Intelligence and Analytical Approaches for the Crime-Gang-Terrorism Nexus

John P. Sullivan and Nathan P. Jones

Abstract

This paper discusses the range of intelligence challenges and approaches to addressing the cross-cutting issues of crime, gangs, and terrorism. These approaches include fusion centers, terrorism early warning, and analysis/synthesis approaches. Tools potentially included within these approaches include red teaming, transaction analysis, intelligence preparation for operations (IPO), social network analysis (SNA), as well as automated open-source early warning tools and datasets to support a range of analytical activities, information-sharing, and the production—or co-production—of intelligence.

Keywords: intelligence, crime, gangs, terrorism

Inteligencia y enfoques analíticos para el nexo crimen-pandillas-terrorismo

Resumen

Este documento analiza la gama de desafíos y enfoques de inteligencia para abordar los problemas transversales del crimen, las pandillas y el terrorismo. Estos enfoques incluyen centros de fusión, alerta temprana de terrorismo y enfoques de análisis/síntesis. Las herramientas potencialmente incluidas dentro de estos enfoques incluyen red teaming, análisis de transacciones, preparación de inteligencia para operaciones (IPO), análisis de redes sociales (SNA), así como herramientas y conjuntos de datos automatizados de alerta temprana de código abierto para respaldar una variedad de actividades analíticas, información. el intercambio y la producción —o coproducción— de inteligencia.

Palabras clave: inteligencia, crimen, pandillas, terrorismo

doi: 10.18278/ijc.10.1.8

针对犯罪-团伙-恐怖主义关系的情报与分析方法

摘要

本文探讨了关于犯罪、团伙和恐怖主义的交叉问题的一系列情报挑战与应对方法。这些方法包括情报融合中心、恐怖主义预警和分析/综合方法。这些方法中可能包含的工具包括红队、交易分析、行动情报准备（IPO）、社会网络分析（SNA），以及自动化开源预警工具和数据集，用于支持一系列分析活动、信息共享、以及情报的生产或合作生产。

关键词：情报，犯罪，团伙，恐怖主义

Intelligence is essential to understanding, anticipating, and interdicting transnational organized crime, gang violence, and terrorism. These intersectional illicit activities demand crosscutting, multilateral intelligence to support prevention, enforcement, and ultimately prosecution of the spectra of complex interaction among a range of non-state actors—including criminal enterprises, mafias, gangs, and criminal armed groups (CAGs), and insurgents—and terrorists.[1] These activities have numerous interlocking motivations among a range of actors across multiple potential jurisdictions. These actions range from street crime, through extortion and street violence to further criminal enterprises, through political and insurgent objectives.[2]

The intersection between criminal and political objectives results in a range of operational challenges including high intensity crime, riots, street violence (at the level of civil strife) to criminal insurgency and terrorism (approaching the levels of non-international armed conflict).[3] Multiagency, multijurisdictional (and multilateral) intelligence to support a range of civil and military counter-gang, counter-insurgency, and counter-terrorism operations are essential. Similar missions involve humanitarian and disaster response, such as response to wildland fires, pandemics, and climate security issues—including climate disasters such as climate-related conflicts.[4] This paper discusses the range of intelligence challenges and approaches. These approaches include fusion centers, terrorism early warning, and analysis/synthesis approaches.[5] Tools potentially included within these approaches include red teaming, transaction analysis, intelligence preparation for operations (IPO), identity intelligence (i2), social network analysis (SNA), as well as automated open source early warning tools and datasets to support a range of analytical activities, information-sharing, and the production—or co-production—of intelligence.

Multi-agency, all source, all phase intelligence fusion challenges and approaches

Developing the intelligence needed to effectively address the range of threats and scope of intelligence, from criminal though humanitarian concerns, involves decision support for street crime (intelligence-led policing),[6] addressing gangs, transnational crime, and what is often called 'all hazards' including counterinsurgency, riots, pandemics, and climate change.[7]

Addressing this range of threats and their impact on communities requires calibrating foreign and domestic intelligence while building links to metropolitan and state (or provincial) and local public safety agencies in federal nation states. Essentially, this means linking national intelligence enterprises with a range of law enforcement and public safety agencies (multi-agency intelligence), including public health agencies and medical providers. This is often achieved through the establishment of fusion centers at state and local levels.[8] The national network of fusion centers has been controversial and has been criticized as being ineffective.[9] This criticism persists. In large measure, the perceived ineffectiveness of fusion centers can be linked to the lack of detailed doctrine (or network protocols) for operating, limited training, and ineffective oversight.[10] These issues deserve detailed assessment and analysis, though that depth of analysis is beyond the scope of this paper. The analytical tools that support effective analysis are the main thrust here.

Another framework, which preceded and influenced the fusion center approach, is the terrorism early warning (TEW) group model, initially developed in Los Angeles in 1996.[11] The TEW concept involved linking a network of regional/metropolitan fusion centers to co-operatively develop intelligence.[12] Under that framework, the fusion process involved more that information-sharing and focused on the production of intelligence. The distributed development of intelligence through participation in an intelligence/early warning network is called the 'co-production of intelligence.'[13] Related concepts include 'Strategic Early Warning for Criminal Intelligence (SEWS)' developed by Criminal Intelligence Service Canada.[14]

SEWS relies upon a three step indications and warning process for strategic early warning. Step I defines 'threat perception'; Step 2 involves 'evaluation and monitoring' (i.e., development of a Sentinel WatchList); and Step 3 involves 'assessment and warning' (i.e., Sentinel Assessment) for dissemination to the law enforcement community (See Figure 1).[15] The SEWS process relies upon assessment of likely future scenarios the development of scenarios which then assess a range of possible indicators to drive hypothesis testing.[16] Finally, assessments of likelihood (ranging from severe, high, medium, low, to nil) and a description of possible indicators are shared with practitioners (intelligence consumers).

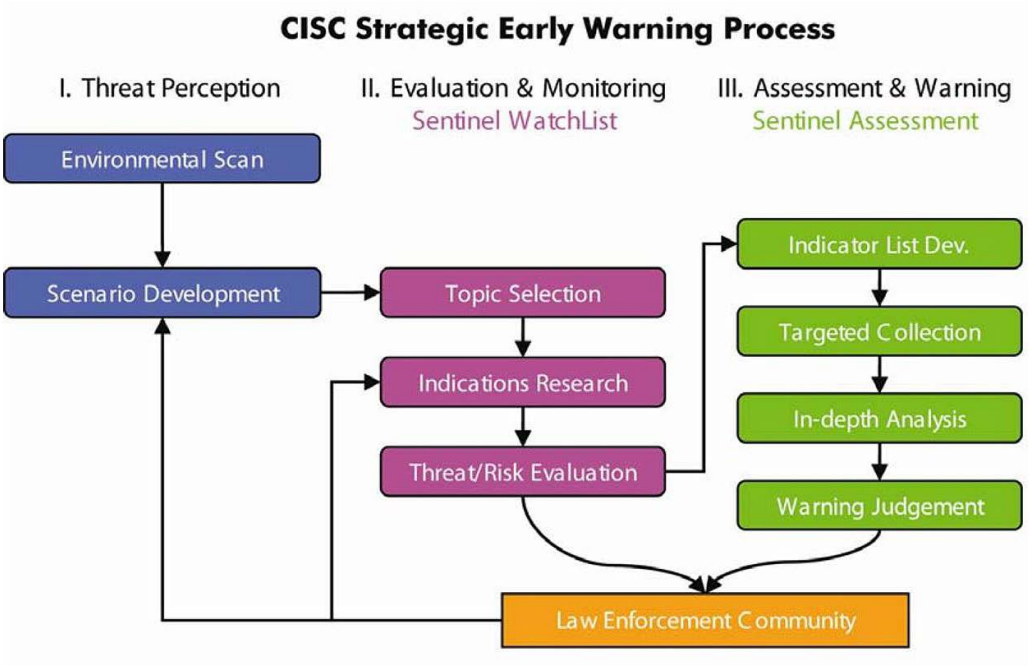

Figure 1: *Strategic Early Warning Process. Criminal Intelligence Service Canada*[17]

Similar frameworks are employed for conflict and crisis early warning for humanitarian situations, disasters, and conflict disasters. Early efforts in this regard include the Integrated Crisis Early Warning System (ICEWS).[18] Conflict early warning and disaster early warning systems are also being explored worldwide. Indeed, disaster early warning is an integral component of the Sendai Framework for Disaster Risk Reduction 2015-2030.[19]

All, of these early warning frameworks can be informed by the work of Col. John Boyd and his conceptualization of the decision cycle, commonly known as Boyd's Cycle or OODA Loop for Observe-Orient-Decide-Act the major components of his model (See Figures 2 and 3). In the TEW model, Boyd's work provides a foundation for assessment—that is the foundation for the analysis and synthesis function embedded in Boyd's Orientation phase became a central component of the TEW analytical tools described in this paper. First, analysis is breaking things down into their component parts; while synthesis involves combining numerous elements of a situation or related data to understand a situation (including forecasting future trends and potentials).

