide, for fun, to randomly take a number between zero and 20 marbles from each bag and put them in a bowl. Once you've done this, you mix the marbles up and pick two marbles from the bowl sight unseen. If the two marbles are both black, you put a black marble back in the bowl. However, if at least one of the two marbles is white you put a white marble back in the bowl. You repeat this process (drawing two marbles, putting one marble back based on this rule) until you are left with a single marble in the bowl, in which case you note the color of the final marble. You then put all the marbles back in the correct bags and repeat the experiment again with different numbers of white and black marbles. After doing this lots of times, you notice that sometimes there is a black marble left and sometimes a white marble left.
   Can you figure out when the last marble will be black and when it will be white?

2. (*Easy Difficulty*) This is same as the first part, except this time when you draw two marbles, if at least one of the two marbles is black then you put a black marble back, while if both of the marbles are white you put a white marble back.
   Can you figure out when the last marble is black and when it's white?

3. (*Hard Difficulty*) For the third experiment, you put a black marble back if and only if the two marbles you draw are different (i.e. one white and one black). If they are the same color (both black or both white) you put a white marble back.
   Can you figure out when the last marble is black and when it's white?

DECLASSIFIED NSA DOCUMENT COLLECTIONS

Declassification & Transparency

As NSA/CSS reviews records under the Freedom of Information Act or Mandatory Declassification Review provisions of Executive Order 13526, we will make the material available to the public via the NSA.gov website on the Internet. In addition, NSA/CSS periodically conducts "Special Topical Reviews" of categories of records, such as the Gulf of Tonkin, USS Liberty, UKUSA, and posts those records to this site. Lastly, in accordance with the federal Open Government initiative, we will identify subjects and records for which there is a general public interest. We will meet transparency goals by reviewing those records and including them on this web page.

Declassification & Transparency Index

FOIA Reports and Releases

Historical Events, Figures and Documents

PURDUE UNIVERSITY
Libraries

DECLASSIFIED NSA COLLECTIONS

Historical Events, Figures and Documents

- C130 Shootdown
- Communication Intelligence Board
- Cuban Missile Crisis
- European Axis Signal Intelligence in World War II
- Foundations of COMSEC
- *Gamblers Ruin* an Article by Tom Lehrer
- Gulf of Tonkin
- John F. Kennedy Assassination
- Korean War
- NSA 60th Anniversary
- Oral History Interviews
- The Beale Papers
- Truman Memorandum, Oct, 24, 1952
- UKUSA Signals Intelligence Agreement Documents
- U.S.S. *Liberty*
- U.S.S. *Pueblo*
- VENONA
- Vietnam Paris Peace Talks
- Vietnam POW/MIA Documents
- William F. Friedman Collection of Official Papers

NSA Internal Periodicals and Publications

- Ask Zelda
- Communicators
- Cryptologic Histories
- Cryptologic Quarterly Articles
- Cryptologic Spectrum Articles
- Cryptologic Almanac Articles
- Cryptologs
- History of the Army Security Agency
- History Today Articles
- Inspector General Report, Jan. 7, 2016
- Military Cryptanalysis
- NSA Early Computer History
- NSA Newsletters
- NSA Technical Journal Articles
- NSA/CSS Policies
- Untangling the Web (PDF)

PURDUE UNIVERSITY
Libraries

The SIGINT Background

by David A. Hatch with Robert Louis Benson

Contents

Introduction

Since the revelation of the vital role of cryptology in World War II, the contribution of communications intelligence (COMINT) and communications security (COMSEC) in postwar conflicts has become a frequent question for many, particularly scholars and veterans' groups.

This short summary of the cryptologic background to the Korean War is intended to provide only a general overview of the conflict from a cryptologic perspective and give initial answers to some of the more important questions about intelligence support

1964 GULF OF TONKIN RELATED COMMAND & TECHNICAL MESSAGES-AUG. 2-AUG. 26

Related Command and Technical Messages from 02 Aug 1964 to 26 Aug 1964 - Release 1

