SHTF INTELLIGENCE

Samuel Culper

AN INTELLIGENCE ANALYST'S GUIDE TO COMMUNITY SECURITY

SHTF Intelligence: An Intelligence Analyst’s Guide to Community Security

About the Author

Samuel Culper is a former Military Intelligence NCO and contract intelligence analyst. He spent three years in Iraq and Afghanistan on various missions including interrogation operations, biometrics and targeting support, and senior-level advising.

He now runs Forward Observer Magazine and teaches the craft of Intelligence to preparedness groups around the country.

Website: https://readfomag.com

Email: shtfintel@readfomag.com

This book is dedicated to the men and women who
endured catastrophe to promote the traditions
of Liberty and private property;
to God-fearing Americans who may
very well endure catastrophe again to save them;

And to the audience of Forward Observer,
without whose support none of this could have happened.

I am deeply thankful for your encouragement and support for what we do.

Contents

Introduction to Intelligence & Community Security 9

Section I
- Chapter One: A Brief Overview of Intelligence 15
- Chapter Two: Understanding the Intelligence Cycle 24
- Chapter Three: Building Your Intelligence Section 36
- Chapter Four: Intelligence Analysis 58

Section II
- Chapter Five: Developing Intelligence Collection 100

Section III
- Chapter Six: Intelligence Preparation of the Community 134

Section IV
- Chapter Seven: Targeting 149

Appendices
Appendix A: IPC / Area Study Example 156
Appendix B: Intelligence Requirements Templates 172
Appendix C: Community Security Strategies 175
Appendix D: Military Intelligence Creed 181
Appendix E: Screening Sheet 182
Appendix F: Operation Urban Charger Data 183

Endnotes 189

Guide to Chapter Subsections

Intelligence Disciplines 20
Intelligence Moves Beyond the Threat 22
Intelligence Cycle Phase One 27
Intelligence Cycle Phase Two 31
Intelligence Cycle Phase Three 31
Intelligence Cycle Phase Four 32
Intelligence Cycle Phase Five 32
ACE Organization 38
ACE Operations 48
Vignette: Operation Urban Charger 52
Subject Matter Expertise 60
Curing Analytical Bias 61
Arriving at Accurate Conclusions 66
Analytic Tradecraft 69
Predictions & Outcomes 76
Intelligence Task and Products 78
METT-TC Analysis 80
Battle Tracking 82
Intelligence Summary 88
Situational Template 90
Order of Battle 90
Table of Organization & Equipment 94
Open Source Intelligence (OSINT) 101
Human Intelligence (HUMINT) 104
Imagery Intelligence (IMINT) 126
Signals Intelligence (SIGINT) 132
Define the Community Environment 136
Describe the Community's Effects 140
Evaluate the Threats 141
Determine Threat Courses of Action 146

Introduction to Intelligence & Community Security

At the heart of Intelligence Preparation of the Battlefield, or IPB as it's called in the Army, is understanding the elements of terrain and how they affect friendly and enemy forces. IPB products are prepared and updated daily around the globe by militaries for their operations and contingencies. They are the bedrock of military operations because they inform the commander and his battle staff of what the battlefield looks like, or will look like. These Intelligence products have historically been built for force-on-force engagements; analyzing the terrain for friendly artillery, tanks and infantry fighting the artillery, tanks and infantry of the enemy.

A battlefield's physical terrain offers advantages and disadvantages to invading and defending fighters, regardless of cause, creed or nationality. The battlefield doesn't choose sides by itself; the battlefield just is. It's the terrain that's the tool and it can be an asset or a liability. Physical terrain like hills, mountains, roads, lakes, rivers, bridges, and buildings can quicken the advance of an army or stop it dead in its tracks.

And it's this incredible utility of best using the battlefield's terrain that has enabled fighters for Millennia to punish larger armies, defend more ground, expedite an invasion, and perhaps most importantly, predict what an enemy leader and his fighting men will do in a given situation.

Military leaders since time immemorial on all sides have exploited these terrain effects to great success or peril. French Emperor and military leader Napoleon Bonaparte was said to have had his aides scour libraries in search of maps and books detailing the foreign lands of his campaigns. Attaining an expert knowledge of the battlefield terrain contributed to his success: of the 60 battles he fought over his career, he won 46 and lost seven.[1] Confederate General Robert E. Lee was commissioned into the U.S. Army Corps of Engineers in 1829. By the end of the Mexican War in 1848, Lee had participated in every major battle, and had provided U.S. Army General Winfield Scott with detailed reconnaissance information.[2] He was a practitioner of terrain analysis and it's part of what later made him a brilliant Confederate commander. T.E. Lawrence, better known as Lawrence of Arabia, lived among the Arabs and he understood the human terrain. That's what enabled him to lead Arabs in a successful guerrilla campaign against the Ottoman Empire.

"If I always appear prepared, it is because before entering on an undertaking, I have meditated for long and foreseen what may occur." - Napoleon Bonaparte

---

But there's another type of terrain that we need to understand as future participants in low intensity conflict. As we survey the past decade and more of American warfare in the Middle East and Southwest Asia, we see a great need to understand not just the physical terrain, but also what's called the human terrain. As opposed to naturally-occurring features or man-made obstacles of the physical kind, the human terrain includes the people, their feelings and opinions, their wants and desires, their languages and cultures and collective histories. When adversaries, especially numerically inferior guerrillas, can take their message to the people, they open up a parallel war. Not only are our adversaries trying to kill the enemy and stay alive themselves, but they also lobby or coerce tribes, groups or individuals for support. This "war of the people" can't be won on physical terrain or by conventional means alone. For as much difficulty as there is in patrolling a remote mountainside, the human elements of those who inhabit it make the fight much more complex. These human factors can lead to making war on the enemy among the people more difficult than is respected or appreciated.

After spending more than three years in Iraq and Afghanistan as an Intelligence Analyst, I can admit the shortcomings of the Army's IPB products in the way of human terrain. Having a poor understanding of the populace is one area that greatly contributed to the enemy's successes in both countries. The local insurgents understood the people and, in many cases, we didn't. We understood the insurgents, but generally not their base of support. The human terrain, just like the physical, can be leveraged. Just like an army leader can force his adversary to fight on unfavorable physical terrain, so can the army leader force his adversary to fight in unfavorable human terrain.

Mao Tze-Tung famously said that the guerrilla should move through the populace like a fish moves through the water.[3] The Army's approach to the wars when I arrived in both countries was largely still to sort through all the water in order to find the fish, when we should have been working with the water to find and expel the fish for us. (Hindsight is often 20/20. There were always voices that supported a populace-centric version of warfare, however, it was not always adopted by battalion leaders.) The Army, as good as it is at killing people, was wholly unprepared to fight a "war of the people" on that scale. The conflicts in Iraq and Afghanistan proved that conflict is already costly and messy enough, but not understanding all the elements of the operating environment makes it more expensive, both in financial terms and in human lives. The years spent playing 'catch up' in that part of the world reignited scholarly and academic approaches to warfare that emphasize sociology and psychology; lessons learned the hard way by the Army every few decades since fighting the insurgents of the Philippine War in the late 19th century. That "parallel war" of tribes and non-combatant populations is much more important than was given credit to by many commanders in the early and mid-2000s.

For as long as IPB has been practiced, it will be practiced into the future. But it's difficult to say just what that future will look like for those interested enough to read this book. Billions of dollars are spent on national defense and intelligence gathering at home and abroad, and leaders and policy makers still don't know exactly what to expect. The world is a big place filled with a lot of people, after all.

And while we - you and I as preparedness-oriented individuals who share an interest in protecting our families and communities - don't have billion dollar budgets, we also don't have to deal with the world, or the nation, or even an entire state. What belongs to you is your home and community. That's your area of responsibility and that's where most of your preparedness time and resources need to be directed. People often don't believe me upon hearing it for the first time, but the fact of the matter is that your greatest and most immediate threats are likely the unprepared folks who already live around you.

> "We expect a great deal from intelligence. We ask intelligence to describe in detail places we have never seen, to identify customs and attitudes of societies fundamentally different from our own, to assess the capabilities of unique and unfamiliar military or paramilitary forces and to forecast how these societies and forces will act in the future. Most notably, we want intelligence to enter the thought process of an enemy commander and predict, with certainty, what course of action he intends to pursue, possibly even before he knows himself what he is going to do."
>
> Marine Corps Doctrinal Publication 2: Intelligence

A very large part of this book is geared towards threat analysis and reducing uncertainty about the future, giving you a realistic expectation of what the future may hold. Throughout the course of this book, we must remember four things:

Rule number one is that this is very much a thinking man's (or woman's) book. It's going to require of you a great deal of mental effort. You will be asked to identify and evaluate threats and form logical conclusions on those threats' capabilities and intent. I highly recommend against "winging " or "eyeballing" it. Measure twice, cut once, as they say. Intelligence analysis is a lot like long distance shooting. What is the chance that, on the first shot and without knowing the distance or windage, a marksman can hit a 750-meter target? Probably not good. But with some experience in shooting long distance targets, and armed with the knowledge of distance and windage, the skilled marksman can consistently hit his target. Before he began shooting long distance, however, he mastered the fundamentals of shooting closer targets. We have to consistently hit the 25- and 50- and 100-meter targets before moving onto targets at longer ranges. And just like in grade school long division, we in intelligence have to show our work. The more we guess, the more room we create for error. But if we're deliberate about finding the right answer, following the right steps and making good judgments, then we're more likely to be successful. Focus on getting the process right and the results will follow.

Rule number two is that no matter what happens, life will continue. If your expectation of the future is a catastrophic event, first understand that you can't predict when it will occur. If it's going to happen, then it's going to happen, and it's out of your control. The best we can do is adapt to its effects and spend our lives to ensure better lives for future generations. A few of the predictions floating around the preparedness community today are so dire and devastating that, if they were to come true, one should seriously consider whether or not life would even be worth living. That brings us to number three.

Rule number three is that the more extreme the prediction, the less likely it is to occur. As of this printing, America is likely to continue its slide in quality of life, perhaps into the Second or Third World. (The Second World refers to the socialist states formerly under the USSR, while the Third World refers to all other states outside the alignment of either the Western and Soviet worlds. Third World states are also referred to as "developing nations" and are most typically marked by very corrupt officials, shorter life expectancies and poorer quality of education for the average subject.) The state of geopolitics being what it is, we may fight another world war; perhaps even another civil war or conflict here at home. Economic "collapse", what I still consider to be the most likely scenario and whether it's by our own government grinding the gears of prosperity to a halt or another government doing the same through economic or cyber warfare/terrorism, is still a series of events. The likelihood that, overnight, everything we have come to know about America suddenly ends is very low. Given any catastrophic event, we're likely to see increases in crime (both at the hands of government and other criminals) and possibly terrorism, even if only regionally; and decreases in the American standard of living. Use that as a starting point and maybe even an ending point when considering the future of your community. The chance of an event that sends this civilization back into the Stone Age, such as an electromagnetic pulse (EMP) within the next ten years, isn't zero, but it's not 50 or 100 percent, either. It's probably not much higher than zero. A 2008 EMP Commission report estimated a die-off rate of up to 90% following the first 12 months after a nationwide blackout. That's a very startling prediction. The level of fear generated by that report alone somehow has not been assuaged, even given the low likelihood of an event like that happening. It's not that we can say that these things won't happen; it's just that they're unlikely to happen. In the event that a very extreme and catastrophic event occurs, I'll refer you back to rule number two.

And number four is that fear is a great motivator but a sadistic master. We can't allow fear and emotional responses to overcome our ability to reason and think critically. And we can't allow fear to rob us of joy and good opportunities in the present. I once had a student back out of an Intelligence for Preppers class I was teaching because it was being held more than 60 miles from where he lived. He was fearful that if North America was hit by an EMP while he was in class, then he couldn't get back home. He decided to miss the class and now he's without the direct knowledge passed to the others who did attend. I hope he reads this book.

I strongly suspect that in a catastrophic event or long-term emergency, we're likely to see various forms of tribalism, whether it's along lines of criminal activity like gangs, familial or ethnic ties like clans, or ad hoc organization where multiple small threats become one larger threat… a lot like the organizations we saw in Iraq and Afghanistan. And just like in those countries, Intelligence information was a lot more than just about the physical terrain. And so was born Intelligence Preparation of the Community.

While I don't know exactly what America will look like in another two or five or ten or twenty years, I do know that the likelihood of being prepared for an emergency is much higher for those who put these words into action. I wrote this book to educate Americans about a small slice of Intelligence work and to inform the Patriot and Prepper communities that Intelligence can be — must be — incorporated into their preparedness plans. Understand that volumes have been written about Intelligence, and many more will be written into the future. This is not a comprehensive Intelligence manual; neither is it a replica of U.S. Intelligence doctrine. I've taken elements of this doctrine and applied them to a community-centric approach to Intelligence. I've taken Intelligence Preparation of the Battlefield, the Army's answer to understanding the battlefield through Intelligence, and created Intelligence Preparation of the Community, or IPC. This book describes this comprehensive IPC process through which you can increase your community security and overall preparedness.

As Former United States Marine Corps Commandant General Charles C. Krulak famously instructed, I want this book "to equip the man, not man the equipment."[4] In order to help equip you, I've created a "To-Do" list at the end of each chapter where you'll find a list of homework or "due-outs" that concisely spell out each of the tasks you'll need to accomplish.

It's my intention that after studying this book - reading it once for familiarization and again for retention - you:

- are enabled to gain information superiority and become an expert on your community;

- are enabled to identify threats before they arise;

- are able to stand up a community intelligence section capable of producing threat intelligence;

- are able to produce Intelligence Preparation of the Community (IPC) products;

- and are able to teach others about the IPC process.

Without completing an IPC product, it's nearly impossible that people in our community will be able to accomplish all the security requirements above. If you read and do not complete the process, then you will find yourself in a similar security shortcoming. Doing IPC isn't fast or easy but it has to be done now while information is still cheap and simple to obtain. During an emergency, the information you need to survive will come at a premium.

Section I - Building An Intelligence Element

Chapter One: A Brief Overview of Intelligence

Learning Objectives:

- Understand the great need for intelligence
- Understand what intelligence is and is not
- Understand the different intelligence disciplines
- Understand how intelligence can be used in the community

If the lights went out tomorrow – if some catastrophic event occurred, perhaps the event for which you are preparing – then the only thing more important than determining the cause is the ability to anticipate its effects on our community. A cyber terror attack that disables portions of the power grid for 12 hours is going to produce much more different conditions than the persistent effects of a viral epidemic. In addition to the physical and financial effects, there will be psychological effects that might be felt into the next generation (9/11 or the Great Depression, for example). Myriad catastrophic possibilities exist, so it's difficult to say just what a collapse scenario would look like; however, we can take an educated guess. Although less likely, it's entirely possible that we could see grid-down conditions that lead to full societal collapse; or a more likely but partial collapse caused by any number of triggers; or what's most likely: simply a very quiet devolution of the American quality of life (which we're already seeing) where we slip into the second- or third-world. No matter the cause, one thing that Intelligence does for us is that it allows us to reduce uncertainty. [5] It makes little sense to prepare for a highly unlikely event, when we can establish scenarios that are more likely to occur based on an examination of the facts, instead of on a gut feeling or fear mongering.

One of the largest problems facing our prepared communities is the condition of being the least-most prepared. You probably know someone who falls in that category. These folks have the most preparations – the most stored food and water, the most medicine, the most firearms and ammunition – but are actually among the least prepared for the future. They may have have tons of gear but no clue how to use it; or they may be a small island of preparedness in a bottomless sea of needy families. Either way, all their preparations are less likely to sustain their family and more likely to sustain whomever capitalizes on their lack of preparedness.

This rhetorical argument illustrates the folly of being the least-most prepared: let's say that in the next 24 hours, the residents of your home will experience a catastrophic event. We could prepare for a fire by putting a fire extinguisher in each room, but they will do us no good during a hurricane. We could prepare for an earthquake by retrofitting our home to the highest safety standards, but it would do us little good during a flood. We could arm each of our family members in attempts to survive a Golden Horde scenario, but good luck surviving a fatal epidemic with all those guns. Although might be seen as counterintuitive, preparing for every scenario is actually making us much less prepared for any scenario. Very few of us have the time and resources to prepare for every threat, but that's exactly what many of us are doing. Even if we had the resources, we'd be spreading ourselves too thin by preparing for all scenarios, even those that are highly unlikely. So the million-dollar questions are, before we begin to prepare, for what exactly are we preparing, and are we prioritizing our preparations according to the most likely threats? How can we determine between a likely scenario for our area and an unlikely one? All these are questions best answered through Intelligence collection and analysis.

The people who fall into the category of the least-most prepared may have all the "stuff" but they still have lots of uncertainty. They haven't started to answer the million dollar questions above for themselves, and they haven't critically examined why they think the things they think. In all honesty, they are probably preparing for the events of which they're most afraid instead of preparing for the events that are most likely to affect them. They're the residents of the home who are preparing for an unknown event either by preparing for everything or by preparing for the wrong things. They don't know when it's going to happen; they don't what it's going to look like; they don't know how it will affect their home and community; they don't know what threats will be posed to them; and they don't know the sources of these threats. Having all the stuff does us little good if we haven't identified and don't understand the threat we're facing. And when we don't understand the threat, we make ourselves extremely vulnerable to strategic shock; that is, being exploited by a threat we didn't know existed or for which we weren't prepared. In one sentence: your stuff is useless to you if you aren't prepared to defend it, and you aren't prepared to defend it if you don't know how it's going to be threatened.

So we in the preparedness community have to examine our immediate surroundings first. It's very unlikely that a biological attack is going to directly affect you, because the footprint of that attack is very small. It's very unlikely that martial law is going to directly affect you, because the requirements for imposing martial law are so large, even in small areas. Do the math: there just aren't enough State or Federal forces to span the entirety of the United States. (For every 1,000 U.S. citizens, there are less than seven military personnel[6]; and fewer than three U.S. law enforcement personnel[7].) Martial law is more likely to occur in confined areas, especially in larger cities. On average, chances are good that those areas won't include where you live. So what's much more likely is that the second- and third-order effects of these events are going to affect you. It's our job as Intelligence analysts to identify those effects and describe how they will affect our homes and communities.

Immediate threats are going to come from the immediate vicinity. We start with those who are most likely to directly affect us: our hungry or otherwise needy neighbors. Through Intelligence, we begin to look at our communities and suss out which individuals or households are likely to be in need, therefore identifying potential threats to community security and/or stability. These threats to security and stability aren't necessarily violent in nature, but certainly retain that potential.

Understanding global trends and worrying about financial collapse, Ebola, and other causes of unrest is a poor replacement for understanding your community environment. During a SHTF event, when faced with an immediate threat – a threat on your doorstep, for instance – you're going to care a lot less about what caused the unrest in your community, and a lot more about how to deter these threats by networking with your neighbors to build resiliency and security. That means that we should focus a lot less time on the cause of any event, and a lot more time on the effects of those events. We can't predict with any certainty what's going to happen or when it will happen. We *can* predict with some certainty how the various causes of instability will affect our community, and understanding this first will enable you to be among the best prepared.

I think the proverbial "nine meals from anarchy" is an adequate initial description of any SHTF event. That idiom describes the length of time between a disruption in public services and logistical systems, and empty grocery stores being the least of your worries. [8] The higher the population density, the shorter that window becomes. The more the people, the greater the need. How your living conditions are affected may vary greatly in any scenario, but the critical need for threat intelligence will stay the same. It doesn't matter whether you live in Star Valley, Wyoming or on Staten Island, New York; you will need threat intelligence as part of your day to day survival.

