IRTPA's Broad Impact: CI, Law Enforcement, and Counternarcotics

Counterintelligence: Changing Landscape, Unprecedented Threat

William Evanina

William Evanina is founder and CEO of the Evanina Group, advising business leaders on strategic corporate risk. He served as director of the National Counterintelligence and Security Center (NCSC) (2014–21).

The United States faces counterintelligence threats of unprecedented sophistication and persistence from nation states, cyber criminals, and hacktivists. The landscape of these challenges has changed dramatically in the 20 years of the IRPTA's existence. Corporate America and academia have become the new CI battlespace for our adversaries, especially China. Cyber has merged with CI threats to become one of the main vectors perpetrated by nation-state actors and their intelligence services.

Today's CI landscape grows every day with new and sophisticated tools, techniques, and surface areas of attack for our adversaries. The 2020–2022 National Counterintelligence Strategy of the United States of America, prepared by NCSC and promulgated

IRTPA's Broad Impact

Year	Organizational Change
1994	National Counterintelligence Center established
2001	Office of the National Counterintelligence Executive (NCIX) established
2002	50 USC 401 directs the ONCIX to produce, on an annual basis, a national counterintelligenc strategy
2004	As a result of IRTPA, NCIX moved into newly established ODNI
2005	First *National Counterintelligence Strategy of the United States* is approved by President George W Bush
2006	Joel Brenner appointed as NCIX
2009	Robert Bryant appointed as NCIX
2014	National Counterintelligence and Security Center established, combining NCIX, Center for Security Evaluation, and National Insider Threat Task Force; William Evanina is appointed as director
2015	Congress makes director of NCSC subject to the Appointments Clause.
2020	Evanina confirmed by the Senate as director
2021	Michael Orlando appointed as acting director
2023	Michael Casey appointed as director

Under the Office of the Director of National Intelligence, the National Counterintelligence and Security Center is Congressionally designated to facilitate the strategy and policy of our nation's counterintelligence apparatus. NCSC was created in 2014 to be a center within the ODNI that combined the Office of the Counterintelligence Executive with the Center for Security Evaluation, the Special Security Center, and the National Insider Threat Task Force. This effort effectively integrated and aligned counterintelligence and security mission areas under a single organizational construct. Since 2015, the director of NCSC, dual-hatted as the National Counterintelligence Executive, has been a Senate-confirmed position.

by President Donald Trump on January 8, 2020, set five priority pillars for the CI community:

- Protect the nation's critical infrastructure
- Reduce threats to the US supply chains
- Counter the exploitation of the US economy
- Defend American democracy against foreign influence
- Counter foreign intelligence cyber and technical operations

When Congress enacted the Counterintelligence Enhancement Act in 2002 or 20 years earlier when President Reagan signed Executive Order 12333, none of the above pillars were CI concerns nor even parts of the deliberative process. The CI community was primarily the CIA and FBI (where I spent 24 years as a Special Agent), and espionage was the greatest concern, coming on the heels of Robert Hanssen, Aldrich Ames, and others who betrayed the nation. Additionally, the CI community then had not considered the concept of nontraditional nation-state intelligence collectors and cyber operators.

Blurred Lines

Threats to critical infrastructure, protection of our supply chain, malign foreign influence, and cyber and technical operations emanate with few exceptions from our nation-state adversaries' intelligence services and/or rogue criminal entities supported by those same intelligence services. This overlap creates analogous blurred lines in authority and responsibility of US federal agencies combating these foreign efforts. No specific federal

entity has authority, jurisdiction, or strategic planning on the threats manifested every day in our nation. The most difficult part of this landscape is that the majority of the CI activates seen in the United States are manifested within corporate America and academia. The theft of trade secrets and intellectual property has become a significant strain our economy and holistic CI defensive efforts.

