ICAC Required Reading (courses@readfomag.com)

COLLECTION
OSINT
MICE/RC (HUMINT)

ANALYSIS:
BESTMAPS
BICC/E
Judging Single Source Information
Intelligence & Probability
Intelligence Cycle
Intelligence Requirements

Acronyms

Analysis & Control Element (ACE)
Area of Operations (AO)
Area of Interest (AI)
Area of Responsibility (AOR)
Counterintelligence (CI)
Course of Action (COA)
Extreme Rule of Law (EROL)
Human Intelligence (HUMINT)
Information Security (INFOSEC)
Intelligence Requirement (IR)
Mine Resistance Ambush Proof Vehicle (MRAP)
Most Likely Course of Action (MLCOA)
Most Dangerous Course of Action (MDCOA)
Operations Security (OPSEC)
Open Source Intelligence (OSINT)
Personnel Security (PERSEC)
Priority Intelligence Requirement (PIR)
Signals Intelligence (SIGINT)
Tactical Questioning (TQ)
Without Rule of Law (WROL)

OSINT

Open Source Intelligence (OSINT) information makes up 80-90% of all intelligence information because there are so many sources and collectors. Every website, news report, magazine article, and speech produces OSINT information. Every Patriot is a sensor, so it's incumbent on us to utilize all these collectors of intelligence information because they make that information so widely available. A good intelligence analyst doesn't have to *know* everything, he just has to know where to find it. The entire internet is our intelligence repository.

From Pittsburgh Tribune:

As intelligence agencies spend billions of dollars on covert programs that sweep up private data, they're neglecting … open-source research… some former intelligence officials say. Some answers that spies hunt are broadcast on blogs, not stashed on hidden flash drives.

I quote Air Force General (Ret.) Michael Hayden, once director of both NSA and CIA, often mainly because he talks a lot in his retirement, but also because what he says matters.

"How much (information) do you have to steal anymore? The answer is a lot less than you used to," said retired Gen. Michael Hayden…

"Stealing information is really important, but we've got to recognize there's so much more information out there," Hayden said.

OSINT collection is an intelligence task that *any* Patriot can do, and ought to be doing.

HUMINT

A few days ago we talked about intelligence requirements. As a quick recap, we create intelligence requirements for information we want to collect. For example, your intelligence requirements might include:

– What threats exist in my AO?

– Identify the strength and disposition of the Leroy Jenkins Gang.

– Identify likely targets for the Leroy Jenkins Gang.

(For new readers, the Leroy Jenkins Gang is the primary threat in this blog's AO… which reminds me: threats don't always have to be kinetic. DIME/PMESII describes a host of other factors – diplomatic, political, military, economic, social, infrastructure, information. Each of these things could pose a threat to your organization or community. That'll be an article for later.)

At any rate, we've identified information we want to collect. The next step is identifying who has placement and access to that information we want, and recruiting them to collect for us. We'll call this our source nomination process. When we analyze potential sources, our first step is to identify their placement and access: what information are they likely to know, or likely able to collect? If we determine that a potential source wouldn't be able to satisfy our intelligence requirement, then he falls of the list for that requirement. So if we're identifying threats in our AO, my list of potential sources would include law enforcement officers, local news reporters, elected officials (city board, county commission, mayor, etc.), and other civil service workers. A law enforcement officer might not know about potentially weak bridges and other infrastructure, but the county engineer likely would. If there's infrastructure in need of repair or upgrade (a bridge, electrical grid, etc.), while it's not a kinetic threat, it might pose a threat to future operations and I want to know about it.

MICE/RC factors specifically refer to Human Intelligence (HUMINT) collection and source recruitment, but they apply to all realms of influence. When we discuss HUMINT collections, whether it's tactical questioning (TQ), interrogation, or source operations, we should consider our sources' motivating factors. Whether we're direct questioning a witness after a firefight (TQ), attempting to elicit information from a detainee (interrogation), or recruiting a source with unique placement and access to information we want (source operations), we will do so in light of MICE/RC motivating factors. It's rare that we can just directly ask for information, or task collection, without giving something in return. In MICE/RC, we offer tangible goods, feelings, problems, and solutions.

Material. The traditional MICE/RC factors use Money here; however, since this is for post-SHTF we can no longer consider just 'money'. While money is an option, post-

SHTF there will be a myriad of individuals willing to trade information for material goods that ease their suffering: food, water, medicine, toiletries, firewood, and the list goes on. This is essentially a negotiation but don't promise anything you can't provide. If you recruit a formal source and you task that individual to get involved in and collect on the Leroy Jenkins Gang in return for moving his family into your community (protection), then be sure that you can follow through. One downside to the Material motivator is that individuals may fabricate information in return for payment. When sources begin to question their usefulness – say, after they've been exhausted of intelligence information – it's time to consider their recourse: what will they do to continue keeping the rewards coming? If you suspect that they're fabricating information, then it's time we stop dealing with that individual. Not only is it a waste of time and resources, but continued meetings with them no longer justify the risk. Another downside is the law of diminishing returns. As an individual accepts more risk in order to collect information for you, the more they may want in return. Is the *potential* collection worth their desired reward? Are they asking more than you can deliver? It bears repeating: follow through on your promises. You might burn more than just yourself.

