Deloitte.
Insights

FEATURE

Applying commercial intelligence to counter weapons of mass destruction

Exploiting underutilized commercial data sources can enhance actionable intelligence in an evolving threat environment

Wendin D. Smith, PhD, Kari Crowley, Eric Carr, Mark Freedman, and Allison Blauvelt

As weapons of mass destruction threats evolve, using traditional tools to detect malicious activity may not suffice. Analysts can turn to commercial intelligence methodologies to enhance intelligence efforts.

IN MAY 2019, the United States seized a North Korean–flagged cargo vessel.[1] During the previous year, the *Wise Honest* ship had attempted to transport 25,500 tons of coal from North Korea to international purchasers. The US government's complaint against the *Wise Honest* detailed the ways North Korea used the vessel to violate US and United Nations sanctions designed to counter the proliferation of weapons of mass destruction (WMD).[2]

The US complaint revealed that American banks had unknowingly facilitated transactions in US dollars that paid for services and equipment for the *Wise Honest*, thereby violating domestic laws and international sanctions pertaining to WMD development.[3] However, these banks did not intentionally help the *Wise Honest*; they simply got lost in the complexity of modern financial transactions—a labyrinth of countless actors transacting worldwide in near-real time. The fact that these banks were not aware of the violations demonstrates the difficulty of identifying such activities.

The *Wise Honest* case is one example that demonstrates how nefarious actors can exploit the complexity of commercial and financial systems to fund state-supported weapons programs.[4] With the right tools and know-how, however, the increasingly digital nature of trade and commerce can support solutions to counter illicit activities, especially WMD proliferation. By leveraging next-generation commercial data analytics, supply chain risk management, human capital transformation, and other commercial intelligence methodologies, the United States, its allies, and partners can expand strategies to better understand and effectively counter WMD threats. (For the definition of commercial intelligence, see sidebar, "What is commercial intelligence?")

WHAT IS COMMERCIAL INTELLIGENCE?

Commercial intelligence refers to intelligence gleaned from open-source, commercial, and proprietary data sources from all over the world. It is published in English and foreign languages, capturing data from sources such as business ownership records, shipping information, litigation filings, and international and regional news media. It can be exploited by practitioners with extensive due diligence experience in the mergers and acquisitions, banking, and financial sectors.

Navigating a complex commercial and financial environment

The ability to purchase items from all over the world with one click of a button, and to track shipments of goods in real time, are just two examples of the benefits derived from the complex and data-driven nature of commercial and financial transactions. This complexity is supported by the volume of commercial data available and the myriad international and technological venues where these financial transactions take place.

It is estimated that from 2018 to 2024, the digital payments market, such as online purchases, mobile banking, and cryptocurrencies, will double due to smartphones and online banking applications.[5] These digital payments travel through international, technology-driven supply chains—traversing multiple legal jurisdictions—and create digital exhaust from an ecosystem of international suppliers, customers, regulators, and other actors.[6] While devices and digital venues support modern commerce, they, unfortunately, also can be used to unintentionally aid malignant actors.

While devices and digital venues support modern commerce, they, unfortunately, also can be used to unintentionally aid malignant actors.

Address evolving WMD threats: Traditional tools only go so far

WMD development and proliferation occurs in an increasingly complex operating environment. The same venues that facilitate legal global business and spur economic growth can also be utilized by illicit actors. In addition to using circuitous trade routes to ship goods, money, and illegal materials, proliferators use digital financial transactions, cryptocurrencies, and newly established, sometimes one-time-use front companies to circumvent authorities and finance WMD proliferation.

These activities can result in "clean" entities or entities less likely to be monitored through traditional counterproliferation approaches (sanction lists), or national technical means (satellite monitoring) being involved, unwittingly, in illicit transactions. Such methods of obfuscating identity increase a WMD proliferator's ability to evade detection, boosting the probability of success. In times of crisis, such as the COVID-19 pandemic, proliferators may seek to take further advantage of shifting national attention, supply chain disruptions, and resource challenges to continue undetected development and proliferation of WMD or related materials.