Cyber and ransomware threats, combined with the consistent, if not growing, insider-threat epidemic facing our nation, creates a modern view of counterintelligence. CI is no longer just catching spies from adversarial countries; it's not just espionage and counterespionage. Granted, catching spies in the US and around the globe is still an important role for the intelligence and law enforcement entitles. However, counterespionage it is just a small portion of "countering" the intelligence collection efforts from our adversaries.

Numerous foreign intelligence officers continue to collect intelligence and attempt to recruit US citizens and identify the plans and intentions of US leaders to benefit their home countries. They primarily work from within their respective embassy complex. However, the increasingly problematic and costly threat to our nation is asymmetric, via nontraditional collectors and cyber capabilities; this requires a radical strategic shifting of our nation's strategy, resources, and commitment to defend, deter, and defeat this threat.

The CI lexicon has also dramatically expanded in since the creation of IRPTA with the development of the private sector as the new battlespace for this aggressive and nefarious behavior by Russia and China and their intelligence services. The emergence of Wikileaks has added the genre of "hacktivists" to the ever-evolving counterintelligence threat. Hostile intelligence services continue to attempt to recruit US government and military personal to spy. This concept, which has evolved into today's insider-threat problem, has dramatically affected our government and military apparatus in the past 20 years.

Economic espionage has blossomed the past 20 years as well. The impact, just from an economic espionage perspective, is that the US economy loses upward of $400 billion to $600 billion per year from the theft of trade secrets and intellectual property just to the PRC. This equates to upward of $6,000 per year for each American family of four, after taxes. This does not consider the economic and reputational damage due to cyber breaches and data exfiltration. Meanwhile, PRC companies such as Huawei, ZTE, as well as Russia-based Kaspersky, among others, conduct legitimate business in the United States but also serve as intelligence collection platforms for their host country's intelligence services.

Grave Threats

The existential CI threats to our nation emanate from the PRC services, which are the most complex, pernicious, strategic, and aggressive our nation has ever faced. The US private sector, academia, research and development entities, and our core fabric of ideation have become the geopolitical battlespace. The Ministry of State Security, People's Liberation Army, and the United Front Work Department drive a comprehensive and whole-of-country approach to their efforts to invest, leverage, infiltrate, influence, and steal from every corner of US success.

The PRC also employs its intelligence services along with the strategic and programmatic efforts of science and technology investments, academic collaboration, research partnerships, joint ventures, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions. Beijing also continues to utilize nontraditional collectors to conduct the plurality of their efforts in the US, hiding in plain sight. Engineers, businesspersons, academics, researchers, and students are shrouded in legitimate work and research. The nontraditional collector can also become an unwitting tool for PRC intelligence while innocently participating in

business or academia in the United States.

In conclusion, it is hard to image that when IRTPA was created, and subsequently serving as an organizational umbrella for CI, that such a landscape transformation would occur to include the sophistication of tools and expansive resourcing by our adversaries.[a] ■

a. For a retrospective on CI, see John Ehrman, "What Are We Talking About Now, When We Talk About Counterintelligence?" *Studies in Intelligence* 68, No. 1 (March 2024).