Ideology. The Soviet defector in 1989 who provides US intelligence with information on the Soviet nuclear program or air defense systems. A neighbor who calls the police and then you to report that your house is being broken into. An employee of a three-letter agency who reports a deliberate and malicious trend of spying on innocent Americans. (Just look at how Snowden burned NSA because his ideology was stronger than his fear of reprisal.) These are examples of source reporting based on ideological motivations. We share the same ideology, and we want all Patriots to be safe and protected from threats and unconstitutional activities. In a post-SHTF environment, there will be known or unknown Patriots in positions of authority, and with placement and access to sensitive information. We want this sensitive information, so we might play to our shared ideology. Our first step is to identify these people, and then identify which of our intelligence requirements they might meet. A sheriff's deputy and Oathkeeper might be willing to tell us that the County Sheriff doesn't believe that the Second Amendment applies to all citizens. This deputy just answered an intelligence requirements- threats in the AO – because the Sheriff is now identified as a threat. Or maybe, hopefully, the deputy tells us that the Sheriff has plans to physically resist any regime attempt to outlaw and confiscate personal firearms. In either case, we're told this because we've convinced this deputy that both of us are on the same ideological side, and because the deputy understands that this information is beneficial to the populace.

Compromise. Think of compromise in this case as leverage; it's the whip as opposed to the carrot. *We know you're having an affair, so vote No at the next meeting or we'll tell your wife. We know you're skimming money on those contracts, so collect this information for us or we'll turn you in.* Yes, this is blackmail and/or extortion but it's an ugly reality of the spy world. HUMINT handlers and those involved in source operations find good reasons to motivate individuals who are unwilling to collect, and compromise can be a very powerful motivator. I would urge caution, however, because a potential source's ideological beliefs may be stronger than the fear over their compromised

situation. In this case, or any others, our potential source could explain his situation to his superiors without our knowledge, and we could find ourselves at considerable risk the next time we meet with our potential source. Death is a reality, and so are criminal charges. In any event, the collection should always justify the risks, and that's a determination you have to make, especially when attempting to leverage a source who has compromised himself.

Ego. We might run approaches called Pride/Ego Up and Pride/Ego Down. Pride and ego are universal feelings, and we play to both high and low levels of each. A potential source might enjoy the feeling of pride when he collects for us because we encourage him and shower him with some praise. Maybe he doesn't get that in his work, and will continue to collect for us because we enable that emotion. Pride/Ego Down in source recruitment is just the opposite: instead of playing up a source's ego, we're playing it down. These people might be willing to collect for us to prove their own authority and power, especially if we call into question their own importance. We might introduce a monetary reward in this manner: *We don't believe that you can get us that information because you're not that important to the organization… but if you can prove to us that you have that amount of power then we can do this for you*. We could collect on seemingly innocuous topics like strength and disposition, leadership, personalities, and biographical information, or if we turn Pride/Ego Down into Material, then we could utilize both motivators and have him produce more important information.

Revenge. Some would argue that revenge falls into ideology, but I include it as its own motivator. This is the wife of a husband who beats her, or an employee of a company who wronged him. Individuals out for revenge can be critically detrimental to an adversarial organization (and to friendly organizations by the same logic). We identify the individual out for blood against the Leroy Jenkins Gang, and then we play on his desire for revenge and direct that anger/hatred to achieve a positive development for us. The downside here is the loose cannon, who is initially responsive to tasking but over time considers his own goals more viable or beneficial than ours. Assessing the source who's out for revenge is a critical part in planning his collection. If you suspect that you're losing control over a Revenge source then you have two options: use him up or let him go.

Coercion. This is my least favorite in the MICE/RC spectrum but it can be a strong motivator. As opposed to compromise where we utilize a pre-existing fear, with coercion we are creating a justified fear. *Get us the contents of that report, or you'll come home to an empty house. Plant this bug in your boss's office or we'll kill you*. We are coercing a source's cooperation through threats of force and violence. I don't recommend this in general but understand that it's used, especially by nefarious actors. It might even be used against you.

MICE/RC presents us with a wide range of options when attempting to recruit sources. A good deal of planning and research on a potential source will yield the benefits of knowing which motivator you should use, and motivators should be used only in order of most effect. Your source may not be motivated by money as much as he is ideology; ego

as much as he is compromise. Keep in mind that sometimes the greatest motivation for collection is a combination of MICE/RC factors.

BESTMAPS Information

When we approach Intelligence, it's important to consider the full spectrum of relevant information. Errors of omission are still errors. Collecting some information is good; collecting as much relevant information as possible is better.

So when we consider Intelligence collection at the community or county level, we ought to be methodical and thorough in our generation of Intelligence Requirements and tasking/directing collection. To do that, we use a the acronym, BETSTMAPS. You must incorporate the BESTMAPS acronym in your Intelligence Preparation of the Battlefield/Community.

We start with **Biographical**. Biographical information includes names and identities, education and work history, familial relationships, and geographical and other associations. It's how we learn about the key human terrain in our Area of Operations (AO). Remember, there's physical terrain – things like mountains and rivers – and there's the human terrain. The human terrain includes the demographics, as well as those who influence and how they influence our AO.

Next is **Economic** data. What are the economic drivers in your AO? What needs to keep working to keep those in your community working? How will fuel rationing affect your local economy? How will a bank holiday affect your local community? These are some really good Intelligence Requirements that fall under the Economy, that you'll need to answer.

After that, we find **Sociological** information. Do members of your AO belong to a specific identity? Are they overwhelmingly hard-working and independent, or are they dependent on government hand outs? Are they religious? Are they kind and friendly, or abrasive and exclusionary? How do they segregate themselves, and along what lines what lines are they self-segregated? We're using this information to better map and understand the human terrain.