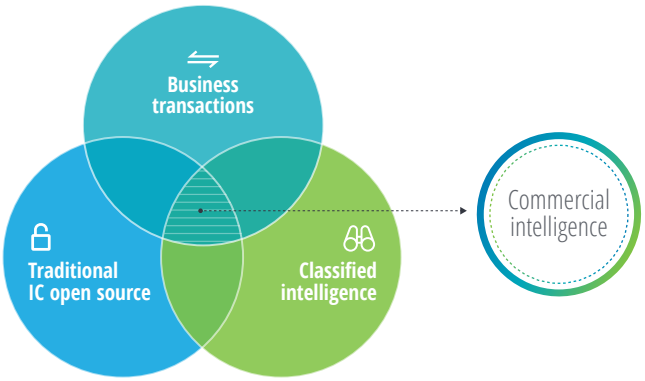
Traditional tools for countering WMD may not suffice in this modern environment. Traditional intelligence disciplines (INTs) include human-derived intelligence, signals intelligence, imagery, and intelligence derived from physical properties of a system, such as chemical or electromagnetic emissions. These traditional INTs can be successful in capturing certain types of relevant WMD information, such as the qualitative descriptions of the status of a nuclear program, phone or email communication between a proliferator and a buyer, or the construction of new missile silos.

Open-source intelligence (OSINT), such as information obtained from data freely accessible online or via some commercial providers, is also used by the intelligence community (IC).[7] Historically, however, the IC has focused on OSINT related to social media monitoring and foreign language media outlets.[8] Commercial intelligence analysts exploit additional sources to enhance the intelligence picture, including corporate records, bills of lading, business ownership records, and analysis of other business transactions (figure 1). These commercial intelligence tactics can be further enhanced with purpose-built data analytics platforms that utilize the large amount of data produced by financial exchanges to capture data trails left by commercial transactions.[9]

FIGURE 1

A complex commercial and financial environment

By exploiting underutilized sources, commercial intelligence can complement traditional tools and enhance intelligence efforts



Business transactions

CORPORATE RECORDS:
Contracts, business directors, beneficial ownership

DIGITAL TRANSACTIONS:
Bitcoin and other cryptocurrencies

INTERNATIONAL TRADE:
Bills of lading and other shipment data, vessel ownership and registration, port documentation

Classified intelligence

HUMAN INTELLIGENCE (HUMINT):
Interviews, espionage

SIGNALS INTELLIGENCE (SIGINT):
Electronic transmissions and communications

IMAGERY INTELLIGENCE (IMINT) AND **GEOSPATIAL INTELLIGENCE (GEOINT):**
Satellites and other national technical means

MEASUREMENT AND SIGNATURES INTELLIGENCE (MASINT):
Forensic and technical analysis of weapons tests, weapons effects, and industrial capabilities

Traditional IC open source

FOREIGN LANGUAGE
media reporting

SOCIAL MEDIA
monitoring

Source: Deloitte analysis.

Intelligence analysts are typically inundated with vast amounts of data that could potentially drain time and resources.[10] New commercial intelligence methodologies aimed at quickly collecting, distilling, and assessing large amounts of unclassified, open-source data can effectively use large amounts of data, eliminate information silos, and provide a clearer analysis to support the detection of malicious activity.[11]

Leveraging commercial intelligence to thwart WMD risks

Advanced commercial intelligence methodologies can supplement traditional IC tools to produce more actionable intelligence. Because commercial intelligence is unclassified and easily shareable, it can support a government's countering weapons of mass destruction (CWMD) mission by producing a clearer analysis across national security agencies and with foreign partners. Commercial intelligence is also incredibly useful for lead generation, providing necessary details and identifiers that allow more efficient use of classified intelligence tools and assets. In particular, CWMD stakeholders can utilize commercial intelligence–driven solutions in three key areas: data analytics, supply chain risk management, and human capital transformation. Here's what they can consider:

IDENTIFY AREAS WHERE COMMERCIAL INTELLIGENCE CAN AUGMENT EXISTING CWMD METHODOLOGIES

Data analytics methodologies and tools can help agencies identify WMD proliferators and illuminate weapons networks. Commercial intelligence relies on unclassified data that is not widely accessed because it often resides in commercial and proprietary databases. Key financial transaction data may be accessible only through corporate ownership records, financial disclosures, and court filings that may require paid access and specialized knowledge to identify anomalous behavior.

