Frontier Assessments Unit

A Transatlantic Team Executing Innovative Methods to Surface, Target and Collapse Next-Generation Subterranean Hostile Networks

Mission Statement | Unique Capability Set

Dr. Ryan Clarke | Hans Ulrich Käser | LJ Eads

Zurich | Washington DC

Table of Contents

The Problem: Hostile States and Highly Networked Non-State Threat Groups Have Developed New Models of Operation

Government leaders and intelligence/investigative professionals have developed advanced capabilities to combat threats posed by hostile nations as well as non-state threat groups. These capabilities are the product of decades of experience and all of its associated successes and setbacks. The net result is a professional core of seasoned investigators with field-validated methods and models that have proven remarkably effective from the Cold War period to the present. However, what happens when these two previously separate and distinct domains merge and become interoperable in pursuit of hostile state goals?

While state backing for terrorist groups can be traced back to at least the 1970s, state/non-state merging in other domain areas is a recent development. The abrupt nature of this shift has been generated by rogue states that are attempting to cause damage in target countries (mostly Western democracies) through asymmetric means. Intellectual property theft (especially dual-use technologies), cybercrime, subversion operations, synthetic narcotics trafficking, and insider sabotage within critical industry are some examples of the state/non-state nexus seeking to generate strategic effects without firing a shot.

The strategic concept is to continuously degrade and demoralize an adversary to a point where the need for overt state actions to achieve goals become minimal or even non-existent. A country that is drained of its most advanced dual-use technologies, facing increasing social problems (i.e., synthetic narcotics overdoses and associated disorder), experiencing increasing economic hardship and has serious concerns over the reliability of critical infrastructure in a crisis presents a considerably 'softer target'.

Firing ballistic missiles results in immediate attribution and a full-spectrum range of consequences. However, there are now new methods for achieving military-style effects in a less dramatic manner that makes specific attribution a more difficult endeavor. This requires hostile nations to harness the networked structures of non-state groups for mutual benefit.

The Threat: Hostile States Sponsor and Instrumentalize Non-State Networked Groups for Hybridized Warfare, Infiltration, Subversion, and the Capture of Key Institutions

The current strategic environment is the most complex, nonlinear and fundamentally less stable than at any point in human history. Simultaneously, security risks are becoming increasingly hybridized with hostile state sponsorship of non-state actors to subvert and destabilize target societies prior to the undertaking of overt kinetic operations. Countries such as Ukraine and Taiwan are clear cases in point in addition to numerous other examples of ongoing operations across multiple Western and Asian nations. Western leaders and national security agencies face an exponentially increasing number of geographically distributed, networked, and highly adaptive threat groups that are actively engaged in illicit strategic technology acquisition as well as psychological operations, sometimes simultaneously.

Technological developments have also opened legal recourse to capabilities that can seriously threaten societal and kinetic targets at a massively increased scale. These groups operate seamlessly across national borders and generate often-fragmented, disparate data trails behind them in faint signal form. For example, in recent years we have witnessed continuously expanding interoperability between organized criminal syndicates and terrorist groups, hostile

states and non-state proxies, and even the infiltration, subversion, and hostile nation-state capture of key domestic and international institutions across the world.

These accelerating international risks in these domains and others clearly represent new types of threats at greater scale, sophistication, and with intentionally fragmented organizational structures designed to frustrate investigations. These threat groups have been able to temporarily outpace many executive branches of government, law enforcement organizations, intelligence agencies, militaries and financial sector leaders due to the latter's current reliance on investigative methods and analytical tools that were developed during a previously less complex period; a different battlespace.

The Age-Old Question: Target, Approach, or Observe?

While threat group networked structures are the strategic unit of analysis, specific individuals across this network structure are key. Once the key individual/s of a networked threat group that pose serious (for example) subversion, narcotics trafficking and/or financial sanctions evasions risks is identified and a pattern of life is generated, a whole new range of strategic-level questions arise:

- Do we immediately arrest this individual?
- Do we approach and attempt to convince them to work with us?
- Do we not alert this individual in any way and observe them for maximum intelligence collection or investigatory value?