020302Z Aug	From DIRNSA B205/241-64 (64.7KB)
020429Z Aug	From DIRNSA B205/242-64 (31.8KB)
	From CTG 72.1; 020531Z Aug (35.0KB)
020716Z Aug	From USN-27 Critic (44.6KB)
	From CTG 72.1; 020807Z Aug (16.7KB)
020808Z Aug	From CTG SEVEN SEVEN PT FIVE (21.6KB)
020829Z Aug	From CTG 72.1 (37.3KB)
020947Z Aug	From DIRNSA B205/243-64 (81.5KB)
020949Z Aug	From CTG 72.1 (60.2KB)
	From CINCPACFLT; 020919Z (25.6KB)
021008Z Aug	From CTG SEVEN SEVEN PT FIVE (59.2KB)
021124Z Aug	From DIRNSA B205/244-64 (47.2KB)

ACTION PRECEDENCE	INFO PRECEDENCE	SPECIAL HANDLING
FLASH	IMMEDIATE	NONE

FROM: DIRNSA

DATE: Ø1 AUGUST 1964

TO: COMSEVENTHFLEET
[redacted]
CINCPACFLT

INFO: JCS
CNO
SSO MACV
[redacted]
USN-27
NSAPAC REP VIETNAM ~~(C)~~
HQ NSAPAC
[redacted]
NSAPAC REP PHIL

DISTRIBUTION
ADP
ADN
PØ5
PØ4
B
B2
B22
B26
DRF
PØ55

NSA25X1
NSA25X3

S E C R E T KIMBO

B2Ø5/241-64

SUBJ: POSSIBLE PLANNED ATTACK BY DRV NAVY ON DESOTO PATROL

USN-27 SPOT REPORT 2/Q/VHN/R26-64/Ø11924Z REPORTS SIGINT

TAB

SUGGESTIONS THAT DRV NAVY MAY INTEND ATTACK UPON DESOTO PATROL.

FYI, IN RELATION TO THIS POSSIBILITY, DRV NAVAL COMMUNICATIONS

OF 3Ø AND 31 JULY REPORT AN ATTACK ON HON ME ISLAND (19-21N/105-

USS LIBERTY INCIDENT JUNE 8 1967

What's New?

On 08 June 2007, the National Security Agency (NSA) finalized the review of all material relative to the 08 June 1967 attack on the USS Liberty. This additional release adds to the collection of documents and audio recordings and transcripts previously posted to the site on 02 July 2003.

The attack on the USS Liberty, like others in our nation's history, has become the center of considerable controversy and debate. It is not NSA's intention to prove or disprove any one set of conclusions, many of which can be drawn from a thorough review of this material. Instead, through these public releases, we intend to make as much information as possible available for the many scholars, historians, academia, and members of the general public who find interest in analyzing the information and forming their own conclusions.