Commercial intelligence analysts apply expertise in corporate records and business transactions to map relationships between individuals and business entities, collecting unique identifiers (names, emails, phone numbers, addresses) and identifying points of influence in a network. In the case of the *Wise Honest*, investigators were able to build the legal case utilizing Automatic Identification System (AIS) data and bills of lading that pointed to sanctions evasion activities.[12] Other transportation data that can expand the intelligence picture include vessel travel histories, Harmonized Commodity Description and Coding System (HS) code numbers, ship identifiers, and port documentation. The quantity of data can be overwhelming—in terms of maritime trade alone, there are more than 3,600 cargo vessels that have traveled between China and the United States in the past year.[13]

Commercial analysts understand access requirements and use a range of tools to collect and interpret the vast quantity of data. **Data scraping and social media analytics tools** can be leveraged to gather further information. **Artificial intelligence (AI) and machine learning (ML) tools** can help sift through data for key markers. After the information is analyzed, next-generation visualization tools can bring insights to life through **network mapping, simulations, and graphical data representation** to support a more complete intelligence picture.

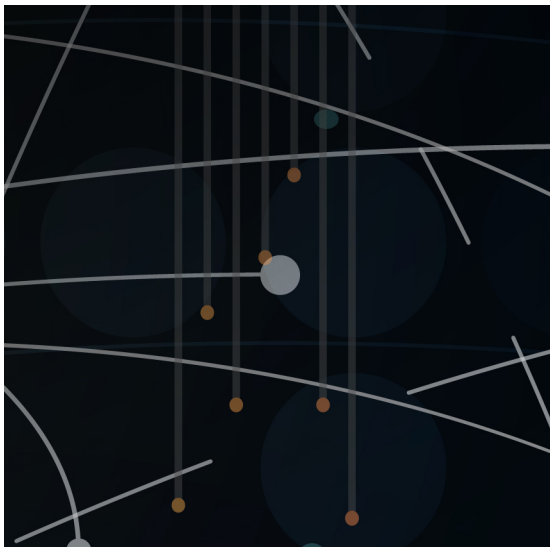
ADOPT SUPPLY CHAIN RISK MANAGEMENT PRACTICES TO ENHANCE CWMD MISSIONS

Risk management can support the US government's efforts to analyze and mitigate WMD development and proliferation in supply chain ecosystems. Supply chain risk management methodologies typically use commercial intelligence to map supplier networks and identify and mitigate risk. Those same supply chain risk management tools can be applied to CWMD missions seeking to analyze an adversary's WMD supply chain and identify points of vulnerability and opportunities for interdiction.

Commercial intelligence analysts can find supporting open-source and commercial data to highlight specific facilitators, front companies, and supply chains used for suspicious transactions, and potential illicit sale of dual-use items.

Network mapping can enable better monitoring of dual-use goods that have civilian and military purposes to potentially create a WMD. **Expert vendor vetting** by supply chain analysts can be key to understanding sublevel supplier networks of goods, equipment, or services. For example, when illuminating the supply chain for a foreign government's weapon platform, a cursory look may correctly identify the primary manufacturer that provides the system to the government. However, research by Deloitte teams has found that public procurement records, media reporting, and trade data can reveal multiple additional subtier suppliers, widening the network to dozens of involved companies and hundreds of individuals. Any one of these can be a witting, or unwitting, vector for WMD proliferation. Through **network illumination and supply chain pattern identification**, commercial intelligence analysts can find supporting open-source and commercial data to highlight specific facilitators, front companies, and supply chains used for suspicious transactions, and potential sale of dual-use items, destined for the sanctioned regimes. Commercial intelligence can be key to identify procurement or transportation of materials that violate WMD proliferation sanctions across the globe.

