Criminal Investigations
and Network Analysis
A DHS CENTER OF EXCELLENCE

CINA Annual RFP, Winter 2021-22: Submission and Review Process

CINA is seeking white papers presenting research ideas intended to address questions and challenges that CINA, DHS, and/or its federal partners are currently facing, or are expected to be facing in the near future. This RFP invites proposals that will address main challenges represented by the four research themes of the CINA Center. Submissions will be accepted through **Jan 31, 2022**. CINA leadership and DHS center managers and sponsors will review white paper submissions, and will request detailed statements of work for proposals selected for further review. A formal request for full SOW development does not guarantee a grant award. Projects typically range from 6-24 months in duration (pre-transition) and have funding levels from $50k to $250k per year. Research projects selected for funding are expected to start work between July – September, 2022.

In keeping with the mission, nature, and authorities of the CINA center, research proposals are expected to produce algorithms, methods, and/or tools which advance the state of the art and that may subsequently be used by DHS, law enforcement, and others to advance their understanding of, and ability to disrupt, criminal network operations. Also of interest are studies and knowledge products that advance our understanding of criminal network operations and investigations of them. Research proposals which are primarily software or hardware development efforts, or which directly support law enforcement actions as part of the research project activities, are outside of the scope of the center's operation.

A white paper submission should contain the following sections and is expected to be no more than five (5) pages in length, single-spaced, 11- or 12-point font with 1" margins. Appendices beyond five pages or external links should only be used when necessary to convey a critical aspect of the proposed research.

White paper sections:

- **Executive Summary**
- **Problem**: Description of the essential problem area.
- **Prior and Related Work**: Discussion of prior work, related work, and state of the art.
- **Approach**: A sufficiently detailed description of the proposed approach to address the identified problem.
- **Data**: Describe the data or datasets to be collected and/or used for the research.
- **Team Experience and Resources**: Provide evidence supporting the team's ability to perform the proposed effort.
- **DHS Relevance**: Identify the DHS component or components most likely to be interested in the conduct and outcomes of the proposed research.
- **Timeline**: A high level timeline for the project.
- **Cost Estimate**: Rough order of magnitude cost estimate for the project.
- **References**: Not included in page count.

White papers will be subject to a formal review process, including evaluation by external subject matter experts, to identify those proposals that will be invited for full SOW development and will be considered for potential grant awards. The full SOW, if requested, should contain the following sections and is expected to be no more than ten (10) pages in length, single-spaced, 11- or 12-point font with 1" margins. Appendices beyond ten pages or external links should only be used when necessary to convey a critical aspect of the proposed research.

Statement of Work sections:

- **Project Title**
- **List of Principal Investigators/Other Personnel**
- **Overall Budget**: Broken down by cost type (direct and indirect) and quarter.
- **Background and Purpose**: Including executive summary, purpose, operational need and alignment to DHS strategic goals, and impact to the HSE and specific stakeholders.
- **Research Objectives and Resulting Products**
- **Technical Approach and Risks**
- **Data**: Describe the data or datasets to be collected and/or used for the research, and how the data will be (or was) collected, protected (if needed), de-identified (if needed), and shared (if appropriate).
- **Project Milestones**
- **Customer Engagement and Requirements**
- **Technology Transition Plan and Intellectual Property Management**
- **References**: Not included in page count.

Key Themes for this RFP

This RFP invites proposals that will address main challenges represented by the four research themes of the CINA Center:

Challenge Area 1: Criminal Network Analysis

Today, sophisticated networked criminal activities cross communities and borders in pursuit of illicit profit, wreaking havoc on societies and devastating communities around the world. The criminal networks pursuing these activities have evolved from simple, localized, mostly hierarchical structures into complex, distributed, highly sophisticated networks that operate across the physical and cyber spaces, and also at a variety of scales, ranging from local to international. Detecting, analyzing, monitoring, and dismantling such activities presents a number of scientific and operational challenges. Overall, we seek to advance our understanding of the operational models of these networks (e.g. their characteristics, interdependencies, vulnerabilities, decision-making process, and recruitment mechanisms), and our ability to capture and analyze relevant information from diverse data sources (ranging from authoritative to open-source content).

