

ENHANCING YOUR INTELLIGENCE AGENCY INFORMATION RESOURCE IQ

PT. 1: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Presenter Professor Bert Chapman

Purdue University Libraries

PURDUE
UNIVERSITY
LIBRARIES

OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

- Establishing this agency recommended by 9/11 Commission.
- Established in 2004 by the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458)
- Codified at 50 USC 401 et. seq.
- This office now heads the U.S. Intelligence Community. Previously held by Director of Central Intelligence (DCI) who also served as CIA Director.
- The Director of National Intelligence (DNI) is presidentially appointed and subject to Senate confirmation. 7 individuals have held this position.

CURRENT DNI DAN COATS

- Former Indiana Senator
- Served on Senate Intelligence Committee



ODNI MISSION, VISION, & GOALS

- Leading Intelligence Community (IC) to deliver most insightful intelligence possible.
- Making the nation more secure due to a fully integrated IC.
- Integrating intelligence analysis & collection to inform decisions from the White House to the foxhole.
- Driving responsible and secure information sharing.
- Setting strategic direction & priorities for national intelligence capabilities.
- Developing and implementing Unifying Intelligence Strategies across regional and functional portfolios.
- Strengthening partnerships to enrich intelligence.
- Advancing cutting-edge technologies to provide global intelligence advantage.
- Promoting a highly-skilled intelligence workforce.
- Aligning management practices to best serve the intelligence community.

ADDITIONAL ODNI FACTS

- DNI is President's principal intelligence advisor.
- Manages the National Intelligence Program Budget of over \$50 billion except for military intelligence.
- Responsible for President's Daily Brief staff and National Intelligence Council.
- IC Inspector General established in 2010.
- Cyber Threat Integration Center added in 2016.
- Staff size approaches 2,000 with more than half working in mission focused centers.
- Over 40% of employees are on rotation from other intelligence agencies.
- Employs fewer contractors than government and military staff.
- ODNI National intelligence managers are responsible for evaluating individual global regions (Africa) or intelligence functions (Counterintelligence).



UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

LEADERSHIP

Director (DNI)
Deputy Director (DDNI)
Chief Management Officer (CMO)

CORE MISSION

Deputy DNI for Intelligence Integration (DDNI/II)

| | |
|---|---|
| Mission Integration Division (MID) | National Counterproliferation Center (NCPC) |
| National Intelligence Council (NIC) | National Counterterrorism Center (NCTC) |
| National Intelligence Management Council (NIMC) | National Counterintelligence & Security Center (NCSC) |
| | Cyber Threat Intelligence Integration Center (CTIIC) |

ENABLERS

| | |
|--|-----------------------------------|
| Acquisition, Technology, & Facilities (AT&F) | Partner Engagement (PE) |
| Chief Financial Officer (CFO) | Policy & Strategy (P&S) |
| Chief Human Capital Officer (CHCO) | Systems & Resource Analyses (SRA) |
| IC Chief Information Officer (IC CIO) | |

OVERSIGHT

| | |
|--|-------------------------------------|
| Office of Civil Liberties, Privacy and Transparency (CLPT) | Office of the General Counsel (OGC) |
| IC Equal Employment Opportunity & Diversity (EEOD) | Office of Legislative Affairs (OLA) |
| IC Inspector General (IC IG) | Public Affairs Office (PAO) |

NATIONAL INTELLIGENCE COUNCIL (NIC)

- Established 1979.
- Responsible for producing finished intelligence analysis.
- Promotes exemplary use of analytic tradecraft & standards including alternative analysis, new analytic tools & techniques, and wider IC collaboration.
- Provides senior policymakers with IC coordinated views including National Intelligence Estimates (NIE)
- Prepares IC principals and represents the IC at National Security Council meetings.
- Using non-U.S. Government experts in academe and private sector to broaden IC's knowledge and perspectives.
- Although most work is classified, some is publicly available, including...



GLOBAL TRENDS SERIES

- Produced every four years since 1997
- Analyzes multiple topics shaping the International environment. Jan. 2017 ed. below



GLOBAL TRENDS PARADOX OF PROGRESS

A publication of the National Intelligence Council

| | |
|----|--|
| 1 | The Map of the Future |
| 5 | Trends Transforming the Global Landscape |
| 29 | Near Future: Tensions Are Rising |
| 45 | Three Scenarios for the Distant Future: Islands, Orbits, Communities |
| 63 | What the Scenarios Teach Us: Fostering Opportunities Through Resilience |
| 70 | Methodological Note |
| 72 | Glossary |
| 74 | Acknowledgements |

ANNEXES

85

The Next Five Years by Region

159

Key Global Trends

Meanwhile, states remain highly relevant. China and Russia will be emboldened, while regional aggressors and nonstate actors will see openings to pursue their interests. Uncertainty about the United States, an inward-looking West, and erosion of norms for conflict prevention and human rights will encourage China and Russia to check US influence. In doing so, their “gray zone” aggression and diverse forms of disruption will stay below the threshold of hot war but bring profound risks of miscalculation. Overconfidence that material strength can manage escalation will increase the risks of interstate conflict to levels not seen since the Cold War. Even if hot war is avoided, the current pattern of “international cooperation where we can get it”—such as on climate change—masks significant differences in values and interests among states and does little to curb assertions of dominance within regions. These trends are leading to a spheres of influence world.

Nor is the picture much better on the home front for many countries. While decades of global integration and advancing technology enriched the richest and lifted that billion out of poverty, mostly in Asia, it also hollowed out Western middle classes and stoked pushback against globalization. Migrant flows are greater now than in the past 70 years, raising the specter of drained welfare coffers and

one another to create political order in an era of empowered individuals and rapidly changing economies? To what extent will major state powers, as well as individuals and groups, craft new patterns or architectures of international cooperation and competition? To what extent will governments, groups, and individuals prepare now for multifaceted global issues like climate change and transformative technologies?

Three stories or scenarios—“Islands,” “Orbits,” and “Communities”—explore how trends and choices of note might intersect to create different pathways to the future. These scenarios emphasize alternative responses to near-term volatility—at the national (Islands), regional (Orbits), and sub-state and transnational (Communities) levels.

- **Islands** investigates a restructuring of the global economy that leads to long periods of slow or no growth, challenging both traditional models of economic prosperity and the presumption that globalization will continue to expand. The scenario emphasizes the challenges to governments in meeting societies’ demands for both economic and physical security as popular pushback to globalization increases, emerging technologies transform work and trade, and political instability grows. It underscores the choices governments

Global Trends and Key Implications Through 2035

The rich are aging, the poor are not. Working-age populations are shrinking in wealthy countries, China, and Russia but growing in developing, poorer countries, particularly in Africa and South Asia, increasing economic, employment, urbanization, and welfare pressures and spurring migration. Training and continuing education will be crucial in developed and developing countries alike.

The global economy is shifting. Weak economic growth will persist in the near term. Major economies will confront shrinking workforces and diminishing productivity gains while recovering from the 2008-09 financial crisis with high debt, weak demand, and doubts about globalization. China will attempt to shift to a consumer-driven economy from its longstanding export and investment focus. Lower growth will threaten poverty reduction in developing countries.

Technology is accelerating progress but causing discontinuities. Rapid technological advancements will increase the pace of change and create new opportunities but will aggravate divisions between winners and losers. Automation and artificial intelligence threaten to change industries faster than economies can adjust, potentially displacing workers and limiting the usual route for poor countries to develop. Biotechnologies such as genome editing will revolutionize medicine and other fields, while sharpening moral differences.