Additionally, as warehouses, factories, and ports increasingly implement **Internet of Things (IoT)** solutions, more data will be generated and could provide greater insights into inventory anomalies. Increased supply chain transparency supported by commercial intelligence and expertise could enable faster, agile responses to detect WMD development or proliferation activities.



INVEST IN THE WORKFORCE TO BUILD STRONG COMMERCIAL INTELLIGENCE APPARATUSES

Human capital transformation can help the US government realize the full potential of robust commercial intelligence and address evolving WMD challenges. Commercial intelligence requires tailored expertise with specific data sources, methodologies, and tools available in the market. Analysts will increasingly need **technical knowledge in the commercial space**, especially to identify anomalous behavior or abnormal business practices involved with global transactions.

Analysts in this field may have **skills that include big data analytics, global trade evaluation, industry analysis, commercial data investigations, and native language capabilities**. These skills can be combined to provide helpful commercial data pertaining to CWMD. Corporate records are often created and maintained at a regional level. As a result, there are more than 500 different websites globally that can be used to identify and validate beneficial ownership, each uniquely suited to different investigative targets.[14] Even with the aid of aggregators, analysts need to understand the intricacies of the primary sources and search in the local language to identify the relevant record. Analysts must possess the knowledge of where relevant data is located, how to procure the information, and what data would be valuable.

Analysts must also have the capability to assess the collected data and accurately distinguish between real and doctored or falsified information. These commercial intelligence skills can be applied to track down court records in foreign jurisdictions to find additional identifiers, scan foreign language social media feeds, or follow ownership in offshore jurisdictions.

A **culture within the IC that ambitiously invests in OSINT as an integral component of all-source reporting** can be critical to creating an effective commercial intelligence capability on par with other classified INTs. The US government can support this culture by investing in resources and attracting top talent to support a robust commercial intelligence capability necessary for CWMD efforts in the digital age.

As WMD development and proliferation threats continue to evolve and diversify, governments will need novel solutions to protect citizens and national interests. Commercial intelligence offers a valuable addition to the CWMD toolbox—purpose-built for a world in which the amount of newly generated data is exploding annually. Government agencies responsible for CWMD can use these emerging capabilities by:

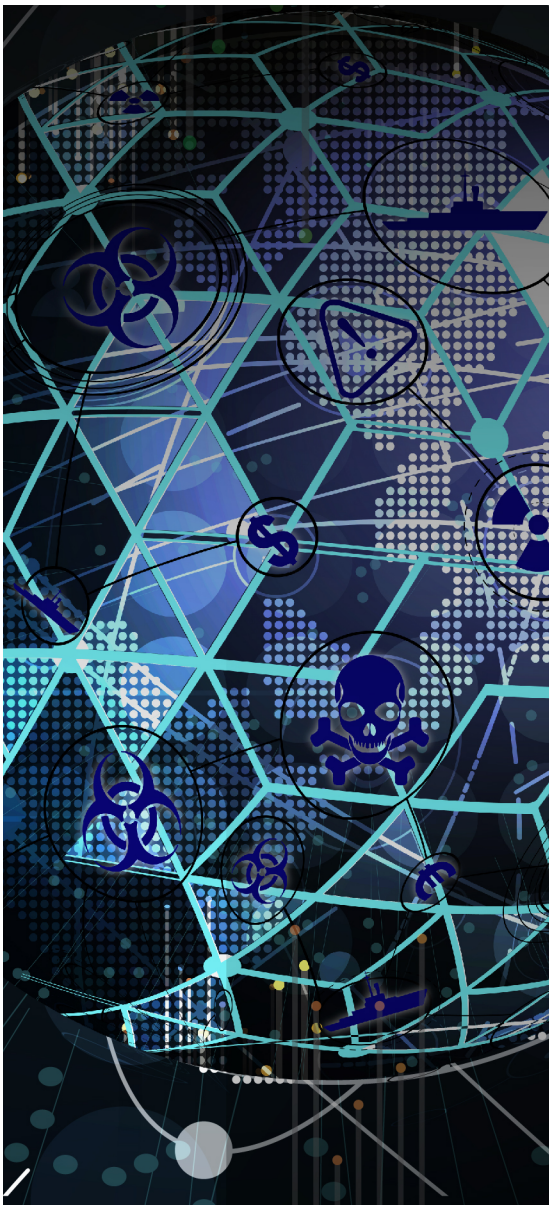
Commercial intelligence offers a valuable addition to the CWMD toolbox—purpose-built for a world in which the amount of newly generated data is exploding annually.