Release Contents

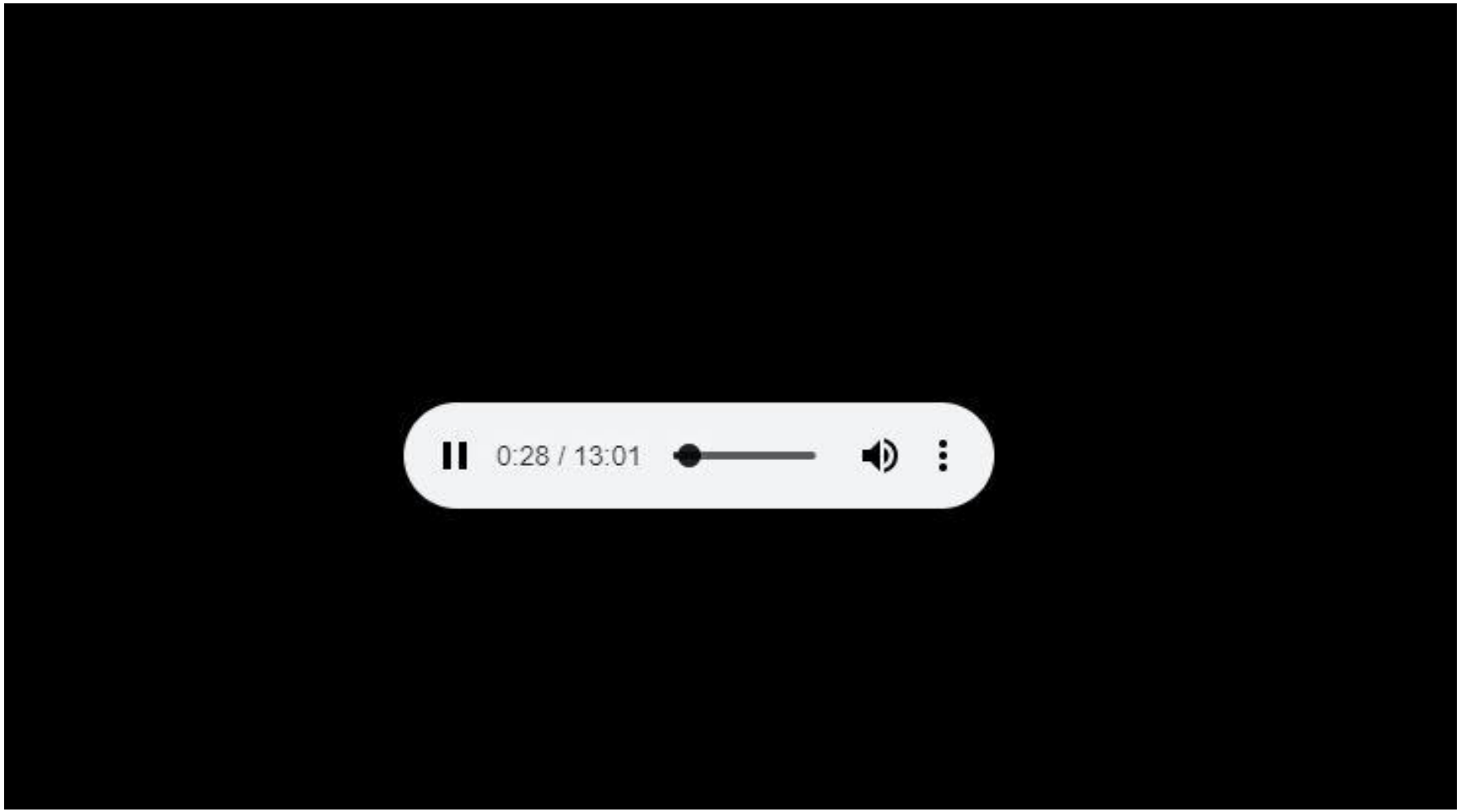
- Chronology of Events
- Oral History Interviews
- Audio Recordings & Transcripts
- Follow-up Reports
- DIRNSA Messages
- USS Liberty Messages
- U.S. Navy Messages
- Naval Security Group Messages
- Field Unit Messages
- Joint Chiefs of Staff Messages
- CINC Messages
- National Military Command Center Documents
- U.S. Air Force Messages
- Defense Intelligence Agency Messages
- State Department Correspondence
- Miscellaneous Memoranda and Reports
- Photographs

Audio Recordings & Transcripts

Within an hour of learning that the Liberty had been torpedoed the Director, NSA, LTG Marshall S. Carter, USA, sent a message to all intercept sites requesting a special search of all communications that might reflect the attack or reaction. No communications were available. However, one of the airborne platforms, a U.S. Navy EC-121, had collected voice conversations between two Israeli helicopter pilots and the control tower at Hazor Airfield following the attack on the Liberty. The recordings are in Hebrew and contain time counts in English that were added by the intercept operator.

- Audio Recording Labeled 104, dated 8 June 1967, 1229Z-1244Z
  Transcript (in English) PDF Format - 8,076KB
- Audio Recording Labeled 105, dated 8 June 1967, 1247Z-1319Z
  Transcript (in English) PDF Format - 2,866KB
- Audio Recording Labeled 130, dated 8 June 1967, 1307Z-1311Z
  Transcript (in English) PDF Format - 821KB

Date Posted: May 3, 2016 | Last Modified: May 3, 2016



PURDUE UNIVERSITY
Libraries

(815) 5/5

[redacted]

PAY ATTN: THE SHIP HAS NOW BEEN IDENTIFIED
AS AN EGYPTIAN SHIP. YOU ARE RETURNING HOM

(815) [redacted]

RGR.

[redacted]

(815) [redacted]

AFFIRMATIVE. 810 CONTACTED YOU ALSO.