In the above context, topics of interest include but are not limited to:

- **Network analysis:** Network structure discovery and modeling, activity detection and disruption, link prediction, multilayer network analysis, and artificial intelligence or other approaches to facilitate the automation of such analysis.

- **Criminal network operations:** Advancing our understanding of how such networks recruit members, organize their operations (including assessing the extent to which they rely on technology to pursue their goals), advertise their services, communicate and interact internally and externally (e.g. with other illicit networks, such as terrorist networks), invest their profits, and how they respond to threats.

- **Cryptocurrency, blockchain, and money laundering:** Tracing money laundering operations through digital currency services, including the nexus of illicit networks and terrorism, as well as trade-based money laundering activities and ransomware/cryptocurrency patterns.

- **Illicit supply and value chains:** Improving our ability to map illicit supply and value chains in the physical and cyber spaces, identifying the nexus of various illicit chains (e.g., human trafficking, counterfeit goods, opioids, weapons, terrorism), and devising methodologies and tools to assess vulnerabilities and weaknesses of these chains.

- **Increasing speed, efficiency and accuracy of network analysis:** Techniques to facilitate quick and accurate exposure of network connections for investigators using diverse data sources acquired from different sources and jurisdictions.

Challenge Area 2: Dynamic Patterns of Criminal Activity

Analyzing criminal activities across the physical and cyber spaces and over time, to identify relevant patterns and trends, is essential for the emergence of more effective response strategies. As the analysis of patterns of criminal activity meets big data, we are facing newfound challenges and opportunities. Some challenges and opportunities are associated with the breadth and diversity of relevant datasets, and the ability to study relevant patterns at both macro and micro spatiotemporal settings. Conquering these challenges will allow us to better understand how, where, and when criminal activities occur, and to better predict where they will be occurring next.

In the above context, topics of interest include but are not limited to:

- **Innovative spatiotemporal pattern detection:** The detection of relevant spatiotemporal patterns from diverse datasets, and the ability to contrast such data to diverse complementary datasets (e.g., sociodemographic or economic data) in order to advance our understanding of the correlation between place and crime and the mechanisms that drive the birth and death of crime hotspots, including forecasting future hotspots with machine learning and other tools.

- **Predictive analytics:** Innovative approaches for the discovery of cascading patterns of complex networked criminal activities in order to advance our ability to predict forthcoming events, detect emerging threats, and devise appropriate response strategies.

- **Convergence:** Convergence of different criminal networks and activities, e.g., drug networks and human smuggling (for example shared actors and routes**)**, or connections between Illegal Unreported and Unregulated (IUU) fishing and human trafficking in supply chains into the United States.

- **Current crime patterns:** Network analysis of retail theft, identifying the sponsors and beneficiaries of grey market movement of electronics, vulnerability in emerging alternative payment mechanisms and legislation to counter threats, identification of hotspots for illegal border crossing, and analysis of crime concentration or related metrics. Research to identify key hubs of criminal activity in the US.

Challenge Area 3: Forensics

In the context of networked criminal activities as they are studied by the CINA Center, the center's research interests span both traditional and digital forensics. Traditional forensics are boosted by the emergence of technological solutions that may revolutionize the manner in which they are conducted. Digital forensics presents some emerging challenges, as digital evidence is no longer just specific to information obtained from computers or smart phones, but now includes smart devices, the internet of things, vehicles, and a myriad of sensors - essentially anything with the ability to store and or process digital data. Accordingly, investigators require updated methods for the acquisition and analysis of data stored on digital media.

In the above context, topics of interest include but are not limited to:

- **Field collection, filtering, and triage tools:** Tools and techniques for collecting digital data from cyber physical and embedded systems in the field, to include approaches and algorithms for filtering at the point of collection and performing field triage on digital devices and media prior to seizure (of particular interest are methods which apply across a wide range of devices based on ubiquitous access interfaces and common internal structures). Also of interest are studies which catalog data retention and transmission behaviors of digital devices, whether embedded or standalone.

- **Accessing encrypted containers, media, and devices:** Methods for accessing and decrypting encrypted digital content on devices (broadly applicable methods are of the most interest, but device- or class-specific mechanisms are of interest as well), methods for virtualizing devices and encrypted storage to facilitate research, exploration, and brute force methods of access and decryption, and parallel processing algorithms and techniques for brute force and analytic processing.