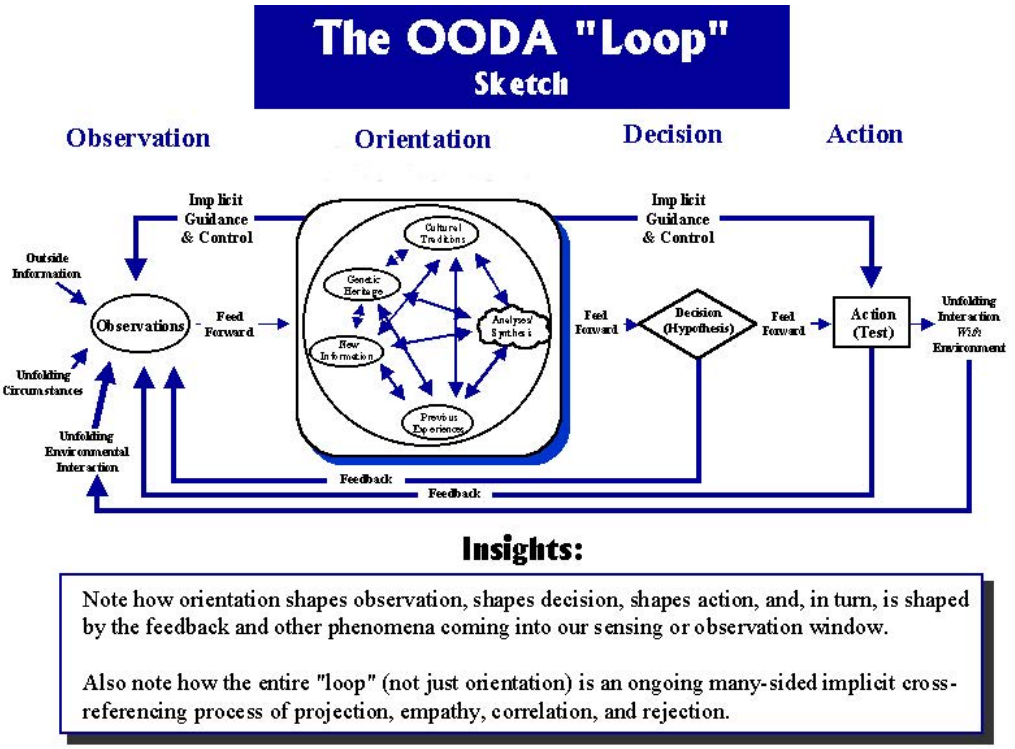

Figure 2: *The OODA Loop (Boyd's Cycle) as captured by Chuck Spinney.*[20]

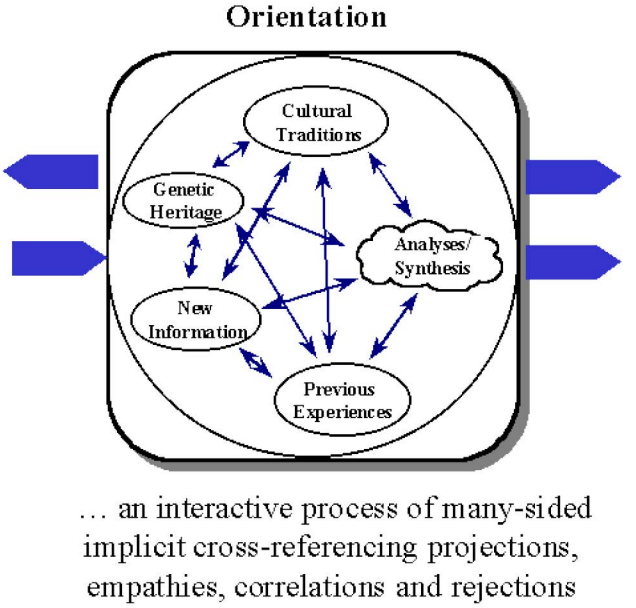

Figure 3: *Expanded view of Orientation Phase of OODA Loop.*[21]

The first major tool described here is the 'Transaction Analysis Cycle' developed by Sullivan. The Transaction Analysis Cycle (Figure 4) provides a means of sensing potential threat activity in a non-linear fashion to enable on-going assessment of unfolding situations.

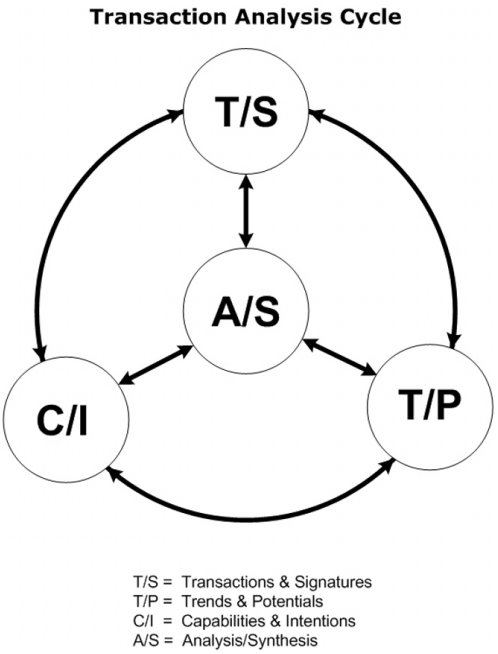

Figure 4: *Transaction Analysis Cycle.*[22]

Essentially:

> Individual transactions (such as acquiring finances, expertise, acquiring material, munitions or capability, recruiting members, conducting reconnaissance, mission rehearsal, conducting an attack, etc.) have signatures that identify them as terrorist or criminal acts, or consistent with the operations of a specific cell or group. These transactions and signatures (T/S) can then be observed and matched with patterns of activity that can be expressed as trends and potentials (T/P), which can ultimately be assessed in terms of a specific actor's capabilities and intentions (C/I). At any point, the analytical team can posit a hypothesis on the pattern of activity and then develop a collection plan to seek specific transaction and signatures that confirm or disprove its hypothesis. The transaction analysis cycle provides a common framework for assessing patterns, hypotheses, and social network links among a range of actors within a broad spatial and temporal context, making co-production of intelligence and situational understanding viable.[23]

This approach can assist in the development of 'geo-social' analysis such as mapping criminal networks through social network analysis or developing 'Identity Intelligence' (i2).[24] Network configuration, key hubs and actors (including relationships and roles, financial and logistical activities) are core elements of analysis in both transaction analysis and i2. Within the i2 framework, **AC²E** or "*Attribution* (who is it/who did it); Connections (nodes, position); *Context* (what does it mean in relationship to everything else?); *Exploitation* (what can we do with it?)" key questions.[25] Sources for gaining this information include traditional intelligence disciplines: human intelligence (HUMINT), communications intelligence (COMINT), measure and signals intelligence n(MASINT), geospatial intelligence (GEOINT), and criminal intelligence (CRIMINT or ILP). Both open-source intelligence (OSINT) and social media intelligence (SOCMINT), as well as epidemiological intelligence (Epi-Intel) need to be added to this armamentarium.

Intelligence Preparation for Operations (IPO) is another tool employed in the TEW model. IPO adapts the military Intelligence preparation of the battlefield/battlespace to the civil environment. It provides a common tool set for developing situational understanding and course of action development. Its four steps are:

- **Step 1: Define the OpSpace** (that is define the operating environment, including named areas of interest (NAIs) and critical infrastructure;

- **Step 2: Describe OpSpace Effects** (that is develop the geosocial picture and memorialize them in response information (or target) folders that describe population, terrain, weather, and place them in context. Cultural features, geospatial mapping and intelligence, cyber intelligence (CyberINT), and organizational dynamics are described;

- **Step 3: Evaluate OPFOR (PTEs) & Threats** (that is develop playbooks through adaptive red teaming to describe the potential opposing forces (OPFOR) or potential threat elements (PTEs), including gangs, mafias, criminal armed groups (CAGs), types of threat vectors (e.g., Chemical, biological, radiological, nuclear, explosives, drones, cyber, combined arms, etc. and influences). Tools here include deep indications and warning (deep I&W) and Epi-Intel (for biosecurity issues);

- **Step 4: Determine OPFOR & Friendly COAs** (that is develop actionable intelligence communicated through mission folders that measure alternative courses of action for both the OPFOR and Friendly forces. This includes integrating resource status (restat) and situation status (sitstat) conducting operational net assessments (ONA), threat assessments, and issuing advisories alerts and warnings.