The answers to these questions involve going down very different investigative pathways and involve literal life and death decisions in some cases, such as if a threat group is known to engage in acts of terrorism.

This is the fundamental question that has challenged governments and security professionals for generations. How can we more reliably determine what the direct and indirect consequences of our actions on this networked threat group are going to be over the near, medium, and long term? How do we calculate cost-benefit analyses of specific courses of action more precisely? While these are by no means trivial questions, their answers lie in the newly emergent field of multi-domain network graph analytics of which the Frontier Assessment Unit is a demonstrated leader.

This set of analytical methods and technologies enable an individual/s to be placed within a broader organizational network context and to identify and determine the nature of strong, moderate, and weak connections to other members. This enables determinations to be made as to how these connections will be specifically impacted by various courses of action over various timeframes.

This approach also enables governments and investigators to surface critical structural vulnerabilities, such as overreliance on one specific bank account or private wealth manager, front company, or even a car. It is within this framework where the primary, secondary, and even tertiary impacts of a particular course of investigative or intelligence action can be empirically determined using threat group-specific aggregated data represented in network graph form.

The Strategic Solution: Frontier Assessment Unit Network Graphs

Based in historically neutral Switzerland in the middle of Europe, the Frontier Assessment Unit serves as the pioneering and much-needed transatlantic capability to fundamentally enumerate threat group networks, map and assess the full spectrum of these abovementioned issues. The Frontier Assessment Unit will also simultaneously generate decision-relevant options for Western governments, law enforcement agencies, intelligence services and uniformed armed forces.

Individual country-centric approaches to tackling these challenges are no longer effective as threat groups themselves have clearly modified their own network structures, modes of operation and strategic aims in order to attempt to degrade (and eventually subdue) multiple Western countries simultaneously. Unlike other research units, the Frontier Assessment Unit allocates all funds to operational and investigative functions. With no unnecessary overheads, this decisive capital efficiency enables the discovery and surfacing of key findings at a fraction of the cost of its country-centric counterparts

In order to enable a full strategic understanding of the emerging national security situations such as those outlined in the analysis, network graphs are essential. Network graphs represent the most effective method for aggregating data from multiple sources, distilling down complexity, and representing key strategic intelligence information in the most high-fidelity form for network structure enumeration and precision targeting applications.

The developments described above pose a range of network mapping and targeting challenges for governments as well as critical infrastructure and service providers in the private sector. Previous notions of 'red lines' and other traditional deterrents no longer have validity in the current strategic environment. Worse yet, hybridized and networked hostile activities largely go unnoticed in the West, as current analytical capabilities are too disjointed and the analysis too narrowly focused on the traditional kinetic and linear dimension of interstate conflict. This threat has most evidently materialized in the form of large-scale concerted cyberattacks and data theft against a wide range of public and private actors of strategic significance. Reliance of private actors on governments to provide full-scale protection against state-sponsored hostile activities directed at them further increases the vulnerability of the soft underbelly of liberal Western societies.

However, recent breakthroughs have equally provided a new arsenal of tools to cope with speed and complexity. Advanced multi-lingual search unveils the traces of dispersed activities from a broad variety of actors. Multi-domain data aggregation, and knowledge representation via network graphs then ties seemingly unrelated or benign activities to a common hostile purpose with a strategic threat vector. Strategic net assessment integrates these capabilities to provide a robust, fact-based description of current-state dynamics and is the most effective method for successfully navigating the new threat environment.

The Frontier Assessment Unit Method: 360 Degree Profile-Generating Data Models That Induce Operational Pressure

While the more difficult to quantify motivations such as nationalism and ideology can account for some of these hostile activities, other factors are also operating. Involvement in state-sponsored activity can prove to be transformative experience for non-state groups, both financially and in terms of power differentials relative to other rival non-state groups. There

are numerous examples across Latin America, Europe, the Middle East and Asia of non-state groups experiencing exponential growth in strength and resources due to hostile state sponsorship.

However, beyond the initial 'honeymoon period' between a hostile state and a non-state group/s, what holds the joint partnership together over multiple years, or even decades? Mutually reinforcing interests, often in the financial domain. The greater the accruing financial capabilities, the more ambitious and risk-tolerant this state/non-state nexus becomes. The correlation has been observed across multiple recent historical cases, from Russia to the former Yugoslavia to Iraq.

360-degree profile models uncover mutually reinforcing interests (often but not only in the financial domain) and allow decisionmakers both in the public and private sectors to understand the strategic importance of disparate and seemingly unconnected groups and anticipate their hostile activities. Some key units of analysis for data model generation are field-based leaders of the non-state group and their government handler/s. Data models must be focused on identifying specifically what maintains the credibility of a specific leader in question. Why do subordinates continue to follow their orders? Why do they continuously take risks that could result in severe consequences for themselves?

Case Study One | Subversion Operations Against Democracies

While the various nations that are engaging in these types of hostile activities against Western democracies are driven by different strategic goals and desired end-states, the most aggressive and capable can trace at least the initial components of their programs back to the Tools, Techniques, and Procedures (TTPs) of the Cold War, such as:

- Active measures.
- Demoralization.
- Destabilization.
- Normalization combined with the formation of United Fronts.

These concepts have transmogrified across multiple geographies and are being put into direct application on a daily basis. While this is problematic for a range of reasons, this overall consistent superstructure provides unique analytical opportunities to develop more universal methods for precision targeting through the use of network graphs.

Given the continuously adapting and amorphous network structures of these threat groups, cross-examination of suspects often do not yield strategic-level results for investigators and other personnel. Sometimes these less-than-optimal results are attributed to an individual being a fully committed ideologue. While this is occasionally the case, more often it can be attributed to the fact that this individual is simply not aware of the overall networked structure that they operate as a single node within.

However, as is the case with all human organizations, there is always at least one connector node in the form of an individual or small group that is required to move across (mostly) compartmentalized cells. This is often necessary to ensure consistency and compliance with the overall strategic intent and direction of the organization's leadership and to also aggregate material information to 'report up the chain'.

While information regarding who these individuals are and how they operate can be restricted and effectively controlled at the human-to-human level, these 'cross-pollinators' emit faint but detectable and interpretable signals through their mobility patterns, financial activities, electronic communications, and a range of other unavoidable human activities that enable a pattern of life to be established.

This fragmented data aggregation and analysis is accomplished by the use of multi-domain network graphs that ingest, structure, and characterize these fragmented data streams and convert them into a clear situational intelligence picture.

Case Study Two | State-Sponsored Synthetic Narcotics Trafficking

The greatest operational risk in synthetic narcotics trafficking is not the actual production and distribution of the 'product' itself, it is actually managing the revenue generated by these activities. High-velocity synthetic narcotics in pill form generate massive amounts of cash that has to be deposited into internationally-connected financial institutions and 'converted into electrons' as fast as possible.

The physical cash dependency of state-backed synthetic narcotics trafficking syndicates represents a consistent vulnerability with no near-term remedies. Electronic payment systems, credit cards and other cash alternatives all have mature detection capabilities and face legal liability for facilitating illicit transactions. Even the use of the dark web presents risks given its anonymity and the associated risks of theft with no recourse.

This surfaced dynamic lends itself to data model generation to determine exactly how the mechanics of these cash management operations work and what critical inputs are required to enable them to operate consistently and at the scale required. It is through the development of the data model that investigators will gain insights as to where exactly to strategically 'turn the screws' to achieve operational degradation effect and/or stimulate massive evidence generation by forcing an illicit network to behave erratically.

An established policy of some rogue states has been to directly support and control the development of an alternative pharmaceutical industry with key advanced components being placed inside their own territory. The long-term goal is to become 'the pharmacy of the world' with critical global dependence on rogue nation-controlled supply chains, from pill manufacturing to lab coats. One highly problematic outcome of this exercise has been the development of synthetic narcotics for export that are manufactured in pharmaceutical-grade factories.