Ideas and Identities are driving a wave of exclusion. Growing global connectivity amid weak growth will increase tensions within and between societies. Populism will increase on the right and the left, threatening liberalism. Some leaders will use nationalism to shore up control. Religious influence will be increasingly consequential and more authoritative than many governments. Nearly all countries will see economic forces boost women's status and leadership roles, but backlash also will occur.

Governing is getting harder. Publics will demand governments deliver security and prosperity, but flat revenues, distrust, polarization, and a growing list of emerging issues will hamper government performance. Technology will expand the range of players who can block or circumvent political action. Managing global issues will become harder as actors multiply—to include NGOs, corporations, and empowered individuals—resulting in more ad hoc, fewer encompassing efforts.

The nature of conflict is changing. The risk of conflict will increase due to diverging interests among major powers, an expanding terror threat, continued instability in weak states, and the spread of lethal, disruptive technologies. Disrupting societies will become more common, with long-range precision weapons, cyber, and robotic systems to

Sharing Water Will Be More Contentious

A growing number of countries will experience water stress—from population growth, urbanization, economic development, climate change, and poor water management—and tensions over shared water resources will rise. Historically, water disputes between states have led to more sharing agreements than violent conflicts, but this pattern will be hard to maintain. Dam construction, industrial water pollution, and neglect or non-acceptance of existing treaty provisions aggravate water tensions, but political and cultural stress often play an even larger role.

Nearly half of the world's 263 international river basins lack cooperative management agreement as well as only a handful of the more than 600 transboundary aquifer systems. Moreover, many existing agreements are not sufficiently adaptive to address emergent issues such as climate change, biodiversity loss, and water quality.

Health. Human and animal health will increasingly be interconnected. Increasing global connectivity and changing environmental conditions will affect the geographic distribution of pathogens and their hosts, and, in turn, the emergence, transmission, and spread of many human and animal infectious diseases. Unaddressed deficiencies in national and global health systems for disease control will make infectious disease outbreaks more difficult to detect and manage, increasing the potential for epidemics to break out far beyond their points of origin.

- Noncommunicable diseases, however—such as heart disease, stroke, diabetes, and mental illness—will far outpace infectious diseases over the next decades, owing to demographic and cultural factors, including aging, poor nutrition and sanitation, urbanization, and widening inequality.

Converging Trends Will Transform Power and Politics

Together, these global trends will make

83 Introduction

85 The Next Five Years by Region

- 89 East and Southeast Asia
- 101 South Asia
- 107 Middle East and North Africa
- 115 Sub-Saharan Africa
- 123 Russia and Eurasia
- 129 Europe
- 135 North America
- 143 South America
- 149 The Arctic and Antarctica
- 155 Space

159 Key Global Trends

- 161 People
- 169 How People Live
- 175 How People Create and Innovate

Russia and Eurasia

The next five years will see the Russian leadership continue its effort to restore Russia's great-power status through military modernization, foreign engagements that seek to extend Russian influence and limit Western influence, nuclear saber rattling, and increased nationalism. Moscow remains insecure in its worldview and will move when it believes it needs to protect Russia's national interests—as in Ukraine in 2014—or to bolster its influence further afield, as in Syria. Such efforts have enabled President Putin to maintain popular support at home despite difficult economic conditions and sanctions, and he will continue to rely on coercive measures and information control to quash public dissent. Moscow will also continue to use anti-Western rhetoric—and a nationalist ideology that evokes the imperial and moral strength of the Russian people—to manage domestic vulnerability and advance its interests.

The Kremlin's ideology, policies, and structures—and its control of the economy—enjoy elite and popular support, notwithstanding significant repression of civil society and minorities.

- This **amalgam of authoritarianism, corruption, and nationalism** represents an alternative to Western liberalism that many of the world's remaining autocrats and revisionists find appealing. In Moscow's view, liberalism is synonymous with disorder and moral decay, and pro-democracy movements and electoral experiments are Western plots to weaken traditional bulwarks of order and the Russian state. To counter Western attempts to weaken and isolate Russia, Moscow will accommodate Beijing's rise in the near term but ultimately will balk before becoming junior partner to China—which would run counter to Russia's great power self-image.

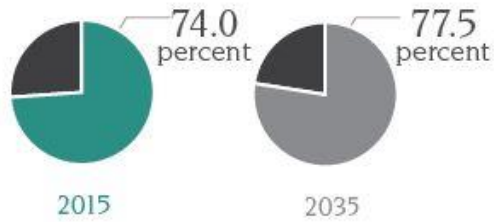
Russian insecurity, disappointment, and distrust of the liberal global order are firmly rooted in the simultaneous enlargement of NATO and the European Union (EU) following the Cold War, motivating its actions abroad; its use of "gray zone" military tactics, which deliberately blur conditions of war and peace, is likely to continue. Russia's various moves in recent years, however—in Georgia, Ukraine, and Syria, and via support to far-right populist parties in Europe—raise three important questions:

RUSSIA

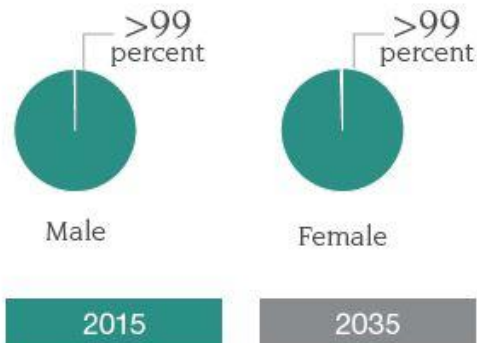
2035 Population Projection:

135,674,000

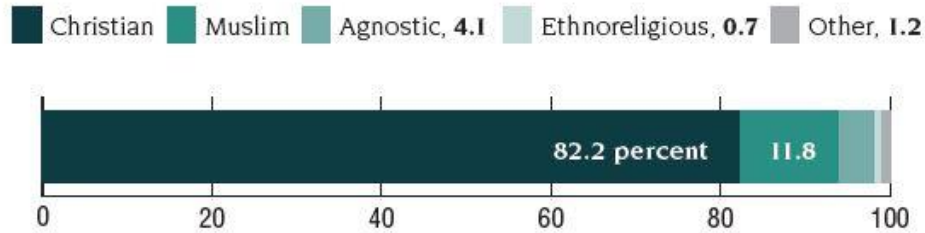
Percent Urban



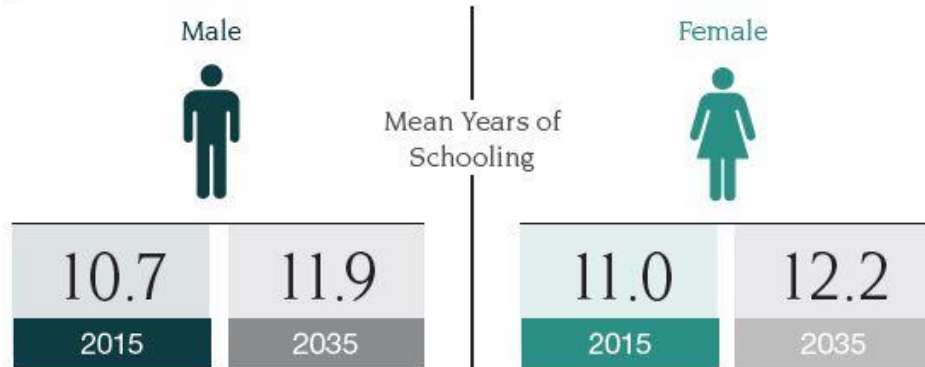
Adult Literacy, 2015



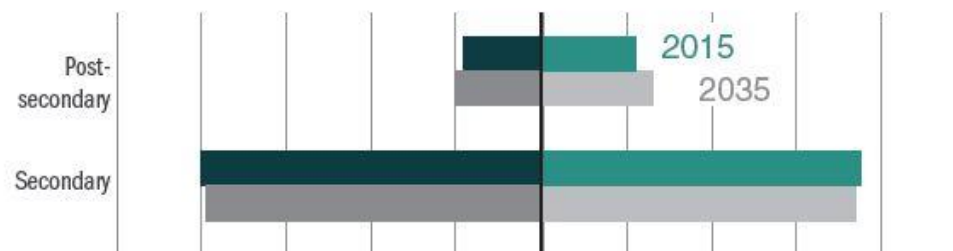
Religion, 2015^a



Education, 2015 and 2035



Highest Educational Attainment



TUMBLR SITE SOLICITS FEEDBACK



[SUMMARY & TABLE OF CONTENTS](#)