These steps exploit a range of sensors (data inputs, including people and technical means, such as video (CCTV), automated license plate readers (ALPRs),

CNRN detectors, and overhead imagery (including commercial feed and drones). The goal is to scan, monitor, and forecast or in Boyd's framework: observe, orient, decide, and act. The operational tempo determines the focus varying from indications and warning (I&W) through operational net assessment (ONA). Both current and future operations are relevant, and the analysis should identify centers of gravity and decisive points for action. The framework must consider deception and counter-deception, swarming and counter-swarming, limit group think, and moderate decision analysis pitfalls and dynamic including 'mirror imaging.' Finally, it considers all facets of the event horizon, including threats and potentials, capabilities and intentions, and ONA. The IPO framework relies upon all source, all phase fusion. IPO is described graphically below (Figure 5).

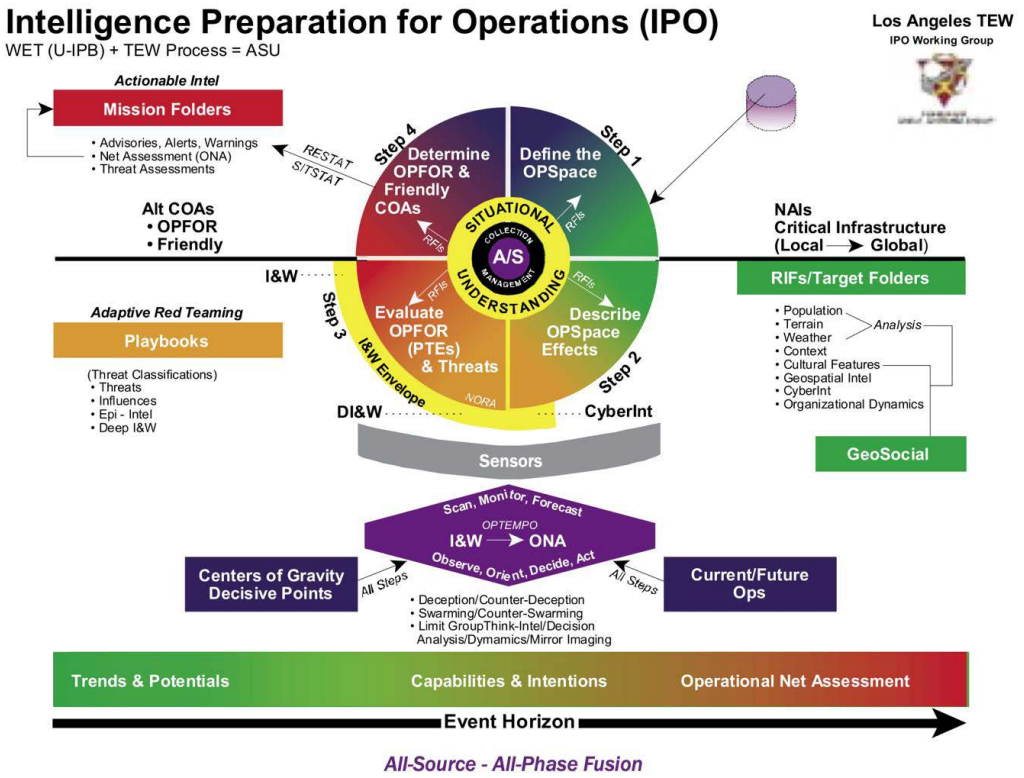

Figure 5: *Intelligence Preparation for Operations (IPO).*[26]

The IPO process was developed through a series of expert consultations and field tested through a series of analytical red teaming exercises and wargames.[27]

Academic and open source (OSINT/SOCMINT) approaches

Social network analysis (SNA) stems from many social science and mathematical disciplines utilizing notions of graph theory, statistics, sociology, computer

science, and the socially embedded nature of humans to understand groups networks, organizations, etc. It is more broad than social networks like Facebook, though social networks such as Facebook, Twitter, and private messaging applications, can be rich sources of data for the study of licit and illicit networks.[28] As Everton and other SNA scholars describe, SNA assumes that the behavior of actors is influenced by the structures of the social relations in which they are embedded.[29]

Shortly after the 911 attacks by al-Qaeda, Arquilla and Ronfledt identified new networked threats in a seminal edited volume and *First Monday* article on the Netwar concept which postulated that both bright (Legal) and dark (illicit/illegal) will take advantage of new networked forms of organizations in their competition with hierarchies.[30] If illicit actors are increasingly using technology and networked forms of organization, then a natural way to study and garner intelligence on them is through social network analysis.

SNA focuses on actors that are of the same type, such as people. In 2-mode networks (Networks connecting two types of things) it may focus on e.g., people (1) and meeting attendance (2) which in turn link the people through mutual attendance at meetings. These have been used in criminal network analysis through e.g., law enforcement surveillance on mafia meetings and attendance, etc.[31] Link analysis on the other hand links people to cell phones and other non-human units in networks such as a roadside bomb network which may include humans, cell phones, and explosives.[32] Phone records or court documents can also be good sources of open source intelligence on the structure of criminal or terror networks for social network analysis.[33] Scholars such as Krebs have also utilized open source media to build and analyze networks of terrorist organizations such as Al Qaeda and the Hamburg cell.[34] Scholars have long identified SNA as useful for intelligence purposes. Harvard scholar Malcolm K. Sparrow wrote on the use of SNA for law enforcement intelligence in 1991.[35] Other scholars have pointed to the expansion of SNA because of the ubiquity of personal computers giving more researchers and intelligence gatherers and analyzers access to the powerful capacities software provides. SNA has been heavily used in the law enforcement intelligence community, e.g., one of the authors' former students works in an antihuman trafficking taskforce with the Houston DA's office, a position she earned in part based on her SNA experience from graduate school.[36]

Interestingly, academics who have studied how intelligence analysts use SNA, found that while scholars were focused on leadership targeting in illicit networks, analysts were often using SNA to identify unidentified network participants. Analysts also complained of access to powerful software, but a lack of training on how to take advantage of it. The authors of the study which was limited to Australian law enforcement intelligence analysts urged more cooperation between law enforcement and scholars to alleviate these issues.[37]

Table 1. *A Sample of SNA Software packages*

A Sample of SNA Software Packages
UCINET (Low cost)[59]
ORA (Moderate cost)
Analyst Notebook (High cost)
Palantir Gotham (Very high cost)
R (Free though difficult to use for the uninitiated)
Python (High difficulty)
Gephi (Free)

Source: Authors' elaboration

While we can think of SNA as highly quantitative, anyone who has built a dataset immediately recognizes the role of coding qualitative data as a major part of the endeavor. Thus, scholars have pointed to the necessity of combining qualitative research with quantitative social network analysis to triangulate into research results that combine the best elements of both methodologies. This is a point that Kenney and Coulthart have made when they advocate for the use of ethnography in conjunction with quantitative SNA to eliminate false positives.[38] This academic research leads to an important discussion vis-à-vis SNA, namely the ethical implications of which false positive identification (as a criminal or terrorist) is one of many.

Gathering datasets: What is possible? What is legal? What is ethical?

The ability to gather information on individuals and groups from disparate open-source data sources and then analyze and combine it with other datasets using SNA and similar algorithms sometimes called 'big data' is a powerful intelligence tool. It can also be harmful to the civil liberties of the individual. It allows governments and non-state actors to violate the rights of privacy, that may not have been explicitly written into constitutional systems, but were certainly assumed based upon rights included, such as those protecting the citizenry from undue search and seizure. It does not take much imagination to realize the kind of dystopia this technology and analysis can lead to assuming the normal pace of technological development.

One SNA platform that has received criticism for how it has been utilized in the public and private sector is Palantir.[39] It should be noted that a tool, is just that, a tool. In the hands of the ethical and well-regulated it can be used properly, but in the hands of the unchecked and unregulated, it can be used in Orwellian fashion. As reporting from Bloomberg demonstrated, this was the case in government

agencies in Los Angeles and in the security departments of major companies such as JPMorgan Chase & Co. As Bloomberg describes:

> The company's engineers and products don't do any spying themselves; they're more like a spy's brain, collecting and analyzing information that's fed in from the hands, eyes, nose, and ears. The software combs through disparate data sources—financial documents, airline reservations, cellphone records, social media postings—and searches for connections that human analysts might miss. It then presents the linkages in colorful, easy-to-interpret graphics that look like spider webs.[40]

The colorful easy to understand 'spiderwebs' are the visualizations of link analysis a close SNA cousin and largely based upon SNA algorithms. A primary critique was the ease of creating false positives through linkages to criminal or terror actors.