One of these 'products' is fentanyl-laced heroin, which represents a combination of a (mostly) legal opiate, fentanyl, with the lethal and illegal substance of heroin. The most problematic manifestation of these developments can be found in the triangular dynamics between Asia, Mexico, the United States and now increasingly Europe. Even with the supposed mobility restrictions associated with the COVID-19 pandemic, the Nueva Generacion Cartel, a key Mexican drug cartel, has achieved strategic superiority over a range of other well-armed and violent drug trafficking cartels operating in Mexico, including the Sinaloa Cartel.

These surprising developments have largely been attributed to the Nueva Generacion Cartel's current control over Mexico's Pacific ports, something which has allowed it to essentially monopolize control over the import of key precursor chemicals from rogue states in Asia.

These developments have surprised many seasoned experts across the full spectrum of the national security apparatus in the United States and elsewhere. However, with around 100,000 annual drug overdose fatalities in the United States and these risks spreading to Europe,[1] it is essential that these phenomena are fully mapped, assessed, and key outputs effectively distributed to key decisionmakers and field-based personnel. Network graphs are the most effective, field-tested, and proven method in achieving these endpoints.

Frontier Assessment Unit Fusion | Rogue States, State-Owned Banks and the Nueva Generacion Cartel: From an Amorphous to a Target Rich Environment with Network Graphs

Above and beyond importing precursor chemicals for manufacturing fentanyl-laced heroin, the Nueva Generacion Cartel also maintains pharmaceutical-grade factories that are owned by foreign interests on its territory. These factories have largely foreign management teams and produce synthetic narcotics for illegal export to the United States. This illicit business does not require a heavy transportation infrastructure footprint as even small regional airports and basic quality road networks suffice. These cargo shipments do not require much space in pill form and are also rather lightweight.

Despite the light transportation infrastructure footprint, these illicit pill manufacturing factories are energy intensive and are highly sensitive to power supply disruptions. These factories are also often in remote areas that are not connected to the Mexican National Grid. Because of this, the foreign management of these factories have had to innovate and implement high-performance remote power solutions to ensure uninterrupted continuity of operations. The purchase and/or importation of these remote power solutions represents one example of a unique data point to track, assess, and contextualize in network graph form alongside other data generated by other cartel-related activities.

Drug trafficking syndicates in rogue states (which cannot operate independently without the government) have defied the predictions of many and have proven capable of navigating a complex and violent environment to establish themselves as the leader of Mexico's synthetic narcotics industry. However, the foreign syndicates currently prefer to 'hand off' distribution in the United States to both Mexican cartels and American criminal syndicates with a percentage of US-generated profits flowing back down to the foreign syndicates in Mexico.

---

[1] For example, please see 'Fentanyl Flow to the United States', DEA Intelligence Report, January 2020. DEA_GOV_DIR-008-20 Fentanyl Flow in the United States_0.pdf
'Complexities and Conveniences in the International Drug Trade: The Involvement of Mexican Criminal Actors in the EU Drug Market', Europol and the United States Drug Enforcement Administration, December 2022. Europol_DEA_Joint_Report.pdf (europa.eu)
H.Res.39 - Expressing the sense of the House of Representatives that illicit fentanyl-related substances are a weapon of mass destruction and should be classified as such', United States House of Representatives, 17 January 2023.
H.Res.39 - 118th Congress (2023-2024): Expressing the sense of the House of Representatives that illicit fentanyl-related substances are a weapon of mass destruction and should be classified as such. | Congress.gov | Library of Congress

Rogue state-owned financial institutions play a critical role in enabling this illicit business, especially through mobile banking applications that enable Mexican drug traffickers to utilize these networks. In order to capture and effectively analyze all of these multidimensional activities and distill key information down into decision-relevant form, network graph capabilities have become essential.

