DataWalk

Using Data Analysis to Disrupt Threat Networks

A DataWalk White Paper For The Military and Intelligence Community

Intelligence is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity that results in the product and to the organizations engaged in such activity.

Don't confuse activity with results! Successful intelligence operations are cyclical and continuous throughout an operation. The cycle should begin anew following the detainment of a target and their debriefing along with exploitation of any materials recovered. You should be specifically working to dismantle an adversary network through carefully planned and executed targeting. In this paper we discuss universal pathways that all intelligence analysts can take to successfully keep this cycle going and render criminal networks ineffective.

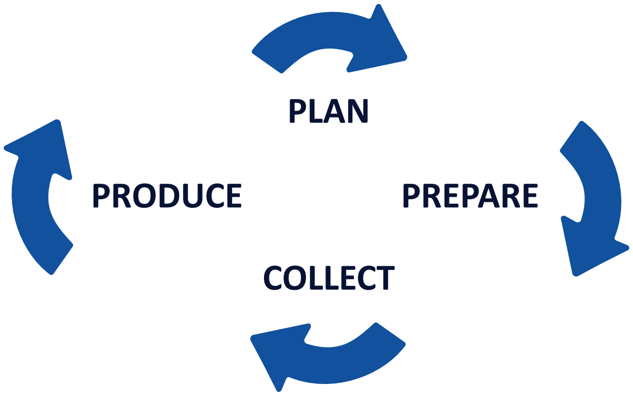

Figure 1. The cyclical nature of analysis

All analysts deal with information, and it is their ability to analyze this information that determines their rate of success. Things like financial records and past nefarious activities are pieces of information that can seem completely disconnected, but by physically mapping out these data points, an analyst can analyze the information, identify network members, determine hierarchies, examine group dynamics, and help devise strategies to disrupt or destroy adversary networks.

When evaluating intelligence value, analysts should consider the type of intelligence and the source. Here are some considerations about the main sources of intelligence:

Human Intelligence (HUMINT)

HUMINT is intelligence gathered by means of interpersonal contact and relationships as opposed to the more technical intelligence collection disciplines such as signals intelligence (SIGINT) and geospatial intelligence (GEOINT). HUMINT is defined as a category of intelligence that is derived from information collected and provided by human sources. Typical activities conducted to collect HUMINT include interrogations of detained persons and conversations with persons having varying degrees of access to information. When evaluating the accuracy of HUMINT an analyst must take into consideration the placement, access, motivation, suitability, susceptibility and accessibility (PAMSSA) of the source. After a source has provided information that is published into multiple reports, a source evaluation must be conducted by comparing the reported information against intelligence or information gathered from other sources and disciplines. The result of the evaluation gives the analyst a measure of the accuracy of the provided information.

Signals Intelligence (SIGINT)

SIGINT is intelligence gathering by interception of signals, whether communications between people or from electronic signals not directly used in communication. As sensitive information and communication is often encrypted, signals intelligence involves the use of cryptanalysis to decipher messages. It is important to note that SIGINT's technical data is considered to be highly accurate and aids in developing pattern of life (POL) on targets/members of threat organizations. However, the content of the message can often be highly inaccurate. Another note includes the proclivity of threat organizations to use pro-words during communication as an operations security (OPSEC) measure.

Geographic Intelligence (GEOINT)

GEOINT is derived from the exploitation and analysis of imagery and geospatial information that describes, assesses, and visually depicts physical features and geographically referenced locations and activities. GEOINT reveals how human intent is constrained by the physical terrain and aids in the confirmation of a threat organization's course of action. Utilizing time-stamped imagery, an analyst with GEOINT can uncover previous pattern of life and anticipate future pattern of life through time and space.

Network Targeting Analysis

After evaluating your intelligence, you can start to fill out your network chart. Keeping a network organization chart is very important for understanding the hierarchy within your targeted network. It also provides an invaluable tool for explaining the hierarchy of a network to others. It's simplest to use a computer program for this as criminal organizations tend to change frequently based on personnel problems, member's arrests, injuries, or deaths, and many other factors. It's also easier to move nodes around on a screen with all the information contained in the node, rather than trying to keep track of everything on paper

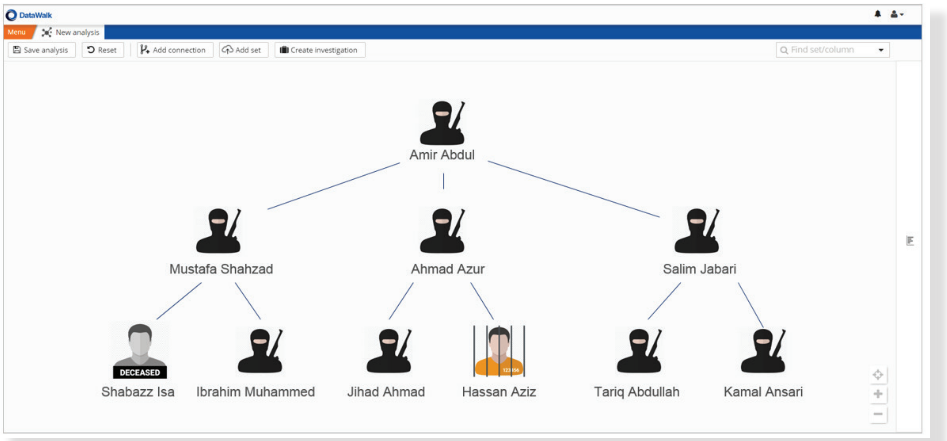

Figure 2. Example of a network organization chart.

Once you have diagrammed your network, you can determine where to target in order to disable the network.

Finding the right suspect to target is arguably the most time-consuming step in analysis, because filling out a network and understanding the hierarchy will never fully be finished. The very nature of criminal activity is its fluidity. Ask yourself these questions when deciding who to target:

- Are there criminal histories or outstanding warrants that could be leveraged to gain information about or influence the network?

- Do you have enough information on individuals that, if arrested, would disable or disrupt the organization?
- If you need more information to arrest a suspect, who within the organization has the PAMSSA t provide it to you?
- Once an arrest happens within an organization most phones are changed immediately, along with POL. Is this arrest worth that disruption? Carefully consider this, as you will have to discover phones and likely social media accounts all over again.

Once you have answered these questions and decided who you will target, you need to figure out how to physically locate them.

- They are humans like you; they have habits and POL that can be exploited.
- Pay attention to social media. If a large part of a suspect's POL is seeing a girlfriend but the suspect posts about a break up, you need to adjust and realize the suspect's POL will be changing.
- Should you target them when they are with other organization members and risk more disruption for more possible arrests? Weigh the benefits and risks of this approach.

When your suspect is arrested, have the most up-to-date information and all available background ready. You can predict, but never fully know, who your suspect will be with when detained. If you have the intelligence/evidence to bring in other associates, be ready to provide that should your suspect be with other organization members.

Once arrested your suspect can become a source of HI. It is vital to gain the cooperation of an arrestee early if they are to provide reliable information pertinent to the ongoing investigation. Do not let this opportunity pass! Do not simply let the suspect be charged for their crimes and processed, when you could be using their knowledge to further disable or disrupt their criminal network. Analysts should be involved in every step of the interrogation process, especially the interrogation of the suspect. Asking someone "what bad guy stuff have you been doing?" will not typically result in valuable intelligence, which is why the analyst should provide targeted questions the suspect is likely to know based on their position within the network.

- Before an interrogation, fully exploit any phones or laptops.
- Arm the interrogator with all background information and this specific suspect's PAMSSA. If you're going after the John Smith smuggling ring and you arrested a corner drug dealer, don't ask questions about John Smith himself. One of the biggest mistakes made in interrogation is asking about things of which the suspect has no knowledge. This informs the suspect that you are missing intelligence, and the suspect is less likely to provide information because they will believe you do not know the extent of their crimes and cannot charge them.
- Vet information as it comes from the suspect. Don't let the suspect go for multiple interrogations with a fake story and then read the reports later.
- Keep in mind that arrested suspects will likely lie and will only provide you information if they believe that it serves their own best interests. If you have contradictory intelligence such as an SI report indicating Harry is superior to your suspect, but your suspect claims Harry is subordinate to him, weigh that information. Harry or the suspect could be lying in order to seem more, or less, important.

Now you have brand new information to run through your evaluation process. Use this new information to update your network chart and start the targeting process all over again.

- Usually the arrest of your suspect results in a multi-INT dump. Make sure to look at everything. Do not lean too much on one source because no source on criminal activity is infallible.

- Pay attention to reflections throughout the organization. If you think you caught a corner drug dealer but the network is talking about the capture of someone of importance, do not default to believing what you have outlined in your network chart. Building a network chart isn't a science, and you could have misplaced your suspect in your network analysis.
- Always have your eye on the next step to realizing your goal of disabling this network. How does the intelligence from this capture fit, or not fit, with your current picture?
- Approach analysis as a scientist. Be objective and evaluate every piece of intelligence. Do not let the intelligence fit into your picture of the network, but rather change your picture as new intelligence

Software Technology Can Be The Key

Using data analysis software to support the intelligence analysis process can be incredibly helpful. Software such as DataWalk can make it far easier to:

- Organize data and "connect the dots" across many different data sources, including external databases.
- Efficiently, effectively generate insights and intelligence from even large sets of diverse data.
- Create and maintain network diagrams (e.g., link charts).
- Analyze the geospatial relationship of people and activities within the network.
- Do exclusionary searches, such as looking at all financial transactions for a network but filtering out anything under $10,000.
- Visually see outliers in information (e.g., you can easily search for all people your suspect contacted more than 50 times in the last week, etc.).
- Effectively share and disseminate information. Dissemination is a large part of what an analyst does, so you need to be able to effectively communicate all the evidence against the suspect to many others.

Always remember the nature of the people you are chasing, keep your network chart updated and bring to work each day a clear goal of disabling that network.

DataWalk is a next-generation analytical platform for intelligence-led decision making, which easily connects many large data sources for fast visual analysis and collaborative investigations. To learn more about DataWalk, visit datawalk.com.