Finally, SNA can also be ethically combined with geospatial analysis. A simple example provided by Lowenthal is the overlaying of social media SNA data over a map to determine where a given topic is being discussed most. Lowenthal provides the examples of the National Geospatial Intelligence Agency (NGA) using social media to map refugee flows out of Syria.[41]

Open source GEOINT: ACLED

Geospatial intelligence or GEOINT is a key collections area that focuses on that which is connected to the earth. It is often associated with imagery be it gathered via satellite, French hot air balloon, planes, or unmanned aerial vehicle (UAV). GEOINT is not always imagery however, it can also be intelligence represented on maps and visualized. The National Geospatial intelligence Agency (NGA) is one of the key agencies utilizing GEOINT and encouraging open-source intelligence tools in this area via its NGA Pathfinder program.[42]

One example of an open-source intelligence and scholarly tool is The Armed Conflict Location Event Data Project (ACLED). ACLED data on political violence events including their location down to the nearest municipality throughout much of the world.[43] This allows open source researchers to visualize and map ACLED data free via Tableau Public.[44] The ACLED data set is a U.S. nonprofit funded by the "Bureau of Conflict and Stabilization Operations at the United States Department of State, the Dutch Ministry of Foreign Affairs, the German Federal Foreign Office, the Tableau Foundation, the International Organization for Migration, and the University of Texas at Austin."[45]

ACLED stemmed from the dissertation research of founder Clionadh Raleigh working on geospatial datasets for conflict in Africa in 2005. It expanded

to other regions with funding from other sources including governments. More recently the dataset has expanded into Latin America and the Caribbean.[46] One strength of the data set is that it defines its coding rules locally to capture data that might otherwise be ignored. For example, there can be debates about what constitutes political violence vs. criminal violence. This is particularly important in areas like Latin America where scholars have pointed to issues of 'criminal insurgency'[47] and 'third generation gangs'[48] wherein criminal groups take on political aims in furtherance of criminal goals and subtly change the nature of the state and society itself in a move toward state transformation.

Another key advantage is that it collects local level data and does not limit itself to violence between the state and rebel groups as some data sets do. This allows for a richer data set with more varied actor types which is key in the Mexican context where self-defense forces may interact with various paramilitary criminal organizations, government forces at the local state and federal level, etc.[49] In the following two figures, situations of combat involving the Cártel de Jalisco Nueva Generación (CJNG) and Cártel de Sinaloa (CDS) with Mexican security forces are used to demonstrate the visualization potentials afforded by the ACLED platform.

Figure 6 below is a demonstration of the ACLED data and ability to visualize in Tableau Public. The figure displays the incidence of CJNG/CDS combat with Mexican state forces and shows widespread CJNG combat throughout the country.

Figure 6: *CJNG/CDS Combat with Mexican Military/National Guard/Law Enforcement.*[50]

Figure 7 below, again uses CJNG/CDS incidence of combat with Mexican state forces to demonstrate how, in Tableau Public, researchers can hover their cursor over specific data events and view summaries of the political violence events. All of these are free to visualize if shared in Tableau Public. Researchers must take care not to share the underlying data and properly cite ACLED under their terms of attribution.

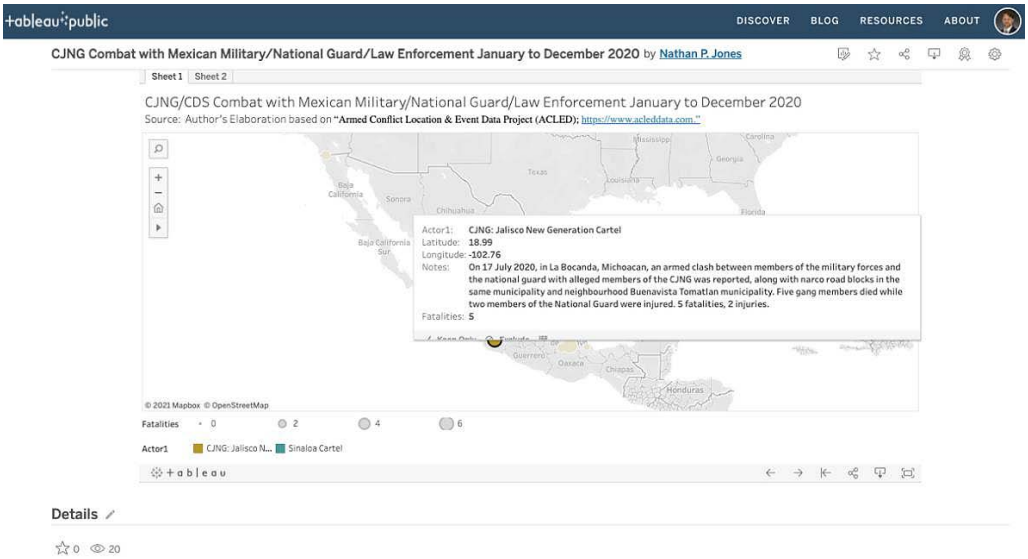

Figure 7: *CJNG/CDS Combat with Mexican Military/National Guard/Law Enforcement highlighting note visualization capability in ACLED Data and Tableau Public.*[51]

Another strength of the ACLED data source is its open access nature. While it has moved to a pay model beyond a certain number of downloads or depending commercial use, it is freely accessible to the general public for research purposes. This increases its utility and the ability to evaluate it.

While an exhaustive discussion of the advantages of the ACLED dataset is beyond the scope of this paper given size constraints, particularly relevant tools within ACLED are the curated datasets and hubs by region. "The Early Warning Research Hub" is another ACLED tool relevant to our discussion of intelligence and illicit networks. This hub contains useful tools for predicting violent hotspots including a volatility and risk tool which shows where political violence is deviating above baseline norms, a "subnational hotspot mapper," a "global threat tracker," and a "conflict pulse" tool which forecasts behavior "a week into the future."[52]

The ACLED subnational hotspot tracker compares state or province violence in the most recent week to the most recent preceding month. It then ranks those regions by the greatest increases in political violence. The ACLED volatility and risk index can then be used on those areas to give a sense of the frequency of violence and whether the surge is out of the ordinary for the area using a baseline average of weekly events for the previous three years. It then measures the difference based on the number of standard deviations above normal to provide a risk level. The Global Threat Tracker jumps to the national level and assesses "countries at risk of violent escalation." It should be noted that the conflict pulse tracker appears—as of November 2021—to only cover ISIS affiliated and Islamist groups in Africa, the Middle East, and South Asia.

The following three figures use data from the contemporary insurgency in Mozambique to demonstrate the conflict analysis potentials of the ACLED platform.

The map in Figure 8 shows a high concentration of violence in the Cabo Delgado province of Northeastern Mozambique using ACLED data. The violence is concentrated along the coastline and is largely attributed to an Islamist insurgency.

In an example of open-source intelligence and investigative reporting, *The New York Times* was able to paint a picture of the insurgent attacks on Palma through satellite imagery, interviews, mapping, and video analysis. It was an attack in which the government failed to respond and left the local population to face the insurgency on its own. Hundreds of thousands have been displaced in the region according to the *Times* and our 2021 analysis of 'strategic developments,' a category of the ACLED data that also includes looting and other non-regular events, shows that there were numerous instances of looting/property destruction resulting in, or likely to result in displaced persons in the region in 2021. See Figure 9 below which also includes a portion of the Tableau Public interface.

In March 2021, ISIS-linked insurgents in Mozambique launched an attack on Palma in the energy rich Cabo Delgado region. There is a large foreign direct investment project in a Liquid Natural Gas (LNG) facility in Palma led by the French company Total. Military forces provided security for LNG site, but not Palma despite claims to the contrary. [53] The insurgent group, Al-Sunna wa Jama'a, founded in 2017, is mostly local and claims ISIS allegiance via the Islamic State Central Africa Province since 2019. However, analysts such as Joseph Hanlon of the London School of Economics argue this is a local insurgency and has loose ties to ISIS.[54]

Figure 10 quantifies the data on the location and concentration of violence in Mozambique as largely limited to the Cabo Delgado region which is energy rich and home to a large foreign investment in an LNG facility. Figures 6-10 are a limited sample of the ways that ACLED data can be visualized to rapidly produce GEOINT on criminal and insurgent networks.

Crime-Terror Nexus

We can view the Mozambique insurgency as targeting this region to deny the government resources, or in the hopes of the insurgency capturing these resources and profits, or for other local reasons. In terms of the crime-terror nexus the notion of the insurgency targeting the region for natural gas profits is most interesting for our discussion. Property destruction such as the burning of buildings, a criminal act in and of itself, can also have the effect of clearing people from a territory. Looting can have the effect of funding the insurgency via criminal conduct and taking

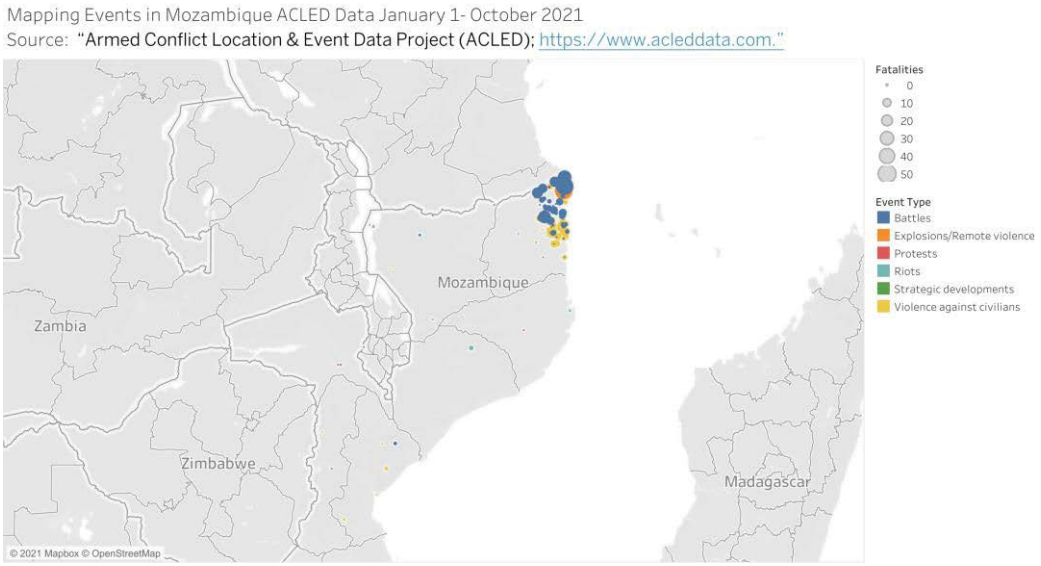

Figure 8: *Mapping Events in Mozambique ACLED Data January 1-October 2021.*

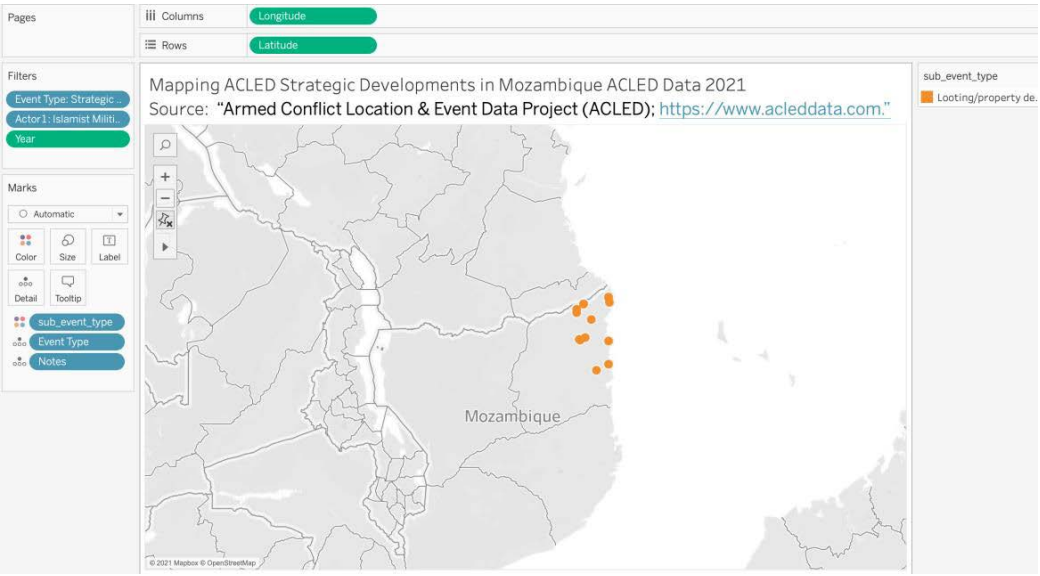

Figure 9: *Mapping ACLED Strategic Developments in Mozambique ACLED Data in Tableau Public 1 January-October 2021.*

control of LNG facilities in the hope of selling on the international market can also fund an insurgency as had has been done by groups such as ISIS.[55] Criminal armed groups such as the CJNG which are profit-motivated criminal groups will also engage in insurgent/terror tactics and paramilitary activities in their combat with government forces and rivals. These groups also attempt to win the support of the population by engaging in 'social banditry' as we have recently argued, wherein they attempt to purchase the support of the population.[56]

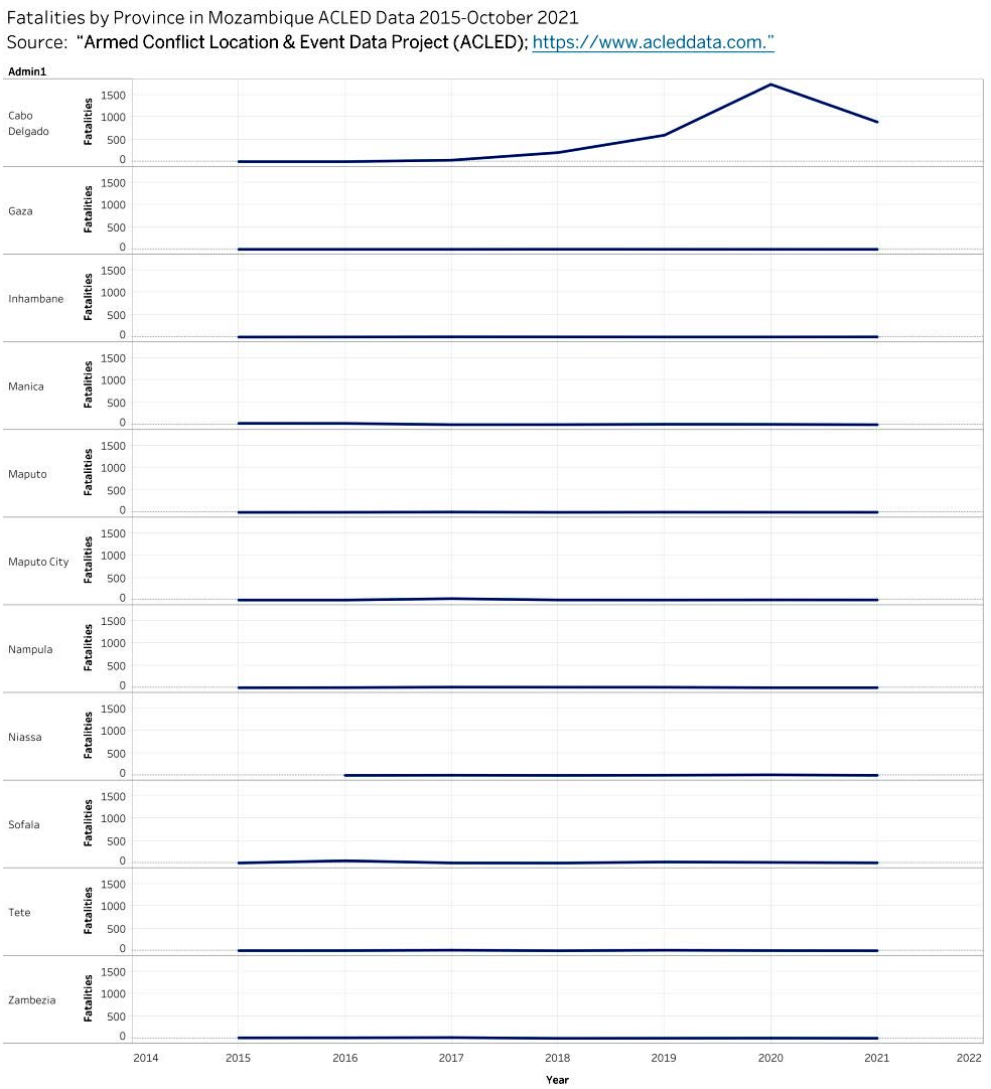

Figure 10: *Fatalities by Province in Mozambique ACLED Data January 1-October 2021.*

ACLED and U.S. Crisis Monitor

ACLED also provides specialized analysis projects such as the U.S. Crisis Monitor for 2020 built with Princeton University's Bridging Divides Initiative and the Princeton School of Public and International Affairs' Liechtenstein Institute on Self-Determination. This dataset brings ACLED coverage to the United States and focuses on the period immediately before and after the George Floyd murder and the subsequent wave of demonstrations. Figure 11 below is a visualization of U.S. Crisis Monitor Data for 2020 reproduced from an ACLED Press release that visualizes Right-wing militias, Black Lives Matter (BLM) protests, and Covid-19 demonstrations.

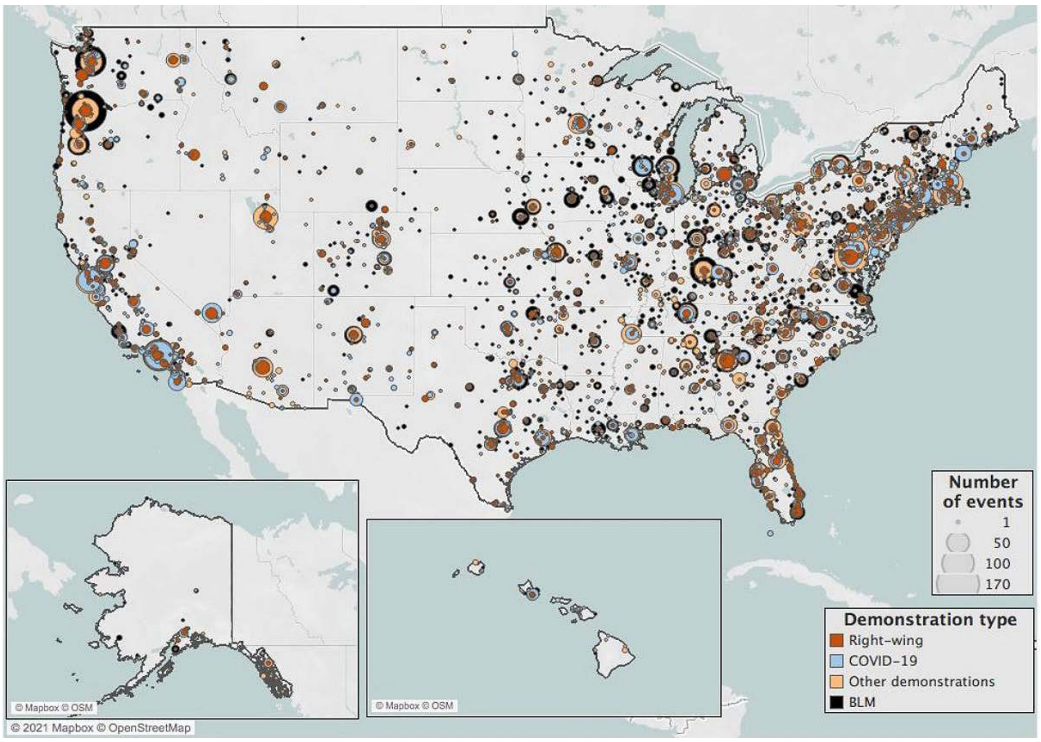

Figure 11: *"Demonstrations by Type" Reproduced From ACLED.*[57]

Figure 11 demonstrates the widespread character of demonstrations in the United States in 2020 and the geographic concentration of those events. Figure 12 below visualizes ACLED US Crisis Monitor Data to map event type and size events by the number of fatalities associated with them.

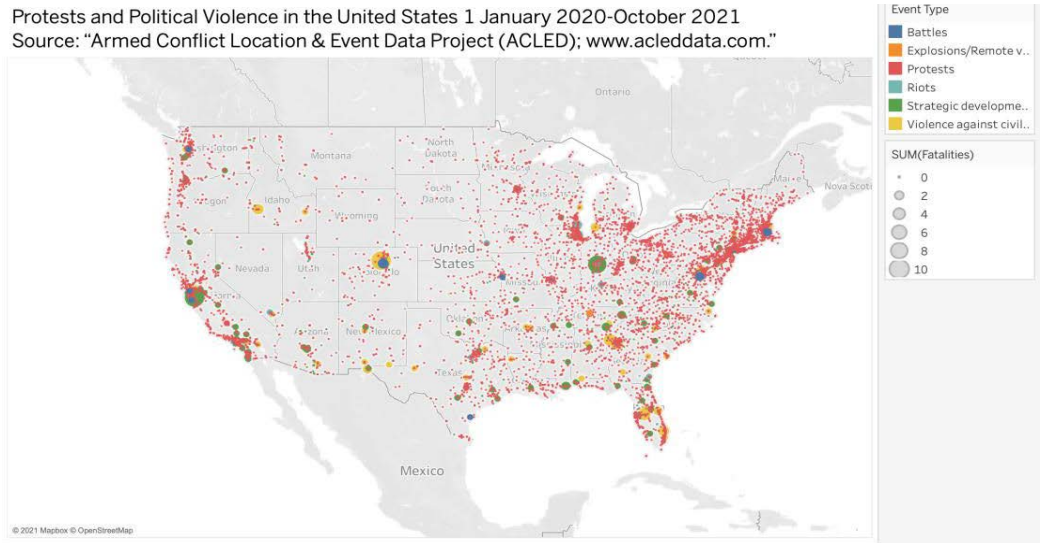

Figure 12: *Protests and Political Violence in the United States 1 January 2020-October 2021*[58]

Figure 12 allows us to see that most demonstrations involved no fatalities and many of the events that led to significant casualties were either in the 'strategic developments' or the 'violence against civilians' categories. These fatality incidents were often mass-shooting events unlinked to demonstrations. The above figures demonstrate the GEOINT potentials of the ACLED data set and other tools like it.

Conclusion

Meeting contemporary intelligence needs requires a suite of analytical tools and organizational structures to support a range of analytical activities, information-sharing and the production of intelligence. Here we emphasize the need for networked co-production of intelligence to address the comprehensive range of threats facing contemporary society and the public agencies (as well as public-private partnerships) protecting them and ensuring the delivery of critical infrastructure lifelines and services. In this paper, we reviewed intelligence fusion, terrorism early warning, strategic early warning for strategic crime, transaction analysis, identity intelligence and intelligence preparation for operations (IPO). We also examined academic and open source (OSINT/SOCMINT) approaches and tools that complement the 'all-source fusion' approaches. Together, this discussion provides a foundation for assessing new intelligence analysis approaches and potentially new organizational and technological frameworks for protecting the populace and a meeting the range of human, technological, and natural threats and hazards facing our increasingly complex globally-connected society.

Endnotes

1 See, for example, Tamara Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism." *Global Crime*. Vol. 6, No. 1, 2004: pp. 129–145, https://doi.org/10.1080/1744057042000297025; John P. Sullivan, "Criminal–Terrorist Convergence: Intelligence Co-production for Transnational Threats." *International Journal on Criminology*. Vol. 3, no. 2. Fall 2015, https://www.criminologyjournal.org/uploads/1/3/6/5/136597491/criminal–terrorist_convergence.pdf; Alex P. Schmid, "Revisiting the Relationship between International Terrorism and Transnational Organised Crime 22 Years Later," *ICCT Research Paper*. The Hague: International Centre for Counter-Terrorism. August 2018, https://icct.nl/app/uploads/2018/09/ICCT-Schmid-International-Terrorism-Organised-Crime-August2018.pdf; and Mark Shaw and Prem Mahadevan, "When Terrorism and Organized Crime Meet." *Global Initiative Against Transnational Crime (GITOC)*. 17 October 2018, https://globalinitiative.net/analysis/when-terrorism-and-organized-crime-meet/.

2 See John P. Sullivan, "Terrorism, Crime and Private Armies." *Low Intensity Conflict & Law Enforcement*. Vol. 11, Nos. 2-3, 2002: pp. 239–253, https://doi.org/10.1080/

0966284042000279018; and John P. Sullivan and Robert J. Bunker, "Drug Cartels, Street Gangs, and Warlords. *Small Wars & Insurgencies*. Vol. 13, no. 2, 2002: pp. 40-53, https://doi.org/10.1080/09592310208559180.