One thing that separates those who are least-most prepared and those who are best prepared is access to early warning information and threat reporting; in other words, access to timely information in order to produce Intelligence. Regardless of the trigger event and your community environment, you're going to find yourself in one of two situations:

1) You're not going to have enough information to make timely, informed decisions; or
2) You're going to have so much information that you will be unable to find enough accurate information on which to make those timely decisions.

If I were a betting man, my money would be on the former for many in the preparedness community; at least until you've finished this book, in which case I hope that you find yourself somewhere in the middle. All other things being equal, the latter of the two is the better situation. With some knowledge and practice with the tools available – the tools I describe in this book – you should be able to manage.

KEY TERMS:

Intelligence – information having been triaged for accuracy and then analyzed; meets the needs of timely decision-making.

I*ntelligence Information* – raw, unrefined and unverified data

Intelligence can do a lot for us. Before we get into *how* to incorporate Intelligence into our preparations, we have to cover some bases. First base is the difference between *Intelligence* and *Intelligence information*. If we imagine a thousand-piece puzzle, then each puzzle piece is a separate piece of Intelligence information. It's not likely that I could examine one puzzle piece and accurately describe the contents of the whole puzzle. But as we begin to put the puzzle pieces together – first the edges and working our way in – then we begin to see the whole picture. We're combining different pieces of information to get a better idea of the whole picture. Now we're dealing with Intelligence.

All Intelligence is information, but not all information is Intelligence. In other words, hearsay or the Internet rumor mill is decidedly *not* Intelligence. Information doesn't become Intelligence until it's checked for veracity (truthfulness) and produced as finalized Intelligence. And only one type of person can produce Intelligence: the Intelligence Analyst. There's good reason why nations don't act on information; they act on Intelligence. Information is subject to the whims of its originators and not necessarily to the harsh grind of reality. Ultimately, finished Intelligence should be that harsh grind of reality.

Intelligence provides the Who, What, When, Where, Why and How of the battlespace. We as Intelligence Analysts are the fuel filter in a highly functioning engine; the fuel being Intelligence information itself. The Intelligence gatherers are the gas station attendants, to use a crude analogy, constantly pumping information into the tank. Without that Intelligence information, the machine doesn't have the fuel to accomplish the mission. Without a filter, inaccurate information is pushed into the engine, so it's our job as analysts to ensure that we're running on the highest-octane information available. And without our Intelligence, the driver of our machine doesn't know where to go. Each player has a critical role in Intelligence; whether it's collection, analysis, or the pointy end of the spear receiving the Intelligence.

Second base is that Intelligence answers, "So what?" A news report of a train wreck is just a puzzle piece. As we begin to put numerous puzzle pieces together, we may find out that several train cars have spilled chlorine. Further, we find out the spill's location. The next question is, "So what?" How will it affect you? Until now, we've just been dealing with Intelligence information, but when a chemical expert comes on the air and says that the maximum affected range is two miles (for instance), now it's Intelligence. The local emergency management people have verified the contents of the spill, examined its relation to the environment, and know enough about the properties of chlorine to make a forecast or projection. Without that subject matter expertise, the rest of us would be left wondering if we were in immediate danger. Having lots of data is great, but without an expertise and understanding of the relational context of the information; the information alone is often insufficient.

There's a reason why the Central Intelligence Agency likes to recruit candidates based on expertise and experience, rather than just an ability to do anything else. Someone who grew up in Syria and who speaks flawless Arabic can be turned into a spy more easily than a native English speaker can be turned into a Syrian. The best Russian analyst in the U.S. Intelligence Community, no matter how skilled he is at Intelligence analysis, would not do much good were he placed in an office covering West African tribes and warlords. He no longer holds an expertise and is now at a grave disadvantage. Two paragraphs summed up: become an expert on your community.

Third Base is knowing that good Intelligence should be five things: timely, relevant, accurate, specific, and predictive or actionable. In my experience, accuracy and timeliness are next to godliness. The availability of an accurate Intelligence report doesn't matter if it's too late to inform decision-makers. There's a cutoff for when consensus must be reached or a decision made. Information that comes after a decision is made, after the effort and resources are given direction, is useless. As Intelligence Analysts, we should always strive to produce this greatly needed Intelligence before it requires action. We don't have the luxury of knowing if the Intelligence we've produced will become necessary an hour or a month from now, but we should have it when we need it. That requires a lot of foresight; a lot of strategic, one-step-ahead sort of thinking. Still, chances are good that a small Intelligence element like the one you build for your community or prepper group will be so busy tackling today's problems, that anticipating and producing for tomorrow's will be diffficult. But no matter what problems we're working on, the Intelligence we produce must be timely. For instance, if an Army unit was moving to secure a village in Afghanistan on Tuesday, producing Intelligence on Wednesday would be of lesser value, perhaps no value at all. Before beginning a project, ensure that you know what's called the Latest Time Intelligence of Value, or LTIOV. That's the cutoff date for when our Intelligence is no longer relevant, so be sure to beat the clock.

Intelligence is relevant. After all, that's part of what separates it from the white noise of information. If we aren't producing Intelligence that's relevant to the mission, then we're simply wasting time and resources. In our cases, the mission is providing for community security. So that means that the farther we get away from our community, the less relevant most information is likely to become. Spending less time oscillating on global or national events (the triggers) and more time understanding the effects those events will have on the community, will produce large dividends for our levels of preparedness.

Intelligence should be accurate. As an Intelligence analyst, it doesn't take long to make a name for yourself, good or bad. Providing accurate intelligence is predicated on a few things, most notably of which is subject matter expertise. One takeaway you should get from reading this book is that the ability to think rationally and critically, and speaking and writing clearly, is of the utmost importance. Analysis without critical thinking is often poor analysis. We must also be able to think logically and rationally. Remember that what's rational to us isn't always rational for an adversary. That's why we have to get inside the enemy's head and think like he things. The last ingredient in our accuracy recipe is having accurate information to begin with. Driving directions that include making the first left, the second right, and then the first left, seems fairly straightforward as long as the correct starting point is also identified. When I was a sergeant, I had a really great section leader; probably the greatest Chief Warrant Officer (CW4) the intelligence community has ever produced. He used to say to new analysts, and I've committed it to memory: Using perfect logic on inaccurate information will lead your perfect logic very, very astray.

Intelligence should also be specific. When everything we do is time-sensitive; when our guys our out on patrol or when you've identified a threat in your community, we need to produce the most clear and concise Intelligence possible. No one has time to come back for clarification. There's a large difference between saying that there's gang activity around Shady Dell Park and saying that there are eight gang members using Shady Dell Park as a staging area for robberies. We have to be specific as possible with everything we know. The more we're able to convey quickly to our action arms, the more prepared they can be to bring security to the area.

Intelligence Disciplines

An intelligence discipline is a category of intelligence available for collection; we might also call them "types" of intelligence. Although there are many types of intelligence generally available, especially to those organizations with billion dollar budgets, we at the community level are likely to have a very limited number. The more we can access, the better off we are. In fact, our ability to produce good intelligence may be directly related to the types of disciplines we can make available. For your awareness, I'll cover the entire list of major disciplines, beginning with the first four that are most likely available to us. (Information on how to collect intelligence through these four disciplines is available in Chapter Five.)

<u>Open Source Intelligence (OSINT)</u>, most often referred to as the most underutilized and under appreciated type of intelligence, is often the most widely available. According to the U.S. Intelligence Community, 80 or more percent of all intelligence information globally comes from open sources. OSINT includes things that are openly broadcast, like television or radio news reporting, magazines and other publications, and most of what can be found on the internet. In fact, with a few caveats, Google can be one of our best facilitators of intelligence information. Although not often highly considered, local events like town halls, city council meetings, and political gatherings can also be considered OSINT. Because it's the most available, OSINT should become one of our top collection priorities.

<u>Imagery Intelligence (IMINT)</u> is information derived from maps and photographs. Maps of our communities and broader areas are an example but we're also going to include geospatial information software like Google Earth, ArcGIS, FalconView, or any number of free, open source tools available on the web. IMINT allows us to visualize physical terrain and its geographic layouts without having to expend the time and resources to travel to these places. Lesser considered IMINT sources could also include full-motion video from traffic or security cameras, as well as drones. IMINT can carry with it some limitations, such as old or outdated map data; however, it is an indispensable source of the intelligence information we'll need. More recently, Geospatial Intelligence (GEOINT) is being used to describe information about environmental factors; the physical attributes of the physical terrain. Whereas IMINT captures what the physical

terrain looks like, GEOINT could describe factors like soil composition and density ("Is the ground of this open space capable of supporting a staging area for heavy equipment?"), and climatic and environmental effects on the physical terrain ("Does this area flood?" or "How much snowpack will there be in February?").

Human Intelligence (HUMINT) is intelligence information derived from human sources. Through HUMINT, we can gain access to information that we could never gather on our own. The dramatized spy films, for instance, where CIA or MI6 case officers leverage and recruit foreign nationals to infiltrate criminal or terrorist organizations are a great example of the use of HUMINT. For our purposes, we'll focus more on localized collection from cooperative and witting sources.

Signal Intelligence (SIGINT) is derived from signals, including from communication devices like cell phones and the internet. You may have heard that it's used to target terrorist leaders around the globe. From the jungles of Columbia and the Philippines to the deserts of Iraq and Yemen to the mountains of Afghanistan and lots of places in between (including your hometown), the U.S. Government's intelligence agencies rely heavily on the use of SIGINT. Through even very rudimentary capabilities, we can leverage this Gold Standard of intelligence collection to provide early warning, through a subset of SIGINT called Communications Intelligence, or COMINT.

Technical Intelligence (TECHINT) involves physical components or descriptions of them in order to understand the technology or engineering behind them. TECHINT data includes the technical aspects of foreign weapons, vehicles, equipment and and material. These weapon systems may be acquired and reverse-engineered, or other disciplines can be used to collect the technical data; however, understanding how any piece of technology works plays a critical role in an ability to counter it.

Measurement and Signature Intelligence (MASINT) is derived from ambient environments where any component emits a noise, vibration, signature or other disturbance. MASINT includes air and ground radar and acoustic detection. Metal detectors, for instance, may identify buried land mines based on metallic signature. And unmanned ground stations are able to identify vehicles based on their noise or vibration signatures.

There are other, smaller intelligence disciplines and subsets of these disciplines, however, these are the most common. Although we'll discuss how each can play a role for us, we'll focus the core of our energy on developing collection for the first four: OSINT, IMINT, HUMINT, and SIGINT (or COMINT). Standing up a basic collection capacity for these disciplines doesn't require a technical ability or sensitive, specialized equipment. In most cases, we can begin collecting intelligence information from each of the four by the end of the day.

Intelligence Moves Beyond the Threat

So much of Intelligence is threat-based. Directly from the Army's Military Intelligence Creed, our job is to "… find, know, and never lose the enemy." But it really goes farther than just the need to identify and track threats. Unlike war several decades ago where nations were pitted against each other, much of conflict around the globe today involves civilians; non-combatants. French Emperor Napoleon Bonaparte is widely credited with uniting the three branches of national warfare: the government, the military, and the people. Similarly, during World War Two, this nation saw the American workforce get involved with industrial production that by 1942 dwarfed any other nation in the war. But these where times when militaries enjoyed the luxury of largely being the only people on the battlefield. Today, whether it's the Taliban in Afghanistan, various Shia and Sunni militias in Iraq, the Islamic State across the Middle East, Boko Haram in Nigeria, or the numerous insurgencies of the Philippines (and we're leaving out dozens, potentially hundreds of other small conflicts), much of warfare is centered around the populace. These conflicts are population-centric, and so will be the conflicts of a post-SHTF environment. A battlefield crowded with civilians is an army's nightmare and a potentially a guerrilla's paradise. Average people are simply a part of most battlefield's today. We call this the human terrain – the people with needs and desires and opinions who make up the surrounding populace – and it's imperative that we learn how to use the human terrain to our advantage, because if we don't utilize them, then our adversaries will use them. Understanding the human terrain, then, is critical for several reasons; and the same reasons apply to you they apply to any military analyst.

Understanding the environment in which we live – including both the physical and human terrain –comes under our purview. A great use of our time is getting to know who our neighbors are, who holds influence, who is influenced, and how our community works. The better we understand our community, the better we can predict how it collectively responds to an emergency, how it will respond to a potential threat, and how it will respond to our desire to bring security to the area in which we live.

Should you experience a SHTF event, there are going to be people – and probably lots of them, depending on the scenario – who will find the end of their pantry just before going out to search for food. Unless you can't see your neighbors, it's a safe bet that well within 72 hours, someone in your community will be in need.

Without having been attuned to the problems we face as a nation and without having learned so much from so many in this community, I certainly would be in the same position as many Americans. My life would have resembled the average American's, consisting of working (or voting for a living), playing video games (or watching cat videos on YouTube), and being a pop culture, cable television reality show glutton. This is the state of many Americans, although many are 'waking up' and coming around to seeing the likely instability of the future. But what's possibly worse than all this, is that many Americans simply don't know their neighbors and have no sense of community. It's said that no man is an island; well, no household is, either. Surviving even simple threats requires teamwork at the community level. It's said that the learning curve of combat is vertical. Well, without networks developed in the community now, surviving even simple threats will exhibit a much steeper learning curve as well.

According to a 2010 Pew Research poll, nearly thirty percent of American adults didn't know their neighbors names and the same amount only knew some of their neighbors. [9] A 2014 poll of Britons found that a third of them couldn't identify their neighbors in a photo lineup[10], and I can only imagine the number has to be in the same ballpark here in the States. Frankly, this is a shared failure of the community members.

If we fall into either of these categories, then we have a significant problem. Were it not for being introduced into the prepper community, I wouldn't know my neighbors. I wouldn't know their occupations or the names of their family members. And my neighbors wouldn't know or recognize me in the community, much less on my own front door step. Somewhere in that window of three days without electricity, you might have an unknown community member approach your home.

If a stranger were to approach my home, I would have no way of knowing if he was a friendly community member out checking to see why the power was off, or a potentially violent individual out and about because his family is out of food. Or maybe this individual approaches your neighbor's home. The chances that my next-door neighbor could differentiate between the two scenarios would be slim, too. But if we knew most or all the people in the community, differentiating friend from foe would be much, much easier. Believe it or not, knowing the people in our community and building rapport with them is a function of Intelligence. Whether or not you realize it, we're collecting information about these people and making informal judgments on their disposition and how they're likely to act during an emergency. The guy who lives two doors down is a firefighter. Or maybe he's a drug dealer. Without learning about him, you simply won't know, nor will you have the opportunity to meet and read him; a step which would be contributing to your own security.

Without Intelligence information, we're going to be at a severe disadvantage. That severe disadvantage is simply unacceptable because it's preventable. The bad news is that many people will potentially find themselves in this bad situation, but the good news is that it doesn't have to be this way.

Chapter Two: Understanding the Intelligence Cycle

Learning Objectives:

- Understand the OODA Loop
- Understand each phase of the Intelligence Cycle
- Understand the generation of Intelligence Requirements
- Understand ways to quicken the production of time-sensitive intelligence

A fighter pilot by the name John Boyd (Col., USAF, Ret.) was first to describe the process by which a human makes sense of his surroundings and decides on a course of action. He called it the OODA Loop, which is an acronym that stands for Observe, Orient, Decide, Act (OODA). The first step in this process is to Observe an event or environmental factor. Let's say that you're driving down an interstate and you Observe the near simultaneous brake lights of several cars ahead. You're going to Orient yourself to this observation by informally judging the distance between you and these vehicles and recognizing that you may need to brake your vehicle as well. You'll likely Decide that you need hit the brakes if you want to avoid a car crash. This decision has come about as the result of the first two steps, Observe and Orient. If you had not Observed and Oriented yourself to the situation, you After the decision is made, you will Act by applying pressure to the brake pedal in order to avoid a car crash. This is the four-step process by which humans examine their environment, make a decision, and act (or react).

Typically when we're discussing the OODA Loop beyond an initial description, it's in reference to either increasing the speed of our own decision-making processes, or disrupting the OODA Loops of our adversary; thus slowing down his decision-making processes. Both of these concepts are directly related to Intelligence. If we were to survey our OODA Loop and apply it to the Intelligence Cycle, we'd find that without Intelligence collection, we can't Observe; and without Intelligence analysis, we can't Orient. If our organization, whether it's an Army unit or a community security team, can't observe and orient ourselves to changing conditions in the battlefield or community, then we greatly increase the risk of mission failure. This is the absolute value of Intelligence.

In order to speed up our own decision making OODA process, we need to Observe events as quickly as possible. The sooner we can see or hear about an event or changing battlefield condition, the sooner we can begin to Orient, and then Decide, and then Act. The longer it takes to Observe and Orient, the slower our organization will come to a decision and act.

In Intelligence, Observing and Orienting are typically two separate tasks completed by two separate groups. We have the Intelligence Collectors who Observe (and report) and the Intelligence Analysts who receive these reports and Orient (or analyze). If we view our ACE as the brain, then we're going to need to feed that brain with information. Intelligence Collection, therefore, is represented by our senses, constantly receiving raw data from the operating environment and transmitting this data to the brain to be analyzed. The cooperation of Intelligence Collection and Analysis is best described by something called the Intelligence Cycle.

We're likely to continually suffer from a lack of time and resources, in and out of SHTF environments. The only way we can make up for a lack of time is to become more efficient at what we do, and the only way we can make up for a lack of resources is to identify which areas will require the most from us, and prepare to prioritize ahead of time. In this section, we'll discuss the Intelligence Cycle, which is going to help us become more efficient, thus saving time, and how to anticipate our requirements, which will maximize the efficacy of what resources we do have.

There are five steps of the Intelligence Cycle and it's important to understand a few things about it; the first of which is that the Cycle is on-going. We begin with the receipt of mission, and only cease our activities upon completion of the mission, which in our case would be a return to normal living conditions. The second is that there may be numerous and simultaneous loops inside the Intelligence Cycle for various missions or security needs.

The reason we use the steps of the Intelligence Cycle is to ensure a methodical approach to supporting the mission. Without the Intelligence Cycle, we skip steps or make errors of omission, which compromise 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 can result in friendly casualties, in killing the wrong guys, or in negatively affecting the understanding of our Area of Operations (AO), which could lead to strategic shock.

Think of the Intelligence Cycle like visiting a physician when you are ill. He doesn't start prescribing you medicine without first asking you questions and taking some diagnostic measurements. He first begins to identify the problem by asking about your symptoms. Then he creates a list of possible causes, 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. He ask you a few questions that are designed to elicit responses that give him clues as to your illness. Then he performs some analysis based on your feedback, then he identifies a course of action. The course of action is a Operations problem, which is separate from Intelligence. We in Intelligence don't concern ourselves with making the decisions; we just provide the Intelligence to leaders who then make decisions. But for our part, like physicians, we begin by asking questions — what we call Intelligence Requirements — so that we can direct collection.

Just like your visit to the physician begins his mission of curing you, so does our work begin with a visit or direction from a commander. We receive a mission from our leadership - maybe it's neutralizing a threat like the Leroy Jenkins Gang or humanitarian assistance to our community after a flood - and we get to work providing Intelligence support to that mission. That begins with Phase One of the Intelligence Cycle.

KEY TERMS:

Intelligence Gap - information that we don't currently know, but need to know; literally a "gap" in our Intelligence holdings.

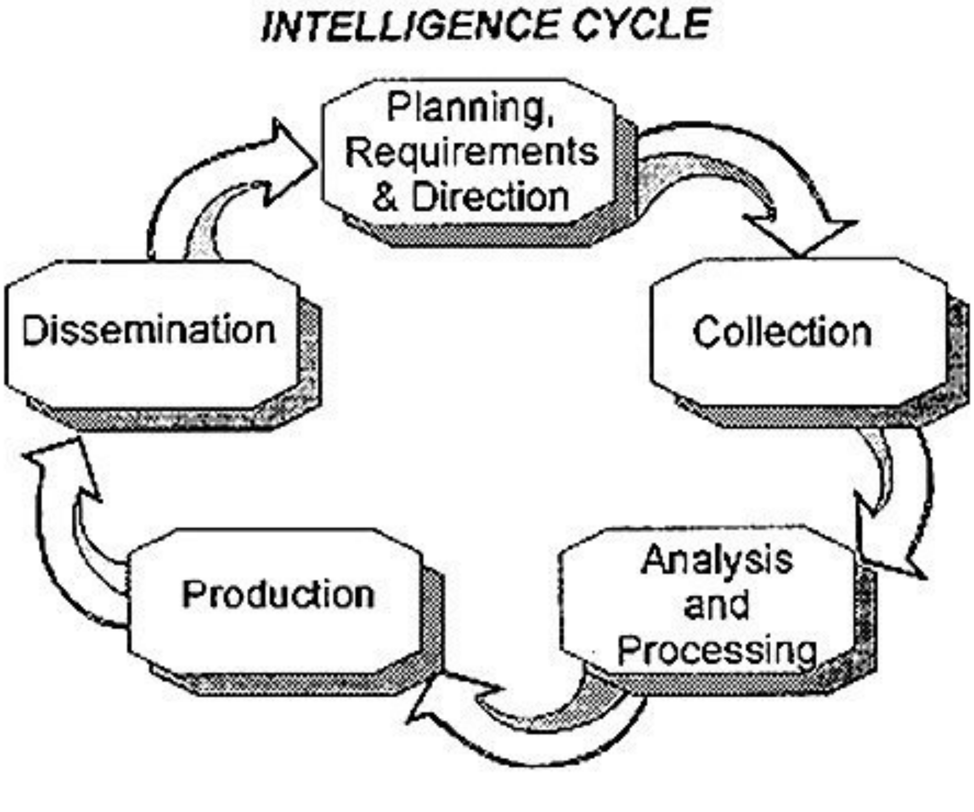
Intelligence Requirement – a question or statement that clearly describes an *Intelligence Gap* in order to direct collection of Intelligence information.

Enduring Requirement - an Intelligence Requirement that needs to be monitored and updated through a certain date or time.

Ad Hoc Requirement - an Intelligence Requirement that supports a specific event or only needs to be answered once.

Analysis & Control Element – the ACE is the central Intelligence element where analysis is conducted on gathered Intelligence information.

Area of Operations – referred to as the AO, this is your community or any area where you anticipate activity.



PHASE ONE: Planning, Requirements, and Direction

In Phase One, we plan the workflow of our intelligence support to an operation. We receive a task or mission from the commander, or recognize a new threat or development in the community, and begin to plan and direct for that new threat or new development. We begin generating Intelligence Requirements for the information we don't know. These are requirements... Intelligence Collectors are required to answer them as a part of a grand strategy to analyze the threat or operating environment, or plan for future operations. It's our job as Intelligence Analysts to generate these requirements.

There's likely to be a lot that we initially don't know. In the case of the Leroy Jenkins Gang, we might begin by asking some questions about the members of the gang, how many there are, where they are, and what they've been doing. In the case of a community flood, we might begin by identifying what areas have been affected and which have been unaffected, asking which members of the community have been affected and which have been unaffected. These are all Intelligence gaps.

For our purposes, generating Intelligence Requirements isn't difficult; we simply ask questions and write them down. An Intelligence Requirement is an Intelligence gap, or something we don't know, stated in the form of a question or statement. 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 holdings – and then the ACE generates an Intelligence Requirement for it.

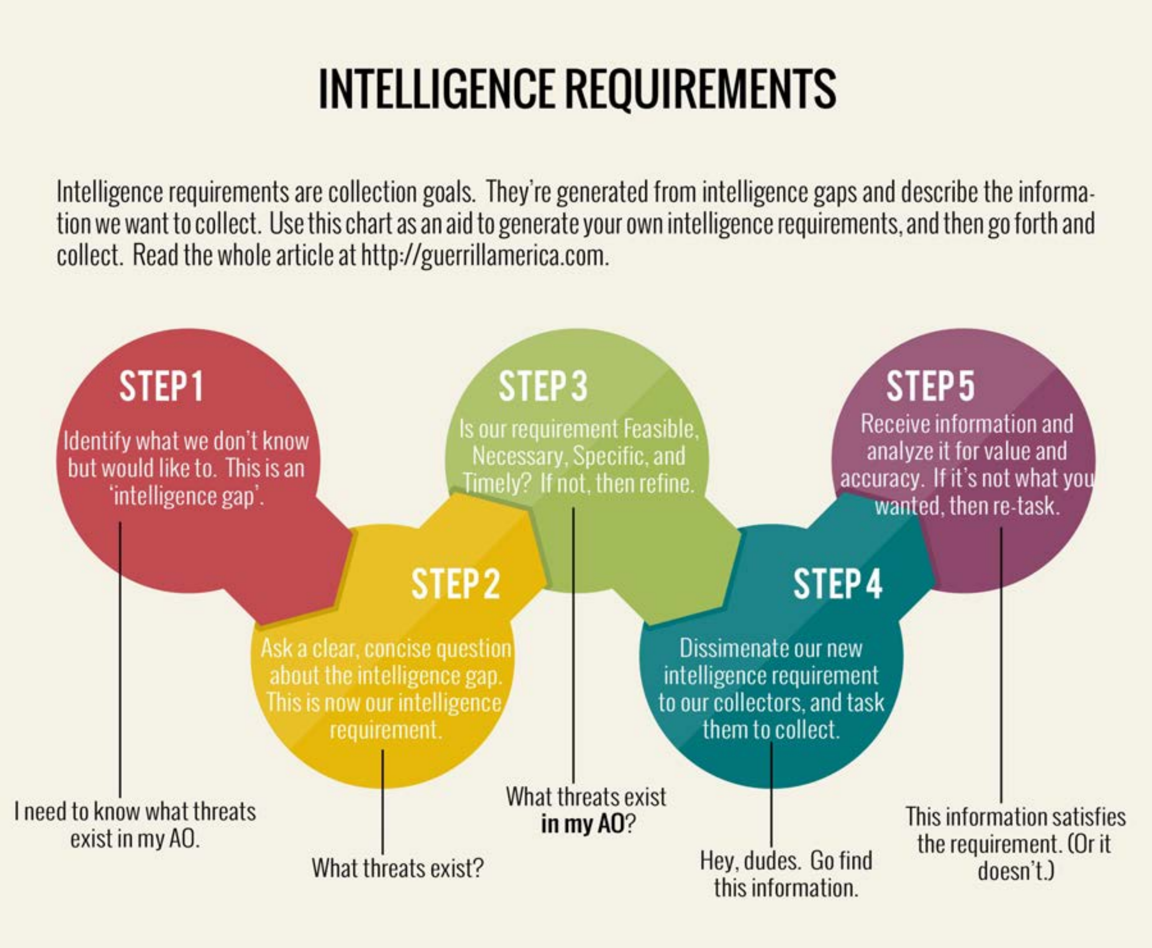
Generating Intelligence Requirements is the first step and they must be considered before any collection begins. Members of the ACE support the mission and there's information that we absolutely need to know in order to do our jobs. It's our responsibility, therefore, to direct collection so Collectors and their sources can provide us with this vital information. Without knowing what information to target, our Collectors might provide us with information of no Intelligence value. That makes us less efficient and degrades our ability to support the mission, so it's very important that we generate good Requirements. It's the responsibility of Intelligence Collectors to target and develop sources that produce the information we need. That's their job, but that doesn't happen without them first receiving our requirements and direction.

In a post-SHTF scenario, a few Intelligence Requirements might be:

What threats exist in our AO?
What is the size and strength of the Leroy Jenkins Gang?
Identify sex offenders who live in the AO.
What areas in our AO will be affected by the flood?

If you're new to generating Intelligence Requirements for your AO, then these are great examples you should copy (just substitute 'Leroy Jenkins Gang' for any criminal organization or activity in your area, and 'flood' with any other natural or man-made disaster. You will find dozens of pre-made Intelligence Requirements in Appendix B in the back of this book.).

The four example requirements above meet our four criteria for good Intelligence Requirements. Remember that time and resources are likely to be at a premium value, therefore, we must be clear and concise with how we relay information. No Intelligence Collector or fellow Analyst will have time to seek clarification for what you meant or intended. The importance of an ability to think, speak and write clearly can't be understated.



INTELLIGENCE REQUIREMENTS

Intelligence requirements are collection goals. They're generated from intelligence gaps and describe the information we want to collect. Use this chart as an aid to generate your own intelligence requirements, and then go forth and collect. Read the whole article at http://guerrillamerica.com.

STEP 1

Identify what we don't know but would like to. This is an 'intelligence gap'.

I need to know what threats exist in my AO.

STEP 2

Ask a clear, concise question about the intelligence gap. This is now our intelligence requirement.

What threats exist?

STEP 3

Is our requirement Feasible, Necessary, Specific, and Timely? If not, then refine.

What threats exist **in my AO**?

STEP 4

Dissimenate our new intelligence requirement to our collectors, and task them to collect.

Hey, dudes. Go find this information.

STEP 5

Receive information and analyze it for value and accuracy. If it's not what you wanted, then re-task.

This information satisfies the requirement. (Or it doesn't.)

The following four criteria form the rubric for forming clear and concise Intelligence Requirements.

Necessity

Are our Intelligence Requirements necessary? *Yes, this requirement is necessary because the Leroy Jenkins Gang poses a threat to our security and livelihoods.* Identifying Vladimir Putin ate for breakfast yesterday is not a necessity. All our Intelligence Requirements compete for a limited amount of attention, time and resources.

Time spent collecting one piece of information is usually 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.* These threats may be gang or violent criminal elements, or corrupt law enforcement (or 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 our 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 security operations on Monday for an area north of town, then any Intelligence Requirement may be useless by Tuesday. The ACE should be included in future operations planning for the express purpose of two things: to provide Intelligence Preparation of the Battlefield information (covered in Chapter Six) and mission/threat analysis, and for generating Intelligence Requirements in order 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.* Asking, *When will the enemy attack and where?* is a poor Intelligence Requirement because it asks two questions, both of which are vague because they're unbounded by time and geography. A much more specific Intelligence Requirement might instead ask is, *Where will the Leroy Jenkins Gang attack in the next 72 hours?* or *Identify locations the Leroy Jenkins Gang will target in the future.* What's even better is that these requirements can now be enduring with no expiration, and we can hopefully be provided with continual early warning of future attacks.

Our Intelligence Requirements should continually be reviewed in the context of our criteria. If the Requirement never met or no longer meets our criteria, then it needs to be updated, refined, or removed. It's important to keep a master list of our Requirements – the things we need to know in order to perform analysis – so that we can track outstanding requirements that haven't been answered. That's the job of the Collection Manager, a role which we'll cover in a later section that describes how we staff an ACE.

Further, we have the ability to distinguish between *enduring* requirements and *ad hoc* requirements. It's important for the Collection Manager to understand the difference between the two; after all, he has the keys to our list of Intelligence Requirements. An enduring requirement is one that continually needs to be answered. "Identify the changes in security posture at City Hall," is an example of an enduring requirement because we continually need to identify those changes. They might reflect changes in government policy or indicate threat intelligence that law enforcement receives during the SHTF event. Ad hoc requirements, on the other hand, are in support of an event or can be easily answered one time. "How many security personnel are present before the rally starts?" is an ad hoc requirement in support of a single event. After the rally begins, we no longer have a need, as stated by the requirement.

Once we develop a master list of our Intelligence Requirements, we need to identify which need to be satisfied most quickly. These will become our Priority Intelligence Requirements, or PIR, which deserve our greatest attention. These requirements elevated to PIR based on the mission and Commander's Intent. For instance, if the current mission is battling the Leroy Jenkins Gang north of town, our PIR will most likely include requirements about identifying and tracking the members of the gang, monitoring the status or strength of the gang, and/or identifying what potential courses of action they will choose next.

The last consideration of PIR and IR are how we're going to organize them. Perhaps the easiest way to track our requirements is to simply number them. This method works best when dealing with fewer requirements. For instance, a very short IR list might look like this:

PIR #1: What threats exist in our AO?
IR #1: What is the size and strength of the Leroy Jenkins Gang?
IR #2: Identify sex offenders who live in the AO.
IR #3: What areas in our AO will be affected by the flood?

As soon as another Intelligence gap is identified, a new Intelligence Requirement will be generated, becoming IR #4. When an Intelligence Requirement is satisfied by information provided by one of our collectors, it can be removed from the list.

A more complex way to manage our Intelligence Requirements is by assigning them some nomenclature, such as both a digraph and number. (A digraph is a set of two letters.) For instance, our Intelligence Requirements regarding corruption in law enforcement might be assigned "LC". L stands for law enforcement, and C stands for criminality. Then we'd number our requirements (for instance):

LC1: Identify criminal activity the Sheriff involved in.
LC2: Which members of law enforcement in the AO are involved in corruption?
LC3: Which members of law enforcement in the AO support the Leroy Jenkins Gang?

"DA" might stand for Drug Activity. "NG" might stand for National Guard; and "LJ" might stand for Leroy Jenkins. In any case, label your requirements in a way that both the ACE and your Collectors can easily identify.

These are two ways that I recommend. Your nomenclature can be as general or complex as is required; however, we need to maintain an efficient process and clearly understand how our requirements are organized without getting bogged down by superfluous features.

PHASE TWO: Collection

In a perfect world with fully-staffed Intelligence sections, Collection and Analysis are separate tasks performed by separate individuals. In this perfect world, Phase Two of the Intelligence Cycle is the only phase that doesn't require the involvement of Intelligence Analysts; it belongs solely to Intelligence Collectors.

Being that we live in the fallen world that we do, and considering our time and resource requirements in a post-SHTF environment, it may very well be that we have to wear *a lot* of hats, especially if we're a very small group. In Chapters Three and Five we'll cover Collection in great detail and what our options are for having Analysts also do some Collection. Phase Two's corresponding step of the OODA Loop is Observe.

PHASE THREE: Analysis & Processing

In Phase Three, we're reviewing the incoming Intelligence information and triaging it according to several factors; the first of which is relevance. Let's determine which is relevant and needs immediate attention, and which is less of a priority or perhaps is of no priority at all. For instance, if our mission is to provide aid to flood victims in our community, then we'll ensure that information about the flood, its victims, and how both are affecting the community are analyzed before information about what the Leroy Jenkins Gang is doing. If the mission changes to defending community members from the Leroy Jenkins Gang, then we'd re-prioritize our attention according to the mission.

After sorting incoming Intelligence information to find the most relevant and necessary information, we'll need to examine each piece of reporting in order to ascertain its accuracy. We may be able to confirm or deny new information when we compare it to old information. In essence, we're grading this information on its consistency with what's already been reported and found to be accurate or is likely to be accurate.

It's also in this step that we deconflict information. For instance, if Source A says that Leroy Jenkins is white and Source B says that Leroy Jenkins is black; how will we know who's telling the truth? Making sense of conflicting or seemingly conflicting reporting can be one of the most difficult tasks for an Intelligence Analyst.

Another part of Phase Three is identifying new Intelligence gaps. When we identify a new Intelligence gap — for instance, how many individuals in the AO are named Leroy Jenkins? — then we need to generate an Intelligence Requirement so that the information can be collected. When we're reviewing new information, it may very well be that we identify new Intelligence gaps. When this is the case, we generate those new requirements, which begin a new and concurrent loop in the Intelligence Cycle again.

Phase Three's corresponding step of the OODA Loop is Orient; we're taking observations and attempting to make sense of them. In the next chapter, I provide additional considerations for Analytic tradecraft that will be helpful, if not necessary, to your ACE.

PHASE FOUR: Production

In Phase Four, we're taking the conclusions of our analysis and putting it on paper, so to speak. In the Intelligence Community, perhaps we're preparing a brief for senior leaders, or writing a White Paper on our findings. In the Community ACE, we might be preparing and updating maps, or updating an Order of Battle product on the Leroy Jenkins Gang, or collating a list of known criminals in the community. In any case, we want to take our finalized Intelligence and put it into a product that's easily consumed or that can be transferred for consumption.

PHASE FIVE: Dissemination

Finally, in Phase Five, we're taking our finished Intelligence product and putting it into the hands of our 'customers'. Typically we want to ensure the widest dissemination for threat Intelligence. That list of known drug-traffickers in your community might be disseminated in the form of a Be On the Look Out, or BOLO, list. The BOLO harkens back to the day of Wanted posters that enabled the men wearing tin stars to find that gang of bank robbers or perhaps a murderer. Law enforcement today might call these its Top Ten Most Wanted List or All Points Bulletin (APB). Or if your ACE is responding to a commander's requirement, however, we need to ensure that our timely Intelligence reaches him in a similarly timely manner. If our Intelligence includes information on or regards a nearby community, we may want to get our product to their citizens as well. One might think that Phase Five completes the Intelligence Cycle, and he would normally be correct. If our Intelligence products, however, spur another question or set of requirements from our command, then the Intelligence Cycle starts all over and we complete each process until we're able to provide Intelligence that satisfies our new requirement. It's at this phase of the OODA Loop that we hand over our Observations and our conclusions from Orientation to the decision-makers. They Decide on the best Course of Action and our action arms Act (or React) on that decision.

On a further note regarding dissemination, it's vitally important for us to get threat intelligence out to the people who need it most: the members of our team and community. Tom Glenn, a former National Security Agency (NSA) SIGINT officer, once told a tragic story about the lack dissemination of threat intelligence.[11] Early on in the Vietnam War, U.S. forces were losing a huge amount of pilots and aircraft to North Vietnamese Army (NVA) MiG. (These MiGs were Soviet-build interceptors, purpose built to track down and eliminate enemy aircraft.) The U.S. Navy lost 530 in combat. The U.S. Air Force lost over 1,700 aircraft. (In fact, the NVA finished the war with 16 pilots becoming aces. The US finished with just two. Part of that reason was because U.S. forces didn't strike main radar installations out of fear of killing Russian and Chinese advisors. So this allowed the NVA pilots to have an enormous advantage in finding US fighter pilots in the sky.)

