MITRE | Center for Technology & National Security

SERIES
Number 4

INTELLIGENCE AFTER NEXT

BUILDING A COUNTERINTELLIGENCE ANALYTIC CADRE

By Jacqueline Poreda

Create a Counterintelligence Cadre

The introduction of advanced cyber techniques, persistent, ubiquitous surveillance and advanced self-learning penetration technologies leveraging artificial intelligence has significantly altered and accelerated the counterintelligence threat landscape. To address this new threat landscape, a counterintelligence analysis cadre should be established to integrate the full range of counterintelligence disciplines to effectively monitor, assess, and share foreign CI threat information. This includes traditional counterintelligence disciplines such as cyber, technical and security analysis, as well as a deeper focus on economic espionage and foreign influence. The counterintelligence community must adapt now to effectively respond to these complex threats.

The Congressionally-mandated formation of the National Counterterrorism Center (NCTC) after the 9/11 attacks serves as a useful model for the counterintelligence community. Creating a cross-agency counterintelligence counterpart to the NCTC – with the authorities and capabilities to integrate and analyze all foreign counterintelligence threat information – will significantly improve the Intelligence Community's (IC's) ability to meet the counterintelligence challenges now and into the future.

Introduction

Counterintelligence analysts must protect the U.S. homeland, American diplomatic, civil and defense missions, and sensitive national information from a wide range of threats from state and non-state actors. They monitor foreign activity domestically and overseas; understand cyber, technical collection and intelligence methods; and provide warning, threat, response, and opportunity analysis to enable the U.S. to prevent, thwart, and respond to foreign actions. These missions have become increasingly complex as foreign intelligence threats become more sophisticated.

THE INTELLIGENCE COMMUNITY SHOULD CONSIDER DEVELOPING A CENTRAL CADRE OF COUNTERINTELLIGENCE (CI) ANALYSTS WITH THE AUTHORITIES AND CAPABILITIES TO MORE FULLY INTEGRATE CI DATA TO PROTECT THE U.S. FROM FOREIGN THREATS

Today, state and non-state actors target not just the federal government, but also state, local and tribal governments and the private sector. Adversaries recognize that their own national security and intelligence goals can be achieved by conducting intelligence activities against entities outside of the federal government structure, including against critical infrastructure companies, social media and technology firms, and other private sector industries. State and non-state actors are also increasingly exploiting emerging technologies – such as commercial cyber tools that are accessible and affordable to a wider range of adversaries.

Foreign actors have a wide range of motivations, including:

- Seeking to undermine fundamental principles of free speech and democracy
- Gaining a competitive economic or technological advantage.
- Stealing military secrets to compete with the U.S. defense industrial base
- Achieving national objectives by harming U.S. critical infrastructure and supply chains
- Gaining insight into the activities of the IC and allied services, particularly as it relates to sources and methods, technical collection, tradecraft, and analysis.

Since these threats cover an increasingly broad landscape, counterintelligence analysis must employ – and integrate – a wide range of disciplines, including foreign influence, technical collection, cyber intelligence, and supply chain analysis. In addition, counterintelligence analysis needs to consider – and again, integrate – information from a wide range of sources. Counterintelligence analysis cannot rely solely on national collection means such as human, signals and imagery intelligence. Analysts must coordinate with and use information from state, local, and tribal entities as well as private sector companies, because those entities and companies might be directly targeted by foreign actors or witness foreign threats firsthand.

Today the counterintelligence community lacks the means to effectively integrate these disciplines and information, and several structural and functional changes will better position the counterintelligence analyst cadre to effectively accomplish this critical mission. Reforms made to the counterterrorism community – which had similarly struggled with integration – serve as useful benchmarks for changes that could improve capabilities within the counterintelligence analytic community.[1]

Reform the structure

Counterintelligence functions and authorities are divided across the intelligence and law enforcement communities. Today, there are four kinds of counterintelligence organizations across the intelligence community. They include those with a:

- Counterintelligence focus: conducting all-source counterintelligence analysis, including on cyber topics, but without fully integrated security and technical threat analysis.
- Security focus without all-source analysis: focused on security but not on integrated all-source counterintelligence information, and/or only examine home agency data.
- Counterintelligence and security focus without analysis: integrating counterintelligence and security efforts without analysis.
- Cyber focus: focused primarily on cyber threats.

The National Counterintelligence and Security Center (NCSC) has served since its formation in 2014[2] as the nation's lead counterintelligence organization. Its mission, according to its website, is to lead and support the country's "counterintelligence (CI) and security activities critical to protecting our nation; provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S."

The Center's authorities and abilities to lead counterintelligence analytic activities are limited, however. NCSC does not house or employ its own analytic workforce, nor does any part of its mission specifically relate to intelligence analysis. NCSC relies on the "convening" power of the DNI to foster integration across IC agencies. Convening power can be used effectively to explore specific issues, but it omits the authority to prioritize, shape, and deliver analytic production, and, as a result, the counterintelligence analytic community is currently missing opportunities to "connect the dots."

The Federal Bureau of Investigations (FBI), Department of Defense (DoD), Department of Homeland Security (DHS), Central Intelligence Agency (CIA), the Department of Energy (DoE) as well as the military services all play critical counterintelligence roles for specific issues. Each of these departments, agencies and services have counterintelligence analysts who review and assess information available to them, and many of them play key roles for integrating analysis related to specific disciplines. However, no one organization is responsible for integrating all threat information across the range of counterintelligence disciplines, including security and cyber elements.

Another structural challenge for counterintelligence analysis relates to organizational design at the department and agency level. Because counterintelligence analysis spans so many disciplines, the organizational alignment of analysts can vary significantly across the IC and government. Employees who conduct aspects of counterintelligence analysis may be aligned to security, cyber, support, or counterintelligence elements within their agency. This matrixed structure hinders efforts to integrate analysis across agencies because critical information may reside in "non-analytic" departments. For example, an individual assessing technical threats may align to a security element and not have access to all-source information about adversary threats, capabilities and intent. This structure may also prevent some missions – for example, security organizations responsible for supply chain analysis – from obtaining sufficient analytic staff or resources to meet mission needs.

NCTC as precedent for cross-agency information sharing

The 9/11 terrorist attacks revealed that—to the detriment of holistic analysis, time-sensitive warning of adversary plans, and coordinated finished intelligence production—the counterterrorism analytic community was not sufficiently centralized and analysts at various agencies and departments had unequal access to data and intelligence. Analytic offices had pieces of information – one agency had insight into al-Qaida plans and intentions, another had information about the perpetrators' activities on U.S. soil – but no single organization had the ability to integrate and analyze that information. Senator Jon Kyl argued during a Senate Subcommittee meeting in 2003 that the US. needed to "improve our ability to connect the dots between terrorists and their supporters and sympathizers."[3] The following year, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA).

The IRTPA legislation designated NCTC as the primary organization responsible for integrating and analyzing all intelligence relating to terrorism and counterterrorism.[4] To enable these changes, IRTPA required IC and law enforcement agencies to transfer dozens of analytic positions to form the NCTC. It is worth noting that while the IRTPA legislation created a new analytic workforce at NCTC, individual departments and agencies also retained analytic departments to conduct critical counterterrorism analysis. The NCTC analytic workforce was created to add an integrative analytic and information-sharing capability that did not previously exist, not to replace all counterterrorism analysis.

The IRTPA legislation and the creation of NCTC enabled numerous information sharing improvements, including:

- Enhanced situational awareness through daily threat teleconferences with the U.S. CT community.
- Distribution of threat information through the development of common tools and databases, including a central website – which reaches thousands of people in the federal government – for sharing of terrorist threat information.
- Consolidation of watchlists and databases into a single, unified international Terrorist Identities Datamart Environment (TIDE)
- Access for NCTC analysts to over two dozen government systems with different information and intelligence.

The legislation allowed the DNI to create an organization that bridged across authorities to enable the analysis of all terrorism threats.[5] The new analytic cadre, drawn from multiple disciplines and agencies, was thus better prepared to "connect the dots" of disparate intelligence and law enforcement information to identify and warn of threats.

Creating an effective counterintelligence cross-analytic cadre

Comprehensive integration of intelligence – not just piecemeal integration around specific issues – requires the development of a cross-agency analytic cadre with the authorities and tools to conduct this type of analysis. Such a cadre must have the capabilities to pull all pieces of intelligence information together to assess trends, identify threats, and evaluate mechanisms to deter or prevent adversarial activities. The IC's central cadre of counterintelligence analysts should have the authorities and capabilities to:

- Determine which partner service, proprietary, and open-source datasets are of CI relevance
- Gain access to those datasets that are currently often siloed
- Analyze and integrate that data into cadre-produced and -delivered finished intelligence to protect US and allied governments, people, and the private sector from foreign threats.

There are several ways to create the cadre and all options would require changes in authorities and the support of Congress. The cadre could be formed within the NCSC, since the NCSC already serves as the lead counterintelligence agency at the DNI level. On the other hand, because NCSC does not currently have an analytic cadre, and the tools and expertise to manage this cadre, this option is not without disadvantages. The cadre could also be housed with an organization already conducting analysis – such as the FBI, CIA, or NSA – but that could provoke concerns of outsized influence from the home agency. Alternatively, the IC could create an independent entity to house the cadre. While none of these options are perfect, creating the cadre within NCSC may be the simplest solution. It would require expanding NCSC authorities but not creating a new structure or appearing to favor one IC agency over another.