3 On riots, see John P. Sullivan and Adam Elkus, "The Strategic Challenge of Riots: Riot Action and Crowd Power." *Small Wars Journal*. 13 February 2012. Available at https://www.academia.edu/1384839/The_Strategic_Challenge_of_Riots_Riot_Action_and_Crowd_Power/. On criminal insurgencies, see John P. Sullivan, "States of Change: Power and Counterpower Expressions in Latin America's Criminal Insurgencies." *International Journal on Criminology*. Vol. 2, no. 1. Spring 2014, https://www.criminologyjournal.org/uploads/1/3/6/5/136597491/states_of_change.pdf.

4 On wildland fires, see John P. Sullivan, "How Intelligence Can Map Wildfire Risk and Help Reduce Catastrophes." *Homeland Security Today*. 26 July 2019. Available at https://www.academia.edu/39941571/How_Intelligence_Can_Map_Wildfire_Risk_and_Help_Reduce_CatastrophesOn pandemics, see John P. Sullivan and Robert J. Bunker, Eds., *Covid-19, Gangs and Conflict*. (A Small Wars Journal–El Centro Reader.) Bloomington: Xlibris, 2020. Available at https://www.amazon.com/Covid-19-Gangs-Conflict-Journal-El-Centro/dp/1664124349. On climate-related conflicts, see Nathan P. Jones and John P. Sullivan, "Climate Change and Global Security." *Journal of Strategic Security*. Vol. 13, no. 2, 2020: pp. i–iv, https://doi.org/10.5038/1944-0472.13.4.1899.

5 On terrorism early warning see John P. Sullivan and Alain Bauer, Eds. *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*. Los Angeles: Los Angeles County Sheriff's Department. October 2008. Available at https://www.academia.edu/1115115/Terrorism_Early_Warning_10_Years_of_Achievement_in_Fighting_Terrorism_and_Crime; and John P. Sullivan, "The Terrorism Early Warning (TEW) Model for Sensing Novel and Emerging Threat." *Journal of Intelligence & Analysis*. Vol. 22, no. 2, April 2015. Available at https://www.academia.edu/39359421/The_Terrorism_Early_Warning_TEW_Model_for_Sensing_Novel_and_Emerging_Threats.

6 On Intelligence-Led Policing or ILP, see Jerry H. Ratcliffe. *Intelligence-Led Policing*. Cullompton, Devon, UK and Portland, OR: Willan Publishing, 2008. Available at https://www.amazon.com/Intelligence-Led-Policing-Jerry-H-Ratcliffe-dp-1843923394/dp/1843923394/ref=mt_other?_encoding=UTF8&me=&qid=and Jerry H. Ratcliffe, "Intelligence-led Policing." *Trends & Issues in Crime and Criminal Justice*. No. 248. Canberra: Australian Institute of Criminology. April 2003, https://www.aic.gov.au/publications/tandi/tandi248. ILP involves an intelligence assessment of the criminal environment to influence decision-making in order to impact the criminal environment.

7 See John P. Sullivan, "The New Great Game: Military, Police and Strategic Intelligence for Global Security." *Journal of Policing, Intelligence and Counterterrorism*. Vol. 2, no. 2, 2007: pp. 15–29, https://doi.org/10.1080/18335300.2007.9686895.

8 In the United States, fusion centers serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related in-

formation among federal, state, local, tribal, and territorial (SLTT) partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, … emergency response, public health, critical infrastructure protection … and private sector security personnel to lawfully gather and share threat-related information." See "National Network of Fusion Centers Fact Sheet," *U.S. Department of Homeland Security*. 30 September 2021, https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

9 Recent criticism is reported at Cyrus Farivar, "20 years after 9/11, 'fusion centers' have done little to combat terrorism." *NBC News*. 10 September 2021, https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949. For examples of earlier criticism see, for example, Jason Barnosky, "Fusion Centers: What's working and what isn't." *Brookings*. 17 March 2015, https://www.brookings.edu/blog/fixgov/2015/03/17/fusion-centers-whats-working-and-what-isnt/; and Rober O'Harrow Jr., "DHS 'fusion centers' portrayed as pools of ineptitude and civil liberties intrusions." *The Washington Post*. 2 October 2012, https://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html.

10 See for example, Shane A. Salvatore, "Fusion center challenges: why fusion centers have failed to meet intelligence sharing expectations." Master's Thesis. Monterey: Naval Postgraduate School. March 2018, http://hdl.handle.net/10945/58358.

11 See the TEW case study by Sullivan and Bauer, Eds. At Note 5. In addition, see Sunchar M. Rust, "Collaborative network evolution the Los Angeles terrorism early warning group," Master's Thesis, Monterey: Naval Postgraduate School, March 2006, https://calhoun.nps.edu/handle/10945/2964.

12 John P. Sullivan and James J. Wirtz, "Global Metropolitan Policing: An Emerging Trend in Intelligence Sharing." *Homeland Security Affairs*. Vol. V, no. 2, May 2002, http://hdl.handle.net/10945/25069.

13 Initially articulated in John P. Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence" in Panel 5: In Pursuit of the Analytical Holy Grail: Part 1, Innovation in Analysis, Warning and Prediction, Canadian Association for Security and Intelligence Studies. *CASIS 20th Anniversary International Conference*. Montreal, Quebec, Canada. 21 October 2005. Available at https://www.academia.edu/927364/Terrorism_early_warning_and_coproduction_of_counterterrorism_intelligence.

14 *Strategic Early Warning for Criminal Intelligence: Theoretical Framework and Sentinel Methodology*. Ottawa: Criminal Intelligence Service Canada. 2007, https://publications.gc.ca/collections/collection_2013/sp-ps/PS64-107-2007-eng.pdf.

15 Ibid., p. 9.

16 Ibid., p. 15.

17 Ibid., p. 9.

18 See Sean P. O'Brien, "Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research." *International Studies Review*. Vol. 12, no. 1, 2010: pp. 87–104, http://www.jstor.org/stable/40730711. ICEWS was funded by DARPA and currently archival datasets are at the Harvard Dataverse, "Integrated Crisis Early Warning System (ICEWS) Dataverse," https://dataverse.harvard.edu/dataverse/icews?q=&types=datasets&sort=dateSort&order=desc&page=1.

19 See, for example, Amadine Gnanguenon, "Pivoting to African Conflict Prevention: An analysis of continental and regional early warning systems." *Conflict Series*. Brief 3, European Union Institute for Security Studies. February 2021, https://www.jstor.org/stable/pdf/resrep28790.pdf. On disaster risk reduction, see "Early Warning Systems." *UN-Spider Knowledge Portal*. Vienna: United Nations Office for Outer Space Affairs, https://www.un-spider.org/risks-and-disasters/early-warning-systems#no-back; "The International Network for Multi-Hazard Early Warning Systems (IN-MHEWS)." *IN-MHEWS*. Geneva: World Meteorological Organization, https://mhews.wmo.int/en/partners; on the Sendai Framework, see *Sendai Framework for Disaster Risk Reduction 2015-2030*. Geneva: United Nations Office for Disaster Risk Reduction, 2015, https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030. UNODRR

20 Numerous versions of Boyd's model are available. For background see "The OODA 'Loop' Sketch" from Chet Richards, "Boyd's OODA Loop" from John Boyd, "The Essence of Winning and Losing." 28 July 1995, https://web.archive.org/web/20110324054054/http://www.danford.net/boyd/essence.htm. Richards's Power Point presentation is preserved at Slide 4, https://web.archive.org/web/20110723080751/http://www.danford.net/boyd/essence4.htm.

21 Ibid, Orientation phase expanded at https://web.archive.org/web/20110723080623/http://www.danford.net/boyd/essencex.htm.

22 Jon P. Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism intelligence," Op, cit. at Note 13.

23 John P. Sullivan, "The Frontiers of Global Security Intelligence: Analytical Tradecraft and Education as Drivers for Intelligence Reform." *Small Wars Journal*. 22 August 2008, https://smallwarsjournal.com/jrnl/art/the-frontiers-of-global-security-intelligence.

24 See John P. Sullivan, "Criminal–Terrorist Convergence: Intelligence Co-production for Transnational Threats." Op. cit. at Note 1, especially pp. 118-120.

25 Ibid, p. 121.

26 The Intelligence Preparation for Operations (IPO) Process is described in detail in the TEW case study, John P. Sullivan and Alain Bauer, Eds. *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*. Op, cit. at Note 5.

27 See John P. Sullivan, "Analytical Red Team Exercises for Irregular Conflict." *Red Team Journal*. 13 September 2013. Available at https://www.academia.edu/9145455/Analytical_Red_Team_Exercises_for_Irregular_Conflict and James D. Madia, "Homeland Security Organizations: Design Contingencies in Complex Environments," Master's Thesis, Monterey: Naval Postgraduate School, September 2011, https://www.hsdl.org/?view&did=691503.

28 Guadalupe Correa-Cabrera, Rajendra G. Kulkarni, Patrick R. Baxter, and Naoru Koizumi, "Messengers of a Drug War in the Cyberspace: The Case of Tamaulipas. Small Wars Journal," *Small Wars Journal*. 7 September 2021, https://smallwarsjournal.com/jrnl/art/messengers-drug-war-cyberspace-case-tamaulipas.

29 Sean F. Everton, *Disrupting Dark Networks*, New York: Cambridge University Press, 2012; Daniel Cunningham, Sean Everton, and Philip Murphy, *Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis*. Lantham, MD: Rowman & Littlefield, 2016; Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press, 1994; Gisela Bichler, Ali Malm, and Tristen Cooper, "Drug Supply Networks: A Systematic Review of the Organizational Structure of Illicit Drug Trade." *Crime Science*. Vol. 6, no. 1. 2017: p. 2, https://doi.org/10.1186/s40163-017-0063-3; Mark Granovetter. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory*. Vol. 78, no. 6. 1973: pp. 1360–80, http://www.jstor.org/stable/pdfplus/2776392.pdf?acceptTC=true.

30 John Arquilla and David F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation, 2001; David Ronfeldt and John Arquilla, "Networks, Netwars and the Fight for the Future," *First Monday*, 1 October 2001, https://doi.org/10.5210/fm.v6i10.889.

31 Francesco Calderoni, "Identifying Mafia Bosses from Meeting Attendance," in *Networks and Network Analysis for Defence and Security*. Springer, 2014), pp. 27–48.

32 Op. cit. Everton, *Disrupting Dark Networks*, pp. 5–7.

33 Valdis E. Krebs, "Mapping Networks of Terrorist Cells," *Connections*. Vol. 24, no. 3. 2002: pp. 43–52; http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf; Mangai Natarajan, "Understanding the Structure of a Drug Trafficking Organization: A Conversational Analysis." *Crime Prevention Studies*. Vol. 11, 2000: pp.273–98,https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.520.3739&rep=rep1&type=pdf; Nathan P. Jones, W. Layne Dittman, Jun Wu, and Tyler Reese, "A Mixed Methods Social Network Analysis of a Cross-Border Drug Network: The Fernando Sanchez Organization (FSO)," *Trends in Organized Crime*. Vol. 23, no. 2, 1 June 2020: pp. 154–82, https://doi.org/10.1007/s12117-018-9352-9.

34 Ibid. Krebs, "Mapping Networks of Terrorist Cells" and Valdis E. Krebs, "Uncloaking Terrorist Networks." *First Monday*. Vol 7, no. 4. April 2002, http://journals.uic.edu/ojs/index.php/fm/article/view/941/863.

35 Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence:

An Assessment of the Prospects." *Social Networks*. Vol. 13, no. 3, 1991: pp. 251–74, https://www.sciencedirect.com/science/article/abs/pii/037887339190008H.

36 Sam Houston State University, "CJ Alumna Combats Human Trafficking At The Local Level." *Sam Houston State University*. 23 April 2018, https://www.shsu.edu/today@sam/T@S/article/2018/alumna-s-capstone-project-paves-way-to-opportunity.

37 Morgan Burcher and Chad Whelan, "Social Network Analysis as a Tool for Criminal Intelligence: Understanding Its Potential from the Perspectives of Intelligence Analysts." *Trends in Organized Crime* 21, no. 3. 2018: pp. 278–94, https://doi.org/10.1007/s12117-017-9313-8.

38 Michael Kenney and Stephen Coulthart, "The Methodological Challenges of Extracting Dark Networks: Minimizing False Positives through Ethnography," in Luke Gerdes, Ed., *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations*. New York: Cambridge University Press, 2015, https://doi.org/10.1017/CBO9781316212639.

39 Peter Waldman et al., "Palantir Knows Everything About You." *Bloomberg*. 19 April 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

40 Ibid.

41 Op. cit. Lowenthal, *Intelligence: From Secrets to Policy*, p. 107 at Note 42.

42 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. Thousand Oaks: Sage/CQ Press, 2019, pp. 104–8.

43 Clionadh Raleigh, Andrew Linke, Håvard Hegre, and Joakim Karlsen, "Introducing ACLED: An Armed Conflict Location and Event Dataset: Special Data Feature," *Journal of Peace Research*. Vol. 47, no. 5. 2010: pp. 651–60, https://doi.org/10.1177/0022343310378914.

44 *Introduction to ACLED Analysis with Tableau*, accessed 19 May 2020, https://www.youtube.com/watch?v=sZrX37HGFks.

45 "About ACLED," *ACLED*. 13 June 2019, https://acleddata.com/about-acled/.

46 Full disclosure: the authors of this study were contacted early in the expansion to Latin America for their expertise on coding violence data.

47 John P. Sullivan, "From Drug Wars to Criminal Insurgency: Mexican Cartels, Criminal Enclaves and Criminal Insurgency in Mexico and Central America Implications for Global Security." *Working Paper N°9*. Paris: Fondation Maison des Sciences de l'homme. April 2012, https://halshs.archives-ouvertes.fr/halshs-00694083/document; John P. Sullivan and Robert Muggah, "The Coming Crime Wars." *Foreign Policy*, 21 September 2018, https://foreignpolicy.com/2018/09/21/the-coming-crime-wars/; John P. Sullivan, "Maras Morphing: Revisiting Third Generation Gangs." *Global Crime*. Vol. 7, nos. 3–4. 2006: pp. 487–504, https://doi.org/10.1080/17440570601101623; Nathan P. Jones, "Conclusion: The Past, Present and Potential Future of Third Genera-

tion Gang Studies," in John P. Sullivan and Robert J. Bunker, Eds., *Strategic Notes on Third Generation Gangs* (A Small Wars Journal–El Centro Anthology). Bloomington: Xlibris, 2020.

48 Ibid. Sullivan, "Maras Morphing: Revisiting Third Generation Gangs."

49 Op. Cit. Raleigh et al., "Introducing ACLED: An Armed Conflict Location and Event Dataset: Special Data Feature" at Note 41.

50 Authors' elaboration using ACLED Data and Tableau Public.

51 Ibid.

52 "Early Warning Research Hub," *ACLED*. 17 May 2021, https://acleddata.com/early-warning-research-hub/.

53 Haley Willis, Christiaan Triebert, Stella Cooper, Danielle Miller, Aaron Byrd and Christina Goldbaum, "Video: Militants Attacked a Key Town in Mozambique. Where Was the Government?" *The New York Times*. 26 May 2021, https://www.nytimes.com/video/world/africa/100000007760967/mozambique-attack.html.

54 Christina Goldbaum, "ISIS Claims Responsibility for Mozambique Attack," *The New York Times*. 30 March 2021, https://www.nytimes.com/2021/03/30/world/africa/isis-mozambique-attack.html.

55 Louise I. Shelley, "Illicit Trade and Terrorism," *Perspectives on Terrorism*. Vol. 14, no. 4, 2020: pp.7–20, available at https://www.jstor.org/stable/26927661.

56 On the original articulation of social banditry see Eric J. Hobsbawm, *Bandits*. New York: The New Press, 2000; Eric J Hobsbawm, *Primitive Rebels: Studies in Archaic Forms of Social Movement in the 19th and 20th Centuries*. New York: Norton, 1965. On modern applications of the concept in the context of Latin America and criminal insurgency see: John P. Sullivan and Nathan P. Jones, "Bandits, Urban Guerrillas, and Criminal Insurgents: Crime and Resistance in Latin America," Chapter 6 in Pablo Baisotti, Ed. *The Routledge Handbook of Latin America and the Caribbean (Twentieth and Twenty-First Century)*, Pablo Baisotti, Ed. New York: Routledge, 2021, pp. 168–195.

57 Figure 11 reproduced from *"US Crisis Monitor Releases Full Data for 2020." Armed Conflict Location & Event Data Project (ACLED). 5 February 2021.* https://acleddata.com/acleddatanew/wp-content/uploads/2021/02/ACLED_BDI_USCM2020Release_2021.pdf.

58 Authors' elaboration using ACLED Data and Tableau Public.

59 Stephen P Borgatti, Martin G Everett, and Linton C Freeman, "Ucinet for Windows: Software for Social Network Analysis," Harvard, MA: Analytic Technologies, 2002.