[redacted]

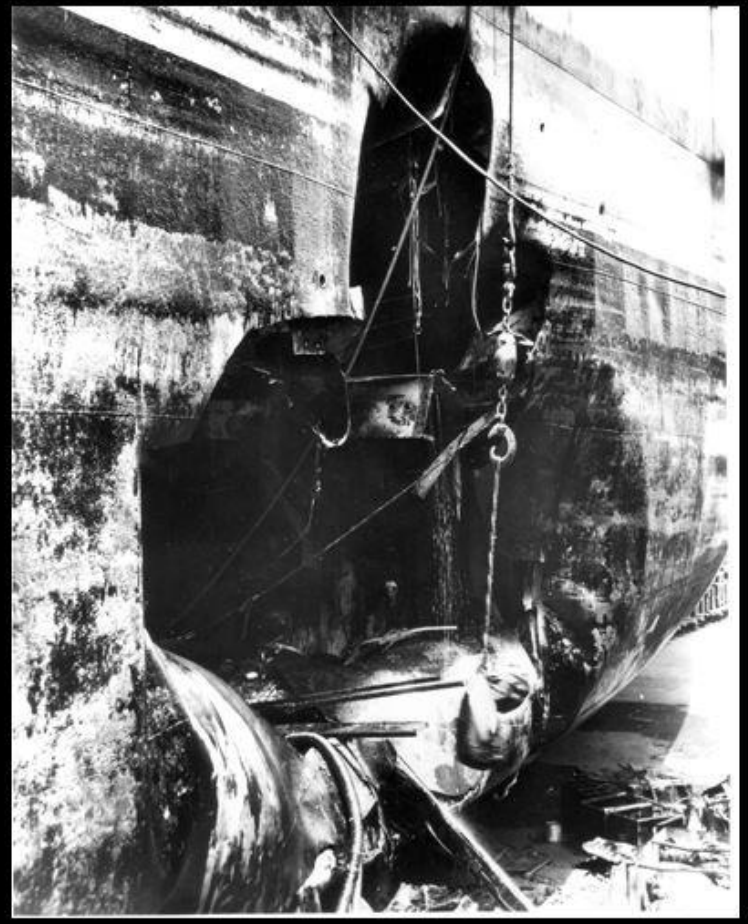
(815) [redacted]

AFFIRMATIVE, QSL, RETURNING.

[redacted]

RGR.

Torpedo Hole from Drydock Floor3



NSA CYBERSECURITY THREAT OPERATIONS CENTER (NCTOC) TOP 5 SECURITY OPERATIONS CENTER (SOC) PRINCIPLES

- Establish a defendable perimeter.
- Ensure visibility across the network.
- Harden to Best Practices.
- Use comprehensive threat intelligence and machine learning.
- Create a culture of curiosity.

- NSA/DHS NATIONAL CAE IN CYBER DEFENSE DESIGNATED INSTITUTIONS (examples)
- Indiana University
- Ivy Tech Community College
- Purdue University
- Purdue University Northwest
- Iowa State University
- Fort Hays State University
- Kansas State University
- University of Kansas

PURDUE UNIVERSITY
Libraries

NATIONAL CRYPTOLOGIC MUSEUM

General Information

Hours: The museum is open to the public Monday through Friday 9 a.m. to 4 p.m. Field trips may be scheduled to begin anytime between 9 and 2 p.m. Most field trips are scheduled for the morning hours so book early to reserve the desired date and time.

Admission

FREE!!!

Chaperones

A minimum of one chaperone for every ten students is required. Additional chaperones are welcomed and encouraged.

Gift Shop

The museum shop is open Monday through Friday 10 a.m. to 3:30 p.m. If you would like students to have an opportunity to visit the store, please schedule additional time in your trip. Students are only permitted in the gift shop with the teacher's approval and when accompanied by an adult. Because the store is small, only six students and a chaperone are permitted in the store at one time. The store carries a variety of items emblazoned with the National Security Agency emblem. Items range from pencils to clothing and books

Transportation

No public transportation is available to the museum. Ample parking is available for cars and buses. Click here for map and directions.

PURDUE UNIVERSITY
Libraries

For images of many of the exhibits listed below, please visit our National Cryptologic Museum Current Exhibits Image Gallery.

- 18th Century Cipher Device
- African-American Experience
- American Civil War
- American Civil War: U.S. Army Signal Flag
- American Civil War: Union Code Book
- American Revolutionary War: Revolutionary Secrets
- USAF C-130
- U.S. Army RU-8D
- Cold War: GRAB II Elint Satellite
- Cold War: Great Seal
- Cold War: U-2 Incident
- Cold War: U.S.S. Liberty
- Cold War: U.S.S. Pueblo
- Cold War: VENONA
- Computer Development: Cray Supercomputers
- Computer Development: Harvest Tape Drive
- Computer Development: RISSMAN
- Computer Development: StorageTek
- NSA/CSS Cryptologic Memorial
- SME PED
- Friedman, Safford and Washington
- Hall of Honor
- Hobo Life
- Hobo Communications: A Brief History of Hobos and Their Signs
- The Kahn Collection
- Korean War
- Language
- The Magic of Purple
- National Cryptologic Museum Library
- Rare Book Collection
- September 11th Memorial
- Vietnam War
- Women in American Cryptology
- World War 1: American Black Chamber
- World War 1: Radio Intercept Site

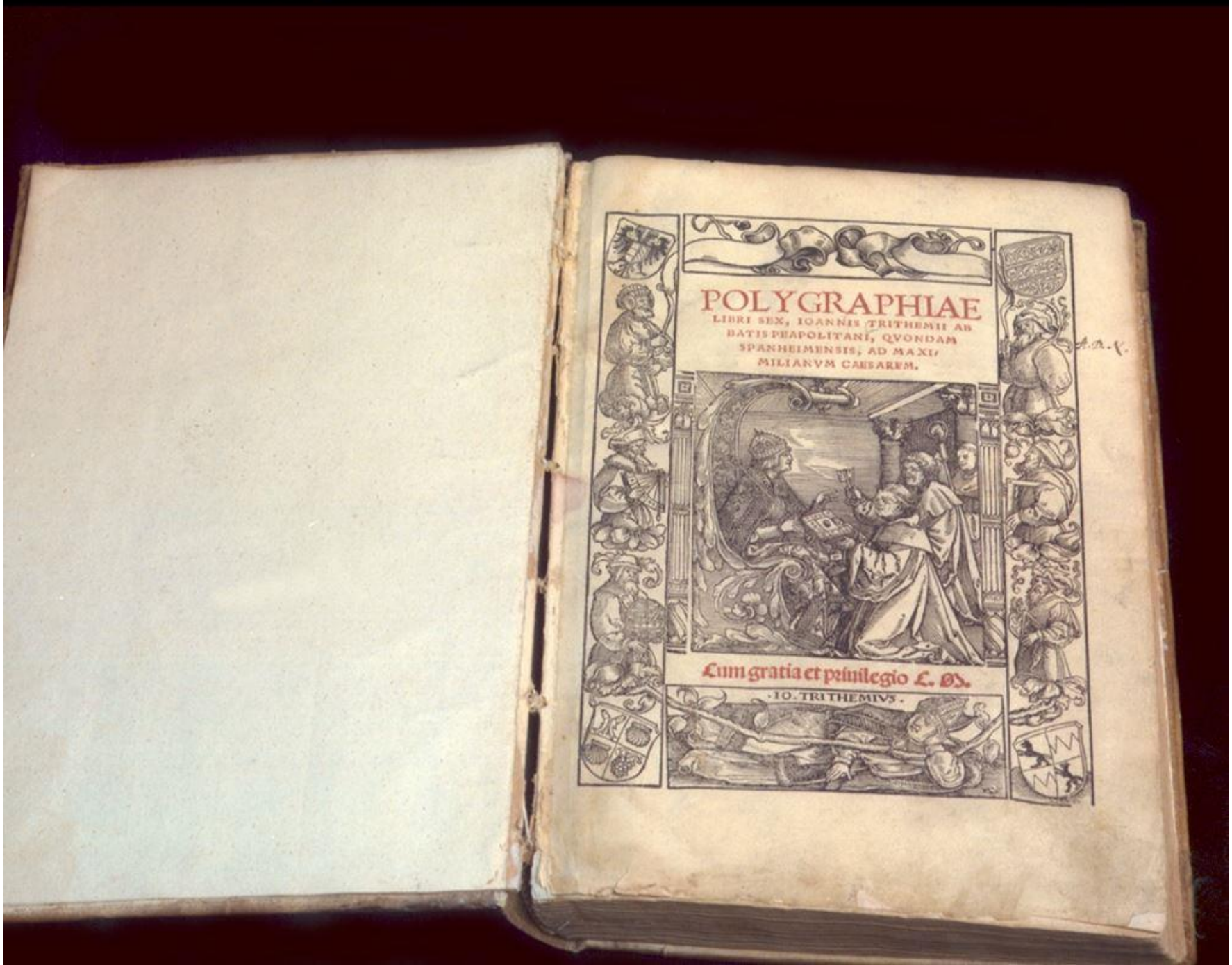
18th Century Cipher Device

PURDUE
UNIVERSITY
Libraries

COLD WAR: GREAT SEAL

On August 4, 1945, Soviet school children gave a carving of the Great Seal of the United States to U.S. Ambassador Averell Harriman. It hung in the ambassador's Moscow residential office until 1952 when the State Department discovered that it was 'bugged.' The microphone hidden inside was passive and only activated when the Soviets wanted it to be. They shot radio waves from a van parked outside into the ambassador's office and could then detect the changes of the microphone's diaphragm inside the resonant cavity. When Soviets turned off the radio waves it was virtually impossible to detect the hidden 'bug.' The Soviets were able to eavesdrop on the U.S. ambassador's conversations for six years. The replica on display in the museum was molded from the original after it came to NSA for testing. The exhibit can be opened to reveal a copy of the microphone and the resonant cavity inside. (Next slide)

PURDUE
UNIVERSITY
Libraries



POLYGRAPHIAE
LIBRI SEX, IOANNIS TRITHEMII AB
BATIS PEAPOLITANI, QVONDAM
SPANHEIMENSIS, AD MAXI-
MILIANVM CAESAREM.

Cum gratia et priuilegio C. M.

IO. TRITHEMIVS.

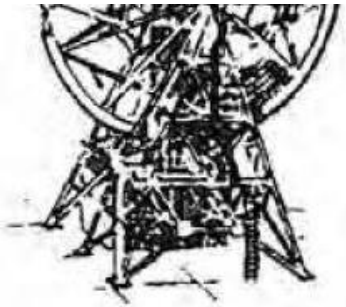
World War I: Zimmermann Telegram Exhibit

NSA Civil Liberties and Privacy Office

Review of U.S. Person Privacy Protections in the Production and Dissemination of Serialized Intelligence Reports Derived from Signals Intelligence Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act

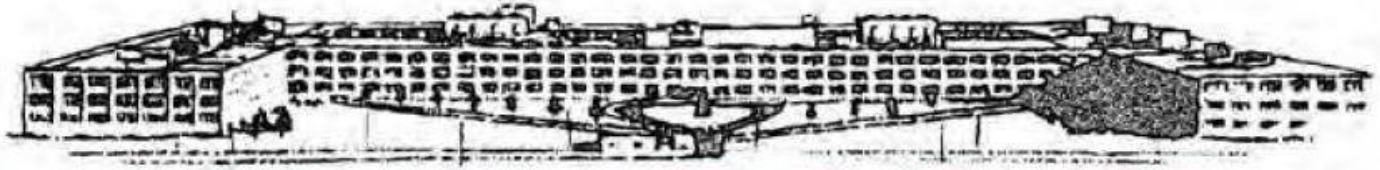
Rebecca J. Richards

HISTORY OF AMERICAN CRYPTOLOGY DURING COLD WAR 1945-1980 (1 OF 4 VOLS.)