1. **Identifying areas where commercial intelligence can augment existing CWMD methodologies.** Data analytics methodologies and tools can help agencies identify WMD proliferators and illuminate weapons networks. Those same tools can support response efforts in the event of a WMD incident, helping to digest real-time reports, determine casualties, inform personnel tasked with decontamination, and monitor follow-on developments.

2. **Adopting supply chain risk management practices to enhance CWMD missions.** Supply chain network mapping and vendor vetting can ensure the dependability of CWMD countermeasures and equipment, as well as support US government efforts to analyze and mitigate WMD development and proliferation.

3. **Investing in the workforce to build strong commercial intelligence capabilities.** Human capital transformation including the development of new career tracks, rigorous training, and tradecraft development can help the US government maximize commercial intelligence and meet the challenges of the evolving WMD environment.

Commercial intelligence analysts can utilize unclassified open-source data along with advanced AI and ML tools to provide clearer intelligence pictures and counter evolving and dynamic WMD threats. But investment in data analytics tools, risk management methodologies, or workforce transformation will likely only be successful if accompanied by a cultural transformation that begins to value the contribution unclassified commercial intelligence can make to existing CWMD efforts. Utilizing commercial intelligence effectively can enhance the US government's ability to escape from the modern maze of commercial transactions and protect its citizens and allies from WMD threats.



Endnotes

1. Sarah N. Lynch and Michelle Nichols, "US seizes North Korean ship it accuses of violating sanctions," Reuters, May 19, 2019.
2. U.S. Department of Justice (DOJ), "North Korean cargo vessel connected to sanctions violations seized by US government," press release, May 9, 2019.
3. Ibid.
4. Edward Wong et al., "Armored cars, robots and Coal: North Korea defies US by evading sanctions," *New York Times*, March 9, 2020.
5. Market Reports World, *Digital Payments Market 2019 Global Industry Trends, Share, Size, Demand, Growth Opportunities, Industry Revenue, Future and Business Analysis by Forecast – 2024.* Marketwatch.com. May 15, 2019. Accessed February 1, 2020; Deloitte, *The future of digital payments: Choices to consider for a new ecosystem*, 2019.
6. Mark Cotteleer and Brenna Sniderman, *Forces of Change: Industry 4.0*, Deloitte Insights, 2017.
7. Cortney Weinbaum et al., "Better utilizing publicly available information," *Perspectives and opportunities in intelligence for US leaders* (Santa Monica, CA: RAND, 2018), pp. 31–43.
8. Heather J. Williams and Ilana Blum, "Introduction," *Defining second generation open source intelligence (OSINT) for the defense enterprise* (Santa Monica, CA: RAND, 2018), p. 1.
9. Cortney Weinbaum and John N.T. Shanahan, "Intelligence in a data-driven age," *Joint Force Quarterly* 90 (July 2018): pp. 4–9.
10. Joseph W. Gartin, "The future of analysis," *Studies in Intelligence* 63, no. 2 (June 2019).
11. Sandra Erwin, "With commercial satellite imagery, computer learns to quickly find missile sites in China," *SpaceNews*, October 19, 2017; Cristina Versino and Giacomo G.M. Cojazzi, "Strategic trade analysis for non-proliferation," *Nuclear non-proliferation and arms control verification* (New York: Springer Nature, 2020), pp. 373–90; Cortney Weinbaum et al., "Better utilizing publicly available information," RAND Corporation, pp. 31–43; Barry Rosenberg, "Intel community grapples with key open source intel," *Breaking Defense*, September 10, 2019.
12. DOJ, "North Korean cargo vessel connected to sanctions violations seized by US government," press release, May 9, 2019.
13. Windward, "Cargo vessels above 15m length making port calls in the EEZs of China and the United States in the last year," accessed October 6, 2020.
14. OpenCorporates, "All company registers," accessed October 5, 2020.