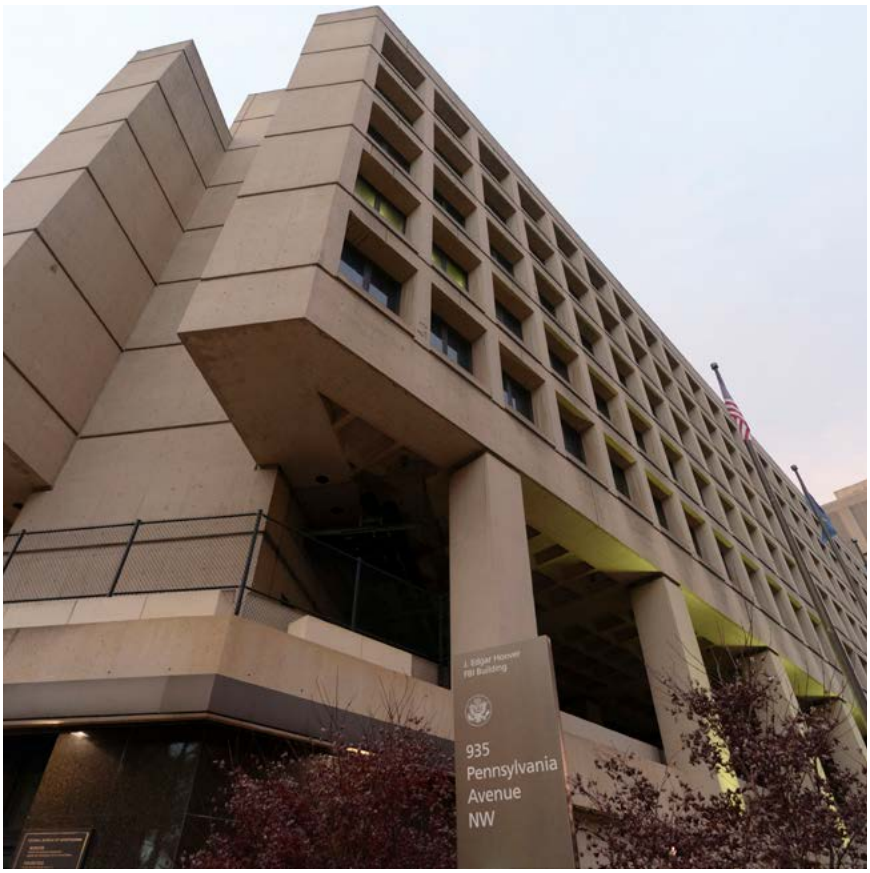
IRTPA and the FBI

John S. Pistole and Valerie E. Caproni

John S. Pistole is the president of Anderson University. He served as administrator of the US Transportation Security Agency and as a deputy director of the FBI (2010–14). Valerie E. Caproni is a judge in the United States District Court for the Southern District of New York and former general counsel of the FBI.

Before and After 9/11

This essay cannot be a history of the FBI, but the FBI's history is important in understanding the Bureau that existed on the morning of September 11, 2001, and appreciating how it transformed itself, with assistance from IRTPA, into a key member of the US Intelligence Community, while remaining the preeminent law enforcement agency in the country. Since its founding in 1908, the FBI has had the responsibility of enforcing federal laws, ranging from classic crimes like bank robbery and major thefts, to its later role (even before the National Security Act of 1947) of protecting the country from intelligence threats, both homegrown and those emanating from overseas. That responsibility includes international and domestic terrorism, as well as more than 300 other crimes and intelligence matters.



J. Edgar Hoover FBI Building

That said, before 9/11 and IRTPA, the FBI was primarily viewed, both inside and outside the agency, as largely a reactive law enforcement agency; when a crime occurred, the FBI could quickly deploy large numbers of well-trained special agents and others to gather the evidence, ascertain the individuals who were responsible, and pursue those people through the use of standard law enforcement techniques until sufficient evidence had been developed to arrest and prosecute the responsible persons.

But the FBI also had counterintelligence and counterterrorism responsibilities. In fulfilling those obligations, the FBI acted more like a national security agency and member of the IC; arrests and prosecutions were not the goal of the investigations. Those missions were, however, dwarfed by the FBI's law enforcement mission. While agents working CI and CT interacted with the larger IC, agents in those roles were a small percentage of the total workforce, and analysts in similar roles were also small in number.

Breaking Down the Wall

For reasons that are well beyond the scope of this article, over the years, policies and practice had built a divide, which DOJ dubbed "the Wall," between those two missions and had imposed limits on the circumstances in which the FBI could collect information inside the United States. Attorney General Guidelines as well as orders from the Foreign Intelligence Surveillance Court had erected barriers to the ability of agents working intelligence investigations to seamlessly share that information with agents working on criminal investigations. Those rules became the metaphorical wall that hobbled the FBI's ability to use all of the tools in its toolbox to keep the country safe, and it came under intense scrutiny and criticism when information sharing difficulties became widely known after 9/11.