The NSA received the location and vector information from NVA MiGs and other aircraft through the collection of SIGINT; however, they couldn't pass on that information because it was so highly classified and the pilots and air control of the Air Force and Navy weren't cleared to receive it. It wasn't necessarily the position of those tracked aircraft that was so highly classified, but the method used to determine their locations. The NSA was wiling to share the tactical information directly with American pilots, however, the air control denied them direct communication. Air control wanted the relay from NSA, first, and then air control would communicate it to the pilots. For a period of time, the NSA refused. But the NSA finally broke down and started providing this greatly needed tactical information to air control, and air control relayed that information to the pilots. They ended up saving a lot of lives of American pilots. That's an unfortunate example of the "green door" that separates intelligence staff from everyone else; what we call the "green door syndrome". Another Vietnam-era story is told of the Army Security Agency, which garnered a poor reputation during the time for similar reasons of not sharing critical threat intelligence.[12] If we have solid threat intelligence but we don't share it, or we can't get it out to those who need it, then the intelligence is worthless. Intelligence is not for us in the ACE; it's for the people who need to know about threats in the area. Having a green door is important to protect information - we can't share source information or, sometimes, how our intelligence information is collected - however, don't contribute to mission failure by not sharing good intelligence with those who need it. Sometimes it's appropriate to have a very flat and open distribution of vital intelligence in order to save lives.

These are the five phases of the Intelligence Cycle. A quick recap, starting from the first phase, has us:

1) Developing Intelligence Requirements that will support the mission
2) Collecting information that answers those requirements
3) Triaging the information for veracity and piecing it together
4) Compiling the analyzed information into finished Intelligence
5) Disseminating the finished Intelligence product(s)

Earlier in this chapter, we discussed the OODA Loop and how it applies to the Intelligence Cycle. The faster we get through our own OODA Loop, the faster we can produce Intelligence. Now that you know the five phases of the Intelligence Cycle, let's discuss five ways that we can speed it up.

One of the most basic things we can do is to simply understand our mission and the commander's intent. We know that Intelligence drives the fight, but the mission drives Intelligence. Having a poorly defined mission at the outset is a sure way to waste a lot of time with Intelligence support because we may end up supporting a part of the mission that becomes irrelevant or unnecessary. The Army uses the Military Decision-Making Process, or MDMP [13] to make decisions. For our purposes in conducting Intelligence for community security, that process is relatively unimportant, except to note that Mission Analysis and Course of Action Analysis both utilize input from the Intelligence section. These two steps will be covered in greater detail later in this chapter. Defining the mission and mission planning are functions of the Operations staff, which is out of our hands. We in Intelligence support mission planning by providing timely, relevant, accurate, specific and predictive or actionable Intelligence. Understanding the mission is truly our first step.

The second thing we can do to speed up our part of the OODA Loop (Observe and Orient) is to generate solid Intelligence Requirements. The faster that our Intelligence collectors know these requirements, the sooner they can begin reporting back that intelligence information. Prioritizing our critical requirements (PIR) will also help; these PIR give our collectors direction to collect most quickly the information we need the most.

In my experience, leaders will often ask questions for which we may be unprepared to answer. During a commander's brief on a local insurgent group in Iraq, for instance, I was asked about the security status of Iraqi Army outposts and logistics hubs. Although I could see where he was going with this line of thinking, that the insurgent group might decide to attack softer targets if the Iraqi Army's security was sluggish or had lapsed, I didn't know off the top of my head the current status of Iraqi Army security in these places. (In all fairness, that's really a question better suited for his Operations staff, however, I was the target of opportunity and he didn't really care.) So we had to go back and submit Requests for Information about these Iraqi Army installations, which slowed down the Commander's ability to Decide and Act. All this is to say that it's best to be as proactive and knowledgeable about as many things as possible. Who's to say how much downtime will be available in a post-SHTF environment, however, there will likely be lulls and time where no Intelligence support is critically needed. Use this time wisely: get smart on other topics in your AO. Learn about drug trafficking in your AO even if it's not your highest priority. Learn about how any local gangs are organized; know their leaders and members. Data-mine social media and forums and other websites for any information about these potential or current threats. In general, use Open Source Intelligence sources like these websites as much as possible; maybe even let it become your new hobby. (It's much more useful than Fantasy Football.) At the risk of beating a dead horse, we as Intelligence Analysts are called to be the subject matter experts on area threats. The more we know about the AO, the better off our organization is. There's no telling when, or even if, some piece of information that you had time to learn but never did will be useful. The faster we can spin that OODA Loop, the more good lives we save and more bad lives we take.

The fourth thing we can do to be proactive is to have prepared ahead of time lots of Intelligence products like Orders of Battle and Threat Estimates. One of the really great time saving measures is the ability to cross-check a new piece of intelligence information against our current holdings. If we build out a line and block chart of the Leroy Jenkins Gang, for instance, to show its leadership and how the gang is organized, then we can more easily confirm or deny new information with what we already know to be true. If the new source information matches up with what another source is saying about the gang, then we're in a better position to provide positive feedback for that source (covered in Chapter Three). Compare that to not having any of these products updated and readily available; it's going to take us a lot longer to judge the veracity of this new information, which is going to slow down our ability to Orient, thus potentially slowing down the organizational OODA Loop.

And finally the fifth thing we can do is to develop good lines of communication with members of the community. Let's say, for instance, a home was robbed in our AO, so we send out a Human Intelligence collector to interview the victims and report up some Intelligence information. And during this interview, we learn that there were two perpetrators; one had an unidentifiable snub-nose revolver, one was called by the name "Leroy" and they sped away in a 1980s model red Classic Caprice. Now that some information of Intelligence value!

So we at the ACE get that information and we can turn around and produce some Intelligence. We take the name Leroy and the red Classic Caprice into consideration and confirm that it was Leroy Jenkins; and we can also add a snub-nose revolver to the Leroy Jenkins Gang's Order of Battle. Next we make some BOLO sheets and distribute those among the community members. If they can report on any sighting of the vehicle then we may be able to track them down and arrest them. Our ability to increase the number of Observers could greatly increase our the speed of our OODA Loop.

TO DO LIST:

1. Teach your team about the OODA Loop, if they aren't already familiar.
2. Identify additional ways that your team can increase the efficiency of intelligence support to the mission.
3. Begin generating Intelligence Requirements.

Chapter Three: Building an Intelligence Section

Learning Objectives:
- Understand ACE Organization
- Understand ACE Roles
- Understand ACE Responsibilities

Good Intelligence allows your leader to make informed, time-sensitive decisions, and use his finite resources to maximum effect; he and his organization run the risk of mission failure without it. If we as a community are to accomplish the mission, we're going to need timely Intelligence. As we learned from the last chapter, there are two components involved in creating Intelligence: collection and analysis.

Collection – individuals gathering information of intelligence value derived from Human Sources, Open Sources, Imagery and Signals, among others – provide the lifeblood of Analysis: this is timely and relevant information to be analyzed. Without that inflow of relevant information, the Intelligence element – and the rest of the organization by proxy – is flying blind. We'll cover Intelligence Collection in the next chapter, and spend this chapter on building a sound footing for Intelligence operations. It doesn't matter how deep and wide our Intelligence collection is if we don't have a place to process it. This bottleneck is like having all the crude oil in the world: without a refinery, there is no fuel. So let's build a refinery.

We're going to need to build an Intelligence section - the refinery; this is the 'brain' of our community security team that accepts incoming information, processes it and understands its significance, and then translates this raw data into Intelligence that informs leadership and the community about what's happening around them. An organization involved in community security (or what we call in the Army, *stability and support operations*) must have an intelligence element, whether it's one individual doing the best he or she can, a small team of individuals, or an entire section of trained Intelligence Analysts. For our purposes, this Intelligence element is called the Analysis & Control Element, or ACE. It doesn't matter what you call your Intelligence section, as long as sufficient time and effort are put into running it.

The ACE is what's called an "All-Source" organization. That literally means it's responsible for analysis of information from all sources and from all intelligence disciplines; whichever you may have available. Without technical abilities and sensitive collection platforms, the community security ACE is likely to rely on data from Open Source Intelligence (OSINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT) and perhaps Signals Intelligence (SIGINT), if you have available some ham radio operators. This All-Source approach allows us to have a wider range of collection potential, as well as the ability to use information from one discipline to confirm or deny information from another. For instance, radio traffic from local law enforcement indicates that a home in our AO was recently robbed by two men, which confirms HUMINT source information that two men in the same vicinity and at the same time were observed running to a red vehicle with out of state license plates. Because these two separate sources are reporting congruent information, it allows us as analysts to better judge the veracity of this information. These two pieces of information has put us on the path to being able to produce actionable intelligence.

The ACE's real function is to be what we call an 'enabler' of action. The ACE's primary responsibilities, then, are to 1) direct the collection of information of Intelligence value; 2) process and analyze this incoming information; and 3) turn it into finished Intelligence that the commander or leadership can use for decision-making, planning, and action.

Building and overseeing an ACE is going to be one of the most difficult jobs for a community security team. Not only are the tasks and concepts already foreign to most individuals, but these tasks and concepts will need to be employed during a time of already heightened physical and mental stress. Additionally, there may be other priorities competing for our limited resources. This is going to include manpower. There are a handful of things we can do right now in order to help alleviate these potential future burdens.

First, we need to stress the importance of Intelligence as it relates to community security. The people in your preparedness group, security team, or members of the community, for that matter, don't know what they don't know, and it's not likely that they understand the value of Intelligence in the first place. The more our leadership, commander, and/or team members understand about Intelligence, the more likely they will see the extreme value of making it a priority. Illustrating the OODA Loop and how Intelligence plays a critical role in making informed, time-sensitive decisions is probably a very good first step. There are those communities who will implement intelligence and be more prepared, and there will be communities who don't use intelligence; and I believe the difference between the two will be visible.

As you'll see throughout this book, time and time again, intelligence is critical in our ability to stay a step ahead of threats. The principles outlined in this book are the same principles used by intelligence agencies and the military. Those two organizations happen to have roles in fighting terrorism; a mission of which community security is a microcosm. While we aren't involved in fighting terrorists, what we may face in a worst-case scenario is a modified form of terrorism in our communities - in other words, violence against society. And we know that "no other single policy effort [other than intelligence] is more important for preventing, preempting, and responding to attacks."[14]

The second thing we can do is to develop some criteria we can include when scouting out potential ACE members; we need to find those mental giants capable of heavy lifting. There are probably individuals in your community who may not be able to physically contribute to security, but can certainly contribute mentally. These are the people we want.

If we look at the ACE through the lens of any other organization, we'll find that it's always best to assign individuals to the function to which they're best suited. On my first deployment, I was assigned to a small task force. On Day One, I sat down with the Sergeant Major and he asked me about my background and experience in order to find the best place for me. He was a smart guy because not only did he assign me to the best mission that fit my capabilities; but I came away with a sense of pride and responsibility because, as a young specialist, I was assigned a specific mission based on my strengths. It turned out that I was assigned to interrogation operations at the national detention facility. This formed the foundation of my intelligence career. And I'll tell you what: that Sergeant Major got the best work out of me. Treat your ACE Team the same way. Let them excel in positions where they can play to their strengths.

Third, we need to get our Intelligence section designed and staffed as quickly as possible. Any practice we have before a catastrophic event, even rudimentary practice doing some simple threat analysis, is going to be time very well spent. The more we can get our team, even just a couple members, introduced to their work, the more we can rely on them to perform without supervision. The less we have to supervise existing members, the more time we have to train newcomers to pitch in.

The fourth thing we can do is to be deliberate about how we design our ACE. Remember that Intelligence drives the Fight and the Mission drives Intelligence; so how we organize our ACE really depends on our mission. Think carefully about your likely operational requirements. If you live in a rural area, it’s more likely that your operational tempo will be slower than an urban area, which might require 24/7 intelligence support. If you live in an urban area, crime stands a good chance at occurring at any time of day, so we may be required to provide around the clock coverage. Conducting threat analysis (covered in Chapter Six) will greatly aid you in understanding these requirements. But understand that our organization of the ACE can be changed; we must always adapt our organization of the ACE to the mission and security conditions.

Organizing Your ACE

I’ve designed this sub-section to be like a menu: I’ll throw out some ideas, describing each position and its primary responsibilities; and you’ll be able to pick and choose what’s most appropriate for you. Keep in mind that the positions listed below are the whole kit and caboodle. Some of the positions and processes described will be too complex and laborious for a very small community intelligence section, and you may find limited utility in any number of them. Several example diagrams of how to organize your ACE are provided at the end of this subsection. You’ll find them broken down into three categories: 2-3 personnel, 5-10 personnel, and 10+ personnel.

Because there’s a wide array of variables concerning what post-SHTF looks like (and also because we may have significant limitations on our own requirements) we may need few, most or all of the ACE positions described in the paragraphs below. Some positions are going to be better suited for a very active defense of the community, and may not be realistic for every situation.

The best ACE structure is ‘cellular’, with each member or section of the ACE having its own lane. Instead of having the entire ACE focus on one political issue, then jump to a threat issue, then jump to a civil issue; we're going to create teams solely dedicated to each functional area. Members of the ACE become subject matter experts and find a rhythm in what they do. In short, they become much more effective in a race car driving on the same track than on a pogo stick bouncing around from topic to topic, putting out fires as they go.

Each ACE is going to be scaled up or down depending on the size of its AO, community, or personnel limitations; so this is just a general guideline. Also keep in mind that any of these cells may require more than one analyst. Alternatively, if you have a very small number of individuals available to staff your ACE, then one analyst may have to wear multiple hats and cover several topics at once. The latter is not ideal, but make do with the resources you have available.

The ACE Chief

The ACE Chief is charged with being an architect, a leader, a supervisor, a coach and mentor, an Intelligence Analyst, and an expert communicator. It's his job to design the ACE, maximize the efficiency of communication and cooperation, enable the flow of information, communicate with and receive direction from leadership, manage the ACE team, and resolve any operational conflicts that may arise.

The ACE Chief is the last word on finished Intelligence. He should be the foremost expert available regarding Intelligence because he's expected to be the last line of quality control/assurance on Intelligence produced by his ACE team. As a member of the leadership's support staff, his job is to understand the mission and Commander's intent, direct his ACE team in way that best supports the mission, and communicate finished Intelligence with leadership so that they can make good decisions.

In addition, depending on mission requirements and/or the availability of personnel, the ACE Chief is responsible managing how the ACE is organized. The ACE Chief must understand the mission and what his requirements are, and then build a team around the requirements instead of fitting the requirements around the team. If the mission changes from providing humanitarian support to a peacekeeping or offensive one, then the ACE needs to adapt to the new mission. He may need to add a analysts to track a specific threat or event, reassign a member who has had a task that is no longer necessary, and expand or contract the size of his team as is required. Additionally, he may have to do all these things in a time-sensitive environment when he and his team are under duress. Anticipation, preparation and organization are they keys to his ability to succeed or fail as a leader.

Having an ACE Chief who is familiar with Intelligence, is plugged into the leadership's line of thinking, and has an ability to lead his team makes a critical difference in the efficiency of the ACE.

The Collection Manager

The Collection Manager's job is to oversee and manage (supervise, if you will) the ACE's Intelligence Requirements; review proposed Requirements based on Necessity, Feasibility, Timeliness, and Specificity; review incoming Intelligence information that satisfies any Requirements; and remove from the list any Requirements that have been satisfied.

Effectively managing the ACE's intelligence requirements saves us valuable time and resources. Remember that our intelligence requirements drive collection. Without these requirements, our collectors won't know what information to collect. Furthermore, removing these requirements from our list, once satisfied, will allow collectors to know what information still needs to be collected. Without removing requirements that are no longer necessary, we will be wasting the time of our collectors and our sources.

Not only does the collection manager maintain a master list of our requirements, but he also plays a critical role as the bridge between Collection and Analysis. He advises intelligence collectors on the ACE's requirements, effectively directing them to gather the information the ACE needs. And he also works with the analysts to receive and manage the ACE's Requirements so that those pieces of information can be collected. The role of Collection Manager is required to run an efficient ACE.

Threats Analyst

Depending on the number of threats in your AO, threat analysis may be divided into two categories: conventional threats and irregular threats. If there's more than one threat in your AO, I might recommend having an analyst for each type of threat, i.e., one conventional threats analyst and one irregular threats analyst. Depending on the operational tempo and risk each threat poses to your security, you may even need one analyst per threat. The primary responsibilities assigned to a Conventional Threats Analyst or an Irregular Threats Analyst will essentially be the same: "to find, know, never lose the enemy," to borrow from the Military Intelligence Creed (published in Appendix D).

Conventional threats may be law enforcement agencies, military units, or other federal regime or state forces. These groups will typically wear some type of uniform, whether it's camouflage or a badge or other identifier. What sets them apart from irregular threats is that they have *de jure* authority. They are the authority according to the law. In Iraq and Afghanistan, for instance, conventional U.S. Soldiers and Marines went on patrol with their national counterparts, and all wore their respective uniforms. That was a show of presence that built legitimacy and authority, and was intended to build trust in that authority.

Irregular threats, on the other hand, include gangs, militias, looters, mobs, rioters, and insurgents. If they acquire any authority, it's usually *de facto*; in other words, they are the authority because they're armed and present in the here and now. They may be an average member of the general population right now, become an armed insurgent in the next 15 minutes, and then blend back into their daily lives among the populace immediately following. Unlike conventional threats, they don't necessarily conform to any rules; that's what makes them irregular.

This analyst's tasks include tracking these threats and updating the situational templates (SITTEMP) to reflect current disposition and strength. Ideally, the threat

SITTEMP is going to be updated daily, unless these threats are involved in heavy operations, in which case it might require more frequent updates.

In addition to the SITTEMP, the Threats Analyst also tracks all operations and plots these associated events on a map. From this, you might see a well-defined area of operations that shows a unit's or group's boundaries. Tracking these potential or current threat capabilities, disposition, and movements within the AO is this analyst's chief task. (Additional information on these analytical tasks is found later in the chapter.)

Security/Defense Analyst

Understanding the elements of local security, be they local police, country sheriff, active duty or National Guard/Reserve units, a Constitutional militia, or community watch team, is important because their presence, or lack thereof, can directly affect your community! We need to know about law enforcement for a couple reasons. The first is so we can predict how they might react. For instance, under what conditions will law enforcement refuse to enforce the law (such as if violence is so widespread that they're going to be at their homes, protecting their families instead of protecting the populace)? During a SHTF scenario, what will be their top priority - guarding City Hall and critical infrastructure or protecting communities? Which parts of critical infrastructure are they going to protect? Is local law enforcement more or less inclined to cooperate with the enforcement of unconstitutional laws? And the second is so that we can understand their plans and operations. What's the standard operating procedure for law enforcement during 'peace time'? Does your county sheriff have an emergency management plan, and, if so, then what is it? What can we know about law enforcement that will allow us to be better prepared?

Another area for the Security/Defense analyst is military units. Are there military installations in your AO or broader Area of Interest? If so, where are they, what types of units are there, what are the typical missions for these units, and what types of equipment do they have? Are they likely to be mobilized in order to aid civilian emergency management? If so, where might they be most active? We want to answer all these questions and more, so that we can reduce uncertainty, better understand their role in or near the community, and be better prepared.

Political Analyst

This analyst tracks the capabilities and intent of the Federal, state and local governments within the AO and broader Area of Interest, such as the county or state. This analyst's primary focus is political. *How is any level of government affecting or influencing politics within your state or county?* Political and military action will affect one another and this analyst tracks that relationship. As a community security team, you will need someone to break down and analyze what's happening politically in the area. Is the government's mission changing? Is the government looking to affect local law enforcement, and, if so, how? The Political Analyst is going to lean heavily on OSINT reporting from local, state, or national news. This Analyst may be responsible for a daily update or roll-up on what's going on with governance: where they're taking criticism, their plans for stability, their plans for promoting and enforcing unconstitutional laws, how close they are to bending or changing their current policies, how that will affect your state, county and community, and if they appear to be supporting more aggressive policies towards the populace. These are just a few avenues to get you thinking.

Civil Affairs Analyst

Much like a Civil Affairs team, you'll need to track and be involved in matters of the community or surrounding populace. A great relationship with the populace pays big dividends; not only when it comes to their support of your security team, but also in their refusal to cooperate with the intent or goals of any threat elements. One issue that we incurred in Iraq and Afghanistan is that whenever we (US/Coalition Forces) destroyed part of a building or home as a result of collateral damage, we always tried to go back and offer to repair or pay for the damages. That was a necessary step in maintaining a good relationship with the populace. We began to face enormous problems when al-Qaida or the Taliban beat us to the punch and fixed or payed to fix the home that we destroyed, before we had the opportunity to make things right. That's a great way to turn the populace against the Coalition because it exploits the Coalition's apparent inability to protect the populace or lack of consideration towards protecting the populace. These are some of the opportunities that the Civil Affairs Analyst identifies.

A large part of judging public feelings and opinion is identifying and tracking the sentiments of community leaders. Reviewing the local media's reporting of events and judging media bias is also an indicator of how the populace might be influenced.

The Civil Affairs analyst must also be responsible for tracking any Critical Infrastructure in the AO or Area of Interest. Structures like power plants, water treatment facilities, police and fire stations, hospitals and clinics, etc., can critically effect a community. The Civil Affairs analyst must understand the capacity of this infrastructure and know how a failure in any of the public services will affect the community.

Another duty of the Civil Affairs Analyst is to aid Information Operations (IO); things we do to inform and influence the community. Get creative and let the thinkers of your team think outside the box. IO might be a billboard reminding the populace to not aid criminal activity; or it might be a weekly or monthly newsletter published to show the good things the local security team is doing. Maybe that includes pointing out that the security team arrested three criminals, or that they repaired a school or built a playground.

The Civil Affairs Analyst also needs to identify the needs of the community. Nothing says more about a local security group than when they take care of the least in the community. In fact, I believe that a community security team could create a lot of support for themselves if they spent more time taking food to the shut-ins and elderly. In a post-SHTF scenario, there are going to be a lot of needy people. The community security team needs to be involved in these kinds of things as they're able, and the ACE

Civil Affairs Analyst is going to help formulate the strategy for distributing civil attention, and then publicizing those stories to the best of his or her ability. (Typically, Information Operations isn't attached to the ACE, but given our lack of resources, the Intelligence section is the only logical place for this kind of analysis and support.)

Targeting Analyst

Why do we need a Targeteer? Because we may be faced with a without-rule-of-law scenario where the activities of a persistent threat, such as the Leroy Jenkins Gang, need to be disrupted, and its leadership degraded - certainly one of our worst case scenarios. In the wake of having no available law enforcement officers available in our AO, and perhaps without the means to contact them, our security organization will become the only organization capable of protecting the populace. And in order to neutralize threats, we need good intelligence, which means we need a good intelligence analyst.

Our targeting analyst is dedicated to developing actionable intelligence on threat activities, locations and leadership. Utilizing the Find, Fix, Finish, Exploit, Analyze, Disseminate (F3EAD) targeting process, your organization will rely on timely and accurate intelligence from this analyst. (Additional information on the F3EAD Targeting Process can be found in Chapter Seven.)

OSINT Team

While not typically associated with the Analysis, it’s smart to have an Open Source Intelligence Collection Team assigned to the ACE. This team is able to search the internet and monitor open sources in order to satisfy the Intelligence Requirements. In this way, we’re able to expedite the process between an analyst identifying an intelligence gap and a collector who can find the information and respond. (Additional information about OSINT Collection can be found in Chapter Five.)

Although it may seem like a good idea, requiring an analyst to also perform as an OSINT collector is generally a bad idea. Not only do we waste a lot of time and mental energy switching between tasks, but it also requires an analyst to entirely stop his train of thought while searching for information that he may not even find. In fact, he might spend hours looking for information; time that’s, frankly, better spent doing analysis of the information that he does have. The most efficient way is to let two or more individuals become expert in their assigned duties, instead of having to juggle multiple tasks.

HUMINT Analysis Cell

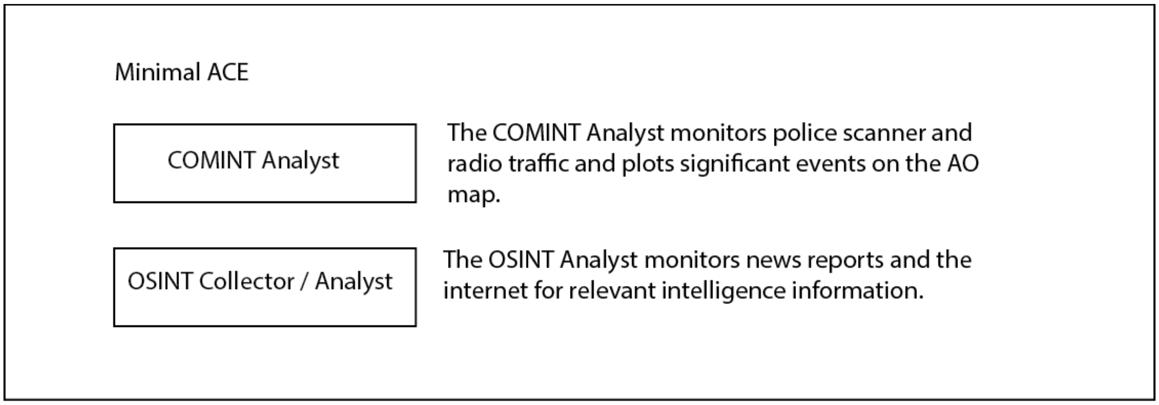
The Human Intelligence Analysis Cell (HAC) carries with an important caveat: it’s only necessary if you have a HUMINT program that’s producing a lot of intelligence reporting. Because the HAC is involved with reviewing HUMINT reports and evaluating source reliability, it's nearly pointless to have one staffed unless it's evaluating numerous sources in an active HUMINT program.

HUMINT reports are funneled through the HAC, where the cell sorts through them and grades HUMINT sources on reliability. The HAC also works with other ACE analysts in order to determine the credibility of information as reported by HUMINT sources. Part of the HAC's job is to check each HUMINT report against other known information in order to confirm or deny the source's reported information. Because the HAC has an important job of judging the reliability of each source and credibility of the information reported, this analyst (or these analysts) are in a unique position to provide feedback to HUMINT collectors. This feedback on source reliability is important for our HUMINT collectors, and improves the operations side of HUMINT by identifying producers of poor information.

Aside from analysis, HAC analysts work with other cells within the ACE to produce intelligence requirements that can be answered by the available HUMINT sources, and aids the Collection Manager by ensuring that the intelligence requirements that can be satisfied through the current crop of HUMINT sources are satisfied.

But perhaps the most important reason to have a HUMINT Analysis Cell is to process and analyze incoming SALUTE reports, an acronym that describes Size, Activity, Location, Uniform, Time and Equipment. A necessary goal of intelligence collection is getting community "buy-in"; that is, getting our community to alert us to any information that could potentially be important, or of intelligence value. These alerts can be put into the SALUTE report format and given to the ACE for inclusion into the current intelligence holdings. (Additional information on HUMINT collection can be found in Chapter Five.)

The Two-Member ACE



The COMINT Analyst monitors police scanner and radio traffic and plots significant events on the AO map.

The OSINT Analyst monitors news reports and the internet for relevant intelligence information.

I understand that many readers will be severely limited by lack of personnel. The bad news is that, in many cases, two individuals dedicated to the ACE may be a stretch, and you may find yourselves constantly behind the curve. The good news is that you now have a better understanding of what may be required, and you should have time to work towards developing a larger team. With few caveats, there's no good reason why you should only have two people available for the ACE. Enlist the help of your neighbors - they're probably going to want security just as much as you are, and you're the intelligence expert so they don't have to be. Provide them direction, whether it's simple collection or analysis they're doing, and ensure that you have as many eyes and ears available as possible. That said, the fewer people involved in our ACE, the more hats we'll have to wear and the less we'll get done.

We don't necessarily need an ACE Chief or Collection Manager; those roles facilitate a greater level of activity - activity we won't be involved in due to our limitation on personnel. If the operational tempo is low - that is, if we have time to react to current events and anticipate new ones - then more can be done to be proactive (such as direct and track collection for generating predictive intelligence). If the operational tempo is high - that is, we're either drowning in a sea of current threat information and can't keep up, or things are happening around us so quickly that we may not even know about them - then the best thing we can do is to 'battle track' what we do know.

If given myself and only one other individual, here's how I'd break down my ACE. (Perhaps you can only be dedicated to the defense of your home, immediate surroundings or AO.) Because our mission, at this point, is basic survival, I would throw everything I have at developing early warning and threat intelligence. We have to quickly develop an ability to identify and locate the threats, and the more we can do now, the better off we'll be in the future.

I would have one analyst sit down with a map overlay and a few pieces of paper, and monitor local radio traffic, specifically a police scanner or emergency management radio frequencies (if law enforcement is still operational). If time and the power grid allow, also listen to emergency broadcasts of local radio or television reports. When relevant information, such as a violent crime or the last known location of threats, is reported, then mark it on our map overlay. (Additional information on battle tracking is covered in Chapter Four.) 'Track' these events and visualize how your security situation is being threatened or could be threatened. For instance, are these threats or events getting closer or staying in the same general location? Have the criminals been arrested or otherwise neutralized, or are they still on the loose? Are these events growing more or less frequent and, based on the context, what might that mean for your security situation? At the end of each day, or perhaps each six- or 12-hour period, this analyst can provide an intelligence briefing to the household or community and ask for any additional information or feedback. This is a great time to generate new intelligence requirements so that we can ensure our intelligence analysis producing the most needed predictive or actionable intelligence possible.

In addition to mapping out these events, which allows us to visualize at least pieces of relevant intelligence information, this analyst also should write down any reported amplifying information, including the time and type of the event, names and number of identities involved, associations to other identities or groups (the Leroy Jenkins Gang, for instance), and any weapons or other equipment involved — in other words, generate a SALUTE report for each event. This work may allow us to identify the activities of specific threats, or determine if there's organized criminal activity in our area, which potentially represents a degrading security situation, which potentially presents a more dangerous threat.

Due to the nature of an environment with a high operational tempo, 24/7 coverage is mandatory. It does us no good if we monitor the radio 18 hours a day, only to suffer from violence sometime during the six hours that we had no coverage. Listening into law enforcement radio traffic, which should include the dispatcher and patrol units, is critical in gaining an understanding of the security environment.

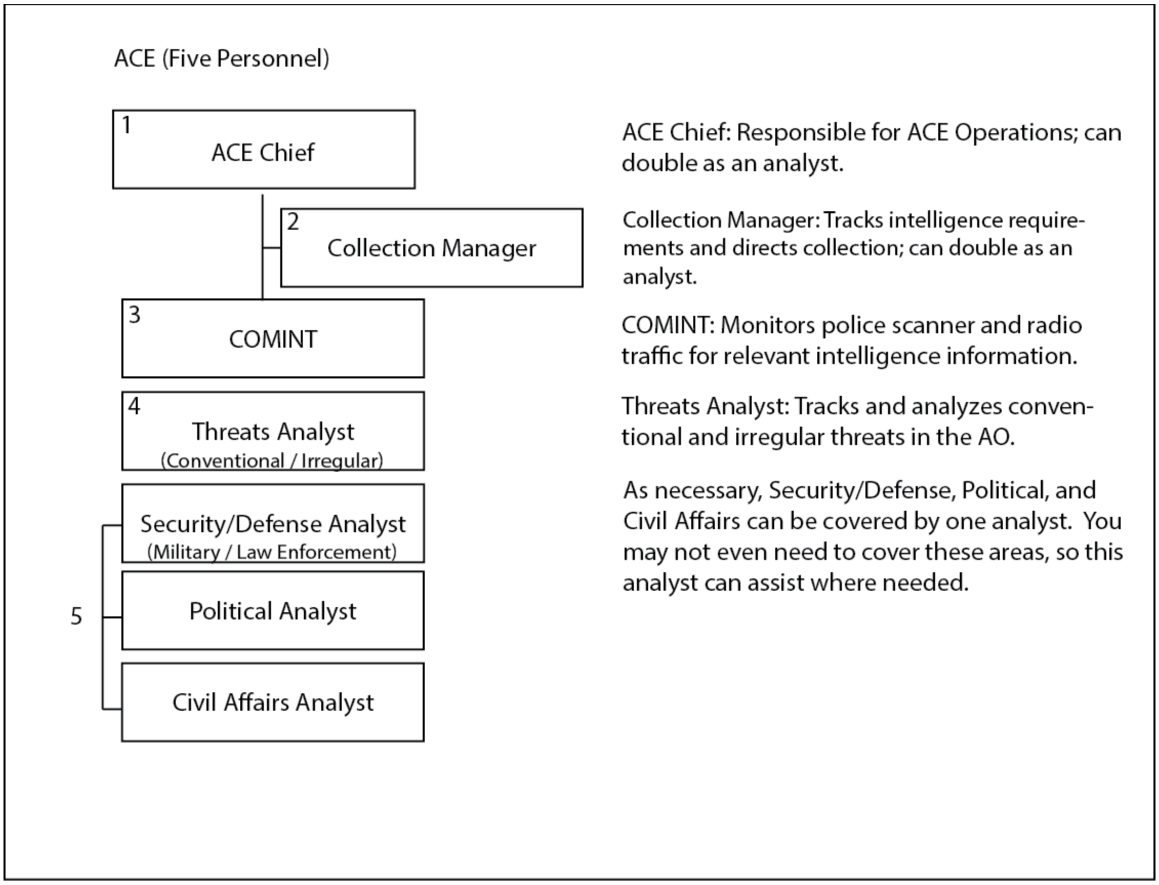
While the first member is involved in battle tracking and developing early warning or threat intelligence, the second member would be involved in, as far as the security situation allows and depending on the operational tempo, collecting intelligence information by speaking with neighbors. If you haven't done so before, inform your neighbors of what's going on and enlist their aid. Have them join the ACE to help make sense of the incoming information, or have them replace you in ensuring that the rest of your neighbors understand the SALUE report format and can participate for their own safety. Have members of the community aid your mission by being on the lookout for any criminal or threat activity. Work with them to develop some way to communicate that information, whether it's a courier or a bubble pack VHF/UHF walkie-talkie. The sooner you get this information, the sooner we can analyze and disseminate it.

After enlisting the help from the community, the second member should re-join the ACE to assist in either generating intelligence requirements and collection management in a low operational tempo environment, or OSINT/HUMINT collection and further threat analysis in a high operational tempo environment.. (Additional information on analytical tasks can be found in Chapter Four.)

The Five-Member ACE

Doubling the size of our ACE to four or five personnel is tremendously advantageous. It allows us to keep our eyes on more parts of our environment, better support our security operations, and, more importantly, be proactive instead of reacting to developments at the last second. As covered in the Two-Member ACE, battle tracking and developing early warning and threat intelligence is our very first step for any ACE, and it's a critical one. Beyond that, and before we can place four additional personnel, we have to consider our mission. Are we still in the survival stage of normal conditions breaking down or are we in broken down conditions where we're now trying to secure our communities? Consider your mission requirements: are we just trying to survive the threat, or do we now have a security element available to begin an active defense? If given five analysts for any, very general SHTF scenario, here's how I'd place them.

We're starting out our five member intelligence section with the ACE Chief. With this many analysts, we need a supervisor to help direct flow and coordination, manage time requirements, and ensure that intelligence is being produced to the level that's necessary. The ACE Chief can double down as the Collection Manager, if necessary, to help track ACE requirements and production. When collection management begins to



ACE Chief: Responsible for ACE Operations; can double as an analyst.

Collection Manager: Tracks intelligence requirements and directs collection; can double as an analyst.

COMINT: Monitors police scanner and radio traffic for relevant intelligence information.

Threats Analyst: Tracks and analyzes conventional and irregular threats in the AO.

As necessary, Security/Defense, Political, and Civil Affairs can be covered by one analyst. You may not even need to cover these areas, so this analyst can assist where needed.

interfere with coordinating ACE efforts and quality control, then we need a dedicated collection manager.

Early warning intelligence and threat analysis are still our top priorities. I would assign at least one, and potentially more, depending on the volume of information. We have to process and analyze this incoming information quickly, so if we become bottlenecked with only one analyst, then we need to add as many analysts as it takes. For now, let’s go with two threat analysts who are primarily involved in battle tracking irregular threats like gangs or looters.

I’m also going to assign a Security/Defense Analyst to begin looking at activity from local law enforcement or security organizations. This analyst is going to begin piecing together what organizations are active, what they’re doing in response, where they’re effective, where they’re ineffective, or if they’re even doing anything at all (aside from being at home with their families). He’s going to battle track these events on his map board and it’s going to give our leadership a much better idea of how law enforcement will positively or negatively impact the local community. I would include this as an intelligence requirement: due to the perceived authority, however diminished or increased it may be, we absolutely have to watch our for criminality among the ranks of law enforcement. In an SHTF situation, proverbial might may very well be making right out of very wrong things. If that’s the case then we’re going to need to assign a conventional threats analyst to track what law enforcement, even if just a few of them, are doing to contribute to criminality and instability.

Another avenue that our Security/Defense Analyst is going to pursue is looking at military units. For instance, if the National Guard or Reserve units begin mobilizing, then who are they, what's their mission, and what's the likelihood that they arrive in our town? How is their presence they going to affect area security? These are all questions with answers that predictive and actionable intelligence for our leadership and community. Knowing that the National Guard is going to mobilize to protect critical infrastructure in the area could mean a lot of things: maybe local criminals go after softer targets as a result, or maybe these criminals are going to be deterred by military presence. The sooner we can determine what the future is likely or unlikely to look like, then the better we can prepare for those scenarios.

I'm also going to want to know what's going on, if anything, with local and state governance. In addition to the ACE Chief, and Irregular and Security/Defense Analysts (and potentially a Conventional Threats analyst), we need eyes on politics and governance. The analysts formerly mentioned are checking out the AO - the tactical level; the town or immediate vicinity - and now we need someone to look at the county, state and/or federal levels. Identify the security situation on a broader level and begin estimating how that is going to affect our community. Is there a Federal response like DHS or FEMA? What's your state emergency management agency doing in response? If they're going to be in the area, then where will they set up and what will they be doing? What statements, if any, have politicians made and what policy, if any, might be enacted at any level by government?

The fifth member is going to be involved in collecting intelligence information to facilitate the topical analysts' work. If the internet is still available, there's going to be a lot of information of intelligence value being produced. Armed with the ACE intelligence requirements, our OSINT collector is going to be searching for information that provides us a better idea of our security picture. His goal is to satisfy as many requirements as possible, as quickly as possible, so that he can begin feeding information to our analysts, thus aiding them in producing greatly needed intelligence.

If the internet is not available, then I might consider tasking this member with HUMINT collection. His job will be to speak to members of the community - including those associated with politics, law enforcement, critical infrastructure - and gather as much intelligence information as possible. In Chapter Five, we'll discuss OSINT and HUMINT collection in greater detail.