Acknowledgments

The authors would like to thank **Ace Stelter**, **Constance Douris**, **Tara Beeny**, and **Laila McQuade** of Deloitte Consulting LLP for their invaluable insights and research support through the writing of this article.

About the authors

Wendin D. Smith, PhD | wesmith@deloitte.com

Wendin D. Smith is a managing director with Deloitte Consulting, where she leads the firm's Countering Weapons of Mass Destruction (CWMD) practice. In prior positions, she had the honor of serving as the senior advisor to the U.S. Special Operations Command for CWMD, and as the deputy assistant secretary of defense for CWMD, Office of the Secretary of Defense for Policy. In prior roles, she has supported strategic initiatives in defense and national security, including key departments and agencies such as the Department's Defense Threat Reduction Agency (DTRA) and the Department of Energy's (DOE) National Nuclear Security Administration. Smith also serves as a formal mentor and on several nonprofit boards.

Kari Crowley | kcrowley@deloitte.com

Kari Crowley has 20 years of research and investigative experience across a broad range of engagements spanning the commercial, federal, and state and local government sectors. Crowley's teams develop intelligence on individuals, entities, and networks from a variety of domestic and foreign sources, and fuse commercial, open source, and social media information with client data to help fill in collection gaps and derive new insights. Crowley spent the first half of her career focusing on commercial clients and markets to include M&A due diligence, asset tracing, fraud, whistleblower, and Foreign Corrupt Practices Act (FCPA) investigations. Since 2008, Crowley has focused on bringing commercial best practices and network targeting to defense, law enforcement, and intelligence community clients, focusing on transnational criminal/drug trafficking organizations, WMD, illicit trade, counterintelligence, and supply chain. Prior to joining Deloitte, Crowley was a licensed private detective in the state of Georgia. She has a degree in psychology from Emory University.

Eric Carr | ericarr@deloitte.com

Eric Carr is a specialist leader with Deloitte Consulting with 25 years of experience in the defense and intelligence communities. He focuses on digital transformation across the Department of Defense (DoD) and Intelligence Community (IC), designing innovative approaches to intelligence collection, analysis, and dissemination, and developing solutions and processes to improve customer experience. Prior to joining Deloitte, he served as deputy director of the Central Intelligence Agency (CIA) World Intelligence Review (WIRe). He also covered weapons of mass destruction on the National Intelligence Council and as an analyst and manager at the CIA.

Mark Freedman | mfreedman@deloitte.com

Mark Freedman is a senior consultant for Deloitte Consulting LLP's Defense, Security & Justice practice. He focuses on strategy and operations in the national security community. Prior to joining Deloitte, he served as chief of staff in the U.S. Department of State's Counterterrorism Bureau. In that assignment and others in government, he advised senior officials on countering ISIS and Al Qaeda, preventing illicit weapons proliferation, and responding to crises overseas.

Allison Blauvelt | ablauvelt@deloitte.com

Allison Blauvelt is a senior consultant in Deloitte's Intelligence & Investigations practice, where she supports federal government clients with antimoney laundering, counterterrorism, counterproliferation, and sanctions targeting efforts. She specializes in conducting all-source intelligence analysis, including acquiring and synthesizing information from classified and unclassified sources such as corporate records, financial data, and foreign language media and litigation.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Wendin D. Smith, PhD
Managing director | Deloitte Consulting LLP
+1 703 340 3669 | wesmith@deloitte.com

Wendin D. Smith is a managing director in Deloitte Consulting LLP's U.S. Government & Public Services (GPS) practice and leads the firm's Countering Weapons of Mass Destruction (CWMD) practice.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Abrar Khan, Sayanika Bordoloi, and Rupesh Bhat
Creative: Sonya Vasilieff and Anoushriya S. Rao
Promotion: Alexandra Kawecki
Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte