
# INVESTIGATIVE SOLUTIONS
# FIGHTING CRIME DIGITALLY

**In today's world, law enforcement continues to be the primary tool for combatting forms of crime impacting global economies and national security. More and more of this crime involves digital evidence and cyberspace, requiring law enforcement officers to continuously leverage technological advances in their investigations. As a result, law enforcement organizations are seeking long-term technical partnerships with industry to evolve their craft into the digital age and strengthen their investigative operations. At MITRE, we focus on improving and automating analytic workflows associated with cybercrime investigations to reduce resource expenditures and increase effectiveness at the enterprise level.**

## Dismantling Organizations Engaged in Cybercrime

Every year, more than 300,000 malicious cyber incidents occur, making cybercrime the leading cause of business interruption globally. Recent estimates put the price of ransomware on businesses at $2M per incident with double extortion techniques, where threat actors not only steal an organization's data but also threaten to sell, publish, or destroy it if the ransom is not paid. Yet, after costly investigations that drain resources at all levels of law enforcement, less than one percent of all cybercrime ends with an arrest.

Most of the resources spent on cybercrime are directed at pinpointing the real-world person behind the keyboard. Drawing on key capabilities built in our support to the federal law enforcement sponsors, we are automating key aspects of the investigation lifecycle.

Our cyber investigative platform integrates and customizes tools that collect and index cyber data, captures analyst findings, and caters analytics to tease out identity signatures. Through DevOps and our tradecraft services, we are enabling law enforcement to close cases with increasing efficiency.

We bring **capability through software platforms and embedded technical services** to rapidly transition technology and evolve analytical tradecraft.

**For information about MITRE's Investigative Solutions expertise and capabilities, contact Chief Engineer Walter Barrett at wbarrett@mitre.org.**

MITRE

## Targeting Financial Laundering Networks

According to the United Nations, global money laundering totals per year are between $800 billion and $2 trillion. To combat money laundering, we have worked hand in hand with the Federal Law Enforcement to unlock financial crime networks, integrate untapped data sources, and perform evidence-based analysis of financial data.

With the global rise of virtual currency, criminals can transfer money without the need for a regulatory intermediary. To address this threat, we are working to integrate intelligence from multiple commercial applications to better attribute accounts and track financial transactions. We continue to research and develop new techniques to monitor illicit transactions on the blockchain.

we are working to **integrate intelligence** from multiple commercial applications to better attribute accounts and track financial transactions.

## Disrupting Transnational Organized Crime

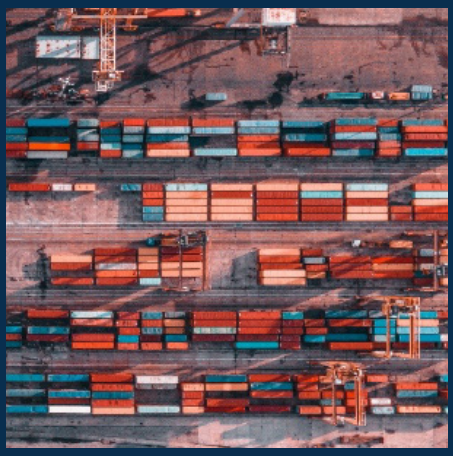
As criminal networks span the globe, efforts to combat them must cross borders as well if we are to identify and monitor illegal markets and target the kingpins of these organizations.

At MITRE, we use data sets and analytic tools to quickly establish the social network connections, business affiliations, and assets associated with individuals. That capability has enabled us to detect criminal activity and actors. We have identified criminal networks and victims associated with sex trafficking and child exploitation.

## Responding to Domestic Terrorism

In recent years, we have seen a rise in individuals and groups motivated by racial animus and anti-government or anti-authority ideologies. The United States does not yet have a consistent threat assessment and management capability available to all of law enforcement to detect these threats.

Today, numerous organizations seek to disrupt extremists' attempts to exploit the internet and impede their ability to indoctrinate individuals online. Building the right toolkit is essential to counter extremist and malign content online. Our tools to establish digital footprints, analyze social networks, and characterize online memes and jargon are designed to aid content filtering and removal programs. We are currently exploring how these tools could be used to identify manipulative information and deny extremists access to platforms that can be used to generate revenue. We seek partnerships that would enable us to serve as a bridge between platform providers and enforcement agencies to improve our near real-time threat assessment.



**Our tools** to establish digital footprints, analyze social networks, and characterize online memes and jargon are designed to aid content filtering and removal programs.

## Core Capabilities

We bring a variety of project experience from across the federal government space and have established a technical capacity in the following areas to bring sharper focus to today's law enforcement challenges.

- **Investigative Analytics:** Specifically catered analytics designed to establish and discover target signatures, analyze digital patterns of life, and fully enrich and trace cryptocurrency addresses. Includes the integration of industry-leading commercial applications and open-source platforms to enhance knowledge sharing.
- **Cyber Technical Intelligence:** Highly customized tools and tradecraft to perform network reconnaissance, end-point analytics, and malware analysis and reverse engineering to aid in dismantling adversary infrastructures and de-anonymizing private network resources.

- **Specialized Forensics:** Comprehensive inspection of artifacts associated with mobile devices, networks, and cloud systems to support evidence collection and investigation. Includes an established approach for remote triage and backhaul of various artifacts relevant for investigations.
- **Digital Data Engineering:** Well-established tools and techniques for harvesting and scraping online platform data sets including the dark web, automated tools for target selector enrichment, and linked data processing and indexing for visualization, discovery, and full text search.
- **Technical Tradecraft Services:** Methods for establishing an online presence while maintaining privacy for research and analysis on the dark web and other online forums. We continue to evolve our tradecraft to meet the changing tactics of bulletproof hosters and other criminals who are building enabling technology for the darknet and privacy markets to evade law enforcement.
- **Tactical Surveillance:** Leveraging industry-developed algorithms that can automatically detect and capture descriptive information about objects in video scenes—such as people or vehicles—we're working to integrate those objects seamlessly into open-source geospatial platforms to aid in multi-camera situational awareness, movement tracking, and forensic analysis. Additionally, we integrate location based mobile datasets with advanced activity algorithms to for pattern of life analysis.

## Software Platforms

Software platforms are a targeted investment to integrate and further develop tools in use across our work program so that they can be applied more broadly and at lower cost to the government.

- **Cyber Investigative Platform (CIP):** CIP is a platform that automates key aspects of the investigation lifecycle. The platform is a shared environment providing tools that aid in the harvesting, exploitation, and analysis of data needed to identify cybercriminals.
- **Tactical Systems Integration Lab (TACSIL):** The TACSIL addresses communication gaps where surveillance is required. It develops and integrates analytic capabilities that enable better exploitation of law enforcement video feeds and other surveillance collection systems.
- **Cryptocurrency Analytics Platform (CAP):** The CAP is designed to integrate best-of-breed cryptocurrency applications and resources so that law enforcement can explore transactions with the best possible context available. We aimed to better de-anonymize addresses, trace through mixers, and monitor for illicit activities on the blockchain.

## Differentiation

The MITRE Corporation is a not-for-profit organization chartered to work in the public interest with expertise in systems engineering, information technology, operational concepts, and enterprise modernization. In the law enforcement arena, we work directly with agents on cases and operations to rapidly modernize systems and technical tradecraft to achieve mission outcomes.

**For information about MITRE's Investigative Solutions expertise and capabilities, contact Chief Engineer Walter Barrett at wbarrett@mitre.org.**

*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.*

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®