ACE Operations

Regardless of which analysts you decide to include in your ACE, we need to design some functionality around these analysts. What we want is a streamlined and very efficient way to receive incoming information, analyze it, and quickly produce accurate Intelligence. We need good cross-channel conversations because our topical areas of analysis often intersect each other; e.g., irregular threats could affect political/governance policy, which could affect the populace and critical infrastructure, which, in turn, could affect local security which may affect irregular threats.

In order to understand the cycle of ACE Operations, I'll refer you back to the Intelligence Cycle (page X). This Cycle is the foundation of everything we do in the ACE. It begins with Receipt of Mission - in our case, during a SHTF crisis, that receipt of mission from the commander might be, "I want to know about all the current threats in our community." And then the ACE gets to work with generating intelligence requirements and directing collection.

Once we inform our commander of all the threats in our community - let's say that there are two repeat sex offenders and the Leroy Jenkins Gang - what can we assume he's going to want? If it was me, I would want my ACE to, at the very least, track the sex offenders in order to prevent any future criminality, and I would want to begin targeting the Leroy Jenkins Gang in order to provide community security. The better we understand our leadership, the better we can understand his intent and anticipate his Intelligence needs.

A very important point to understand is that, as the ACE Chief, I want to have Intelligence ready before the commander actually needs it.

"Sir, we've identified the Leroy Jenkins Gang as the primary threat to the community."

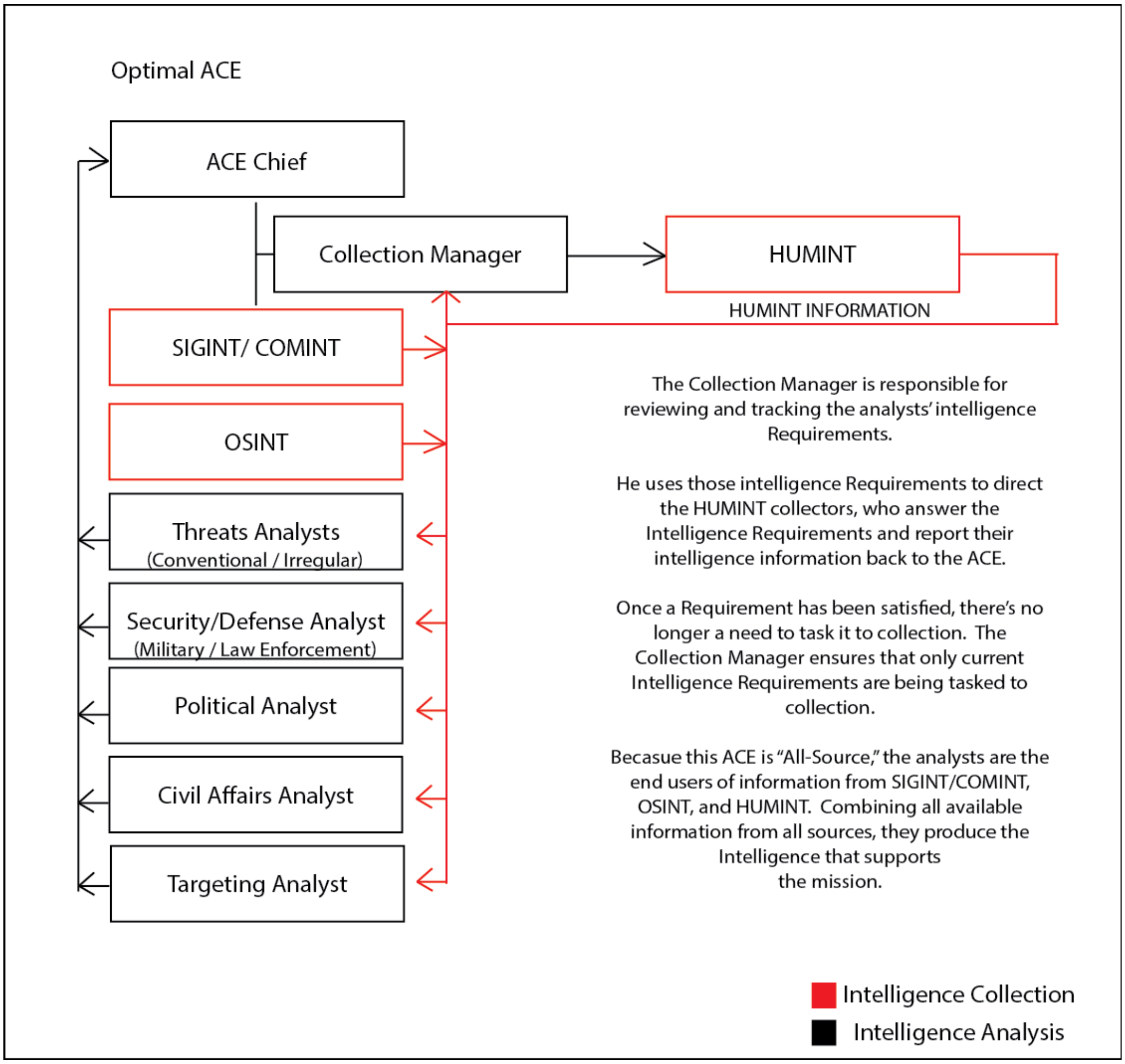
"Great," says the commander. "Give me everything you've got on them."

The position you want to avoid as ACE Chief, is the one where it takes your team hours or days in order to provide intelligence sufficient enough to meet the commander's needs. It would be much, much better, if, after the commander requests all the Intelligence we have, we're able to give him a work-up on the Leroy Jenkins Gang, including their estimated strength, disposition (locations across the battlefield), and recent activities. That pre-mission work begins now, before the SHTF.

Q: Pretend for a moment that the power grid is completely down. We don't know why it's down and we don't know when it's coming back up. If you were the ACE Chief and your commander said that he wanted to know about all threats in the community, what should your first steps be? (Answer on the next page.)

So the commander decides on a course of action and says, "This is the situation, and here's what I intend to do about it." [The very first section of an Army Operations Order (OPORD) is Enemy Forces — which just so happens to be based off the threat intelligence we produced.] This is receipt of a new mission to degrade the Leroy Jenkins Gang's ability to threaten the community, and thus begins ACE Operations in earnest.

For now, follow along with the ACE Operations Flowchart. I'll provide a brief description, and then will elaborate further in the sub-sections below. We've received the mission, which is followed by mission analysis. After mission analysis is conducted and we provide feedback to the commander, we begin planning for providing intelligence support. (Phase 1) Each ACE analyst identifies the intelligence gaps, and then generates intelligence requirements. Those intelligence requirements are then submitted to the Collection Manager, whose responsibility is to review and provide them to our intelligence collectors. (Phase 2) Those collectors involved in our various intelligence disciplines (OSINT, HUMINT, IMINT, and SIGINT) have now received direction on what to collect; they know the needs of the ACE in order to support the mission. It may take minutes, hours, or days, but our intelligence collectors will begin reporting back information of intelligence value. This underscores the need to begin doing this work now. (PHASE 3) Once the ACE begins to accumulate the raw information, it begins the task of actual analysis. Analysts sort the good from the bad and the ugly, and then begin making sense of the remaining available information. (PHASE 4) Once the analyst has created intelligence by answering, "So what?", he begins producing it into a consumable format. He may produce the intelligence onto maps, into white papers, or into briefings. It's very common in the Army to build slideshow presentations that include maps and photos. (I've even had threat briefing booklets printed for the commander and his staff.) Whatever format you chose, the finished intelligence should be easily communicated, understood, and fit for consumption. (PHASE 5) Finally, we disseminate our intelligence products to those who requested it, or those who need to know. If we're answering a question posed by the commander, then we tell him. If we're producing threat intelligence on a group that may threaten the entire community, then it might be prudent to pass it on to the entire community. Either way, this intelligence drives operations. Also keep in mind that, upon having his question answered, the commander may have additional questions or requirements, which may start the Intelligence Cycle all over again.



The Collection Manager is responsible for reviewing and tracking the analysts' intelligence Requirements.

He uses those intelligence Requirements to direct the HUMINT collectors, who answer the Intelligence Requirements and report their intelligence information back to the ACE.

Once a Requirement has been satisfied, there's no longer a need to task it to collection. The Collection Manager ensures that only current Intelligence Requirements are being tasked to collection.

Becasue this ACE is "All-Source," the analysts are the end users of information from SIGINT/COMINT, OSINT, and HUMINT. Combining all available information from all sources, they produce the Intelligence that supports the mission.

One last point to consider for how we manage the ACE: we have the potential in any SHTF scenarios for phase lines. We might categorize these periods of time into three groups: break down, broke down, and rebuild. During the break down, essential services may be slowing or ceasing; we may experience brown outs, black outs, or total grid down; and we may see rising crime rates due to a lack of food, water, and other supplies. This is the proverbial break down of society in which we must be focused on early warning intelligence and being able to track threats as they develop. This is going to require a different focus for the ACE, and we may have to shift fire as we move from break down to broke down.

In the broke down phase, we've essentially hit rock bottom. We may experience the "new normal," however temporary, when society begrudgingly trudges onward through the threat of daily violence over competition for finite resources. Under a worst case scenario, I compare this phase to midway through a course of antibiotics. The medicine killed off weak bacteria in the first few days, with only the strongest bacteria remaining. It's survival of the fittest, which - again, in a worst case scenario - is really going to affect our future. There can only be a few outcomes from this phase: 1) criminal organizations like the Leroy Jenkins Gang gain superiority and become locally analogous with the drug cartels of Mexico; or 2) the government gains back power under draconian measures that Liberty is severely threatened or non-existent. Neither of those scenarios are acceptable to me. That leaves us with option number three: we utilize intelligence to support the rule of law, destroy these threats to our Liberty, and bring back some level of normality with an emphasis on self-government. Option three is our only way forward to the rebuild phase.

The rebuild phase, if even necessary, will require a focus on the needs of the community and civil infrastructure. We may no longer fighting for our survival and security, but for building the right kind of society and the survival of Liberty in it. That brings with it an entirely new set of challenges, and intelligence should play no less a role. We're still going to have to identify threats, even if they're in areas outside our own. Disruptive threats become the norm; disruptions to systems or society, potentially the residual and unresolved fallout from previous phases. Another emphasis will be placed on understanding the physical terrain, namely where to acquire the raw material and resources to rebuild.

A: If you answered that you'd direct your ACE Team to begin identifying Intelligence Gaps and generating Intelligence Requirements, then you're right! In this scenario, it's our job to inform our commander of all threats in the community because he probably intends to begin removing the threats. If the commander's intent is to remove these threats from the community, then what are some Intelligence Requirements that you'd generate?

Vignette: Operation Urban Charger

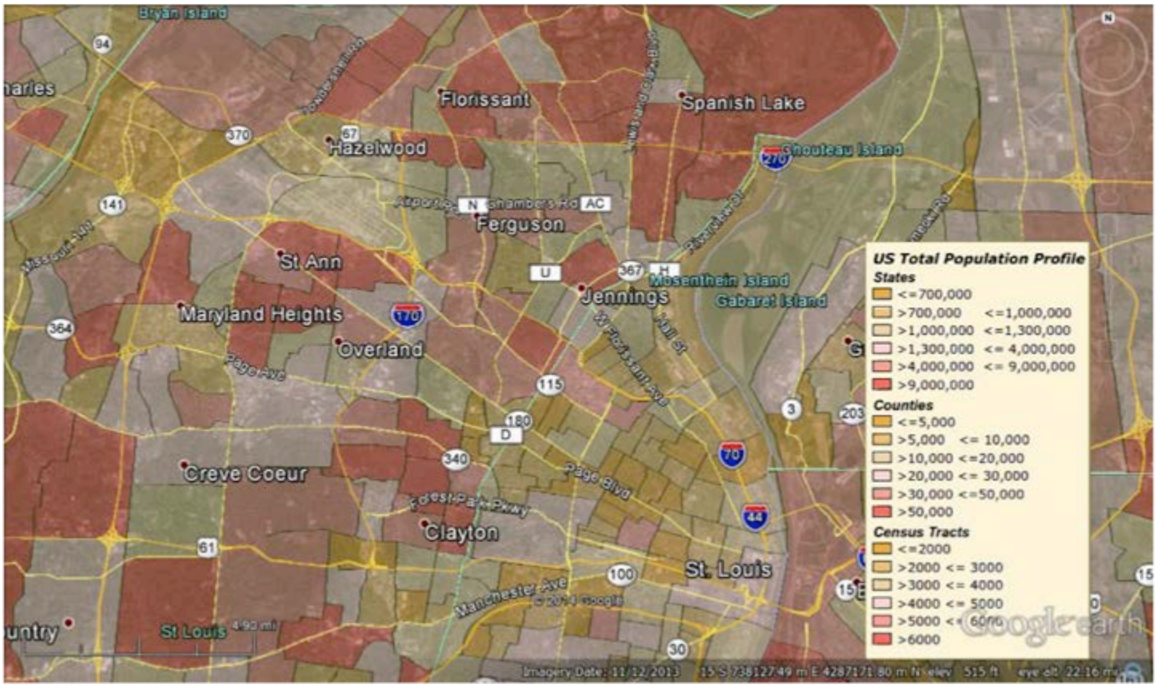
To give you a real-world, practical example of ACE Operations, during the riots in Ferguson, MO in late November 2014, eight volunteers conducted Operation Urban Charger. This was a practical exercise to track the fall out after a black teen was shot by a white police officer. There was a lot of speculation on whether or not the officer was going to be charged with the killing, so we began brainstorming various courses of action based on either of the final outcomes - what would happen if he was charged or if he wasn't? Brainstorming is a vital part of intelligence analysis, because we consider the possibility of so many events and always seek out alternative perspectives. We begin with a list of potential effects, and examine each one in order to determine how likely or unlikely it is to occur. In the brainstorming phase, there are no bad ideas. Get as wide an array of potential outcomes as is feasible and realistic. From this cumulative list, we can begin the process of sorting out all unlikely possibilities from the likely ones.

During Operation Urban Charger, we were able to successfully battle track developments throughout the night. Having our list of what we thought was likely, possible or unlikely during the riots allowed us to anticipate future events based on current trends. It’s this kind of early warning intelligence that we can provide to our leadership or community that saves lives and property.

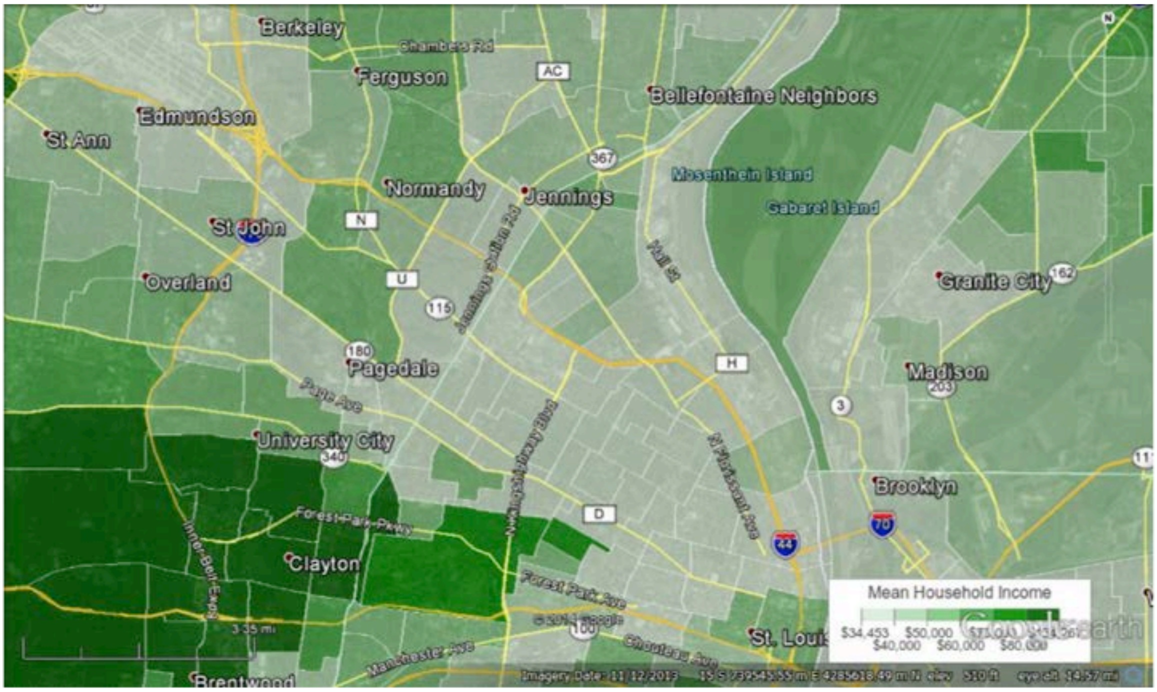
Our final assessment of Urban Charger was that, had this event been local to our area, we could have broadcast numerous and continuous early warning reports to the community. Urban Charger validated the ACE concept, which is traditionally used in the military, for the uses of Patriot-Prepper communities.

Using an internet chatroom as our meeting place, each volunteer was assigned a task as a member of our virtual ACE. As the ACE Chief, I tasked one member to begin Intelligence Preparation of the Community (IPC) in the lead up to the court’s decision. Conducting IPC is the foundation of any analysis of these types of conflicts. In IPC, we examine the physical and human terrain - what we call significant characteristics of the community - in order to determine how an event would effect the community. (Section Two of this book details the IPC process.) Here are three examples of the map data we were able to find.

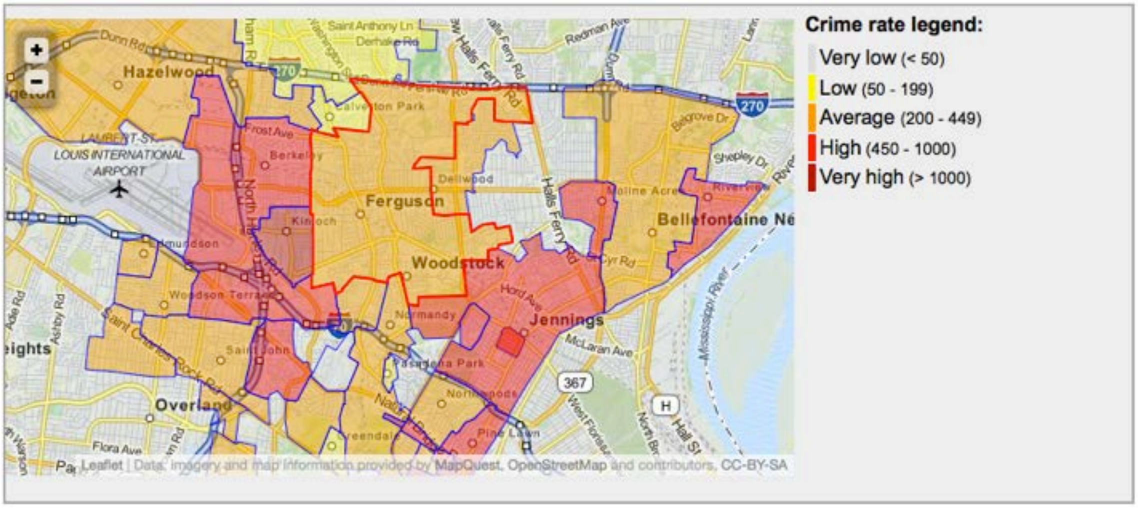
Population Density



Income



Crime Rates



As a part of this IPC process, a second member completed a Table of Organization & Equipment (TO&E) of local law enforcement organizations. As an active duty Army intelligence analyst, he provided an excellent account of the officers and equipment organic to the Ferguson Police Department, as well as from surrounding agencies. This was vital in our ability to estimate, before the decision-related rioting began, law enforcement's capacity to provide security.