The Patriot Act in 2001 was the first sledgehammer to the Wall.[a] That act eased many of the legal restraints on information sharing, including with respect to information that was gathered as part of an intelligence investigation through use of the Foreign Intelligence Surveillance Act. While dismantling the Wall and easing restrictions on information sharing were important benefits of the Patriot Act and of policy changes made at DOJ and FBI in its wake, those changes alone could not transform the FBI overnight into an intelligence-driven organization that operated comfortably both as a law enforcement agency and as a member of the IC.

The FBI's challenges went beyond legal and policy constraints. Many FBI employees who were ostensibly intelligence analysts had not been trained to be analytic, and their work was mostly tactical, not strategic. Special agents who were ostensibly both collectors of intelligence and investigators took pride in the latter but weren't trained to appreciate the unique value of the former. In addition, they were culturally resistant to taking direction from analysts. The statistics that measured success for special agents were arrests and prosecutions, not published intelligence products or information gathered outside of the parameters of an investigation. The FBI's information technology infrastructure was barely ahead of where it was in J. Edgar Hoover's time. Most employees did not have desktop access to the internet or classified connectivity to employees in other components of the IC.

Against that background were studies from numerous entities, many of which culminated in suggestions for how the FBI could improve.b But also against that backdrop were many who believed that the FBI was hopelessly locked by history and would never be able to change its culture to being intelligence-driven rather than reactive. That group vocally supported breaking the FBI apart into a domestic intelligence organization, without law enforcement powers (analogous to MI5 in the United Kingdom), and a law enforcement entity without domestic intelligence responsibilities.

By the time we became general counsel and deputy director in 2003 and 2004, respectively, the FBI had undoubtedly made significant progress toward becoming an intelligence-driven agency with law enforcement powers that was well-integrated into the IC. The FBI had partnered with the CIA, the recently created Department of Homeland Security, and other agencies to establish the Terrorist Threat Integration Center, designed to improve information sharing within the IC. The CIA and FBI had improved bilateral cooperation by reworking the memorandum of understanding that

a. Formally, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.

b. To name a few, the Joint Inquiry into Intelligence Committee Activities Before and After the Terrorist Attacks of September 11, 2001; the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission); and an Office of the Inspector General of the Department of Justice report, "A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks."

governed their respective operations domestically and overseas.

Moreover, the FBI had established an Office of Intelligence, headed by a career intelligence officer, to improve the process of collecting and disseminating intelligence. It had also established a reports-officer cadre to facilitate timely dissemination of intelligence both within the FBI and to the IC. Field Intelligence Groups (FIGs) had been set up in all of the FBI's 56 field offices.

The FBI had tripled the number of counterterrorism intelligence analysts and significantly increased the number of Joint Terrorism Task Forces throughout the country to better facilitate information sharing with our local, state, and tribal law enforcement partners. It had begun the process of reworking its training program, both for intelligence analysts and for special agents, to better enable the workforce to understand the critical importance of collection and information sharing and to maximize the synergies between the two positions. Finally, the Bureau had begun the process of creating career paths for agents and analysts in subject matter specialties (e.g., counterterrorism, counterintelligence, criminal, cyber).

Although substantial progress had been made, there were lingering challenges. As a member of the IC, the FBI received collection priorities from the IC, but the Office of Intelligence could not require collection necessary to respond to the priorities. The analytic approach and collecting intelligence against priorities was a mission not fully embraced by the workforce. And, although the Wall had been significantly reduced in importance, there remained Attorney General guidelines that distinguished between what the FBI could do in criminal investigations and what it could do in intelligence investigations, creating what some saw as career traps for the unwary.

Responding to IRTPA

With IRTPA came significant structural changes to the FBI. The Office of Intelligence was upgraded to a directorate and was combined with the CI and CT divisions into a single National Security Branch (NSB) that reported to an executive assistant director. Using the resources and talents of the Directorate of Intelligence, the EAD-NSB was, in turn, responsible for intelligence collection, processing, analysis, and dissemination. That occurred under the joint guidance of the attorney general and the DNI.

The DI was given responsibility for developing intelligence requirements and a collection management process that managed the transmission of national and FBI requirements to the field. The structure of the FIGs was standardized throughout the country and the reporting structure was changed to ensure the FIGs reported to a senior executive responsible for intelligence matters.

At the same time, other divisions, including the newly created Cyber Division, began to embrace the notion of having intelligence inform and drive their investigations. Those divisions began to use intelligence, national security, and law enforcement authorities seamlessly, and they became more comfortable sharing information more robustly with the IC, even if it related to traditional law enforcement investigations, and early enough to have meaningful conversations with partners about disruption opportunities that might include but were not solely focused on law enforcement action.

The FBI changed its philosophy on how it collected intelligence. Historically, the FBI gathered intelligence through its case-driven investigations. Under the guidance of the DI, the FBI shifted to collecting information pursuant to the intelligence cycle to achieve a comprehensive understanding of threats within each field office's geographic responsibility, and contribute unique intelligence on national-level priorities.

Collaboration within the IC and support to policymakers were enhanced by detailing FBI employees to other IC agencies and by increasing participation in the interagency process. The FBI expanded its analytic investment

in the National Counterterrorism Center, with multiple analysts and special agents assigned there. It also created and expanded the scope of the National Joint Terrorism Task Force at FBI Headquarters to increase and improve information sharing with law enforcement partners. FBI analysts have served as National Intelligence Officers, as directors on the National Security Council Staff, and as director of the ODNI's Cyber Threat Intelligence Integration Center.

Legacy of IRTPA at the FBI

Our knowledge of the current state of play at the FBI is necessarily second hand, as we have both been gone for about a decade; we are grateful to current FBI management for its input into this section.

The implementation of IRTPA forced the whole FBI to learn how to share intelligence with other agencies that have a need to know; and with partners in industry, academia, and state and local governments who are on the front lines of many of today's threats. The FBI can now take classified intelligence and turn it into useful information that can be disseminated at the unclassified level. It would have been unfathomable in 2004 for any FBI division to have written dozens of intelligence products in one year. But by 2023, the FBI was regularly disseminating hundreds of analytic intelligence products at both the classified and unclassified level, many of them coauthored with at least one other US agency.

As noted above, FBI's Cyber Division was created at about the same time as IRTPA, so it has grown and developed almost entirely in the post-IRTPA environment. As such, it provides an interesting case study of how the FBI has learned to work effectively as a member of both the global law enforcement community and the IC.

The FBI's current cyber strategy focuses on imposing costs on this country's cyber adversaries; the goal is to make it both harder and more painful for hackers to succeed. Central to that strategy is working with private sector, law enforcement, and IC partners to develop joint, sequenced operations to maximize the impact of disruptions. The FBI did so in early 2024, for example, when it and its IC partners, using IC and law enforcement authorities, forcibly evicted Russian military hackers from more than a thousand compromised routers belonging to unsuspecting victims in the United States and around the world. IRTPA created the foundation for the close interagency relationships and intelligence-driven investigations that were critical to that successful operation.

Many within and outside the FBI saw IRTPA as FBI's last, best chance to remain a single unified organization with law enforcement and domestic intelligence responsibilities. The changes IRTPA mandated were, nonetheless, viewed skeptically by many and required deep cultural shifts in an organization that had proud traditions. It is fair to say that, in our opinion, IRTPA achieved its goal, overcame the concerns of the skeptics, and allowed the cultural shifts to take hold and to create new proud traditions. We believe the FBI is in a better position now than it was pre-IRTPA, even in the face of difficult headwinds, to achieve its mission of protecting the American people from all threats, foreign and domestic. And to do so while upholding the Constitution and respecting the civil rights and civil liberties of all Americans.

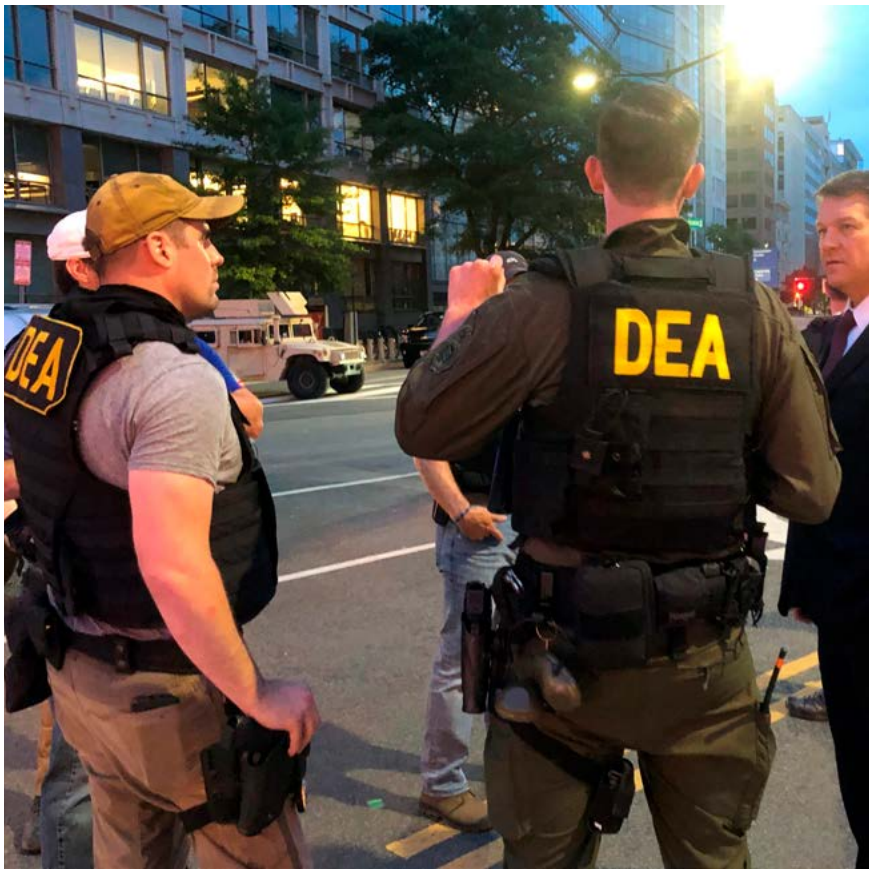
Most encouraging to us is that the FBI acknowledges their work is not over. In February 2024, Director Wray publicly announced a new Five-Year Intelligence Program Strategy to better position the organization to stay ahead of increasingly complex threats and a shifting operating environment characterized by a deluge of data, technically savvy adversaries, ubiquitous technical surveillance, disinformation, and competition for talent. The Strategy identifies technology, training, and tradecraft (both HUMINT and analytic) as key levers to enhance the integration of intelligence functions across the FBI and ensure the FBI maximizes its unique set of legal authorities as a law enforcement and intelligence agency. ■

IRTPA and Drug Enforcement

Barry Zulauf

Barry Zulauf, PhD, is a senior ODNI executive on a joint duty assignment as the DIA defense intelligence officer for counternarcotics and transnational organized crime. He previously served as the IC analytic ombudsman and chief of Analytic Integrity and Standards.

Just as 9/11 changed the world and altered the trajectory of so many lives and careers, it changed my personal and professional life. The resulting passage of the Intelligence Reform and Terrorism Prevention Act, which shaped today's Intelligence Community, compelled me to come back to the IC from drug law enforcement, gave me the ammunition I needed to bring the Drug Enforcement Administration back into the IC, and led to a new phase of my career in analytic integrity and standards for the IC.



A DEA team at work. Photo © Associated Press

From Naval Intelligence to Drug Law Enforcement

After my earlier career as a civilian naval intelligence analyst and in uniform as a naval intelligence officer, on September 11, 2001, I was serving in the DEA. At that time, DEA was not part of the IC. As part of our investigations of drug trafficking in Afghanistan reaching back into the 1990s, DEA had reported on traffickers' ties with the Taliban and Usama bin Ladin himself. We argued that this reporting pointed to the need to bring together intelligence and national security capabilities across the government, particularly between the IC and law enforcement. The pre-IRTPA IC wasn't well organized to do that.

On 9/11, I was at work in DEA headquarters across I-395 from the Pentagon. We witnessed the plane smash into the Pentagon, narrowly missing our building. At the time I was still a reserve officer, and my place of duty was in the Pentagon. If that had been a drill weekend it would have been me. Another narrow miss. Incidentally, 11 September is my birthday and I had planned for a birthday brunch later that morning with my friends in the Pentagon. Another narrow miss. I took all that very personally and decided that day to get back into the IC myself and try to bring DEA with me. Easier said than done.

DEA Rejoins the IC

The fateful events of that day started a five-year effort to bring at least part of DEA—the Office of National Security Intelligence—back into an IC transformed by IRTPA. DEA witnessed the rushed creation of the Department of Homeland Security in the immediate wake of 9/11 and strove mightily to stay out of it, preferring to remain a small, focused drug law enforcement agency. We saw early plans for creation of a DNI and intended to avoid it.[a] The story of that five-year effort is for another time; let's skip to the end, the part where IRTPA helped ease DEAs return to the IC.

Negotiations between DEA, the attorney general, the National Security Council, and the DCI—then still the leader of the IC—had taken from 2001 to late 2005, along the way securing congressional approval. The process of bringing DEA back in the fold, which had begun literally the day after 9/11, had still not come to a conclusion when IRTPA went into effect in December 2004 and the DNI took over leadership of the IC. Among the first things that DNI John Negroponte and CIA Director General Michael Hayden did was to meet with DEA Administrator Karen Tandy and Chief of Intelligence Anthony Placido (and me) to seal the deal.

Bringing DEA into the IC was the first use of the DNI's joint designation authority under IRTPA. I had the honor to serve at the first acting head of the ONSI. The actual instrument is the joint designation signed by Negroponte and Attorney General Alberto Gonzales. Other members of the IC had been created by statute (e.g., CIA with the National Security Act of 1947 and the CIA Act of 1949), or by presidential order, as with President Harry Truman's creation of NSA. Other members have since been brought into the IC by joint designation, e.g., Space Force Intelligence.

Thanks to IRTPA, ODNI had all the machinery in one place to integrate DEA into the IC, such as membership in coordinating bodies like the National Intelligence Analysis and Production Board and Community HUMINT. DEA's intelligence program did what it could to improve connections with the IC and provide higher quality analysis on the drug–terror nexus, aided materially by the early incarnations of ODNI's office of Analytic Integrity and Standards led by Richard Immerman, Deputy DNI for Analysis Tom Fingar, and National Intelligence Council Chairman Chris Kojm.[b] Those contacts, especially with DDNI/A, would prove formative for my later career with ODNI.

After bringing DEA into the IC, I was bought over to ODNI, first at the National Intelligence University and then AIS, where I became the chief. In that role, I was also designated by the DNI as the IC Analytic Ombudsman. From those assignments comes my possibly parochial view that the most far-reaching changes brought in by IRTPA are not the structural ones, but rather those dealing with analytic tradecraft to be implemented in large part through AIS. I would argue that more important than structural changes for the fundamental way that intelligence professionals work were the handful of little-noticed but far-reaching provisions of ITRPA having to do with tradecraft. From where, though, did these tradecraft provisions in IRTPA come?