Transportation & Telecommunications is part of our critical infrastructure. Transportation includes primary and secondary roads, and other lines of drift. How will the infamous Golden Horde or mobs/looters reach your town or community? Which routes are available to them to get to your home? Telecommunications looks at lines of communication, and I'd include public WiFi in this section. It may be important for you to communicate anonymously through the web, and public WiFi is a great facilitator.

Military Geography includes military installations and facilities, as well as police and other security stations. We're talking about geographical locations here. Be sure to map these locations in your AO!

Armed Forces would be the Table of Organization & Equipment of military and police units in your AO. How many units are in your area, what types of units are they, how are they manned, how are they staffed, and what equipment do they have? The same goes for your local law enforcement – how many sheriff's deputies are in your county, how many of them are on duty/patrol at any given time, what areas do they or do they not patrol, etc. Pretty good idea to take a look at this stuff, if you haven't already.

Political is traditionally strictly political, but in our day and age, we really ought to be adding those who influence politics, to include civic organizations. You can include civic organizations under Sociological, as these organizations influence the populace, but you could also include that information here, where appropriate. We need to look at current political leaders on the local level – how are they influencing the populace and your AO? How do they affect security in your AO? How will future or proposed potential efforts affect your AO?

Lastly, we arrive at **Science/Technology**. You could include critical infrastructure like energy, power plants, and water treatment facilities here. We also know that technology can be disruptive, checking the box on one of the four threat categories (Disruptive). How can technology disrupt your security, the populace, or your AO?

BESTMAPS is a really great tool to help you flesh out your Intelligence collection/analysis capacity. It helps us consider topics that we may not have considered, and gives some structure and organization to all the Intelligence information we need to collect and analyze.

BICC/E Analysis

In the past week, we've touched on the BICC/E analytical method. It's best used for developing enemy courses of action (COA). So if a key assumption is that we'll be dealing with irregular threats like gangs, mobs, and criminals, or more conventional threats like regime forces (DHS, federal LEOs, military), then developing potential COAs, including the Most Likely Course of Action (MLCOA) and the Most Dangerous Course of Action (MDCOA), are going to be absolutely critical for your own security.

While we're on the topic, let's talk Early Warning for a second. If you've read this blog for any amount of time, then you should know that good intelligence analysts recognize 'indicators'. A very simple example would be the combination of you purchasing tickets to Disneyland and then filling up your vehicle with fuel. Combined, it's a good indicator that you might be heading to Disneyland in the near future. But maybe you purchased them as Christmas presents for someone else, and you filled up your vehicle because it was nearly empty. In that case, we continue to look for indicators to confirm or deny your COAs, until it can be confirmed or denied. This is a continual process for COAs.

Indicators as early warning work the same way for you as they do for the regime analyst. It's incumbent upon you to build a collection network, and target potential indicators for use as early warning. For instance, recruiting a homeowner who lives near a National Guard armory or regional airport would potentially allow you to receive information about an increase in personnel, equipment, or activity at these places. Post-SHTF, a couple Abrams tanks being delivered to the National Guard Armory is a pretty darn good indicator that they're going to be used, if needed. They'll be a critical factor in your area of operations (AO), so it's a good idea to be in a position to learn that information as early as possible.

Back to BICC/E, this acronym ('bicky') stands for Behavior, Intent, Capabilities, Consequences/Effects. This is a start to finish method of looking at current activity, known or suspected goals, ability to achieve those goals, and the consequences or effects of achieving those goals.

Behavior.

Judging behavior isn't always as simple as it sounds. I blog regularly about the necessity of setting up networks, practicing good security, and collecting and analyzing information of intelligence value, but you have no way of knowing whether or not I do these things in real life. And if you're practicing good security and staying off the radar, then your behavior isn't raising any red flags and your intent is still unknown, even if you're actively building networks and collecting information. Similarly, if we know that the Leroy Jenkins Gang (LJG) is our adversary, but we can't identify who they are (identities – names, nicknames), much less associate them with known events like criminal activity or attacks, then we really can't accurately judge their behavior. We know they exist but we can't pin anything on them, therefore we can't identify their behavior. And if we can't identify their behavior, then we can't disrupt their operations

or planning cycle. Judging behavior can be problematic but not altogether impossible. That's what makes deep and active intelligence gathering efforts so critical.

But once we're receiving information, maybe from law enforcement or the victims, then we can develop a baseline of what this group is doing. Are they more concerned with common criminality and survival through robbing targets of opportunity, or are they engaged in turf warfare with local law enforcement or community security teams? Their behavior is likely to telegraph their intent.

Intent.

What are the goals of the adversary? What's he trying to accomplish; what's his intent? Answer what he's doing today in order to answer what he's going to do tomorrow and beyond. This is where we develop all potential COAs. If the LJG is robbing homes at gunpoint, then their MLCOA is probably going to be to continue what they're doing. (If so, then we need to speak with the robbery victims and learn what happened to them, step by step. This will allow us to identify indicators — maybe the victims say that they saw the same car drive by multiple times before they were robbed, or maybe all the victims are robbed on a specific day of the week or at a specific time. We identify indicators, then patterns, and then we exploit them.)

We have to judge their intent as best we can, so it will probably be helpful to list out all possible intents, and then pare that list down through the process of elimination based on the other BICC/E factors. The more information we've collected on the LJG, then the better we'll understand them, and the better we can make informed judgements about them. Don't be afraid to add a level of probability or confidence in this assessment. If my assessment is that the LJG's intent is to survive, and Leroy Jenkins doesn't want to become a warlord or mafia boss, then I can attach a HIGH or MEDIUM confidence to that statement based on my confidence. That's what I think, given what I know. Just because today we have a HIGH confidence in that statement doesn't mean that tomorrow we can change our confidence, or change the statement altogether in light of new information. The important thing is that we made the best judgement possible so we can continue the BICC/E process.