The cadre should be staffed with analysts with expertise across disciplines, including foreign influence, economic espionage, cyber, insider, technical and security threats, and supply chain analysis. The new organization should also explore ways to leverage state, local and private sector expertise, for example through term-limited advisory positions, to improve two-way information sharing and bring the relative strengths of non-federal governments and the private sector to bear against these complex intelligence threats.

Like its NCTC counterpart, this new cadre should be equipped with the authorities and tools to share intelligence information. This will require new systems and methods to ensure the protection of counterintelligence information without compromise.

The NCTC model of creating centralized analyst cadre positions but retaining CT analysts at each IC agency should also be used for this new counterintelligence cadre. Individual departments and agencies can and should retain counterintelligence analysts to conduct agency-specific counterintelligence functions, including collection, reporting and home agency-tailored insider threat analysis.

Once created, this cross-agency analytic cadre will better enable the DNI to oversee the counterintelligence analytic workforce, as it would force the DNI and individual IC agencies to focus on intelligence and collection requirements and specific requests for information, for example, as submitted by cadre analysts and managers. In addition, the creation of a single cadre would likely expose gaps and differences between analytic capabilities, enabling the DNI to better direct resources, submit access requests for data and tools that will better populate the CI cadre's pool of source material, and develop training requirements.

Challenges

The IC will need to carefully balance security, policy, legal and technical issues to build an effective cross-agency counterintelligence cadre. Significant hurdles include:

- Overcoming cultural differences and occasional distrust between counterintelligence elements of different departments and agencies. Counterintelligence elements can be reluctant to share information outside their agency, and the IC must address these cultural barriers.
- Protecting sources and methods while providing cross-agency analysts with greater access to intelligence information. Intelligence sanitization and content and classification downgrades, where appropriate to protect sensitive sources and methods, will likely aid in this effort to enable more sharing and actionable utilization of restricted intelligence.
- Managing civil liberty and privacy concerns while analyzing various data sources, many of which may contain information about U.S. persons. Enshrining and employing rigorous processes to mask U.S. and Five Eyes identities and purge non-essential personal identification information from cadre-utilized and produced intelligence is likely to mitigate many of these relevant concerns, and various U.S. organizations already employ such processes that could be replicated or leveraged as a model.
- Building mechanisms to support two-way information sharing with state, local, tribal, and private sector partners. The U.S. National Counterintelligence Strategy (2020-2022) states plainly that it is "essential that we engage and mobilize all elements of United States society and fully integrate sound counterintelligence and security procedures into our business practices." Furthermore, the same strategy asserts that efforts should be taken to work with "federal, state and local governments, the private sector, universities, as well as with our foreign partners to counter the threats posed by foreign adversaries." This strategy, written to be executed by the IC, provides the impetus for more action, sharing, collaboration, integration, and holistic analysis to be implemented by the CI community to keep our nation safe.

Conclusion

The passage of IRTPA provides a useful example of the kind of strategic workforce reforms that can improve national security. This legislated response was in large part due to the catastrophic events of 9/11 and the bureaucratic urgency it generated. The counterintelligence community, and its champions both in the executive and legislative branches, should not wait for another event of that scale to implement the changes needed today. The threats against the government, private sector, and even individual citizens continues to grow, and our capability to identify and counter these threats is increasingly failing to keep up. Adopting an approach similar to NCTC for the counterintelligence community – creating a strong and centralized counterintelligence analytic cadre with the appropriate authorities and tools to truly integrate intelligence – will help the nation better address the foreign counterintelligence threats of the future.

Endnotes

1. Information from Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004", 2006, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/CDA_14-25-2004_report.pdf
2. NCSC combined the Office of the National Counterintelligence Executive (ONCIX) with two security organizations – the Center for Security Evaluation and the Special Security Center – along with the National Insider Threat Task Force. The intent was to better integrate the counterintelligence and security missions.
3. Senate Hearing 108-921, September 10, 2003, transcription accessed at https://www.govinfo.gov/content/pkg/CHRG-108shrg93083/html/CHRG-108shrg93083.htm.
4. Information found at https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm
5. Information from Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004", 2006, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/CDA_14-25-2004_report.pdf

Authors

Jacqueline Poreda is a Lead Intelligence Analyst at MITRE with expertise in strategic planning and organizational change. She previously worked as a management consultant at Deloitte.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's analytical workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the IC's analytical community in the post-COVID-19 world.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.