[GLOBAL TRENDS](#)

[JOIN THE CONVERSATION](#)

[SUBMIT A POST](#)



National Intelligence Council

NIC Publications

Special Products

- 2015: Global Food Security Assessment
- 2015: Selected Emerging Agriculture Technologies Through 2040
- 2013: Wildlife Poaching Threatens Economic, Security Priorities in Africa
- 2012: Global Water Security: Intelligence Community Assessment
- 2012: Global Water Security Map
- 2011: The Threat to U.S. National Security Posed by Transnational Organized Crime
- 2011: Transnational Organized Crime (Foldout)
- 2009: The Impact of Climate Change to 2030 Commissioned Research and Conference Reports
- 2008: Strategic Implications of Global Health
- 2008: Strategic Implications of Global Health Map
- 2007: Unclassified Key Judgments - Prospects for Iraq's Stability: A Challenging Road Ahead (from January 2007 NIE)
- 2006: Declassified Key Judgments - Trends in Global Terrorism: Implications for the United States (from April 2006 NIE)

CYBERTHREAT INTELLIGENCE INTEGRATION CENTER (CTIIC)



- Enhances understanding of foreign cyber threats to U.S. national interests.
- Integrates information from network defense, intelligence, & law enforcement communities.
- Supports interagency planning to develop whole-of-government approaches to cyber adversaries.

US ATTRIBUTES WANNACRY 2.0 TO NORTH KOREA

All CTIIC News

Tuesday, 19 December 2017 15:40

Print



White House Homeland Security Advisor Tom Bossert briefed the press on 19 December 2017 regarding the US Government's finding that North Korea was responsible for the [WannaCry 2.0 Ransomware](#) attack in May, which disrupted computer operations in more than 150 countries.

Bossert highlighted the collaboration between government and private sector cyber security experts that led to the attribution, noting this partnership is a key component of the US strategy to mitigate the threat of malicious cyber operations.

- CTIIC Components: Current Intelligence Section
- Analysis Integration Section
- Threat Opportunities Section
- CTIIC established by Presidential Memorandum February 25, 2015
- Dec. 19, 2017 Press Briefing Attributing Wannacry 2.0 attack to North Korea

Is the US Losing the Cyber Battle?



The Aspen Institute's Washington Ideas Roundtable Series on 31 October brought together CTIIC Director Tonya Ugoretz, senior DHS official Christopher Krebs—who oversees the Department's cyber and physical infrastructure security mission—and Deputy Assistant Attorney for National Asset Protection Adam Hickey for a conversation on [Federal efforts overcome the cyber threat](#).

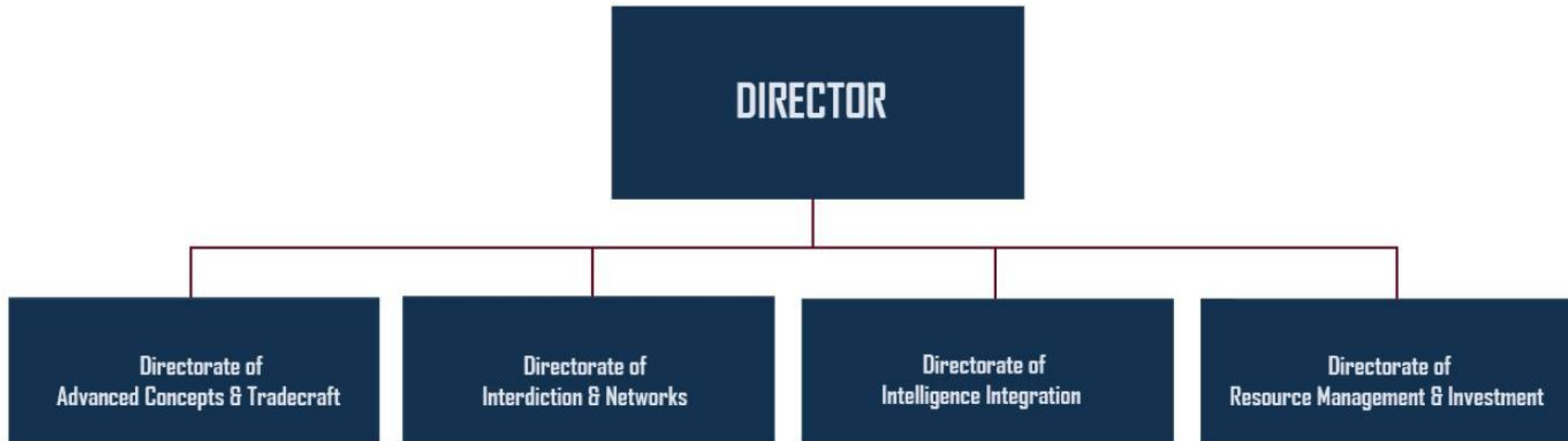
NATIONAL COUNTERPROLIFERATION CENTER (NCPC)



NCPC FOUNDED IN 2005 BASED ON RECOMMENDATIONS FROM WMD COMMISSION

- Helps counter threats against the U.S. from proliferating biological, chemical, nuclear, and radiological weapons and the missiles capable of delivering them.

(U) NCPC Organizational Chart



NCPC WORK ACTIVITIES

- **Implementing Counterproliferation Strategies.** Developing strategies to strengthen the CP mission. NCPC is providing direction and focus for the efforts of the Intelligence Community to address current and looming WMD proliferation issues.
- **Emphasizing Motivations, Intentions, and Disincentives.** Breaking new ground. By moving beyond the traditional approach of treating WMD proliferation as primarily a technical problem, NCPC is instead promoting a multi-disciplinary approach to assessing and addressing the political, economic, cultural and other security issues related to counterproliferation.
- **Countering Proliferation: Beyond Just Report It.** Encouraging CP professionals to go beyond simply reporting on proliferators' progress. By identifying opportunities for decision makers to reverse that progress, the NCPC is enhancing the IC's contribution to countering proliferation.
- **Looking "Over-the-Horizon."** Partnering with senior policymakers, NCPC is leading efforts to develop collection and analytic strategies for emerging, over-the-horizon WMD threats, positioning the Intelligence Community to warn stakeholders of such threats and provide the insights needed to counter them as early as possible.
- **Focusing on the WMD and Terrorism Nexus.** Working closely with the National Counterterrorism Center, NCPC is ensuring that all resources are leveraged within the respective communities to deny terrorists and rogue states access to chemical, biological, radiological or nuclear capabilities.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)