Capabilities.

This all goes back to collection. What's our assessment as to the capabilities of the LJG? On the front end, what is their strength and disposition? What equipment do they have? How many robberies a week are they capable of? Are they capable of attacking harder targets such as police stations or military checkpoints? The LJG carried out three robberies per week for the past month, and then only made one robbery in the past two weeks. Are they running out of ammunition? Have they sustained casualties? Have their capabilities changed? Tracking adversary capabilities is a continual process, and should be updated per changing conditions in their strength, disposition, equipment, or tactics, techniques and procedures (TTPs).

Once we spell out their current capabilities, go back to their intent, or what you believe to be their intent, or your list of all possible intents. Use your assessment of adversary capabilities to determine which goals or intents are within the realm of possibility, regardless if the possibilities match their actual intent (you'll need this list for developing COAs).

Consequences/Effects.

Now that we have our list of possible (or suspected/known) intents, for each intent brainstorm some possible consequences or effects. For instance, if the intent of the LJG is to continue robbing area homes, what will the consequences and effects be? Increased household security, increased awareness, possible kinetic targeting of the LJG, and/or security patrols. Develop all possible outcomes for all the intents, then go back through and select the most realistic or most likely consequences and effects; some intents may have multiple outcomes depending on varying conditions or situations.

Now that we have the consequences and effects for each intent, decide which consequences and effects will be detrimental to the LJG. For instance, if one intent is to continue robbing area homes, and the consequences are that security will be increased, then we've identified a timeline for how long the robberies will continue. They'll continue until the security presence is significantly increased. If it takes a month to spin up a quick reaction force (QRF), or patrols, or community watch, then the robberies will likely last for a month. Now we've just used some analysis to produce accurate (we hope), specific, timely, and predictive intelligence.

Intent versus COA.

I've used intent and COA numerous times in describing the BICC/E analytical method. They're different things, so let me explain just to be clear.

Intent is the overall goal, whether it's a near- or long-term goal, whereas COA is literally their course of action to achieve their intent. If it didn't make sense, I hope it does now. We're going to use the possible intents (as determined by the BICC/E factors) to develop possible adversary COAs.

COA Assessment.

Based on my knowledge of the LJG, I've developed two possible intents: 1) To continue to survive and subsist off the bounty of targets of opportunity; or 2) To clear, hold, and control the area for their own gain. So let's develop some COAs based off this information.

COA#1: The LJG continues to rob area homes until the security apparatus becomes too saturated to carry out operations.

COA#2: The LJG continues to rob area homes until the area is depleted of soft targets, regardless of any increase in the security situation.

COA#3: The LJG continues to rob area homes until they meet significant physical resistance, or suffer losses to operational strength.

COA#4: The LJG will begin to include murder and intimidation to their operations in order to clear, hold and control the area.

COA#5: The LJG will begin recruiting poor youths in order to increase their combat strength.

COA#6: The LJG will begin clearing and holding individual homes to use as bases of operations.

Now we go through our COA Matrix (IPB: Determine Threat Courses of Action), and then identify the MLCOA and MDCOA. Given what I know about the LJG, namely that they're risk averse and lack combat skills, the MLCOA is COA#1, and the MDCOA is COA#4. The most likely COAs are now ranked: #1, #3, #2, #5, #6, then #4.

Once we've ranked the COAs, then we continually assess those COAs against new information to confirm or deny those COAs. In this instance, what do you think are the early warning indicators for the MDCOA? Two that immediately come to mind are recruiting new members and sourcing weapons and ammunition. Even though murder and intimidation are uncharacteristic of the LJG, my knowledge of the gang's leadership could also inform me of changing TTPs. Leroy Jenkins just wants to survive; he doesn't want to kill anyone. But his #2, Mad Dod Jackson, is ruthless and spent time in prison for murder. I know that another early warning for the MDCOA is if Mad Dog Jackson gains influence over or takes control of the gang's operations.

Judging Single Source Information

I briefly took part in a discussion on WRSA a week or two ago about the topic of *single source information*. Single source information, as opposed to multiple source information, is readily available but in many cases difficult to analyze or verify. With multiple source information, the more people reporting the same information, the more indicators we have that the information is true, or is at least being *reported* accurately. Specific pieces of nearly identical information that come from multiple sources corroborate themselves, so to speak. If all four local news broadcasts say that a woman murdered her husband on 15th Ave last night, then I can make a snap judgement that it probably happened… or at least that all four news outlets are reporting accurately what they were told by police. I have four corroborating sub-sources (news outlets) from the same source (police).

Single source information, on the other hand, comes from one source; it's one guy or one news outlet reporting information that can't be found anywhere else. There's likely to be limited to no availability of information to corroborate what our source is saying. Similarly, there may be limited or no time with which we have to reach a decision based on that information. This time-sensitive, single source information manifests itself in the real world through an anonymous tip that the suspect is in a white sub-compact headed north on Backalackadacka Street. Or that the regime security forces regional-coordinator in charge of overseeing gun registration/confiscation is meeting with local leaders at city hall. In some cases, we may have a very short window of opportunity to act. If our assumption that the information is true, then *how fast can we get a Pred to find and hit the car*, or *how fast can we mobilize local FreeFor security elements to disrupt the meeting*?