9/11 and Iraq WMD

Unique in the history of IC legislation, IRTPA included specific language on analytic integrity and objectivity, i.e., analysis that is free from any direct subjective influences resulting from human experience, interpretation, or bias. These, of course, stem from the IC's failure to anticipate and prevent the 9/11

a. DEA had been moved once before into the IC by President Jimmy Carter's Executive Order 12036. DEA spent five years arguing to get out, which it did under President Ronald Reagan's EO 12333, according to this author's interview with then DEA Administrator Peter Bensinger.

b. See Tom Fingar, "From Mandate to Results: Restoring Confidence and Transforming Analysis," elsewhere in this edition.

attacks and to accurately assess Iraq's WMD programs. Among the consequences of those intelligence failures were exhaustive studies by blue-ribbon commissions to identify the problems and identify recommendations to fix them.

First, the 9/11 Commission report placed emphasis on analytic integrity and the need for a set of analytic standards.[a] The commission examined the failures that were seen as leading to the terrorist attacks on the United States. The report called for the creation of a single director of national intelligence, more intelligence sharing, better coordinating an integrating intelligence across all intelligence agencies, and the creation of a national counterterrorism center. More important, in my view, is that the 9/11 Commission found there was a "lack of common standards and practices across the foreign-domestic divide in the IC," with CIA, NSA, DIA, and others on one side and law enforcement elements on the other. Without a common set of standards, intelligence analysts could not speak clearly to one another and couldn't be properly understood by our customers, nor were they clear about what they knew as fact and what they assessed. As important, the WMD Commission[b] examined the degree to which there were perceived and real intelligence failures in the runup to the 2003 invasion of Iraq. The commission found many of the IC's prewar judgments about Iraq's weapons of mass destruction program were flawed:

> *We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure. Its principal causes were the Intelligence Community's inability to collect good information about Iraq's WMD programs, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence. On a matter of this importance, we simply cannot afford failures of this magnitude.c*

Against this backdrop, IRTPA gave the DNI the responsibility for making sure that the IC considers alternative views and is not rushing to a single judgment. Section 1017 explicitly requires analysis of alternatives, precluding starting with a pre-selected answer, such as one intended to suit a particular policy preference, and only selecting evidence to support it. The second provision, Section 1019, lays out the standards in outline form, while Section 1020 established an ombudsman for analytic integrity.

IC Directive 203

In addition to the statutory requirement, analytic standards today are also guided by Intelligence Community Directive 203, administered by ODNI's Office of Analytic Integrity and Standards. Analytic tradecraft standards are covered extensively in analytic tradecraft training courses: understanding sources and methods, explaining uncertainties, distinguishing between what's intelligence and what's a judgment, and analyzing alternatives. What is taught in these training courses is straightforward. The tradecraft standards are presented as a statutory requirement, as well as an ethical responsibility.

Intelligence delivered too late to help the decisionmaker is of no value. There's an old joke that 100-percent accurate intelligence is probably just history. By the time you get perfect information, the window for getting it to the decisionmaker is closed. Based on all available sources of information means that analysts can't cherry-pick the information that they think suits their analysis. Nobody in the chain of command can require you to put together intelligence analysis based on only a certain set of information, even if that is somehow going to be preferable to customers or other decisionmakers.

a. Formally, the National Commission on Terrorist Attacks Upon the United States.
b. Formally, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.
c. Laurence Silberman and Charles Robb, cover letter, Report to the President of the United States, March 31, 2005

IRTPA's Broad Impact

It is trite to say that IRTPA transformed the Intelligence Community in the 20 years since the legislation was passed. From my view, looking back on 37 years as an intelligence professional, IRTPA made possible bringing drug law enforcement intelligence into the IC, along with my beloved Office of National Security Intelligence. As important as that move was in the war against terrorism funded by drug trafficking, it is even more vital today, with more than 100,000 Americans dying each year from fentanyl and other synthetic opioids. IRTPA grounded the intelligence profession much more firmly than ever before in the standards of analytic integrity. Intelligence professionals everywhere can see the transformation in the way we do intelligence. ■