ESTABLISHED IN 2000 AS NATIONAL COUNTERINTELLIGENCE EXECUTIVE (NCIX)

- 2002 Counterintelligence Enhancement Act (P.L. 107-306) provided a statutory foundation.
- Initially placed in the Executive Office of the President, what is now NCSC transferred to ODNI in January 2006 as a result of the 2004 Intelligence Reform & Terrorism Prevention Act (P.L. 108-458).
- 2007 Chi Mak convicted after 20 years of stealing defense secrets for China.
- April 2010 - Wikileaks posts first materials from Bradley Manning.
- October 11 - Obama signs Executive Order 13587 directing DNI & Attorney General to create a National Insider Threat Task Force
- Nov. 3, 2011- Releases report Foreign Spies Stealing U.S. Economic Secrets in Cyberspace – First public identification of China and Russia as active and persistent cyberspace threats to the U.S.
- January 2013 Foreign Economic and Espionage Penalty Enhancement Act signed (P.L. 112-269). Increased prison terms for economic espionage.
- NCSC activities include threat assessments, personnel security, combating insider threats to national security, damage assessments, information sharing and audit data, physical security, supply chain risk management, cyber threats, national and intelligence community strategy development, and advocating for counterintelligence and security resources.

COUNTERINTELLIGENCE

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection
and Industrial Espionage, 2009-2011

Human Targeting

Chance meetings may be more than they appear. Don't put yourself on thin ice.



Foreign intelligence entities target those with access to sensitive information. How well do you know your new "friend"?



Social Media Deception

The signs are all around you. Do you trust that new contact?

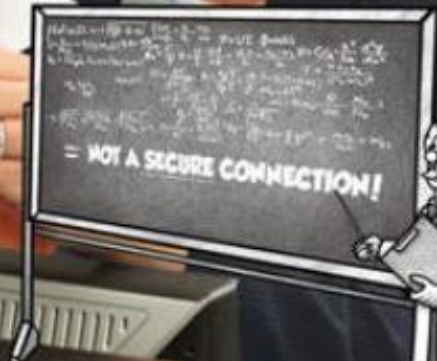


Know the Risk
Raise your Shield

Foreign intelligence entities use social media to develop relationships. Make sure you know your friends and followers.

Travel Awareness

It doesn't take a rocket scientist to know public networks are never private.



Know the Risk
Raise your Shield

When traveling abroad, assume that foreign intelligence entities may be trying to monitor your communications.



NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

National Counterintelligence Strategy of the United States of America 2016



PURDUE
UNIVERSITY
LIBRARIES

MISSION OBJECTIVE 1

Deepen our understanding of foreign intelligence entities' plans, intentions, capabilities, tradecraft, and operations targeting U.S. national interests and sensitive information and assets

The United States faces enduring and emerging threats from FIEs that target our sensitive information and assets or otherwise jeopardize U.S. national interests. These threats continue to evolve in scope and complexity as FIE capabilities and activities become increasingly diverse and technically sophisticated. To meet this challenge, the U.S. Government must continue to evolve its CI programs and activities to improve our understanding of the full scope of current and emerging FIE threats, drive decision-making, and support U.S. national security goals.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Conduct and support collection, investigative, and operational activities that yield intelligence on FIEs' strategic objectives and collection priorities;
- Conduct and support collection, investigative, and operational activities that yield intelligence on FIEs' plans, intentions, capabilities, and activities;
- Penetrate and pursue FIEs in order to holistically understand FIE threats;

- Pursue joint collection and analysis opportunities to expand and enrich reporting and production on priority FIE targets;
- Develop and implement efforts to anticipate, identify, and warn of emerging FIE threats; and
- Conduct and support collection, investigative, and operational activities that identify technical capabilities and threats.

Successful implementation of these actions will yield actionable intelligence on FIE threats to U.S. national security, including joint products that provide policymakers relevant, insightful, and credible intelligence to close the highest priority knowledge gaps. It will also provide warnings to U.S. Government departments and agencies and private sector partners of specific FIE threats to their information and assets.

MISSION OBJECTIVE 2

Disrupt foreign intelligence entities' capabilities, plans, and operations that threaten U.S. national interests and sensitive information and assets


FIEs pursue sophisticated measures to disrupt U.S. plans, policies, and processes and undermine U.S. national interests. All of

NATIONAL COUNTERTERRORISM CENTER



NCTC OPENED ON MAY 1, 2003

- Produces analysis, maintains the authoritative database of known and suspected terrorists, shares information, and conducts strategic operational planning. NCTC is staffed by more than 1,000 personnel from across the IC, the Federal government, and Federal contractors. Forty percent of NCTC's workforce represents approximately 20 different departments and agencies.
- Chairs interagency meetings on terrorist groups, capabilities, plans and intentions, and emerging threats to U.S. interests at home and abroad.
- Chair and/or support interagency groups orchestrating and facilitating an efficient and effective allocation of U.S. government terrorism analysis assets, to include appropriate, planned redundancy.
- Produce integrated and interagency-coordinated analytic assessments on terrorism issues and publishes warnings, alerts, and advisories as appropriate.
- Manage a Joint Operations Center to provide unique insight and situational awareness of developing terrorism-related worldwide issues and events.



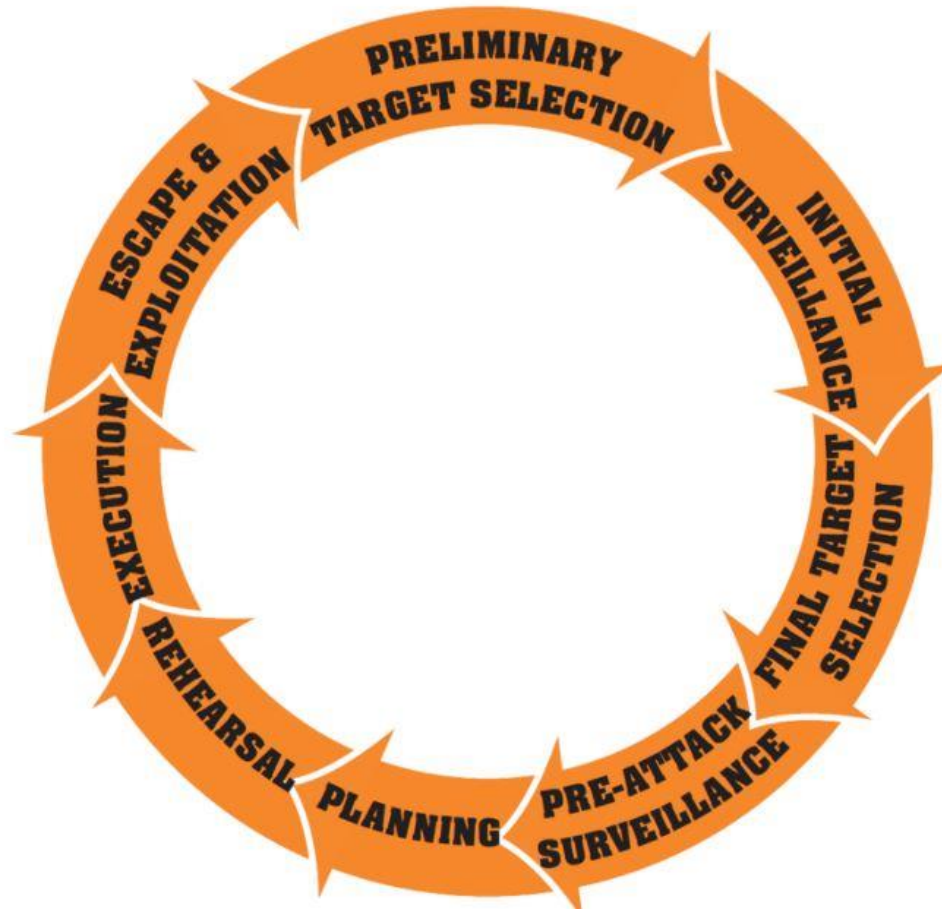
COUNTER TERRORISM GUIDE

FOR PUBLIC SAFETY PERSONNEL

GET STARTED

TERRORIST ATTACK PLANNING CYCLE

Understanding the terrorist attack planning cycle can help first responders and public safety personnel recognize preoperational activities. Terrorists generally plan attacks in observable stages, although specific details, sequencing, and timing can vary greatly and change over time. Preattack surveillance, training, and rehearsals are the stages of the planning cycle that are often observable and can offer opportunities to identify plots and prevent attacks.



INTELLIGENCE FOR FIRST RESPONDERS






The types of products first responders will most likely encounter appear below:

- **Information reports** are typically messages that enable the timely dissemination of unevaluated intelligence within the IC and the law enforcement community.
- **Intelligence Assessments (IAs)** are finished intelligence products resulting from the intelligence analysis process. Assessments may address tactical, strategic, or technical intelligence requirements.
- **Intelligence Bulletins (IBs)** are finished intelligence products used to disseminate information of interest, such as significant developments and trends, to the intelligence and law enforcement communities in an article format.
- **Joint products** are intelligence assessments and bulletins produced in cooperation with other agencies (dual or multiple seals). When written jointly, these products may be formatted differently than the single-seal versions, depending on the format agreed to by participating agencies.
- **Threat Assessments (TAs) or Special Assessments (SAs)** provide in-depth analyses related to a specific event or body of threat reporting and may address nonterrorist threats to national security.

Responder Toolbox is available through HSIN and LEO, and select editions can be found on InfraGard and in the Domestic Security Alliance Council (DSAC) portals.

- **NCTC Counterterrorism Weekly (CT Weekly)**. FOUO compilation of open-source information related to terrorism that may be of interest to federal, state, local, tribal, and territorial first responders and public safety personnel. The CT Weekly can be found on NCTC CURRENT, HSIN, and LEO.
- **NCTC CURRENT**. CURRENT articles are U//FOUO counterterrorism intelligence products published by NCTC and are available on HSIN and LEO.
- **Roll Call Release (RCR)**. The DHS RCR, issued jointly with FBI or as a triseal product with NCTC, is a one-page, U//FOUO informational product written specifically for state, local, tribal, and territorial first responders and focused on a single topic. RCRs highlight emerging terrorist tactics, techniques, and procedures; terrorism trends; and potential indicators of suspicious activity that frontline law enforcement officers may encounter in the course of their official duties. RCRs are available on HSIN and LEO.

Bomb Threat Stand-Off Distances

| Threat Description | | Explosives Capacity ¹ (TNT Equivalent) | Building Evacuation Distance ² | Outdoor Evacuation Distance ³ |
|--|-----------------------------|---|---|--|
|  | Pipe Bomb | 5 LBS/ 2.3 KG | 70 FT/ 21 M | 850 FT/ 259 M |
|  | Briefcase/ Suitcase Bomb | 50 LBS/ 23 KG | 150 FT/ 46 M | 1,850 FT/ 564 M |
|  | Compact Sedan | 500 LBS/ 227 KG | 320 FT/ 98 M | 1,500 FT/ 457 M |
|  | Sedan | 1,000 LBS/ 454 KG | 400 FT/ 122 M | 1,750 FT/ 533 M |
|  | Passenger/ Cargo Van | 4,000 LBS/ 1,814 KG | 600 FT/ 183 M | 2,750 FT/ 838 M |

NCTC FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION

- Authorizes IC to target communications of non-U.S. persons outside the U.S. for foreign intelligence purposes.

The Foreign Intelligence Surveillance Court (FISC) recently approved minimization procedures that permit the National Counterterrorism Center (NCTC) to receive certain unevaluated counterterrorism information acquired pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978, as amended.

NCTC is the primary organization within the U.S. government responsible for analyzing and integrating all terrorism and counterterrorism information possessed or acquired by U.S. government agencies. NCTC's capabilities in this regard will be enhanced by receiving unevaluated Section 702-acquired counterterrorism information, which will not only permit the Center's analysts to develop independent analytical judgments and apply analytic tools to an important source of relevant intelligence, but to receive this intelligence more expeditiously. Unevaluated Section 702 information will significantly advance NCTC's efforts to prioritize and pursue terrorism threat threads and to assist the intelligence, law enforcement, and homeland security communities in responding to identified threats.

NCTC's handling of unevaluated Section 702-acquired counterterrorism information will be governed by standard minimization procedures adopted by the Attorney General and approved for use by the FISC.

TERRORIST IDENTITIES DATAMART ENVIRONMENT (TIDE)

What is TIDE?

The Terrorist Identities Datamart Environment (TIDE) is the US Government's central repository of information on international terrorist identities. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 established NCTC in law and mandated the Center serve as the "central and shared knowledge bank on known and suspected terrorists and international terror groups." TIDE, which contains both classified and unclassified information, is that knowledge bank. It supports the US Government's various terrorist screening efforts by supplying identities to the unclassified Terrorist Screening Database (TSDB), which resides in the FBI-led Terrorist Screening Center (TSC). The TSDB commonly referred to as "the Watchlist," supplies databases "downstream" with identifiers used for screening.

What types of conduct warrant inclusion in TIDE?

Federal agencies nominate individuals for inclusion in TIDE based on evaluations of intelligence and law enforcement terrorism information. Types of conduct that warrant inclusion in TIDE include persons who:

- Commit international terrorist activity;
- Prepare or plan international terrorist activity;
- Gather information on potential targets for international terrorist activity;
- Solicit funds or valuables for international terrorist activity or a terrorist organization;
- Solicit membership in an international terrorist organization;
- Provide material support, e.g., safe house, transportation, or training; and/or
- Are members of or represent a foreign terrorist organization.

INTELLIGENCE COMMUNITY INSPECTOR GENERAL

- The Office of the Inspector General of the Intelligence Community (IC IG) was established pursuant to Section 405 of the Intelligence Authorization Act of Fiscal Year 2010. (P.L. 111-259).
- The IC IG is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies.



OFFICE of the INSPECTOR GENERAL
of the INTELLIGENCE COMMUNITY

SEMIANNUAL REPORT

April 2017–September 2017

Wayne A. Stone
Acting Inspector General of the Intelligence Community

Table of Contents

FORUM

RECOMMENDATIONS

AUDIT

INSPECTIONS

INVESTIGATIONS

IC WHISTLEBLOWING

COUNSEL

| | |
|---|----|
| Statutory Reporting Requirements | 3 |
| Organization and Outreach | 5 |
| Mission and Resources | 6 |
| IC IG Forum | 7 |
| Committee Updates | 8 |
| Five Eyes Review Council | 9 |
| Recommendations | 10 |
| Audit | 12 |
| Inspections & Evaluations | 16 |
| Investigations | 18 |
| IC Whistleblowing & Source Protection | 21 |
| Counsel | 25 |
| Legislative Development & Congressional Engagements | 27 |
| Abbreviations and Acronyms | 28 |
| Hotline | 29 |

THE INSPECTIONS & EVALUATIONS DIVISION WORKS TO **IMPROVE ODNI AND IC-WIDE PERFORMANCE AND INTEGRATION BY EXAMINING INFORMATION ACCESS; COLLECTION AND ANALYSIS; IC PROGRAMS AND ISSUES; AND COMPLIANCE WITH LAWS AND REGULATIONS.**

Completed Reviews

INS-2017-004: Report of Inspection: National Counterterrorism Center, Directorate of Strategic Operational Planning Special Review

The Inspections & Evaluations Division completed an inspection of the National Counterterrorism Center's Directorate of Strategic Operational Planning (NCTC/DSOP). By law, one of NCTC's missions is to conduct strategic operational planning for counterterrorism activities across the U.S. Government (USG).