Our ability to quickly analyze single source information is critically important, so let's go over a checklist that allows us to make inferences quickly about the veracity (re: truth) of the information. Keep in mind that this is a cumulative checklist; the failure of one category shouldn't indicate a failure of reporting accurate information.

Reliability (Source).

Is the source of the information reliable himself? Forget momentarily what he's telling you, and give an honest assessment of how reliable he is as a source of information. If we know this individual, is he someone that you'd trust with your children? Can he be trusted to do the right thing? What are his motivations for passing you this information (MICE/RC)? Has he reported reliably in the past? If he's communicating this information second-hand, then who is his source, and is his source reliable? If at all possible, inquire about the source of this information: *who told you this*, or *how'd you get this information*? Remember that just like the game telephone, the longer the line of sources and sub-sources, the more we have to assume that the information has been modified, or that pieces of the information have been accidentally omitted. Approach his reliability from multiple angles: maybe you don't trust him with your children, but he's

reported reliably in the past. Be objective, not emotional, regardless if you like or dislike this person.

Plausibility (Content).

Is the information plausible under any circumstance or just this one? Could this information be true? Plausible: your county sheriff receiving an MRAP. Implausible: your county sheriff receiving an F-22. Knowing whether something is plausible or implausible dictates that you have a working knowledge of the subjects involved. Scrutinize the plausibility of the information even you if you believe it's plausible at first.

Proximity.

What is the source's proximity to the information or original source? Does he have placement and access to the original source? I'd trust information much more if it came from someone who has continued access to the original source. A cab driver in San Diego who passes me sensitive information about the White House isn't in physical proximity to the original source. In and of itself, lack of placement and access — proximity — to the source of the information raises red flags for me.

Appropriate.

Is it appropriate for this information to come from this source? It would be inappropriate for the cab driver in San Diego to be providing such protected information. It wouldn't be appropriate for him to know that information. How would he know in the first place, unless he a) had a long chain of informants leading back to the White House; or b) had a direct source in the White House. Even under option b, why would such a trusted person from the White House be passing information to a cabby on the other side of the nation? On the other hand, if a White House attorney was telling me information, then it would be appropriate for him to *know* that information, but inappropriate for him to *tell* me that information (unless I was running him as a source).

Expectable/Consistent.

Did we expect this information to be made available? Did we expect this information to come from this source? Is this information expected based on what we already know? In other words, is this information *consistent* with what's already been or being reported? More leaked NSA information being published by the mainstream media is expected. Leaked NSA information being first published by your county's weekly newspaper is highly unexpected.

Support

Do other sources corroborate or come close to corroborating this information? Does what we already know about the subject lend the single source information any

credibility? For instance, hearing that WalMart struck a deal with the makers of RaspberryPi, and will carry 100 RaspberryPi's per store location, would certainly be intriguing. Yes, WalMart has an electronics section and they carry a few electronic gadgets, but a) there wouldn't likely be a market for the RaspberryPi's, and b) they wouldn't likely be ready to sell an item that could undercut many of their other electronic offerings. In this case, because there's no evidence that supports the single source information, I would remain doubtful.

Conclusion.

Should you so desire, you can make a matrix of these six categories and grade each piece of information by how it stacks up. A simple check mark will suffice, however, you may want to assign a grade of 0-3; 0 being no support and 3 being the most support.

Either way, this checklist should give you a good idea of the strengths of certain information, or where it falls short. To reiterate, just because a piece of information does poorly in many or most categories doesn't mean that the information is inaccurate. It just means that it's less likely to be true, or that factors contributing to its veracity aren't readily available or apparent.

Intelligence & Probability

We've previously covered that the four factors of valuable intelligence information are timely, accurate, specific, and predictive. Once we've collected information and analyzed it to create a finished intelligence product, we absolutely must present that information (which is timely, accurate, specific, and/or predictive) in a clear and concise manner. What good is producing great intelligence if the impact or scope of our message is lost through poor communication?

One of the ways we effectively communicate is by assigning probabilities or levels of confidence in our work. In addition to clearly communicating the likelihood of an event, or the confidence we have in our assessment, assigning probabilities also allows you, the analyst, to cover yourself in case you're wrong. We will likely want to avoid using words like always (will) or never (won't).

Because at the heart of intelligence analysis is creating knowledge – synthesizing pieces of separate or loosely-related information to create a deeper understanding of an organization or individual, or to project future activities of the adversary – we generally encounter situations where the information we have is fuzzy or conflicting, so our confidence in our assessment likewise suffers. To quote my old, well-respected section chief, "*You don't always have to be right, but you can never be dead wrong*." There will always be things that we know we know, things that we know we don't know, and things that we don't know we don't know, which means that there will be times that you are wrong. Just don't be dead wrong.

In the case of intelligence analysis on the battlefield, sometimes we're required to make snap judgements with little to no time to prepare, and with little information surrounding the situation. We rely on our understanding of the adversary as a baseline on which to make those decisions. As the intelligence element of a resistance, militia, prepper group, or community defense team, you may find yourself in a similar situation. When we use words like *always, never, will, or won't*, we put ourselves into a corner. If I tell my commander that a compound of a follow-on raid *won't* have an improvised explosive device (IED) in the doorway, but a soldier in my company is killed when he steps through the door, then not only have I irreparably damaged my reputation as an analyst, but I have *directly contributed to getting a fellow soldier killed*. My failure to accurately predict an event or hazard — or deny it's existence in this case — ultimately led to the adversary's success. The ugly truth of intelligence analysis is that sometimes we just get things wrong, but other times we get things dead wrong. Now the doorway IED is just an example (and maybe a poor one) but there will probably be parallels (not involving IEDs) in post-SHTF/WROL/EROL (without rule of law / extreme rule of law) intelligence analysis.