- **Multimedia analytics:** Advanced video and audio analysis solutions that support investigations, including but not limited to advancements in the content-aware transmission of large image data in mobile environments, and the synthesis of multiple views in support of forensics analysis; study relationships between video quality/parameters (e.g., frame rate, resolution, color, and codec) and requirements to identify and track objects.

- **Cyber security**: Tools and technologies for threat hunting, especially in critical infrastructures; tools and techniques to characterize cyber threats and actors, especially considering fusion of cyber and physical environments and data; research into advanced decision support systems to enhance cyber defense.

- **Biometrics:** Methods for circumventing and deceiving biometric authentication mechanisms (may include, but is not limited to, creation of fake biometric inputs), and issues associated with privacy in the use of such information.

- **DNA analysis:** DNA analysis to support detection and investigation of human smuggling and human trafficking activity, to include rapid DNA analysis and genetic genealogy.

- **Substance testing and searching:** Rapid field testing of suspected illegal drugs; research into volatiles and the study of canines; human remain search canines.

- **Statistical statements and forensics:** Studies and research on the validity of statistical statements in forensic analysis and subsequent testimony.

- **Traditional Forensics**: Other forensic science research and development to support the DHS mission and activities.

- **Evidence correlation and discovery:** Methods and algorithms for discovering correlations and associations across diverse evidence sources and types (approaches may be automated or human-assisted).

Challenge Area 4: Criminal Investigative Processes

Criminal investigative processes are transformed through innovative tools and analyses that expand our capability to collect, manage, protect, analyze, and share large amounts of structured and unstructured data. Furthermore, there is an increased need to assess the impact of these investigative processes not only on the networked illicit activities, but also on society at large.

In the above context, topics of interest include but are not limited to:

- **Measures of effectiveness and impact:** Systematic reviews and other approaches to assess the effectiveness and impacts of DHS investigations, interdictions, and disruption activities; also quantifying the real and potential impact of a given criminal network or criminal activity.

- **Assessing intelligence gaps in criminal investigations:** Techniques to assess information gaps in on-going investigations, and use this knowledge to better focus said investigations (e.g. through the recommendation of additional data collection, evaluation, and analysis processes). Also of interest are methods and approaches to automate lead generation and criminal case construction, to include checklists and guides for investigators.

- **Illicit finance:** Research and develop tools and techniques to detect and combat illicit finance, especially that which supports transnational organized criminal activities.

- **Online crime**: Research, especially analytic tools and techniques, to detect, understand, model, and counter online crime.

- **Predictive policing:** Establishing and validating behavioral factors and indicators exhibited by suspected perpetrators to be utilized by law enforcement officers at entry portals via human observation and/or video analytics.

- **Digital identities**: Research into the impact and security of digital identities; also research into the detection of stolen, altered, and forged digital identities.

- **OSINT**: Research into new tools and technologies for collecting open source and social media information that can be utilized by law enforcement within the privacy-related parameters that are of concern to law makers at the federal and state level.

Challenge Area 5: Training

Proposals for training development and delivery across the CINA areas of interest are invited. Synchronous and asynchronous, as well as guided and self-directed, modalities are of interest. Proposals should include development and optionally delivery of new training content and not be limited to the purchase or delivery of existing content. Training may be incorporated into research proposals which also address one or more of the four areas and topics above (e.g., research to develop a new tool or technique and training DHS investigators and analysts on the use of such a tool or technique).

In the above context, topics of interest include but are not limited to:

- **Environments:** Development of realistic, sandboxed, and potentially virtual environments for hands-on training programs for investigators and analysts regarding tools and techniques to improve efficiency, accuracy, and completeness.

- **Specific topics of interest**: Video analytics; cloud forensics; red teaming and forensics (especially around identity systems); data science and analytics; OSINT (especially advanced tools and techniques integrated traditional tradecraft methodologies); cyber threat hunting; machine learning and AI applications and use; biometrics background, relevance, and impact; training individuals to use causal dynamic decision support capabilities within the spectrum of multi-domain operations.