DSOP fulfills this responsibility by integrating all instruments of national power, including diplomatic, financial, military, intelligences, homeland security, and law enforcement, to ensure unity of effort. DSOP coordination officers and assessment officers work with National Security Council staff and all USG departments and agencies to develop strategies, action plans, and assessments to integrate and evaluate all USG counterterrorism capabilities. I&E last inspected NCTC in 2012.

Additional details of this report are in the classified annex.

INS-2017-007: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats

In response to congressional direction, we assessed ODNI's progress implementing its insider threat program (ITP), implementation of safeguards to protect employee privacy and civil liberties, and measures of effectiveness used to determine whether ODNI's ITP detects and deters insider threats. We also assessed ODNI's efforts to identify and remediate information system vulnerabilities on classified networks that an insider threat could exploit.

Additional details of this report are in the classified annex.

Peer Review

During this reporting period, IC IG I&E Division underwent an external peer review by an interagency team led by DOS OIG, with participation from CIA, FBI, and NRO OIGs. The review was conducted under the auspices of the IC IG Forum Peer Review Program and in accordance with the 2017 CIGIE Guide for Conducting Peer Reviews of I&E Organizations of Federal OIGs. The IC IG I&E Division was last peer reviewed in 2014.

The external peer review team determined that IC IG I&E Division's policies and procedures generally met the seven Blue Book standards addressed in the external peer review. Of the four reports reviewed, all generally met the Blue Book standards, and complied with IC IG I&E Division's internal policies and procedures. The review team also provided two observations for improvement pertaining to quality control, and we fully concurred with these findings.

This reporting period, IC IG I&E Division inspectors collaborated with interagency teams to conduct external peer reviews of CIA, DIA, and NGA OIG inspections programs. The results of those peer reviews will be reported in those agencies' respective Semiannual Reports.

Ongoing Reviews

The IC IG I&E Division currently has four ongoing reviews.

Additional details of this report are in the classified annex.



THE INVESTIGATIONS DIVISION INVESTIGATES ALLEGATIONS OF VIOLATIONS OF CRIMINAL, CIVIL, AND ADMINISTRATIVE LAWS ARISING FROM THE CONDUCT OF IC, ODNI, AND CONTRACT EMPLOYEES.

During this reporting period, the Investigations Division continued its efforts in cross-IC fraud matters, working jointly with the FBI, IC OIGs, Defense Criminal Investigative Service, Air Force Office of Special Investigations, and other federal investigative agencies, as well as the DOJ Public Integrity Section and the U.S. Attorney's Office for the Eastern District of Virginia.

Our investigators also spent a significant amount of time on a continuing joint criminal investigation with the FBI, ten other federal law enforcement organizations, and OIGs. We expect this investigation to continue into the next reporting period.

Select Completed Investigations

INV-2016-0004: Time and Attendance Fraud

IC IG initiated an investigation with DOJ OIG after receiving an allegation from an ODNI

supervisor reporting concerns about an ODNI cadre employee's time and attendance, and possible misuse of Military Leave. The investigation concluded that the subject likely violated the statutory prohibition on dual compensation and made false statements in connection with his military duties. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The matter was referred to the Department of the Army for action as appropriate. The ODNI is separately pursuing collection of the improperly earned income.

INV-2017-0001: Unauthorized Media Contacts

The IC IG opened an investigation after learning an ODNI officer was alleged to have participated in an on-air discussion with a national media outlet. Her remarks were aired live during a call-in segment of the show during which she discussed the Benghazi attacks, military surveillance assets in the area, and CIA

and DOS roles. This "covered matter" and her disclosure of her affiliation with the ODNI were unauthorized, and the officer received a Letter of Warning.

INV-2017-0003: Government Travel Card Abuse

IC IG initiated an investigation in response to an allegation that an ODNI cadre officer misused his Government Travel Card (GTC). An analysis of the subject's GTC statements indicated he used his GTC for personal charges and cash withdrawals totaling \$4,495. The investigation also learned the subject received a \$1,500 cash advance for training he did not attend. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The matter was referred to a Personnel Evaluation Board; and the officer, with eleven years of service, was terminated and his security clearance was revoked.

OFFICE OF CIVIL LIBERTIES, PRIVACY, & TRANSPARENCY

- The Office of Civil Liberties, Privacy and Transparency (CLPT) ensures that the IC operates in a manner that advances national security while protecting the freedoms, civil liberties, and privacy rights guaranteed by the Constitution and federal law.
- CLPT is led by the Civil Liberties Protection Officer, a position established by the Intelligence Reform and Terrorism Prevention Act of 2004. Reporting directly to the Director of National Intelligence, the Civil Liberties Protection Officer oversees compliance with civil liberties and privacy requirements within the ODNI and ensures that civil liberties and privacy protections are incorporated into policies and procedures developed and implemented by the elements of the Intelligence Community.

Civil Liberties and Privacy

A. AUTHORITY: The National Security Act of 1947, as amended; the Privacy Act of 1974, as amended; Executive Order (EO) 12333, as amended; and other applicable provisions of law.

B. PURPOSE: This Directive establishes Intelligence Community (IC) policy for the protection of civil liberties and privacy relating to activities conducted by IC elements.

C. APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such other elements of any department or agency as may be designated as an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

2. For IC elements within departments, this Directive shall be implemented in a manner consistent with applicable law and departmental policies governing civil liberties and privacy protections.



**INTELLIGENCE
COMMUNITY
DIRECTIVE**

107

1.00 in

INTELLIGENCE COMMUNITY LEGAL REFERENCE BOOK

OFFICE OF THE DIRECTOR
OF NATIONAL INTELLIGENCE

OFFICE OF GENERAL COUNSEL

The Intelligence Community draws much of its authority and guidance from the body of law contained in this collection. We hope this proves to be a useful resource to professionals across the federal government.

Table of Contents

- [Introduction](#)
- [The Constitution of the United States of America](#)
- [The Principles of Professional Ethics for the IC](#)
- [The Principles of Intelligence Transparency for the IC](#)

Foreign Intelligence Surveillance Act (FISA) of 1978

That this Act may be cited as the Foreign Intelligence Surveillance Act of 1978 .

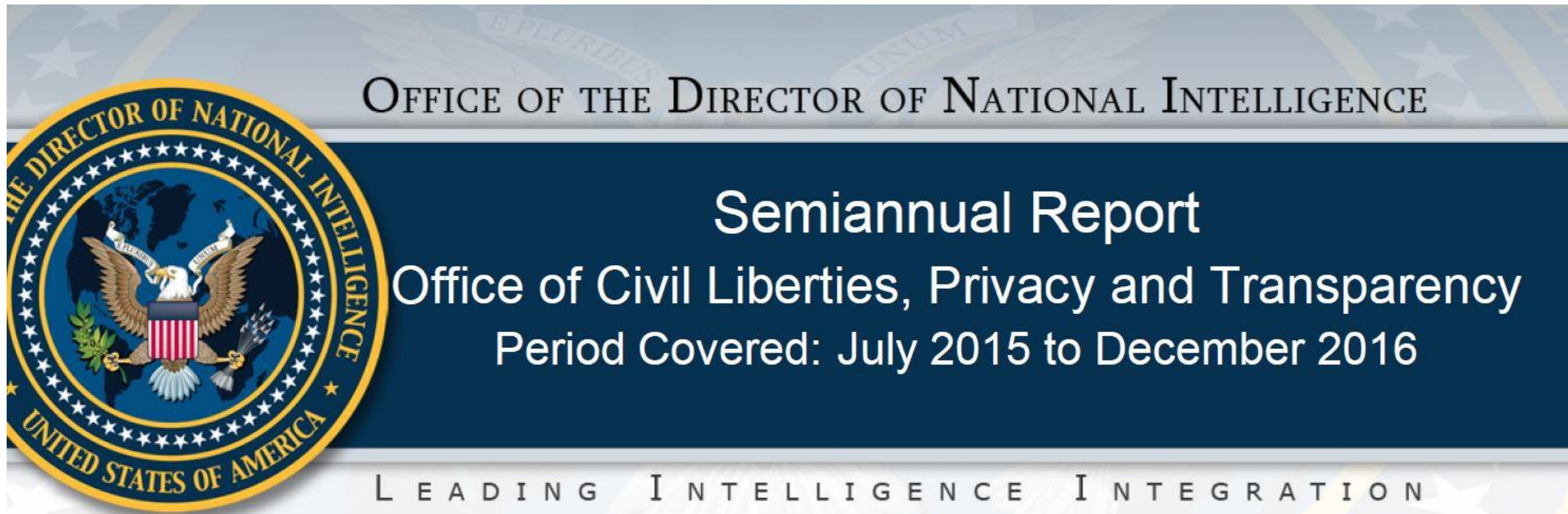
Table of Contents

Title I—Electronic Surveillance within the

United States for Foreign Intelligence Purposes

| | |
|-----------|--|
| Sec. 101. | Definitions. |
| Sec. 102. | Authorization for electronic surveillance for foreign intelligence purposes. |
| Sec. 103. | Designation of judges. |
| Sec. 104. | Application for an order. |
| Sec. 105. | Issuance of an order. |

- Implementing Recommendations of the 9/11 Commission Act of 2007 Public Law 110-53
- Section 803 - Privacy and Civil Liberties Officers, Periodic Reports:



FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) SECTION 702

CLPT continued its routine engagement with NSA, CIA, FBI, and NCTC on FISA Section 702 compliance oversight, including (i) assessing and reviewing notices of compliance incidents to provide to the FISC, (ii) participating in on-site reviews of those elements' targeting and minimization procedures, (iii) developing renewal certifications for submission to the FISC, and (iv) drafting the semiannual Attorney General and DNI Joint Assessment of Compliance with Section 702 procedures and guidelines to submit to Congress and the FISC and, in redacted form, for release to the public. Debate about the privacy and civil liberties implications of Section 702 activities generated many inquiries from Congressional intelligence oversight committees, to which CLPT drafted and coordinated the IC's responses, and from civil society advocates, with whom CLPT met to discuss their concerns. In addition, the PCLOB issued, in February 2016, its second status update on how the government was implementing the Board's recommendations that were issued in its 2014 Section 702 report.

In the area of "FISA-related transparency," CLPT facilitated public release of FISC opinions as mandated by the USA FREEDOM ACT and drafted the unclassified DNI annual reports,

SEC. 804 FEDERAL AGENCY DATA MINING REPORT

Office of the Director of National Intelligence

2016 Data Mining Report

For the Period January 1, 2016, through December 31, 2016

II. NEW ACTIVITIES

The ODNI has undertaken the following reportable activities in the current report period.

A. Intelligence Advanced Research Project Activity (IARPA)

(i) Mercury Research Program

The Mercury Research Program began in 2016 and is expected to end in 2019. The program is developing and testing methods to forecast significant group-level and societal-level events, such as political instability, disease outbreaks, military mobilization, and terrorist activities. The Mercury Research Program is solely focused on using already collected, foreign Signals Intelligence (SIGINT) data for developing and testing forecasting methods. Research teams are evaluating entity extraction approaches and prediction models that are applicable to large volumes of streaming SIGINT data and that can be used to detect changes in patterns of communications that precede events of interest. The focus is not on individuals and particular entities; rather, the data is analyzed only in relation to data features as broadly defined. The Mercury Research Program does not generate individuals'

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)



- Invests in high-risk, high-payoff research programs to tackle some of the most difficult challenges of the agencies and disciplines in the Intelligence Community (IC) .

IARPA FOUR RESEARCH THRUSTS

Analysis seeks to maximize insight from the information we collect, in a timely fashion.

- Anticipatory Intelligence developing technologies that provide decision makers with timely and accurate forecasts for a range of events relevant to national security.

Collection strives to dramatically improve the value of collected data from all sources.

- Computing endeavors to counter new capabilities implemented by our adversaries that could threaten our ability to operate freely and effectively in a networked world.

COLLECTION AREAS OF INTEREST

- Innovative methods or tools for identifying and/or creating novel sources of new information
- Sensor technologies that dramatically improve the reach, sensitivity, size, weight, and power for collection of broad signal or signature types
- Methods for combining different measures and/or sensors to improve performance and accuracy of systems
- Approaches for assessing and quantifying the ecological-validity of behavioral, neuro- and social science research
- Secure communication to and from collection points
- Innovative approaches to gain access to denied environments
- Tagging, tracking, and location techniques
- Electrically small antennas and other advanced radio frequency (RF) concepts

IARPA FUNDED RESEARCH HIGHLIGHTS

- The Babel program has become a goldmine for speech scientists, with over 50 scientific publications citing use of Babel data in 2017 alone. A total of 757 Babel speech data sets have been distributed to 136 different organizations with a goal to continue to advance speech technology research under low-training conditions.
- The SILMARILS program demonstrated trace explosive detection capabilities beyond the program's difficult targets. Phase 1 of the program developed record-setting component technologies for hypercube acquisition speed and power, as well as wavelength coverage and flatness for infrared supercontinuum sources. For this breakthrough, and others, the SILMARILS PM, Dr. Kristy DeWitt, was awarded the Intelligence Community's Award for Individual Achievement in Science and Technology.
- One of the FUSE program's software and models for prediction of emerging technologies is now available to the public. Meta is a tool that helps researchers understand what is happening globally in science and shows them where science is headed.
- The MORGOTH'S CROWN prize challenge used machine-learning approaches to develop algorithms that improve chemical detection on complex surfaces and in cluttered environments.

INFORMATION SHARING ENVIRONMENT

- The Information Sharing Environment (ISE) consists of the people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004 and a direct result of 9/11 Commission recommendations. Law enforcement, defense, and intelligence personnel rely on timely and accurate information to keep America safe, and the ISE makes that happen by:
 - Advancing responsible information sharing to further counterterrorism, homeland security, and counter weapons of mass destruction missions
 - Improving nationwide decision making by transforming from information ownership to stewardship
 - Promoting partnerships across federal, state, local, and tribal governments, the private sector, and internationally

INFORMATION SHARING ENVIRONMENT
ANNUAL REPORT TO THE CONGRESS



interagency CVE Task Force hosted by DHS with overall leadership provided by DHS and DOJ. PM-ISE's focus, in collaboration with the CICC, is to promote the leveraging of ISE capabilities by agencies, to both accelerate the Denver effort, and to provide for nationally scaling the project.



Denver-area teenagers were the target of the Islamic State of Iraq and Levant terrorist recruitment in 2014.

Frameworks and Standards

As partners move forward to implement a robust nationwide ISE, one of the greatest challenges faced in aligning the core frameworks is enabling a wide variety of information sharing and [access agreements](#) among information sharing partners.

Through a grant from the National Institute of Standards and Technology under the National Strategy for Trusted Identities in Cyberspace (NSTIC), and with support from PM-ISE, the non-profit Georgia Tech Research Institute (GTRI) has developed one [potential solution to trust and identity frameworks](#). As part of an NSTIC-funded project, GTRI has begun to pilot a [trustmark framework](#) within the U.S. law enforcement and justice communities—specifically, within the National Identity Exchange Federation. The trustmark framework is designed to scale secure [sensitive but unclassified information sharing](#) by ensuring interoperability to verified identity credentials and by supporting attribute-based access control.

DIRECTOR ANNUAL THREAT ASSESSMENT TO CONGRESS

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY

Daniel R. Coats
Director of National Intelligence

6 March 2018

CONTENTS

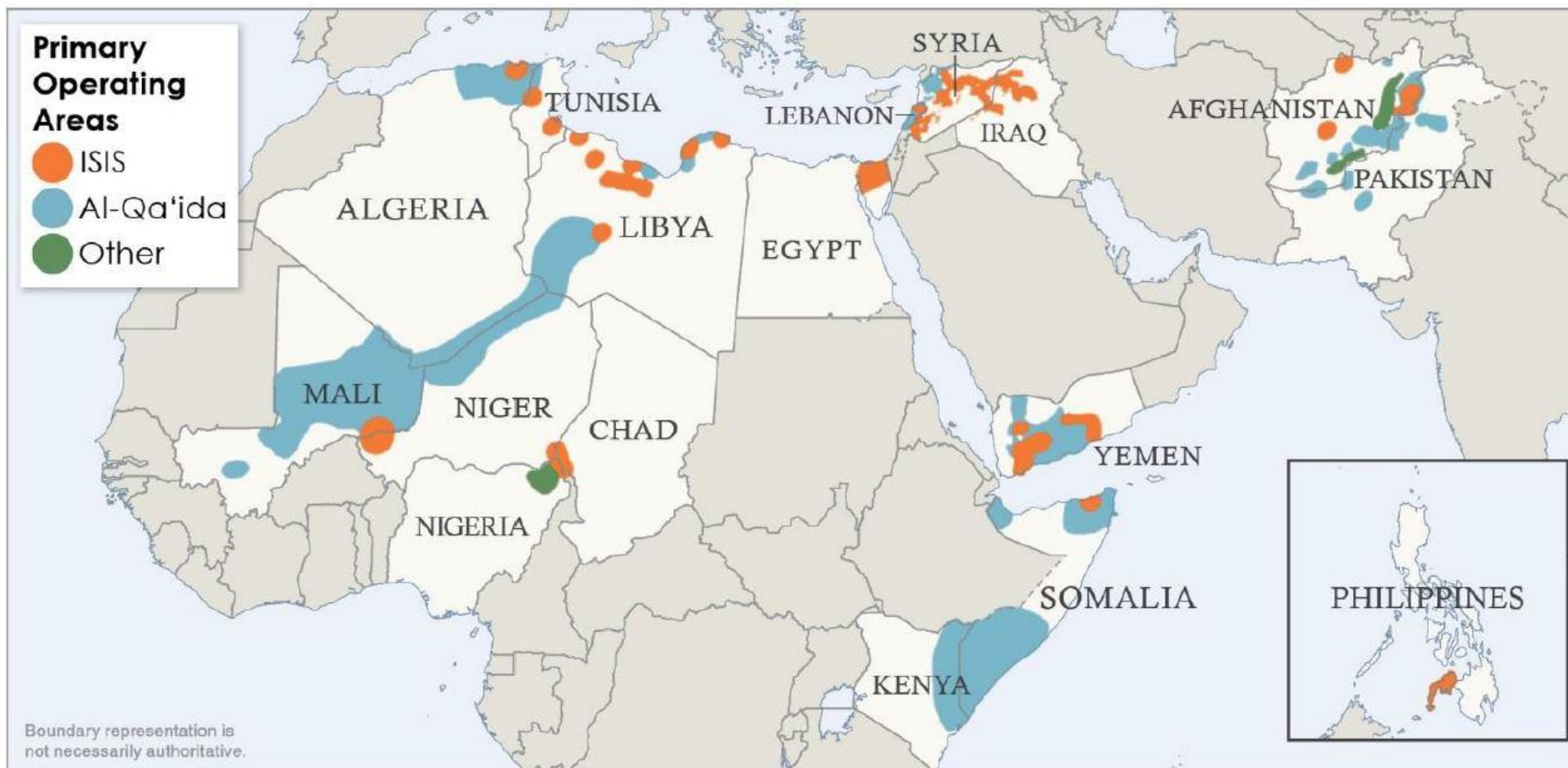
| | |
|--|----|
| INTRODUCTION | 2 |
| CONTENTS | 3 |
| FOREWORD | 4 |
| GLOBAL THREATS | 5 |
| CYBER THREATS | 5 |
| WEAPONS OF MASS DESTRUCTION AND PROLIFERATION | 7 |
| TERRORISM | 9 |
| COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION | 11 |
| EMERGING AND DISRUPTIVE TECHNOLOGY | 12 |
| TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION | 12 |
| SPACE AND COUNTERSPACE | 13 |
| TRANSNATIONAL ORGANIZED CRIME | 13 |
| ECONOMICS AND ENERGY | 15 |
| HUMAN SECURITY | 16 |
| REGIONAL THREATS | 18 |

- In Yemen, Iran's support to the Huthis further escalates the conflict and poses a serious threat to US partners and interests in the region. Iran continues to provide support that enables Huthi attacks against shipping near the Bab al Mandeb Strait and land-based targets deep inside Saudi Arabia and the UAE, such as the 4 November and 19 December ballistic missile attacks on Riyadh and an attempted 3 December cruise missile attack on an unfinished nuclear reactor in Abu Dhabi.

Iran will develop military capabilities that threaten US forces and US allies in the region, and its unsafe and unprofessional interactions will pose a risk to US Navy operations in the Persian Gulf.

Iran continues to develop and improve a range of new military capabilities to target US and allied military assets in the region, including armed UAVs, ballistic missiles, advanced naval mines, unmanned explosive boats, submarines and advanced torpedoes, and antiship and land-attack cruise missiles. Iran has the largest ballistic missile force in the Middle East and can strike targets up to 2,000 kilometers from Iran's borders. Russia's delivery of the SA-20c SAM system in 2016 has provided Iran with its most advanced long-range air defense system.

Sunni Violent Extremists' Primary Operating Areas as of 2017



BENEFITS OF ODNI INFORMATION RESOURCES

- Gain global understanding of security threats and opportunities facing the U.S.
- Learn about the multidisciplinary perspectives being brought to cope with these threats.
- Learn about how the U.S. IC seeks to balance national security with civil liberties and personal privacy.
- Gain enhanced understanding of emerging technologies being used to address, engage, deter, and defeat national security threats.

QUESTIONS?