Now that we covered that, despite what I just told you, sometimes it's okay to use 100% or 0% probability. There's a 100% probability that I'm typing on an electronic device right now (as of writing this). There's a 0% probability that I scrawled this post on an etcha-sketch. These things we know, but when we don't know something, it's okay to

just say we don't know. Instead, we offer what we think along with an assignment of confidence or probability. The most typically used levels of **probability** are:

Likely – ~80+%. We have a high confidence that the sun will rise tomorrow; the sun is likely to rise tomorrow. The president is likely influenced by Marxist ideology. We might call anything in the 90% range *highly likely* or *highly probable*. You might also say that you have a high confidence in an event occurring, or course of action taken.

Probably – ~51-75%. There are *probably* automatic weapons in the drug cartel meeting. You might say that you have a medium confidence in this possibility.

Possibly – ~25-50%. *Possibly* is less 50/50. It's *possible* that Obamacare will be de-funded after 2014. The Leeroy Jenkins Gang *might* target civilians as a part of their intimidation campaign.

Unlikely – 20% or less. The president is *unlikely* to fix the nation's economy. It's unlikely that my dad will purchase a vehicle tomorrow. In other words, there's less than a one in five chance of this happening (which is appreciable). You would have a low confidence in these things happening.

Part of the problem with these predictions of revolution, or collapse, or civil war is that they are most often assigned very high likelihoods within a certain period of time, and then don't end up happening. Instead of coming true, they just rile people up, and get them more scared. I need to write a list of failed predictions in the past year; Infowars is especially destructive in publishing unfounded predictions, and yet people continue to flock to those sites to read more shock information. Let me tell you, **predicting the future is a hard way to make a living** (unless you have no intention of being correct). Most people are dead wrong all the time. Another gem of wisdom from a former branch chief is, "The more extreme the prediction, the less likely it is to be true." That's typical of many, if not all, doom and gloom predictions, but I digress.

Most will assign probability from a gut feeling but that's not a very scientific, academic, or methodical approach, even if they turn out to be correct. We have to consider a myriad of factors when determining the probability of an event. I'll write another post on determining probabilities, but for now, consider a few main factors: intent, ability, and consequences. What's the likelihood that you'll rob a bank today? Pretty low because of the consequences, even if your intent is to acquire more money and you have the ability to attempt it. What's the likelihood that you'll rob someone today? Pretty low for hopefully all of you because even if your intent is to acquire more money, and you have the ability, the consequences would be a disaster for your moral values and consciences.

Some predict that Iran will nuke Israel. Well, they might, but that would spell the end of the Iranian regime right now. So where does that leave our probability? Pretty low, in my estimation. Mutually assured destruction is not a favorable outcome. On the flip side, what's the likelihood that Israel will strike Iranian nuclear sites? It's certainly a possibility but I won't say that it's likely *right now,* yet people have been predicting

exactly this for the better part of the past decade. I don't and didn't work at the Israel desk, so take my opinion for what it's worth.

Intelligence Cycle (New Black Panther Party)

The reason we use the steps of the Intelligence Cycle is to ensure a methodical approach to solving a problem. (The problem in this case is our Primary Intelligence Requirement (PIR): **What threat does the NBPP pose to my community?** I can't answer that question right now, which is why it's an intelligence requirement.) Without the Intelligence Cycle, we skip steps or make errors of omission, which compromises our data and understanding of the problem, which invariably causes us to perform good analysis of poor or incomplete data, which causes us to provide a poor intelligence product, which causes our people to die, or we kill the wrong bad guys, or it negatively affects our national security or foreign policy objectives. In your cases, it negatively affects the understanding of your Area of Operations (AO), and leads to what's called *strategic shock*. Strategic shock is the result of a strategic threat that you didn't know existed, or a failure to acknowledge the strategic extent of that threat.

When I was a sergeant, I had a really great section leader; probably the greatest CW4 the intelligence community has ever produced. I haven't spoken with him in years but it would be nothing short of an American tragedy if he hasn't/didn't make CW5. He was invaluable to me in so many ways, and I really feel badly for everyone in the intelligence community who was not lucky enough to study intelligence under his tutelage. Here's one of the mottoes he taught me, and one that you need to write down and commit to memory: **Using perfect logic on inaccurate information will lead your perfect logic very, very astray.** If we can't define exactly the information we're looking for, then our ability to collect the most accurate information is greatly diminished. That's why we perform the *Planning, Requirements, and Direction* phase of the Intelligence Cycle.

Think of the Intelligence Cycle like visiting a doctor when you are ill. He doesn't start prescribing you medicine without first checking you out. He first identifies the problem: what are your symptoms? Then he creates a list of possible diagnoses, and he refines that list through further testing until he's able to make an accurate diagnosis. My observation is that he uses a process similar to the Intelligence Cycle.

Everyone needs to download the Intelligence Cycle photo attached to this post and follow along as I explain each step of the Intel Cycle.

PHASE ONE: Planning, Requirements, and Direction. In this phase, we planned the workflow of our intelligence operation (or exercise). As the Analysis and Control Element (ACE) Chief, I receive a task from the commander, or I recognize a problem and, using the commander's intent, begin to plan and direct for a new threat or new development. After planning out the workflow with my team, we begin generating intelligence requirements for the information we don't know. We simply ask questions and write them down. During this phase, I'm directing my team to complete tasks as necessary. In the NBPP exercise, I planned the workflow, had potential participants email me and assigned them to a team, and then directed their next steps, which was to generate intelligence requirements.

PHASE TWO: Collection. In this phase, we task out collection. Within the intelligence community, many (if not all) means are at our disposal. We may task out a Human Intelligence (HUMINT) element to collect information in order to satisfy our intelligence requirements (re: answer the questions that we made); or we might task Signals Intelligence (SIGINT) or Imagery Intelligence (IMINT) elements to answer the rest of our questions. In the NBPP case, we're using Open Source Intelligence (OSINT) to collect information about the NBPP *based off our previously generated intelligence requirements*. It's certainly the case that as we learn more about our adversary or other topics of interest that we need to generate new intelligence requirements. The generation of intelligence requirements is itself a persistent requirement: we can't afford *not* to adapt to new or changing information.

PHASE THREE: Analysis and Processing. In this phase, we either collected all available information, or collected all available information within the time constraints provided. (We may have an operation starting next week, in which case the intelligence cycle is time-sensitive; we have to do the absolute best we can with the time we're given.) So after we have our information, we begin analysis. We look at our information through our FACT Filter™ (Feasibility, Aptitude, Consistency, Timeliness), and assess the information for accuracy. Once we've identified which information is likely to be true (we may never know if something is actually true or not) then we conduct our analysis, and create a more complete picture of the threat.

PHASE FOUR: Production. In this phase, we create a finished intelligence product. We should have our analysis completed in a way that it can be clearly and concisely (effectively) communicated. Our finished intelligence product could be a white paper, a powerpoint (aaaaaah!), or a time-sensitive verbal briefing. (If I'm given thirty minutes to prepare to brief the commander on the effects of actioning the leader of the Sheikh Ubudi cell, then I'm certainly not going to waste my time with a powerpoint presentation.) In the NBPP exercise, our finished intelligence product will most likely be a powerpoint converted to PDF.

PHASE FIVE: Dissemination. In this phase, we send our finished intelligence products to those who requested it. In the NBPP exercise, our finished intelligence product will be disseminated to as far as we can send it: to III%, Patriot, and prepper sites (and to whomever has an interest in reading it). There may be further questions as the result of our intelligence product, or we may be tasked in a new direction or given a different mission to support, in which case we start all over at PHASE ONE.

Hopefully that gives everyone a better understanding of how we develop our intelligence operations as they pertain to collection and analysis.

Because our NBPP Intelligence Requirements are due tomorrow, I figured that this would be a good time to share an example of some REALLY GREAT work from a member of the STRATEGIC team. He can identify himself if he so chooses; otherwise it's best to maintain some level of anonymity. The intelligence requirements he generated will follow:

What are the political goals of the NBPP leadership? (Are any running for office or operating in consulting or organizing capacity?) What is the nature of the relationship between NBPP and Nation of Islam (NOI)? Does the NBPP have any other strong relationships with fringe groups? What is Paris Lewis' (aka Malik Zulu Shabazz) current function within the NBPP after stepping down as National Chairman? Is the NBPP leadership actively advocating violence to achieve the groups ends? Are they doing this via public or internal communications? What level of influence does national leadership have at the chapter level?

For those who still owe me intelligence requirements, use this as a baseline to jog your creativity. This is brainstorming, so if you think of an intel requirement then submit it. We may scrap it, or it may generate an idea that we use to form a new intel requirement that we keep.

Intelligence requirements

Discussions of intelligence collection should revolve around the understanding that all collection is directed. That is, your 'control' – in this case, the Analysis and Control Element (ACE) *that everyone should be building* – directs your collection efforts through *intelligence requirements*. These are requirements… you are required to answer them as a part of a grand strategy to analyze the threat or operating environment, or plan for future operations. Requirements are generated from higher, almost always as part of the commander's intent (protecting the populace while ridding the AO of gang elements, for example). As an intelligence collector, you are a taskable element being tasked by the ACE. Be intimately familiar with the ACE's intelligence requirements so that you can answer them.

Under the heading of intelligence requirements, we differentiate between Primary Intelligence Requirements (PIR) – the things we need to know *yesterday* – and all other intelligence requirements. PIRs should reflect the commander's critical information requirements (CCIR) which, as the name implies, are pieces of information the commander considers to be critical. PIRs should receive priority attention because they are our *primary* requirements.

For instance, our PIRs and IRs might look something like this:

PIR 1: What threats exist in our AO?

PIR 2: What threat activities occur in our AO?

PIR 3: What targets are the threats likely to attack?

IR 1: Define the threat operational tempo.

IR 2: What is the strength and disposition of the Leroy Jenkins Gang?

IR 3: Identify the leadership of the Leroy Jenkins Gang.

IR 4: Identify the facilitation/logistical networks of the Leroy Jenkins Gang.

IR 5: What locations are associated with the Leroy Jenkins Gang?

So on and so forth. These are our requirements that we must answer through collection, whether it be Human Intelligence (HUMINT – including surveillance and reconnaissance) or Open Source Intelligence (OSINT), or whatever other means are available.

We can think of intelligence requirements as goals, and generating requirements as goal setting. We set goals to gather information, and then we achieve them.

Generation.

