MITRE

Intelligence After Next

SERIES # 27

OPEN SOURCE INTELLIGENCE FOR COUNTERTERRORISM

by Dan Kolva and Whitney D.

 # 24-2842 11-11-2024

The U.S. Intelligence Community Can Better Use OSINT for Counterterrorism

An Open source Intelligence (OSINT) approach to counterterrorism (CT), particularly foreign terrorist organizations (FTOs), has not been widely adopted by counterterrorism analysts in the U.S. Intelligence Community (IC). Such an approach would be a transformative shift from the current status quo. Analysts have done this work for decades using predominately IC-only closed systems in Sensitive Compartmented Information Facilities. However, embracing big data and the tools that harness these data will likely help the CT community in a resource-constrained environment.[1, 2]

OSINT can likely offer alternatives to traditional closed-source intelligence (all the other INTs), which often is not only expensive and time consuming to build, but also difficult to share with partners.[3] These alternatives can include commercial data and data aggregation tools used by non-governmental organizations for the purposes of counterterrorism. Once put into practice, OSINT can illustrate indications of FTO activity and help provide early warning of burgeoning terrorist attacks. Further, these alternatives can widely contribute to traditional closed-source analysis, where non-traditional and traditional information can be fused together supporting intelligence focused on terrorist organizations.

To mitigate resource constraints, develop new insight into FTO activity, and more quickly share information and intelligence, the IC should lean in and embrace OSINT. As the CT community (and IC writ large) further develops tactics, techniques, and procedures for using OSINT, we can likely better use it to develop indications and warning (I&W) of FTO threats to the United States and to U.S. interests. This would add support to an under-resourced, over-the-horizon strategy for mitigating terrorism threats.[4]

Many non-governmental organizations outside of the IC have developed sophisticated tactics, techniques, and procedures to access CT-related OSINT data and to publicly share that data and their analysis. The IC can more fully tap into these sources to better use exploited and unexploited data to illuminate the business, supply chain, and cyber connections concerning FTOs.

There also are numerous publicly and commercially available information (PAI/CAI) data sets that span business intelligence, cyber, supply chain and logistics, science and technology, topic and trend analysis, as well as advertising. OSINT derived from these tools and data sets can help us understand the capabilities and intent of nation states, their proxies, and non-state actors such as FTOs. Social media aggregation tools, for example, can illuminate overt communications between FTOs and supporters. Determining which tools and data sets can best support counterterrorism priority actions would help the IC better use OSINT for CT.

With strategy or policy to guide the use of OSINT for counterterrorism, the IC can develop new OSINT oriented I&W using the large amount and variety of PAI/CAI and associated tools available. Overall, embracing OSINT will help the CT community find cost-effective and collaborative ways to broadly cover currently denied areas to better understand FTO capabilities and intent.

> Now is the time to develop an OSINT capability for CT. The capabilities exist and are being used by our partners (and likely our threats), so harnessing the power of open source data and tools is imperative.

Strategic Guidance for OSINT and Counterterrorism

IC OSINT Strategy

The Office of the Director of National Intelligence (ODNI), in conjunction with the OSINT Functional Manager (Director/Central Intelligence Agency [CIA]), published its first-ever IC OSINT Strategy in March 2024. Its purpose?

To "strengthen OSINT as a core intelligence discipline and position the IC to capitalize on the full potential of open source data and information to enhance the intelligence mission in a manner consistent with our nation's principles and values."[5] Primary focus areas include data acquisition, collection management, innovation for new capabilities, and developing the workforce and tradecraft.[6] Organizations throughout the IC are currently working to implement this new strategy. By identifying open source tactics, techniques, and procedures that can be used for counterterrorism, we can help CT-focused organizations implement the OSINT strategy.

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, which established the ODNI and associated Centers including the National Counterterrorism Center, directed the use of open source intelligence.[7] Section 1052 of IRTPA expresses the sense of Congress that:

- The Director should establish an intelligence center to coordinate the collection, analysis, production, and dissemination of open source intelligence to IC elements.
- Open source intelligence is valuable and must be integrated into the intelligence cycle.
- The intelligence center should ensure that each IC element uses open source intelligence consistent with its mission.

IC Counterterrorism Strategy

National Security Memorandum 13, U.S. International Counterterrorism Policy,[8] states the lines of effort (LOEs) for U.S. CT are to:

1. Strengthen defenses
2. Build and leverage partner capacity
3. Strengthen our capacity to warn
4. Narrowly focus direct action CT operations
5. Deter and disrupt state supported terrorism
6. Degrade transnational enablers of terrorism
7. Integrate CT with other U.S. foreign policy and national security efforts

It could be argued that open source intelligence contributes to all seven LOEs. However, here we will focus on LOE 3, strengthen our capacity to warn.

The policy states the U.S. government will "build a layered I&W architecture that incorporates a wide spectrum of information types and sources—including expanded use of open source and non-traditional sources of information—and increases collaboration with partners."[9]

With the combination of waning CT resources, reduced access to partners in regions where FTOs are growing, and the desire to build an OSINT capability to support the capacity to warn, now is the time to develop an OSINT capability for CT. The capabilities exist and are being used by our partners (and likely our threats), so harnessing the power of open source data and tools is imperative.

Commercial OSINT, such as the products generated by the Terrorism Research & Analysis Consortium (TRAC) and the Counterterrorism Group (CTG), demonstrates the ability to produce CT analysis we often see in predominately closed-source intelligence. The IC should expand work with commercial organizations like these and develop innovative means to mitigate threats from areas where the U.S. has reduced influence, such as regions in the Middle East and the "coup belt" in the Sahel and West Africa.[10]

> **"The IC must be postured to capitalize on pioneering efforts in the private sector by partnering in new ways with industry and academia to develop, test, and deploy OSINT tools and tradecraft."**
>
> —IC OSINT Strategy, 2024-2026

How do Non-Governmental Organizations Use OSINT for Counterterrorism?

Non-governmental organizations like TRAC and CTG appear to be making great use of open source information and generating open source intelligence, likely filling knowledge gaps on FTOs. Other organizations like the Global Internet Forum to Counter Terrorism (GIFCT) and the Global Network on Extremism and Technology (GNET) focus on terrorism activity in the cyber domain. The Washington Institute's Islamic State Select Worldwide Activity Interactive Map focuses on displaying Islamic State (ISIS) activity in an interactive platform for statistical, geospatial, and visual analysis. These organizations have developed I&W for future terrorist attacks; the IC should make a concerted effort to determine how well the I&W from these groups aligns with the IC's key intelligence questions (KIQs) and associated requirements for counterterrorism.

Terrorism Research & Analysis Consortium

TRAC runs a subscription-based website, meaning analysts need a subscription to see the reports. However, TRAC also has a free "Weekly Analyst Briefing" sent via email, which highlights the latest FTO activities with tactical, operational, and strategic analysis.

According to the TRAC website "TRAC combines one of the world's largest databases of terrorists, terrorist groups, hate groups and their abettors with original, analytical essays on seminal terrorism topics, profiles of vulnerable regions and cities, and live feed of news and analyses."[11] TRAC appears to specialize in analysis of terrorist organization media and messaging, which could be very useful for broader unclassified analysis sharing within the CT enterprise.

TRAC analysis includes insights on specific groups (e.g., the Islamic State and its various branches), as well as countries where the United States has a reduced or limited footprint (e.g., Syria, Iraq, Afghanistan, Democratic Republic of the Congo, Mali, Somalia, and Mozambique). This analysis demonstrates the availability of open sources in areas of limited or denied access. Additionally, TRAC provides insights into ideology, tactics, and terrorist targets.[12]

Recent analytic examples from TRAC newsletters include:[13]

- **Syria**—In March 2024, TRAC documented 128 ISIS operations that were not officially recognized by ISIS. In July, TRAC provided analysis on recent prisoner releases by the Syrian Democratic Forces (SDF) stating "overall, this release of prisoners represents a significant shift in the approach towards dealing with former militants. The SDF and the Arab-Kurdish administration appear to be prioritizing reintegration and reconciliation over prolonged incarceration."
- **Iran**—TRAC reported on the 3 April 2024 complex Jaish al-Adl (Army of Justice, a Sunni-Muslim separatist group) armed assault on several Iranian Revolutionary Guard Corps targets in Iran. "Easily the most sophisticated operation launched by Jaish al-Adl ever, TRAC is certain that the militant group has utilised Iran's current distraction and promise of retaliation against the recent Israeli airstrike that killed Iranian Revolutionary Guard Corps (IRGC) General Mohammad Reza Zahedi, the most senior Iranian officer in Syria. The fact that Jaish al-Adl was about to execute this complex assault on Iranian soil, while Iran is actively engaged in multiple shadow wars globally, underscores the vulnerabilities within the Iranian regime."
- **Mali**—In April 2024, TRAC reported on Jama'at Nusrat al-Islam wa al-Muslimin (JNIM) attack trends. JNIM militants led an armed assault on Malian Armed Forces (FAMA) outside of Bamako in Kasséla, Koulikoro Region, Mali. TRAC highlighted the significance of this attack due to the proximity to Bamako. TRAC also drew comparisons to brazen al-Qaeda (al-Shabaab) attacks in Mogadishu, Somalia, a warning to the Mali government.

- **Togo**—TRAC provided analysis of JNIM activity encroaching on Coastal West Africa. "The notable aspect of the 20 July cross-border attack is the temporary takeover of the Kankanti barracks, suggesting JNIM's intention to establish a permanent presence in Togolese territory along the Burkina Faso border. This strategic move would facilitate the movement of supplies and militants in and out of the country at their convenience."

Counterterrorism Group

The United Kingdom-based CTG "assists in setting up the right systems, tactics, techniques, and personnel to effectively detect, deter and defeat terrorists' attacks. CTG works to understand the terrorist threat, terrorist tactics and methods, individuals participating in the terrorism, and develops and implement systems, strategies, plans, and solutions that detect and prevent terrorist attacks."[14]

The United Kingdom (UK) appears to recognize the need for this type of open source CT work and plans to incorporate it into a new task force. "On April 30, 2024, the British Government announced it would set up a new taskforce…to prevent extremists and "hate preachers" from entering the UK…Extremists and "hate preachers" will be identified through a range of intelligence sources, including the UK embassy network, open source intelligence (OSINT), and by working within local communities across the UK."[15]

As a non-government entity, the CTG plans to continue to provide CT OSINT analysis in support of UK security. "The Counterterrorism Group's Teams will continue to monitor cases of extremism in the UK and overseas that threaten British national security. CTG will track extremist events and monitor the British government's response to analyze their impacts on the UK. Teams will also monitor broadcasts of upcoming national protests and demonstrations and examine them as they occur for displays of extremism, releasing timely reports to alert the public of security risks and possible implications."[16]

Global Internet Forum to Counter Terrorism

The GIFCT is primarily a forum for big technology companies to keep terrorism and terrorism related content off their platforms. As a forum for big tech companies, one of the primary activities GIFCT conducts is hashtag sharing, which allows members to defend against terrorist actors from gaining access and pushing content over these platforms. With hashtag sharing, once violent extremist content is discovered on one platform, it is quickly shared with the other members and blocked on other platforms.

According to the GIFCT website "The Global Internet Forum to Counter Terrorism (GIFCT) is an NGO [non-governmental organization] designed to prevent terrorists and violent extremists from exploiting digital platforms. Founded by Meta (formerly Facebook), Microsoft, YouTube, and X (formerly Twitter) in 2017, the Forum was established to foster technical collaboration among member companies, advance relevant research, and share knowledge with smaller platforms. Since 2017, GIFCT's membership has expanded beyond the founding companies to include over two dozen diverse platforms committed to cross-industry efforts to counter the spread of terrorist and violent extremist content online."[17]

> **"The IC will establish common OSINT platforms to facilitate access to shared data and tools, and we will identify and implement a pathway to deliver IC OSINT products to the broader U.S. Government."**
>
> —IC OSINT Strategy, 2024-2026

Global Network on Extremism and Technology

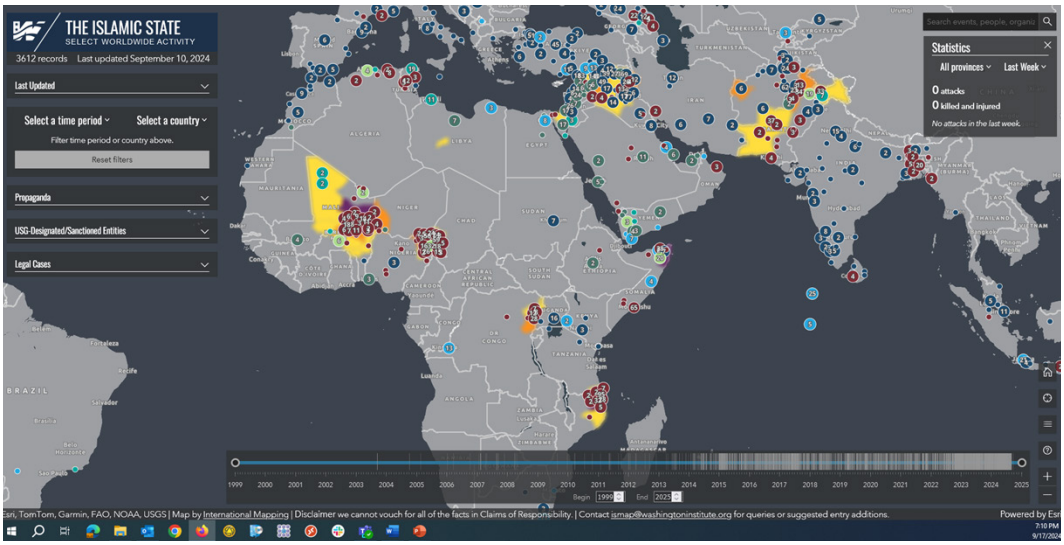
The Global Network on Extremism and Technology is an "academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology."[18]

An example of early warning from GNET includes a product on ISIS using Artificial Intelligence (AI) and broadcasting extremist material via Rocketchat, once considered a digital safe haven for ISIS.[19] Technological advances like AI are developing rapidly and consistently and, like everyone else, FTOs have access to these developments. OSINT specialists at GNET not only shared insights on this FTO use of emerging technology, but also illustrated the use of international partnerships. The three authors are Italian OSINT analysts.

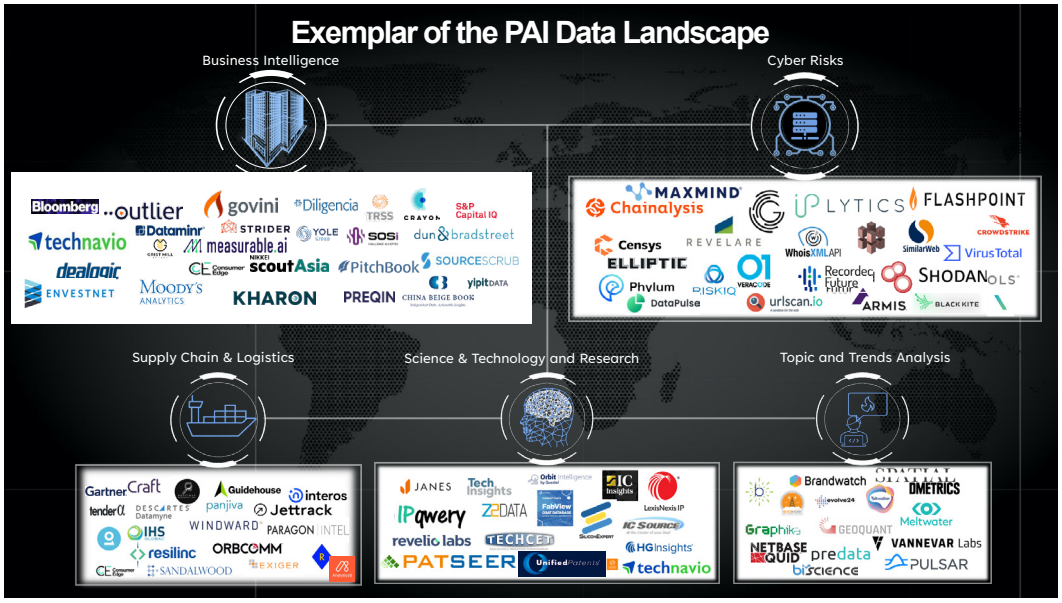
The Washington Institute's Islamic State Select Worldwide Activity Map

The Islamic State Select Worldwide Activity map, developed and maintained by Senior Fellow at The Washington Institute Near East Policy, Aaron Zelin, provides an accessible way to understand the global reach and activities of ISIS. It offers a clear illustration on an interactive map platform[20] and is freely available without a subscription. It is designed for researchers and policy makers as a "living" project, updated continuously to cover new developments as well as modifications to older entries, as needed.[21]

The map includes data beyond the traditional scholarly focus on attack data, offering propaganda from Islamic State media, U.S. Department of State and Department of the Treasury designations and sanctions, and domestic and international terrorism cases.



The Washington Institute's Interactive Map Illustrating a Wide Variety of Islamic State Activity[22]



Exemplar of the Publicly Available Information Data Landscape[23]

Tools and Data Sets for Counterterrorism

There are numerous PAI/CAI data sets available. PAI data can be categorized into business intelligence, cyber, supply chain and logistics, science and technology, topic and trend analysis, as well as advertising (see chart below). Tools are available by which the IC can gain better understanding of potential terrorist activity within a given region. These tools and data sets can illuminate financial pipelines and supply chains in which FTOs acquire basic equipment from witting or unwitting suppliers and supporters. Determining which tools and data sets can best support counterterrorism priority actions would help the IC better use OSINT for CT.

Many of the PAI/CAI data sets revolve around Advertising Technology (AdTech). AdTech data is widely available for purchase and can show wide population trends as well as patterns of life. Many organizations conduct investigative research using AdTech, including law enforcement, news agencies, and of course, companies trying to sell their products. Nefarious actors, including nation states, organized crime, and FTOs also likely purchase and use AdTech resources to identify targets for financial or political gain, or to conduct acts of terrorism.

As described in previously published MITRE Intelligence After Next papers, "as we interact with our phones, websites, and the digital ecosystem, ubiquitous surveillance generates vast amounts of commercial data that creates enduring records of our identity, locations, and connections. This commercial surveillance data is collected, repackaged, and sold in a vast and largely unregulated commercial market and is readily available for purchase by companies around the world and by our adversaries."[24]

It should be noted that using AdTech and the "digital dust" that end points or devices produce can be used for ubiquitous technical surveillance (UTS). Broadly speaking, UTS can illustrate where and when the associated actors (device users) are located before, during, and after times of conflict or attacks, and perhaps assist in determining terrorist activity. The CT community can

better determine terrorist activities by systematically analyzing their signatures within the Internet of Things by using UTS. UTS can be analyzed by using the concept of Data-Driven Analysis and Artificial Intelligence (D2A2).[25] It should be noted that using UTS for CT will take a significant and purposeful effort. Creating value from UTS data requires specific talents, skills, materials, technology, budgets, access to data, and an ability to distribute the resulting information to the CT community.[26]

"To maintain an intelligence advantage in the open source environment, we must embrace new technologies and tradecraft to collect and evaluate open source data."

—IC OSINT Strategy, 2024-2026

OSINT derived from these tools and data sets can help us understand the capabilities and intent of nation states, their proxies, and non-state actors such as FTOs. The tools and data available via PAI and CAI can be organized into (at least) five categories: company networks, cyber, information environment, personal affiliations, and supply chain.

Company Networks

GIFCT, as previously discussed, is a forum composed of many of the largest social media platforms joining forces to reduce FTO use of their platforms. No large media platform wants to be known as the terrorist platform of choice. The same idea could be used to reduce FTO use of other company's products. Products and services used by FTOs are made/provided by companies all over the world. There are business intelligence data and tools available that highlight these products and services, to include who buys or pays for these products and services.[29] The IC should use these data and tools

Using OSINT to Identify FTO Indicators

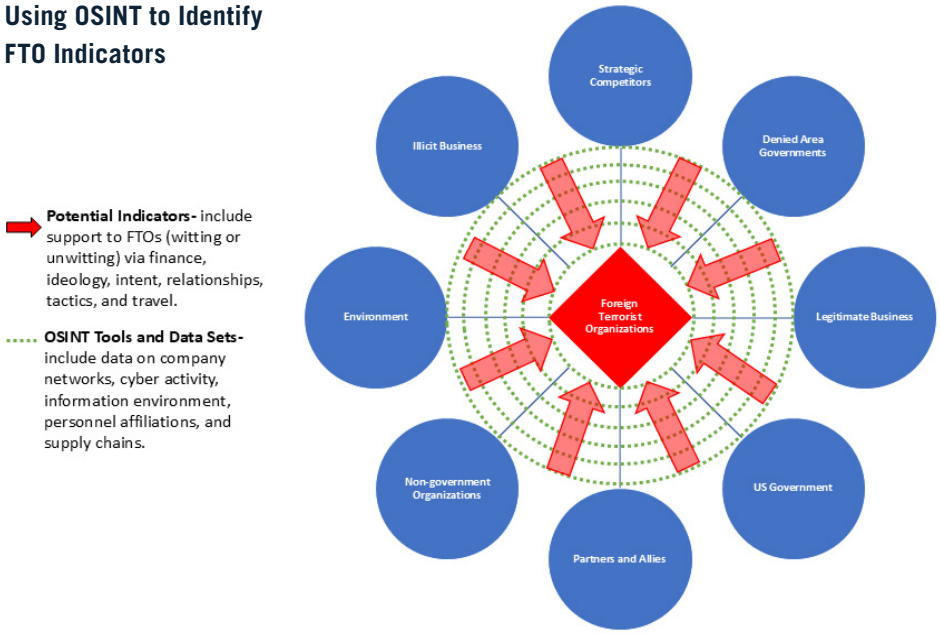


Illustration of how open source data and tools can help us better understand the FTO operational environment and possibly provide indications and warning of potential attacks against the U.S. and U.S. allies.[27, 28]

to highlight these products and services and reach out to the public, private, and government sector partners who may be wittingly or unwittingly providing products and services to FTOs.

Cyber

FTOs with the intent to conduct any kind of activity likely conduct research and potentially plan attacks via the cyber domain. Additionally, bad actors of all varieties can purchase access (via other bad actors) to known vulnerabilities either in conjunction with or in lieu of a physical attack. The IC should make better use of the platforms that provide cyber compromise indicators and aggregated OSINT scraped from clear web and dark web sources, preferably using intent-based indications and warning.[30] Again, open source available data sets and tools like these can help illuminate FTO networks and help provide early warning of attacks and other activities.

Information Environment

FTOs can and likely do make use of the information environment that best supports their cause. Social media insight tools can create analysis on social media platforms and other online media across multiple languages in real-time. Analytic capabilities include mapping associated networks and enabling the identification of linkages among sources.[31] Additionally, tools can look back at historical markers or previous attacks and highlight characteristics in social media that occurred before, during, and after terrorist attacks.[32] Conducting case studies of previous terrorist attacks using tools associated with the information environment could help build specific indicators for future terrorist attacks.

Personnel Affiliations

When individuals are known to be related to an FTO, perhaps through supply chain analysis, company networks, or operatives in the information environment, it is possible to use publicly or commercially available data to better understand the impact those individuals have in a specific region.[33] For example, cross-referencing individuals at the end of a supply chain with known or suspected terrorist actors could be done with personnel affiliation data sets and tools. This can help analysts make connections in networks that are not already known.

Supply Chain

All organizations, including FTOs, require necessities (i.e., food, water, shelter). To train in various combative tasks, much more is required, including weapons, components for explosives, and perhaps heavy equipment for supporting operations like resource extraction.[34] All these activities and the supplies and equipment required, are likely to be shipped from outside the regions where FTOs operate. Non-traditional data and tools are available to help illuminate some of the supply chains supporting FTOs.[35] Data coverage is global, with access to historically opaque markets.[36] Of course, supplies for FTOs are likely to be provided illicitly and are less likely to be available or tracked, leaving potential gaps in the network, but the IC should use the data and tools available to better define those gaps and employ other tools and data for further analysis.

Practical Application of OSINT in the CT Operations Center

Before applying a strategy for OSINT for CT, it is important to acknowledge that access to OSINT data is not always easy. Some analysts may not be able to access PAI data due to policy restrictions or subscription-based data in news or social media platforms for breaking event situations.

Analysts often find ways to create an organic filter/alerting system for terrorism-related breaking events instead of using a paid-for service like First Alert (Data Minor). Often, these filters and other workarounds cannot be replicated at other operations centers or worse, they leave with the personnel who created them. Operations centers also may have Terms of Service restrictions with vendors (typically Application Programming Interface-based issues) that prevent them from using or sharing the information within the IC.

PAI COLLECTION POLICIES

EO 12333 authorizes NCTC to collect publicly available information. NCTC is required to fully protect the legal rights of all U.S. persons, including freedoms, civil liberties, and privacy rights guaranteed by federal law.

NCTC's Policy 9 Guidance (effective 20 December 2016) established NCTC's policy for the collection, use, and retention of PAI for official purposes. The policy aims to help ensure NCTC officers comply with Privacy and Civil Liberties protections.

NCTC Policy 9 defines PAI as information any member of the public could lawfully obtain by request or observation, including public communication that is lawfully accessible to any member of the public. PAI may be obtained from the internet, among other sources, where the internet is a broad term, and encompasses different platforms including social media.

Collection of PAI for official NCTC purposes, among other rules, must be designed to obtain terrorism information. NCTC personnel are prohibited from accessing or using PAI, in any manner, solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States.

Recommendations to Better Use OSINT for CT

Current IC policy and practice are not well suited for CT practitioners to gather information, learn about threat environments, and conduct analysis via OSINT that supports U.S. counterterrorism objectives. Challenges to applying OSINT to the counterterrorism problem set include authorities for analysts accessing and using PAI/CAI, scaling tool and data resources, the U.S. government working within current user agreements with vendors, as well as combining unclassified data with closed source data used by intelligence analysts. The following are some ideas that could help.

Incorporate existing practices. Many non-governmental organizations have developed I&W for future terrorist attacks; the IC should make a concerted effort to determine how well the I&W from these groups aligns with the IC's KIQs and associated requirements for counterterrorism.

Develop a terrorism knowledge management repository. It is against current policy for government CT analysts to collect PAI for mobilization indicators (see PAI Collection Policies) when a direct terrorism nexus is not immediately present. However, analysts may overtly monitor PAI for I&W purposes. It may be viable for external partners outside of the IC to provide this data in a shared forum hosted by ODNI. Like the MITRE ATT&CK knowledge base, which hosts cyber threat actors' tactics, techniques, and procedures, ODNI should consider developing an unclassified knowledge management repository focused on terrorist threats as well as methods countering those threats. This knowledge management repository could be hosted within the NCTC's public facing website.[37] CT information would be more shareable with a wide variety of partners to include state/local authorities as well as applicable business entities.

Incorporate Ubiquitous Technical Surveillance. The IC should consider using UTS specifically for CT. As previously mentioned, using UTS for CT will take a significant and purposeful effort. Creating value from UTS data requires specific talents, skills, materials, technology, budgets, access to data, and an ability to distribute the resulting information to the CT community.

Incorporate PiX for CT. The U.S. Government sponsors a program (Protected Internet Exchange), which assists in sharing unclassified information. The counterterrorism community could better use this forum by adding new partners (state, local, private) who could contribute to CT information sharing.

Share costs for analysis and data acquisition. According to the director of the Open source Enterprise at CIA, "charging for each user with access to a company's OSINT products, for instance, may work for a private firm with 10, 100, or even 1,000 employees, but it scales up astronomically if government agencies want to share OSINT across the entire Intelligence Community, let alone the Department of Defense."[38]

Data acquisition concerning CAI and the tools that help access these data are difficult to manage for the IC. Working with CT-focused non-government organizations and hosting their analysis in a shared venue could help alleviate some data acquisition concerns.

Additionally, expanding ODNI's capability to host data and tools (perhaps via Osiris) could help. Sharing and coordinating the use of CAI is happening between various government departments and agencies now via memorandums of understanding and cost sharing agreements. The IC should survey these examples and develop the standards to share more broadly, quickly, and cost-effectively.

Harness AI for CT. Social media tools are available to aggregate potential mobilization indicators. However, the policies concerning collecting and storing the data, coupled with a shortage of resources and tools that make sense of the data, make it difficult for CT analysts to access it in useable and repeatable ways. Resourcing science, technology, engineering, and math (STEM) projects (i.e., artificial intelligence) focused on collating useable CT information from social media could help. Part of this process should include protecting U.S. persons information, ensuring that the information meets IC requirements for collection, and storing information.

The previously mentioned non-governmental organizations conducting OSINT for CT likely have developed automated tools to assist with the large volume of data analyzed for CT. The IC should learn more about the tools these NGOs have developed and determine potential STEM projects that could better enable analysts to identify FTO indicators using this technology. Projects could be conducted and data tools developed by the wide variety of companies supporting government efforts.

The CT Community Has Much to Gain from OSINT

To mitigate resource constraints, develop new insight into FTO activity, and more quickly share information and intelligence, the U.S. IC should lean in and embrace OSINT. By incorporating a systematic approach to sharing CT information via a shared open knowledge base, facilitating the acquisition of tools and data sets useful for CT, and harnessing STEM for developing tailored tools for aggregating social media associated with CT, we can better use OSINT to develop I&W of FTO threats to the U.S. and U.S. interests, and better mitigate terrorism threats.[39]