American Cryptology during the Cold War, 1945–1989

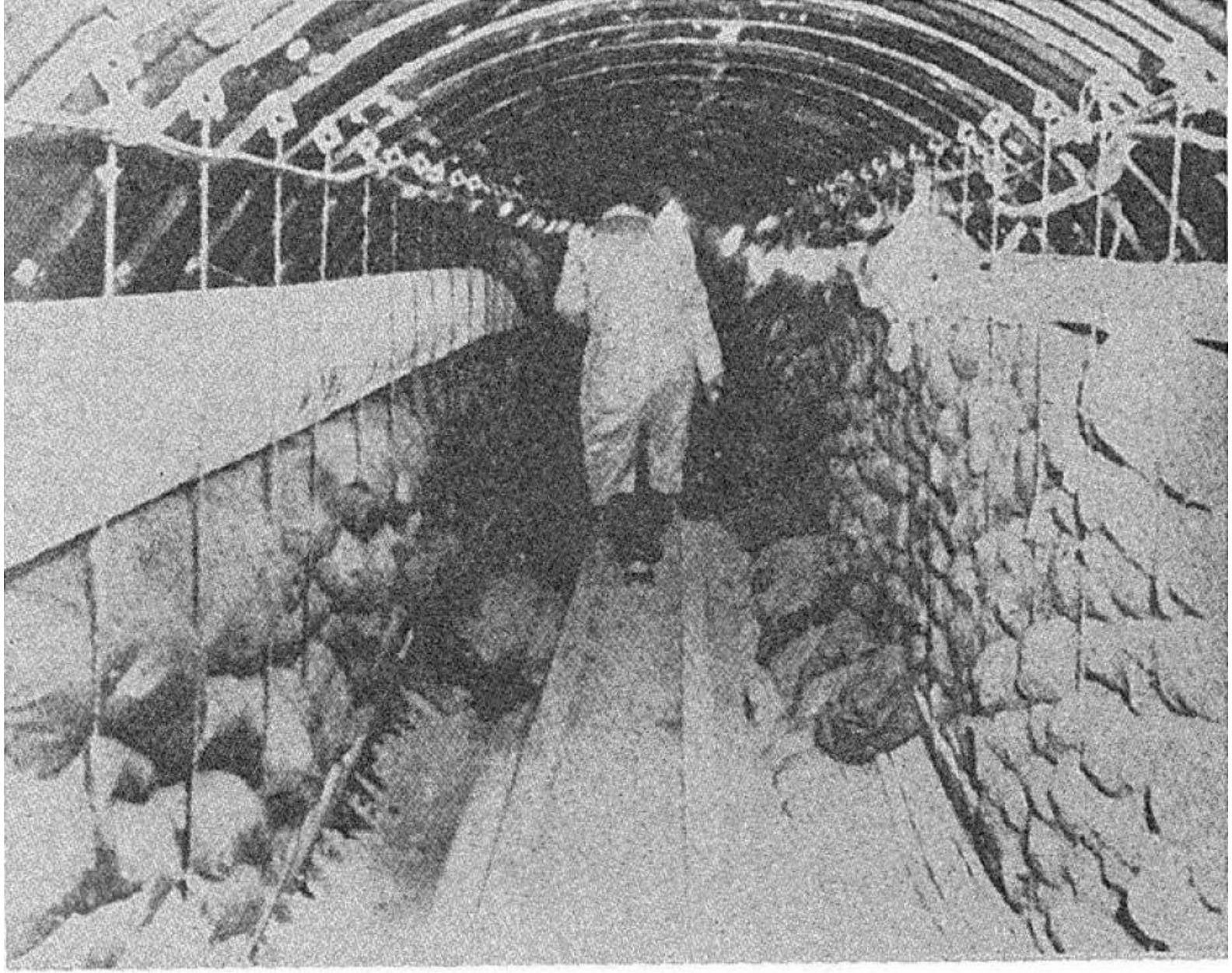
Book I: The Struggle for Centralization 1945–1960



PURDUE UNIVERSITY
Libraries

Chapter 4: The Soviet Problem

Chapter 5: Building the Internal Mechanism



The Tunnel

A Soviet photograph taken from just beyond the chamber where the landline taps were applied (Project REGAL).

(U) A Partial History of ELINT at NSA

[redacted]

(b)(3)-P.L. 86-36

(U) Introduction

(U) What is electronic intelligence, or ELINT? It is primarily information derived from electronic signals that do not contain speech or text (which are COMINT). The "official" description, from the National Security Council Directive No. 17 in 1955, is "the term ELINT is defined as the collection (observation and recording), and the technical processing for later intelligence purposes, of information on foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation sources."[1]

(C) ELINT has two major branches. One branch is technical ELINT (TechELINT), which describes the signal structure, emission characteristics, modes of operation, emitter functions, and weapons systems associations of such emit- are time sensitive – often measured in minutes and sometimes seconds.

(U) Background

(U) ELINT had its start in World War II, with the invention and use of radar by the Allies and the Axis. The U.S. Army Air Forces had a keen interest in ELINT since they used most German radars at the time to target Allied bombers over Germany, and the air forces wanted to know as much about these radars as possible – including how to evade, "jam," or "spoof" them. The Americans and the British started intercepting those radar signals, and ELINT was born.

(C) Immediately after WWII, the USAF in Europe (USAFE) embarked on an aggressive TechELINT and OpELINT program, including

BENEFITS OF STUDYING DIA AND NSA INFORMATION RESOURCES

- Gain historical and contemporary information and insights on military intelligence matters.
- Learn the successes and failures experienced by DIA and NSA.
- Enhance your knowledge base in cryptology, signals intelligence, and cybersecurity.
- Learn how these agencies are concerned with balancing privacy and national security.
- Gain enhanced understanding of the global scope of topics they address and the enormous quantities of information they must process.
- Learn how they are addressing emerging problems in areas such as cybersecurity and communications intelligence which affect national security, domestic and international economics, and personal economic and social activity.

PURDUE UNIVERSITY
Libraries

QUESTIONS?

PURDUE UNIVERSITY
Libraries