An intelligence requirement is an intelligence gap. We identify a piece of information that we don't have, or a question that we can't answer – literally, a gap in our intelligence – and then the ACE generates an intelligence requirement for it. For instance, in a post-SHTF scenario, one intelligence requirement might be, *What threats exist in our AO*? If you're new to generating intelligence requirements for your AO, then that would probably be a good example of a PIR. Intelligence requirements should aks a question, or identify a specific piece of information. (*What are the threats in our AO*, or *Identify the threats in our AO*.)

In this case, the requirement meets our four criteria:

- Necessity. Is our intelligence requirement necessary? Yes, it's necessary because these elements pose a threat to our security and livelihoods. Identifying what they eat for breakfast is not a necessity, unless they're eating Wheaties. In that case, I'd want to know so I can heighten our security. Remember: all our intelligence requirements compete for a limited amount of time and resources. Time spent collecting one piece of information is time spent *not* collecting another. If an intelligence requirement is not a necessity then scrap it. You likely won't have the time or resources to answer it, anyway.

- Feasibility. Can we feasibly collect this information? Yes, we can feasibly identify the threats that exist in our AO. They may be gang or criminal elements, or corrupt law enforcement (and maybe both). Feasibility isn't just what's technically possible; it's what's possible according to your collection capabilities. Yes, it's technically possible to identify what the gang leader ate for breakfast, but it's not likely to be feasible considering your limited capabilities.

- Timeliness. Is our intelligence requirement timely? Yes, identifying threats in our AO is an enduring requirement that we must continually seek to answer. If we're planning a reconnaissance patrol on Monday ten clicks north of town, then the intelligence requirement is useless on Tuesday. The ACE should be included in future operations planning for the express purpose of two things: providing IPB and mission/threat analysis, and for generating intelligence requirements to inform the commander of pertinent information.

– **Specificity**. Is our intelligence requirement specific? Yes, our requirement is specific because it's limited to our AO. Aksing *When will the enemy attack and where?* offers two very vague questions and isn't an ideal intelligence requirement. It's not very specific, and much harder to answer. We want our requirements to be answered with satisfactory information, so we must make them easier to answer.

Intelligence requirements should continually be reviewed in the context of our criteria. If the requirement doesn't meet our criteria, then it needs to be updated, refined, or removed.

Management.

You may generate only a few intelligence requirements, or you may generate dozens depending on your optempo and AO, among other factors. We need a way to organize our requirements, and manage the information collected that satisfies our requirements.

What I propose are two very simple methods.

- Enumeration. Perhaps the easiest way to track our requirements are to simply number them. This method works best when dealing with fewer requirements. PIR #1, PIR #2, PIR #3, PIR #4, and IR#5, IR# 6, etc. Intelligence collectors, when sending up information, should identify which requirements have been satisfied by the collected information. This can be accomplished as easily as writing each answered requirement in parentheses at the end of each paragraph of information.

EXAMPLE: According to Source A, the Leeroy Jenkins Gang (LJG) moved into town during late August 2013. The LJG uses two primary locations. 123 Main Street is used as a headquarters, and 456 Commercial Avenue is used both as a meeting place and drug distribution center. (PIR#1, IR#5)

- Nomenclature. When dealing with a larger list of intelligence requirements, it may be helpful to assign both a digraph and number. (A digraph is a set of two letters.) For instance, if you're interested in corruption among law enforcement organizations, your requirement might be named "LC1000". L stands for law enforcement, and C stands for corruption. LC1000 is a series that might refer to the top level of an organization, whereas LC2000 is the series reserved for middle management, followed by LC3000 which represents low level officers. Or you may use LC1000 for all law enforcement corruption-related information. You can be as specific or general as you'd like with your requirements. DA might stand for Drug Activity so DA1000 might refer to drug dealing, DA2000 might refer to drug trafficking, and DA3000 might refer to the manufacture of drugs (or DA could refer to all drug activity information). In any case, label your requirements in a way that both the ACE and collectors can easily identify. The reason I'd consider using a 1000 series instead of just a 1 is to break down the requirement further. Our requirement might be, *Identify all drug activity within the AO*. If there's a considerable amount of information collected, then searching all the information will be made more difficult by throwing it all into one big pot. I'm partial to smaller pots so when I need to look up information about the Chief of Police, then I know exactly the requirement I want: DA1000. Taking our 1000 series one step further, DA1000 might be a catch-all whereas DA1001 is directly associated with the Chief of Police, DA1002 is associated with the Deputy Chief of Police, and DA1003 is directly associated with the top level support staff (Chief's secretary, administration, etc.).

EXAMPLE: According to the Source A, the Leeroy Jenkins Gang (LJG) moved into town during late August 2013. The LJG uses two primary locations. 123 Main Street is used as a headquarters, and 456 Commercial Avenue is used both as a meeting place and drug distribution center. (DA1000, DA2000)

EXAMPLE #2: According to the Source B, Deputy Barney Fife accepts bribes from drug dealers associated with the LJG. Deputy Fife receives a monthly fee of $500, and 7% of all drug profits. In return for the bribes, Deputy Fife allows the LJG to traffic drugs unimpeded, and use of a unmarked police cruiser. Deputy Fife collects the bribe money each month from a LJG distribution center at 456 Commercial Avenue. (LC2000, DA1000, DA2000)

Conclusion.

Intelligence requirements are a critical component of intelligence collection. Identify the types of information you want to know, and then generate intelligence requirements based off these intelligence gaps. This is a relatively simple process that can be as complex and difficult to navigate as you want to make it. Just remember that we want to be both thorough and efficient, so identify the way that works best for you. Efficiency without thoroughness leads to lacking information; thoroughness without efficiency leads to wasted time in analysis.