References

1. MITRE Corporation, "Intelligence After Next: The Prevailing Narratives about Open Source Intelligence are Misguided," February 2023.
2. U.S. Central Command, "Senate Armed Services Committee Hearing on Posture of USCENTCOM and USAFRICOM in Review of the Defense Authorization Request for FY24 and the Future Years Defense Program," March 17, 2023.
3. MITRE Corporation, "Intelligence After Next: Radical Transparency: Expanding Partnerships with Commercial Intelligence Sharing," December 2023.
4. Combating Terrorism Center, "No Good Choices: The Counterterrorism Dilemmas in Afghanistan and Pakistan," October 2023.
5. Office of the Director of National Intelligence, "The IC OSINT Strategy, 2024-2026, The INT of First Resort; Unlocking the Value of OSINT," April 2024.
6. Office of the Director of National Intelligence, "The IC OSINT Strategy, 2024-2026, The INT of First Resort; Unlocking the Value of OSINT," April 2024.
7. U.S. Congress, "Intelligence Reform and Terrorism Prevention Act of 2004," accessed on 5 September 2024.
8. National Security Council, "Memorandum on U.S. International Counterterrorism Policy," 6 October 2022, acquired by NY Times via Freedom of Information Act on 29 June 2023.
9. National Security Council, "Memorandum on U.S. International Counterterrorism Policy," 6 October 2022, acquired by NY Times via Freedom of Information Act on 29 June 2023.
10. Human Rights Research Center, "The West African Coup Belt and its Waning Humanitarian Situation," 16 April 2024.
11. Terrorism Research & Analysis Consortium, https://trackingterrorism.org/about/, accessed 4 April 2024.
12. Terrorism Research & Analysis Consortium, https://trackingterrorism.org/insights/, accessed 23 July 2024.
13. TRACWatch—Weekly Analyst Briefings received via e-mail between 4 April and 8 May 2024.
14. The Counterterrorism Group website, https://www.counterterrorismgroup.com/moreaboutus, accessed 4 April 2024.
15. The Counterterrorism Group, Counter Threat Center, "Threat Assessment: The UK Government Initiates a Taskforce to Prevent Extremist and "Hate Preacher's" UK Access, A Move Thought to Increase Community-Based Mistrust and Covert Extremist Activity," 11 May 2024.
16. The Counterterrorism Group, Counter Threat Center, "Threat Assessment: The UK Government Initiates a Taskforce to Prevent Extremist and "Hate Preacher's" UK Access, A Move Thought to Increase Community-Based Mistrust and Covert Extremist Activity," 11 May 2024.
17. The Global Internet Forum to Counter Terrorism website, https://gifct.org/about/, accessed 4 April 2024.
18. The Global Network on Extremism and Technology, https://gnet-research.org/about/, accessed 4 April 2024.
19. The Global Network on Extremism and Technology, "AI-Powered Jihadist News Broadcasts: A New Trend In Pro-IS Propaganda Production?" 9 May 2024.
20. The Washington Institute for Near East Policy, "Islamic State Select Worldwide Activity Interactive Map," accessed 14 August 2024.
21. Aaron Y. Zelin, The Washington Institute for Near East Policy, "The Islamic State Select Worldwide Activity Interactive Map," 21 March 2023.
22. The Washington Institute for Near East Policy, "Islamic State Select Worldwide Activity Interactive Map," accessed 14 August 2024.

23. MITRE Corporation, "Data Days," Slide presentation on publicly available information, 15 May 2024.
24. MITRE Corporation, "Intelligence After Next: Surveillance Technologies are Imbedded into the Fabric of Modern Life—The Intelligence Community Must Respond," January 2023.
25. MITRE Corporation, "Deciphering Ubiquitous Technical Surveillance (UTS) with Data-driven Analytics and Artificial Intelligence (D2A2)," June 2024.
26. MITRE Corporation, "Deciphering Ubiquitous Technical Surveillance (UTS) with Data-driven Analytics and Artificial Intelligence (D2A2)," June 2024.
27. NCTC, "Mobilization Indicators Handbook, 2021 Edition," accessed 4 April 2024.
28. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
29. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
30. MITRE Corporation, "Intelligence After Next: Using Intent-Based Indications and Warning to Prevent Terrorist Cyber Attacks," August 2023.
31. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
32. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
33. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
34. U.S. Government Publishing Office, "Hybrid Hearing Before the Subcommittee on National Security, International Development and Monetary Policy of the Committee on Financial Services," 4 November 2021.
35. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
36. MITRE Corporation, Categorization of open source tools and data sets conducted from 2021-2024.
37. ODNI, National Counterterrorism Center's official website, "NCTC Resources," accessed on 30 July 2024.
38. Breaking Defense, "OSINT overdose: Intelligence Agencies Seek New Ways to Manage Surge of Open-Source Intel," 13 May 2024.
39. Combating Terrorism Center, "No Good Choices: The Counterterrorism Dilemmas in Afghanistan and Pakistan," October 2023.

Author

Dan Kolva is a principal for intelligence strategy and policy at MITRE with expertise in strategic intelligence, strategic planning, and counterterrorism. He transitioned to his current role following a 21-year career in the U.S. Army as an air defense artillery and strategic intelligence officer. Dan has a BS from the University of South Carolina, an MS from the National Intelligence University, and a Graduate Certificate in Cyber Threat Intelligence from James Madison University.

Whitney D. is an NCTC Operations Officer leading open source collection efforts and was formerly NCTC's Open source Program Manager. She has 14 years of Intelligence Community and DoD experience working in open source, geospatial, and all-source intelligence. Whitney has a BS in Intelligence Studies with a focus in analysis from the American Military University.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

About NCTC

The National Counterterrorism Center (NCTC) leads the nation's effort to protect the United States from terrorism by integrating, analyzing, and sharing information to drive whole-of-government action and achieve our national counterterrorism objectives.

OCTOBER 2024