This triangular Asia-Mexico-United States case study and countless others clearly represent new types of threats at greater scale, sophistication, and with intentionally disparate and fragmented organizational structures designed to frustrate investigations. These threat groups have been able to temporarily outpace many law enforcement and national security agencies

However, recent breakthroughs in advanced search, multi-domain data aggregation, and knowledge representation via network graphs have provided these dedicated security professionals with a new arsenal to defeat these threat groups who currently believe that the future belongs to them.

Data sources from the representative list below can provide a directly actionable strategic intelligence picture when effectively interrogated and assessed. It is these types of data that can be simultaneously aggregated and converted into network graphs every day for intelligence generation and precision targeting applications:

- Corporate data (multiple types)
- Shipping and flight information
- Import/export documents
- Financial information
- Public utility accounts
- Company blacklist data
- Company director blacklist data
- Trademark data
- License granting/revoking data
- Non-Profit Registry Data
- Multi-lingual patent filing data
- Multi-lingual scientific publishing databases
- Bulk purchases of dual-use laboratory equipment
- Legally intercepted communications and mobility data
- Legally collected social media data
- Debriefing/interrogation notes
- Leaked documents
- Visa and entry/exit registries

- Tax databases

Case Study Three | Financial Sanctions Evasion: Front Companies, Organized Crime and Illicit Hostile State Assets

Eurasian private military companies and organized criminal syndicates are known to be some of the world's most sophisticated and bold organizations with regards to the use of front companies, local nominee company directors, and original source of funds obfuscation. These syndicates are also well known for their 'innovation' in circumventing sanctions regimes by routing into the Western financial system via several other 'clean' financial institutions that are domiciled in currently non-sanctioned countries.

These decentralized and deliberately compartmentalized illicit financial networks pose major emerging challenges for national security agencies as well financial institutions. In the case of financial institutions, the full spectrum of the industry face risks; from the highly transactional (such as investment banks and hedge funds) to the longer term-oriented segments (such as private equity and venture capital). This is also not an issue that is specific to anti-money laundering/anti-fraud teams, compliance, or legal teams; this is a CEO-level issue.

The amorphous structures of Eurasian private military companies and organized criminal syndicates generate a fragmented, varied, and geographically distributed data environment that mostly (if not entirely) involve interests that are not overtly Eurasian. A small trading house in Hong Kong with 5 employees, a logistics company in the United Kingdom with a limited fleet of trucks, and a Singapore-domiciled shipping company can manifest surprising relationships under these acute circumstances.

This is especially the case when secondary and tertiary degrees of connections of each entity are factored into the analysis and a broader tree-shaped network graph is generated. These network graphs are the most proven and effective method for an investigator or analyst to ingest, aggregate, and represent this type of situational intelligence for both strategic decisions as well as law enforcement actions. Network graphs enhance and augment professional expertise, judgment, and dedication.

We Know You Too: Equalizing Information Asymmetries with Data Models

State/non-state nexus operators depend fundamentally on one element: massive information asymmetries. They literally bet everything on remaining clandestine, undetectable and impossible to profile and target. They utilize some of the most advanced tradecraft and can 'reach back' to a state patron for almost limitless funding provided that the objective is sufficiently strategic.

However, these structures all face one unavoidable weakness in that they require intensive interaction with the target country's own overt, licit system. This is visible to many and intensely monitored by law enforcement, intelligence services and responsible private sector executives and technical specialists.

At present, these threat actors still appear to believe that they can 'hide in the sea of noise' as so little is often known about who they are and how they operate. If full 360-degree profiles are generated through the effective use of new data model methodologies, these individuals very quickly become more high fidelity, detectable and prosecutable than they have ever

anticipated. Those who have become used to the anonymity of dark tunnels react erratically and make irreversible mistakes when a flashlight appears.