The remaining volunteers were tasked with monitoring various sources of intelligence information - a human source with placement and access to the local St. Louis, MO law enforcement, the social media accounts of rioters and residents, live cable news coverage of the riot, and, perhaps of most value, radio traffic from law enforcement and emergency communications.

Starting a couple days before the decision, we began the first phase of the Intelligence Cycle - what did we need to know in order to produce intelligence? Here was the list of our initial intelligence requirements:

PIR1: What are the observed TTPs of Local, State and/or Federal Law Enforcement?

– IR1: What is the LE:Protester ratio in the AO?

– IR2: What LE vehicles are on scene?

– IR3: What LE lethal/less lethal weapons are being used?

– IR4: What is the strength and disposition of the LE Agencies?

PIR2: What are the observed TTPs of the National Guard?

– IR1: What is the responding NG unit?

– IR2: What is the strength and disposition of the NG unit?

– IR3: What NG vehicles are present in the AO?

– IR4: What LE lethal/less lethal weapons are being used?

PIR3: What are the observed TTPs of the protestors/rioters?

– IR1: How are the protestors/rioters coordinating command and control?

– IR2: How are the protestors/rioters communicating?

– IR3: What weapons/improvised weapons are being used in the AO?

– IR4: What is the strength and disposition of the rioters?

We also began looking for early warning indicators of the decision. It was our theory that charges against the officer would result in some unrest, but a N*o True Bill* would result in the violence that occurred. That indicator came when we began to hear the National Guard elements move from their staging locations to some forward positions, roughly 90 minutes before the decision was broadcast. This was a good indicator that the National Guard units were preparing for a No True Bill decision, and identifying this indicator immediately allowed the ACE to prepare accordingly. Forward positions for National Guard elements included fire stations, electrical substations, the mall, and some static posts.

What follows in succession of developments we tracked throughout the night:

At about 1900L, we received intelligence information that the National Guard set up a Tactical Operations Center (TOC) at the Target superstore on West Flourrisant Ave. Callsigns observed at this time included Tango1, Tango2, Tango5, and Warfighter33. Warfighter33 was determined to be the callsign for the command element at the National Guard TOC.

From 1900L until the decision was made public, we observed National Guard elements (callsigns Tango1, Tango2, Tango3, and Tango5) picking up and dropping off unidentified personnel at various locations. (The unidentified personnel were likely National Guard troops.) These elements were likely traveling in thin skinned HMMVs. Some elements may have been dropped off at guard posts without transportation. (Other observed callsigns included Tac-A and Tac-B.)

At 1927L, we confirmed air assets above Ferguson; two rotary wing aircraft. These aircraft likely belonged to St Louis Metro Police Department.

At 1940L, intelligence information confirmed the presence of a thin skinned HMMV with an unidentified turret-mounted weapon system on station at a courthouse in St. Louis. There were no reports of any weapon systems mounted on HMMVs in Ferguson.

At 1950L, we received the first report of violent activity when two black males committed armed robbery at the corner of Kingman Drive and MLK Boulevard. At least one of the suspects was armed with a handgun. The level of violent activity steadily increased from this point.

Beginning at roughly 2000L, multiple new units were coming online and conducting radio checks (callsigns included Defender27, Warfighter11, Castle1, and Medic902. It is believed that these were additional National Guard elements, due to the callsign of “Regulator (indiscernible)” and an unidentified medical unit. In addition to the local emergency services frequencies, it was reported that National Guard elements were also using cell phones to communicate.

At 2050L, Squad 238 (local Law Enforcement unit) began receiving small arms fire, and was advised to move their location to avoid escalation of force. This was the first of numerous reports of Law Enforcement elements receiving or hearing small arms fire. Squad 238 was particularly involved in violent demonstrations from the rioters.

After 2100L, all available 200-series units began forming a skirmish line and moving north from their position (NFI).

At 2123L, we received reports of an element from the Fire Department receiving small arms fire (NFI).

At 2130L, a woman reported that her husband was beat up by unidentified individuals, kidnapped and thrown in a van, which sped away (NFI).

From 2130L to the end of ACE Operations, there were numerous reports of looting and other violent activities, which are all included in the Appendix F.

<u>TO DO LIST:</u>

1. Identify the mission.
2. Identify the mission requirements and design an ACE Team capable of providing intelligence support to the mission.
3. Build your ACE and begin working to support the mission.
4. Generate Intelligence Requirements to support the mission.

Chapter Four: Intelligence Analysis

Learning Objectives:

1. Understand what Intelligence Analysis involves
2. Become familiar with conducting Intelligence Analysis
3. Identify Intelligence Analysis tasks you will need to perform

At this point, you should have given some thought to your mission and mission requirements, as well as how you might begin staffing your ACE around the mission. Now let's get into intelligence analysis and the types of analytical tasks and products you might need to complete in order to support the mission.

One of the first things we need to understand is the difference in echelons, or levels, of intelligence. There are three: tactical, operational, and strategic. At the tactical level, we find the most immediately important to us: our home is our tactical environment. Our block or neighborhood is our tactical environment. Our area of operations is our tactical environment. Receiving a SALUTE report of a squad of soldiers at the corner of Hwy 187 and Mulberry Lane, perhaps a mile from you, would be tactical intelligence information. The County Sheriff saying that he's going to increase patrols in your town is tactical intelligence information.

Above the tactical level, we have the operational level, which is the area where we can identify larger trends. This could range from your county to the state or regional area. Operational level intelligence may not directly and immediately affect you, but it's happening in your region and could indirectly affect you. Your state police reporting that they will increase patrolling over the holiday weekend is of operational intelligence value; they will be more active throughout the region. If they begin patrolling in your town or AO or by your house, then it would be of tactical value. Another example would be the mobilization of National Guard units in your state, perhaps responding to a natural disaster. Even if the flooding or hurricane didn't directly affect you, you will have an increased and active presence of National Guard soldiers at the regional level.

And finally we have the strategic level, which is the largest and is national or global in scope. Federal government policy is national, and therefore of strategic intelligence value. DHS reporting that it's hiring 10,000 new employees would be of strategic importance; they are preparing for something nationally. If 400 employees are placed in your state, then it's at least of operational intelligence value to you. If three are placed in your town, then it's of tactical intelligence value, too.

Here's an alternative way to look at these three levels. If your local gun store is out of ammunition, then the information is of tactical value. If all the gun stores in the state are out of ammunition, then it's of operational value. And if all the gun stores in America are out of ammunition, then it's of strategic value.

It's important to understand these levels for a few reasons; first being for the division of our time and attention. Although the tactical level should be our top priority (because it will most likely and immediately affect us), we can't neglect the other two levels. We also can't spend too much time chasing our tails on the strategic. From my experience in the preparedness community, too many folks spend entirely too much time tracking strategic level information because they perceive it to be more important than local level information. In reality, nothing could be further from the truth. If the lights went out tomorrow, then what goes on in D.C. or what's been happening on the other side of the country is much, much less important than what's happening or about to happen in our own AO.

Although it's entirely mission dependent, a rule of thumb I recommend is 60/30/10. Spend 60 percent of your time and attention on understanding the tactical level and how events or conditions will directly affect you. Spend 30 percent of your time on operational information at the state level, and 10 percent of your time on strategic or national information. Those who do the inverse will be at a significant disadvantage because they won't understand how their own communities work, nor will they understand how their communities are going to be affected. It does us little good to be up-to-the-second on what's happening around the globe, but fail at the most basic task of providing intelligence on the tactical level.

Another reason that we should understand the differences between these three echelons is that it narrows our focus. We prioritize what's most important to us: our own area. Your tactical area is unique to you and those immediately around you. Someone in an adjacent town has his or her own tactical area, although you share the same operational and strategic levels. It's much more efficient to become a subject matter expert on your own tactical level first, and then collaborate with other experts of other areas to identify larger trends. On the tactical level, you're focusing on the smallest building block there is. Own that first. Then we can begin incorporating intelligence from multiple tactical areas to build operational intelligence, and then multiple operational areas to build strategic intelligence. Without information dominance at the tactical level first, there can be no operational or strategic information dominance. And in order to provide information dominance, we need knowledgeable and trained intelligence analysts.

KEY TERMS:

Indicator - an observable or potentially observable clue about an organization's condition, capability or intent.

Bias - a way of thinking shaded by prejudice for or against someone or something.

You're going to continually have three jobs when it comes to building a proficient analytic capability: gaining subject matter expertise, removing bias from your thinking and arriving at accurate conclusions.

Subject Matter Expertise

When we're building threat intelligence, the importance of having at least a working knowledge of area threats can't be understated. We call our knowledge goal 'subject matter expertise'. The best Russian military analyst in the world would be nearly useless if assigned a task of analyzing West African tribes and warlords. A global financial analyst from Manhattan would not make a good agricultural analyst in Nebraska for the same reason: without a subject matter expertise, we are severely limited in our ability to make sense of information, particularly because we don't understand it. And the professionals and tradesmen who will conduct intelligence analysis for the community face the same problems, unless they understand the threat and the context in which the threat exists.

Sherman Kent, a former Office of Strategic Services (OSS) and Central Intelligence Agency (CIA) officer and, by all accounts, the father of modern intelligence analysis, once explained that, "It is the context of the situation alone which gives point and meaning to the subsequent elements of the speculation."[15] In determining proper context of a piece of information, we look for four things:

- its relation to other data
- the source's goals and expectations
- the observer's goals and expectations
- our own analytical process

So let's look at an example of an important piece of information in its context. Last year I received an email from a reader who was very concerned because he heard that his county sheriff's department received a Mine Resistant Ambush Proof (MRAP), an armored military vehicle, through the 1033 Program. (The 1033 Program transfers federally-owned equipment to local law enforcement organizations.[16]) He was certain that the MRAP would soon be used by his sheriff for gun confiscation. So we both did some investigation and found out that his sheriff's department did, in fact, receive an MRAP. But there was some context to the situation that he didn't yet know. His county sheriff's department didn't train on the MRAP and couldn't afford the maintenance, so it was only driven a couple times a year, mainly for parades and official events. That doesn't mean that it will never be involved for nefarious purposes, but understanding the context of the situation alleviated his fears that gun confiscation was not on the sheriff's to do list; at least not immediately. He correctly perceived a potential threat, but his initial hypothesis was wrong because he hadn't collected more information.

Another part of understanding information in the proper context is the source's and observer's goals when they report intelligence information. This is much of what makes intelligence analysis, especially the analysis of human intelligence information, so difficult. Could one of our sources bend the truth in order for us to accomplish his or her goal? Of course. For instance, a shop owner in Baghdad once reported the identity and location of an insurgent, who just so happened to be that shop owner's competitor; a rival fruit vendor. Was that significant piece of information ever considered before the competitor's arrest? Nope. But understanding the relationship between the two rival shop owners could have prevented someone from exploiting our desire to arrest insurgents. Receiving a tip that lead to actionable threat intelligence was great, however, a mistake in analysis was made due to a lack of due diligence and not understanding the context of the report.

Your chief task as an analyst involved in threat intelligence is to understand a potential or confirmed threat, in the proper context, as well as he understands himself. We do that through subject matter expertise. So how can we gain a subject matter expertise? Before I deployed to Iraq and Afghanistan, my section had required reading and some homework to get us prepared for being in country. This included everything from reviewing current intelligence reports and products, to reading area studies and books on the Saddam regime or the Taliban, and the Soviet experience fighting the mujahideen in Afghanistan.

For us at the community level, to gain a subject matter expertise, begin collecting information on your community. The longer you've lived there, the more likely it is that you can already be considered an expert. You may know a lot of things about your neighborhood and the greater area, but being an expert alone won't answer the vital questions that you can't. Chances are good that you can still learn more and be a more valuable asset to your team. Visit the chamber of commerce or local tourist office and take all the pamphlets and magazines they have. Find out what information is available from your city or county and begin pouring through it. Even real estate magazines might have some relevance, especially considering that these real estate agents come into contact with all sorts of people who might end up being your neighbors. Beyond that, liaise with local law enforcement or research the web and look at crime statistics to get a good idea of the baseline criminality of your AO. Use state gang websites to determine what gangs, if any, are active in the area. (More sources of information are covered in the OSINT subsection of Chapter Six.) This is all part of your pre-deployment training. Learn as much relevant information as you can while information is still cheap and easy to attain.

Avoiding Bias & Analytical Pitfalls

Sherman Kent once said that our mindset - our experiences and the way we see the world - is the lens through which we see information. On the topic of bias, Kent wrote, "[The intelligence staff] …is made up of men whose patterns of thought are likely to color their hypotheses and whose colored hypotheses are likely to make one conclusion more attractive than the evidence warrants."[17] Consider, for instance, the Bush Administration's relationship with the CIA before the Iraq War. We know that Iraq had weapons of mass destruction; even according to the *New York Times*, not only were at least 17 U.S. soldiers exposed to chemicals stored from the Saddam Hussein regime, but there are still chemical munitions unaccounted for in Iraq.[18] But after 9/11, the Bush administration was committed to the invasion of Iraq, and pressured CIA analysts to find a justification for it. In essence, they said, “Here’s what we want to do. Find a justification for it.” This is an instance of allowing ideology to inform reality. Policy makers should never pressure or coerce intelligence towards or against a finding. Intelligence should always drive policy; in our case, the mission.

Just like we complain when politicians allow their ideologies to inform their reality, so must we complain about ourselves when we do the same. But this condition of allowing ourselves to use poor judgement is not always easily identified. Identifying bias, then, is the best first step in removing it from how we think.

Humans infamously believe what they want to believe, and are therefore more likely to accept a world view that supports their beliefs or ideology. Let’s consider the differences in reporting by MSNBC and Fox News. If President Bush had walked on water, MSNBC anchors would have reported that it was because he didn’t know how to swim. For MSNBC, Bush could do no right. And the same goes for Fox News and Obama (and any non-establishment Republican). We often perceive information based on our opinions, and those pre-conceived opinions become our reality.

And most of the time, as a result, our views and opinions are resistance to change. Have you ever tried to convince a friend or family member of something they didn’t want to believe? It’s not that these people don’t have the ability to understand your argument; it’s that they’re ideologically committed to a particular opinion, and accepting that they’re wrong can be mentally painful. We often ignore information that conflicts with our opinions and readily accept data that confirms what we already believe. This is called *confirmation bias* and it’s a deadly sin for an intelligence analyst. Although it’s human to form an opinion and then look for justification, you’d better serve your community’s security (and your own) if you did the opposite: gather all the available facts, analyze them, and then come to a conclusion.

Another of the deadly sins for an intelligence analyst is that of oversimplifying a problem by using heuristics. A heuristic is a shortcut in human thinking. According to evolutionary biology, modern man has inherited his brain from paleolithic man. Paleo man was not at the top of the food chain, and therefore had to make quick, instinctual decisions for his survival. If while gathering berries, he thought he heard a predator, Paleo man didn’t have time to examine the situation, gather the facts and then form and test a hypothesis. His brain told him to assume the worst — to take a shortcut in thinking, even though he may not arrive at an accurate conclusion — in order to save his life. We’ve inherited that brain and our survival still encourages our psychology to take these mental shortcuts.

In his great book entitled, *Thinking, Fast and Slow*, author and psychology professor Daniel Kahneman explores the two “systems” of human thinking - intuitive and deliberate[19]. To illustrate System 1, he displays a picture of a woman who is clearly angry. He explains that we see that photo and we don’t have to think about what we see; we employ automatic thinking because we recognize and mentally process immediately that her brows are furrowed and slanted, her eyes are glaring and her mouth is positioned as if she is about to yell. We’ve been conditioned to understand the emotions of facial features in nonverbal communication, and it comes effortless to us. It’s intuitive.

To illustrate System 2, Kahneman gives a mathematics problem: 17x24. This problem requires deliberate thinking, as opposed to the intuitive, automatic thinking of System 1. When reading the book, I stared at 17x24 for a few seconds before giving up. I'm not what you would call a "math person" - and even then, the amount of effort required for me calculate the answer in my head was more than I was willing to put forth. So I estimated based on some simple math — it's at least 300 — and even then, it required some deliberate thinking. I saved myself the pain or embarrassment of putting forth a lot of effort, and instead took a short cut by estimating. Was my estimate correct? Of course not. If 17x24 was a threat to me, my family or my community, then I would have failed in my analysis of the problem.

Even though it may, at times, require a lot of work, we can't shy away from solving tough problems through intelligence. We can't afford to examine a problem like the Leroy Jenkins Gang and avoid conducting a thorough assessment because there's too much work involved. A large part of how we perform analysis is based on being as clear and concise as we can be. Although it may be counterintuitive, there's no room for, "I'd rather be safe than sorry," in intelligence analysis because we aren't being accurate; we're being lazy. These heuristics and the human desire to solve problems quickly through shortcuts, at the risk of accuracy, are a form of bias. As the saying goes, "almost" only counts in horseshoes and hand grenades.

On my first deployment, I was given a classified computer terminal and some intelligence reports, and told to read through the reports and tell my supervisor what I thought — in other words, to perform intelligence analysis intuitively which is supremely susceptible to bias. Not knowing any better, I did just what they asked me to do and I made a significant mistake. Specifically, I was responsible for greatly prolonging the detention of a (probably) completely innocent man because I said exactly what I thought. I wasn't necessarily biased against this detainee in particular, but was biased against making a mistake. While I was on the bubble, at the time, over whether or not the detainee was guilty of the accusations against him, I felt it was safer for us that he remained in detention just in case. *What if I'm wrong, we released him, he rejoined the insurgency and then killed an American soldier?* This is not an indictment of that decision, but, right or wrong, that's still a form of bias. I was being biased against the potential for my own errors. He was eventually released anyway, and probably went back to being a poor dirt farmer.

Another form of bias that you may encounter is called "groupthink". Groupthink occurs when members of the group agree on consensus for the sake of agreement and avoiding conflict. In the movie *World War Z*, the protagonist, played by Brad Pitt, links up with an Israeli Mossad officer. The Mossad officer explains examples of failures to put the pieces together: "In the '30s, Jews refused to believe we could be put in concentration camps. In the '70s, we didn't believe we could be massacred at the Olympics." And he speaks about the intelligence failure of the 1973 Yom Kippur War, in which Israel is invaded simultaneously by Egypt and Syria after Israeli intelligence analysts unanimously said that it would not happen. Although these could be examples of another type of bias - *normalcy bias*, in which an understanding of the future is derived from current conditions - each of the three historical events also represents groupthink.

Groupthink happens for a lot of reasons. Oftentimes, group members who might be inclined to disagree can feel pressured into 'giving in' to the majority opinion. The thought process goes, "Well, if most of the group thinks this way, then they are probably right." Another example of going-along-to-get-along groupthink is agreeing with senior analysts or superiors, where the thought process is, "Jim's a senior analyst and he's been here for decades, so he's probably right." Perhaps a supervisor is more likely to be hostile to dissent, or an analyst just wants to avoid confrontation and embarrassment in the event that he's wrong. In each of these scenarios, a potentially good analyst is deferring his potentially more accurate conclusion to the dynamics of the group. And in each of these scenarios, a very avoidable, potential mistake is being made.