Converting Knowledge into Precision Targeting: Generating Executable Options with Anticipated Strategic Effects to Collapse Hostile Networks in the West

Utilizing these unique network graph generation technologies and methods, the primary strategic output of this overall exercise will be to utilize advanced methods in Counter-Threat Network (CTN) analysis and other related analytical fields to generate a range of executable options to identify, isolate and fully characterize and assess the nature of emergent networked hostile networks. CTN-driven targeting options will be tied to specific policy goals and can include, but would not be limited to:

- Fully inform the public about the threats of hostile threat networks in the West. Public exposure of these activities through open-source and independently verifiable information will alarm the public as well as some international collaborators who are not aware of the true intentions of their 'counterparts'.

- Identify which specific domain areas/sectors present the most serious accelerating risks due a concentration of hostile fused operations

- Develop key risk indicators to develop field-validated early warning indicators that a particular domain/sector is being actively targeted by hostile operations

- Formulate and execute precision sanctions against strategic elements of the fusion of hostile interests

FAU Lab: Feedback Loops From the Field, Next-Generation Network Surfacing and Targeting Techniques for Operators and Analysts

While roughly a substantial portion of FAU operations and projects are on-site and field-based with key Western governments and private sector entities, FAU Lab serves as our fundamental research capability and is the FAU's key point of differentiation from other companies. FAU Lab has the strategic task of absorbing field and other technical inputs and utilizing them to develop new targeted methods and technologies. This tight, closed feedback loop ensures that FAU is never static and always maintains its strategic informational and methodological edge over the networked threat groups that it is tracking, targeting and collapsing. In addition to its work in the field, the FAU Lab team has also produced multiple open-sourced seminal works that can be found on our website across critical international security domains such as:

- Bioweapons

- Nanoweapons

- Biochemical Weapons

- Chemical Weapons

- NeuroStrike
- Organized Criminal Syndicates (State-Backed and Non-State)
- Transnational Terrorist Groups
- Subversion Operations
- Offensive Cyber Operations
- Multi-Modal Smuggling Networks (From Synthetic Narcotics to Fissile Material)
- Defense Industrial Base Structure of Hostile States
- Hypersonic missiles
- Direct Energy Weapons
- Cognitive Warfare
- Military-Grade Semiconductor Technologies
- 6G-enabled Weapons Systems
- Weaponization of Financial Markets
- Illicit Military and Dual-Use Technology Acquisition Operations
- Network Graph Generation Methods
- Data Model Generation Methods

The FAU Lab team recently published the world's first and only multi-pathogen, multi-site and multi-lingual strategic net assessment across the full spectrum of China's bioweapons program. Our book, titled '**China's International Military-Civilian Virology Fusion: High-Risk Pathogen Research, Global Linkages and Strategic Implications'** has been utilized by transatlantic security agencies, law enforcement organizations, militaries, senior elected officials and senior civilian leaders for a range of applications. This book pioneered numerous new methods in subterranean network surfacing, mapping and target generation to present a massive, fully integrated global network that was previously unknown and operating with impunity. This is no longer the case.

China's International Military-Civilian Virology Fusion: High-Risk Pathogen Research, Global Linkages and Strategic Implications: Clarke, Dr. Ryan, Lin, Dr. Xiaoxu Sean, Eads, LJ: 9789869777483: Amazon.com: Books

The FAU Lab team have held senior research and faculty positions at and maintain strong fundamental research linkages with the following leading universities and research institutes.

- Massachusetts Institute of Technology (MIT)
- Oxford University
- University of Cambridge
- ETH Zurich
- Center for Strategic and International Studies (Washington DC)
- Royal United Services Institute (London)
- National University of Singapore
- Singapore National University Hospital
- Agency for Science, Technology and Research (A*STAR | Singapore)
- Institute for Defense Studies and Analyses (New Delhi)

FAU Lab personnel have also held senior analytical positions in the following government agencies, militaries and multinational private sector firms:

- Swiss Armed Forces
- United States Air Force
- United States Army
- Armed Forces of Ukraine
- Federal Bureau of Investigation
- United States Marshals
- Julius Bär
- Barclays Capital
- Deutsche Bank
- Booz Allen Hamilton
- Digital Realty