After the 1973 Yom Kippur War, the Directorate of Military Intelligence (whose slogan is, "Freedom of Opinion, Discipline in Action") began instituting reforms aimed at preventing future intelligence failures.[20] Thus, the devil's advocate office was included in order to prevent groupthink. In *World War Z*, the Mossad agent explains that if nine intelligence officers arrive at a consensus, then it's the duty of the tenth man to disagree by playing devil's advocate.

And a smart devil's advocate is one of the best ways to identify and resolve potential bias. By playing devil's advocate, an analyst attempts to poke holes in theories and find faults in arguments. This analytical task should be encouraged because it can enable us to refine our ideas and produce better intelligence.

An example would be that one of your ACE analysts arrives at the conclusion that, post-SHTF, the Leroy Jenkins Gang is going to begin robbing clothing stores for the clothing and accessories the Gang has always wanted. A devil's advocate might question the theory and ask why not liquor stores, seeing as how liquor might not only be more enjoyable but also more valuable in a barter market. This devil's advocate might also ask, "Why clothing? What's the purpose and who are they trying to impress?" If there's no purpose and no one to impress, then expensive clothing and accessories may not even be worth stealing, especially when food, water and other supplies are so vital to their survival.

Another tactic of the devil's advocate is to search for evidence contradictory to the conclusion in question. If one of your ACE analysts determines that the Leroy Jenkins Gang is the greatest threat to the community, then the devil's advocate may begin looking at other threats. During a recent class, I had a student tell me that not only had a neighbor made repeated threats against the student's life, but also that this neighbor was a gun owner. A devil's advocate in this instance might point out that this neighbor could easily be perceived as a greater and more immediate threat and should be prioritized more highly in the community security plan. The Leroy Jenkins Gang may certainly be a larger threat, but considering his stated intent and capability, the unstable neighbor may be a more immediate and dangerous threat, especially when he runs out of medication. The devil's advocate just may have averted disaster by pointing out some potentially contradictory facts.

Similar to playing the devil's advocate, we can 'red team' a situation. In military symbology, red is always the color of the enemy, hence the name *red team*. Put yourself in the adversary's shoes: how would you accomplish the given task if you were the enemy commander? Given your time and resources, what would you do? Red teaming can be a great way to 'work against ourselves' in order to find hidden weaknesses and vulnerabilities that we miss through our own biases. One important note about red teaming from the enemy's perspective, however, is that we must maintain the enemy's perspective. What's logical for him may not be logical for us, and vice versa. Unless we've achieved information dominance, he knows much more about himself that we do. He knows things that we will never know. We may not fully understand his goals and intent, nor may we understand his mission. Red teaming can be a great exercise, as time and the mission allow, however, if we don't understand our enemy, then we won't do very well pretending to be him, either. In other words, you will not be aiding the intelligence effort by pretending to be a different enemy entirely.

Another way to identify and resolve bias is to have an analyst explain his reasoning:

The ACE Chief took off his glasses and responded, "So the Leroy Jenkins Gang is going to begin robbing clothing stores? Interesting; what makes you think that?"

"It's because of the Gang's culture," said the young analyst. "Expensive clothing and accessories represent success, legitimacy and authority; the sense that a person has 'made something of himself'. Because the Leroy Jenkins Gang is fighting for legitimacy against a rival gang, Leroy likely feels that showing off expensive clothing and watches will give him an edge in winning support from his community, because the community's culture celebrates outward symbols of success."

Certainly plausible. But if the analyst can't adequately explain his conclusion, or bases his conclusion on an incorrect premise (perhaps the community *won't* celebrate the appearance of his success) then bias may be to blame. Bias is just one of the limiting factors in the accuracy of intelligence analysis. We should also avoid all manner of "analytical pitfalls."

One of the other ways that heuristic thinking manifests itself is through an analyst's or group's desire to select the first conclusion that "sounds good". For instance, a friend once found a wet area in the passenger-side floorboard of his vehicle. He suspected a leak in his sunroof or windshield and wasted hours attempting to find and fix a hole or damaged seal. But there were several other possibilities that could have been to blame. Why weren't they considered? Because he had already found what he thought was the most likely cause. (It turned out to be condensation dripping from an evaporator case.) Not only did my buddy select the first possibility that "sounded good" but he also focused on too narrow a range of options. What he could have done, instead, is examine the problem further and then brainstormed a list of all potential causes before choosing a course of action. Then, instead of spending hours dedicated to one potential cause, he could have spent 15 minutes on each potential cause before identifying the real one.

The bane of my online existence are the repeated "alerts" about an imminent Chinese or Russian invasion of the U.S. mainland. They are read and shared, and contribute to further ignorance not only about the status and likelihood of these threats, but also about the forms these potential attacks will take. When we share bad intelligence without asking any questions, then we contribute to failure. As for the origin of this information, we can probably blame superficial analysis (or perhaps a need for advertising revenue). Superficial analysis occurs when we quickly look over a few pieces of information and arrive at a conclusion, omitting lots of very pertinent data in the process.

It reminds me of an intelligence product widely disseminated while I was in Afghanistan. One targeting analyst made a poor judgement when he confirmed the arrest of a named target and Taliban leader. That product was shared from his low level post in a district in Helmand Province back through the chain of command, ending at a general's desk aboard Camp Leatherneck. Before it was disseminated so widely, I called to inform him that our target had not been arrested and was still active on the battlefield. But it didn't stop other Marines and contractors from sharing a bad call. In short, no one else did any due diligence or asked how he was able to make that confirmation (he had a gut feeling about it, and the man who was arrested looked the same as a photo of our target — a lungi head dressing and a beard, imagine that). His superficial analysis based solely on appearance and that was his big mistake. He failed to positively identify this detainee, who turned out to be just another poor dirt farmer. Not only did he garner a poor reputation for himself from that point on, but he caused an organization-wide distraction. It's this kind of ignorance and intuition - or perhaps wishful thinking - that so greatly affects others, and it's what we must root out as intelligence analysts.

Arriving at Accurate Conclusions

We've identified our three rules for an intelligence analyst: become a subject matter expert and remove bias in your thinking so that you can arrive at accurate conclusions. Earlier in this chapter, I wrote about prolonging the detention of a probably not-guilty Afghan. Doing just what I was told, I poured through intelligence reporting and came to a conclusion based on what I read. I was not very critical in my approach, and committed a very rookie mistake: taking at face value everything I read. It's this intuitive, unstructured thinking that gets a lot of analysts into trouble.

Former CIA intelligence analyst Richards Heuer wrote a really great book about analysis entitled, *The Psychology of Intelligence Analysis*. He, in fact, was one of the pioneers of what we call "structured analytic techniques." He points out that we humans have a very limited capacity for storing short-term information (try multiplying 17x24 in your head, for instance). So instead of trying to tackle a complex problem in one bite, we break it down into smaller steps - (10x24) + (7x24) - and write them down in order to get our answer. The same can be said of complex questions like, "Is the Russian Federation capable of invading America?" There are lots of different variables and unknowns that we not only need to identify, but also accurately answer, in order to arrive at our conclusion. We might break down this complex problem into land force, sea force, and air force categories, along with a great deal of other factors and sub-categories during our analysis and then cumulatively arrive at our conclusion. Luckily for us at the community level, our problems are not be so far-reaching and complex, however, we will incur problems complex enough.

To understand the difference, imagine solving an complex algebra problem step by step on paper (structured analysis) versus trying to get a ballpark answer (intuitive thinking). Structured analysis, as opposed to intuitive thinking, can be helpful for solving complex problems.

Regardless of whom we credit for its discovery, the Scientific Method has its roots in the 17th Century. And it just so happens that the Scientific Method remains one of the greatest structured processes the intelligence analyst utilizes to conduct his craft. Here's the step-by-step guide:

1. Ask a question or define the problem
2. Identify requirements and gather data
3. Form a hypothesis
4. Test the hypothesis
5. Draw a conclusion

We begin first by observing and then asking a question. *What threat does the Leroy Jenkins Gang pose to our community?* Then we generate our intelligence requirements and gather the data (Phases 1 and 2 of the Intelligence Cycle). The analysis phase of the Scientific method begins with forming a hypothesis based on the collected data. We may be able to form multiple hypotheses based on the given data, partly because we just don't have enough information to narrow down a potentially long list. Our collection assets won't always be able to get us the latest or most reliable intelligence information; that goes exponentially in the case of our community's limited intelligence collection assets. That's just a fact of life for the analyst, so we have to use our best judgement when forming our hypotheses. We can make some key assumptions in lieu of any missing information, as is often the case, as long as we remain as critical about them as we do our facts. Making valid key assumptions — assuming the right things, in other words — can be difficult, and these assumptions should be as carefully crafted as any other pieces of our analysis.

If our work is time-sensitive — that is, an assessment is needed as soon as humanly possible — then we can provide an initial assessment based on our hypothesis. We're saying, "Here's what we think right now, but we haven't had enough time to complete our analysis." And that's another fact of life for the analyst: we won't always have enough time to complete our work.

In Step 4, we get into a bit of a quandary: how can we test our hypothesis in intelligence? It's not prudent to tell our teams, *here's what we think; go test it to see if we're right*. As much as possible, we need to see just how far our analysis will bend, if it doesn't break, before we disseminate it as our assessment. One way we can test our hypothesis is to identify any other information that can confirm or deny what we think.

Let's say that our initial assessment of the Leroy Jenkins Gang is that they pose a high threat to our community because its members have made verbal threats against our community. That's our hypothesis, given the available information. What other types of information should we consider? What can confirm or deny our hypothesis? They've allegedly demonstrated intent, but do they have the capability? Do the sources of these threats have a history of following through, or are they more interested in convincing themselves of their capability through threats? Are the consequences and repercussions worth it for them? Let's say that they were to target our community. The likelihood that they would become Public Enemy Number One, at least for me, is very high. Is that acceptable to them, especially given our capability to disproportionately reciprocate? As an analyst, these would all be points I would consider when testing that hypothesis.

Another way we can test a hypothesis is through lynchpin analysis. In the 19th Century, train locomotives had a lynchpin that connected each car. As long as these train cars were connected by lynchpins, then the engine could pull them all. So imagine one of these long trains slowly working up an incline and nearing the top of a large hill. If we were to pull the lynchpin behind the engine car, then the rest of the train would cease its climb and soon begin rolling backwards. We can test our hypotheses in much the same way: what's the lynchpin that holds your argument together?

Let's examine a previous statement from the junior analyst; namely, that the Leroy Jenkins Gang would begin robbing clothing stores so its members would be seen as more successful and legitimate, and therefore garner more support from the community. What's the lynchpin here? It's that the community would see the clothing and want to support Leroy's gang. If that weren't the case, then the analyst's entire hypothesis could be wrong. So if we could find evidence or prove that the community would support another cause - say, whichever gang could provide them food and water - then we could pull the lynchpin from his argument. The lynchpin in our high threat assessment of the Leroy Jenkins Gang is not that they've demonstrated intent, but whether or not they have the capability. When we test our hypothesis, we're attempting to confirm or deny it's validity.

After a hypothesis has been tested, then it's more likely that we can draw an accurate conclusion. Now I imagine that at this point, some readers are questioning how long this process takes. That's a great question. You've probably heard the saying, "paralysis by analysis" before. That means that an organization fails to Decide and Act because the Orient phase of the OODA Loop takes so long. Our intelligence section can't possibly know everything, even though that may be their goal. So in this attempt to know everything and have all the facts, they withhold an assessment because they continually don't have enough information to be sure of their analysis. This poses as much of a threat to professional intelligence organizations as it does to our community intelligence section. There's nothing wrong with always wanting more information, and in many cases you may fall victim to the paralysis by analysis trap, too. This greatly affects your ability to arrive at accurate conclusions, after all. There are two things we can do in order to prevent this.

The first way we can adapt is being able to anticipate the intelligence needs of the future. The sooner we can start Observing and Orienting to a future problem, the sooner we'll be able to Decide and Act. This ability to be more proactive than reactive is an outgrowth of subject matter expertise of the threats and your operating environment (your AO and community). This is the information dominance that leads to *decision dominance*. This occurs when we've mastered our domain and have greater intelligence than our adversary, thus allowing us to make decisions so quickly that our adversary can't keep up. This initiative comes directly from intelligence, because intelligence drives the fight.

The second thing we can do to overcome paralysis by analysis is to set a deadline for our assessment. If our leadership needs intelligence no later than Tuesday, then each hour before that deadline is another hour spent on vital planning and strategy. It does us no good to get our leadership this intelligence early on Sunday night, if the intelligence is inaccurate. Likewise, intelligence by Wednesday afternoon is next to useless, no matter how accurate it is. Just like shooting, actionable intelligence is a marriage of speed and precision. We want the most rounds delivered on target in the fastest way possible. Without accuracy, speed is relatively unimportant. As you get to know your AO better in the context of intelligence collection and analysis, you should get into a rhythm. You'll get to know your analysts, and become more familiar with timelines and your ability to hit or miss them. Whenever you're given a task from leadership, be sure to understand its attached deadline. Spend plenty of time getting your analysis right; however, not at the cost of not providing anything at all. Much like the quip about decisions, not making one is still a decision.

Analytic Tradecraft

Our ability to quickly analyze information is critically important, and can be difficult. While we as analysts always want to work towards confirming or denying significant information, usually by comparing similar information from different sources, we may not always have that luxury. For instance, our job may be easier is we have numerous, independent sources reporting the same thing. As an analyst, on its face, I'm probably going to be more inclined to believe this information. This is the "all-source" approach that we need to take in analysis.

The opposite of all-source information, however, is single source information, which is one or more reports from only one source. This really can be a double-edged sword for us in the ACE. Perhaps we have one source who is reporting high-level information. His placement and access is so high that not only can no other source can compare to his level or quality of information, but we also can't confirm or deny his information based on what anyone else is reporting. *Should we believe this information? If so, why?* Let's go over a checklist that allows us to make inferences quickly about the veracity of single source information. Keep in mind that this is a cumulative checklist;

the failure of one category shouldn't indicate a failure of reporting accurate information. One last caveat: we're not taking into consideration deliberate deception right now.

Judging Single Source Reliability

Source Reliability — 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. 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? 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. Be objective, not emotional, regardless if you like or dislike this person.

Plausibility — Is the information that he's reporting 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 about the White House. 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 cab driver 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 of all people.

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. If we've been tracking events surrounding the information and we have a subject matter expertise, then judging whether or not we expected a particular piece of information can be useful in determining veracity.

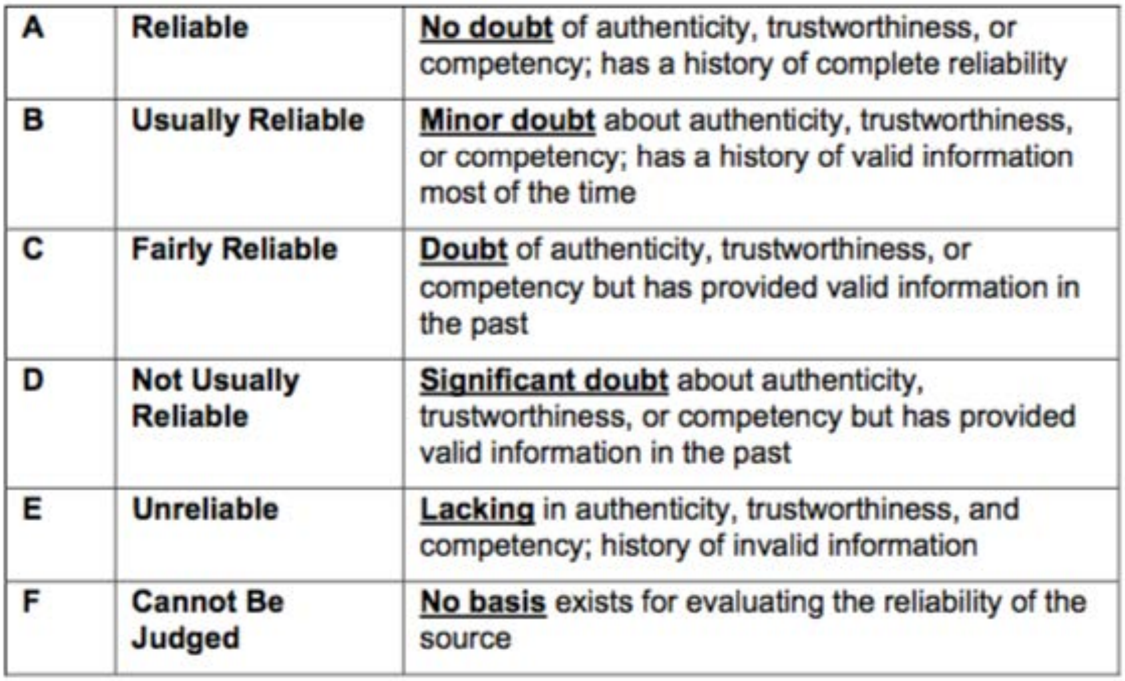
Support — Do other sources corroborate or come close to corroborating this information? Does what we already know about the subject lend the single source information any credibility? For instance, hearing that WalMart struck a deal with the makers of RaspberryPi, and will carry 100 RaspberryPi's per 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.

Judging Source Reliability and Content Credibility

In addition to judging the veracity of information, we also need to judge the reliability of each source and the content of his or her information. Over time, a human source will accrue a "reporting history". The longer this body of work, the better it may allow us to judge their track record of reporting reliable or unreliable information. Depending on the amount of HUMINT being reported, this may require the work of a dedicated analyst, who's a member of the HUMINT Analysis Cell.

For instance, let's say that Source A101 has given his handler enough information to produce seven intelligence information reports. Our collector, in this case the handler, has met with Source A101 on a continual basis over the past month, and the source has been cooperative in producing information. An analyst, then, would be able to go back and review all seven reports in an attempt to identify how reliable the source is overall, as well as determine the credibility of the information he's reported. After reviewing and analyzing this source's reports, our analyst assigns a grade to Source A101 — the source is given the grade of B. In the chart below, we see that B means "Usually Reliable - Minor doubt of authenticity, trustworthiness or competency; has a history of valid information most of the time."

Table B-1. Evaluation of Source Reliability.



A	**Reliable**	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	**Usually Reliable**	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	**Fairly Reliable**	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	**Not Usually Reliable**	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	**Unreliable**	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	**Cannot Be Judged**	No basis exists for evaluating the reliability of the source

The B grade is assigned to just the source; the analyst uses a different grading system for the source's information. After confirming or denying the veracity of each piece of information in the source's reporting history, the analyst is going to assign a content credibility rating. The analyst should keep a running score card for each source report in order to structure the analysis and measure the results. This could be as simple as grading each report, or perhaps each statement or paragraph, and tracking how many 1's, 2's, 3's (so on and so forth) there are for a cumulative approach to grading the source's reliability. If there are more 1's (Confirmed) than 3's or 4's, then the source deserves a higher reliability rating; Usually or Fairly reliable, for instance.

So let's say that Source A101 reported that the local sheriff's office had enrolled into the federal 1033 Program and had attempted to acquire an MRAP. In an effort to confirm or deny this information, maybe the analyst had someone get in touch with a local reporter who confirmed the information. In this case, once the source information was confirmed, the analyst would grade that statement as "1 - Confirmed by other independent sources; logical in itself, consistent with other information on the subject."

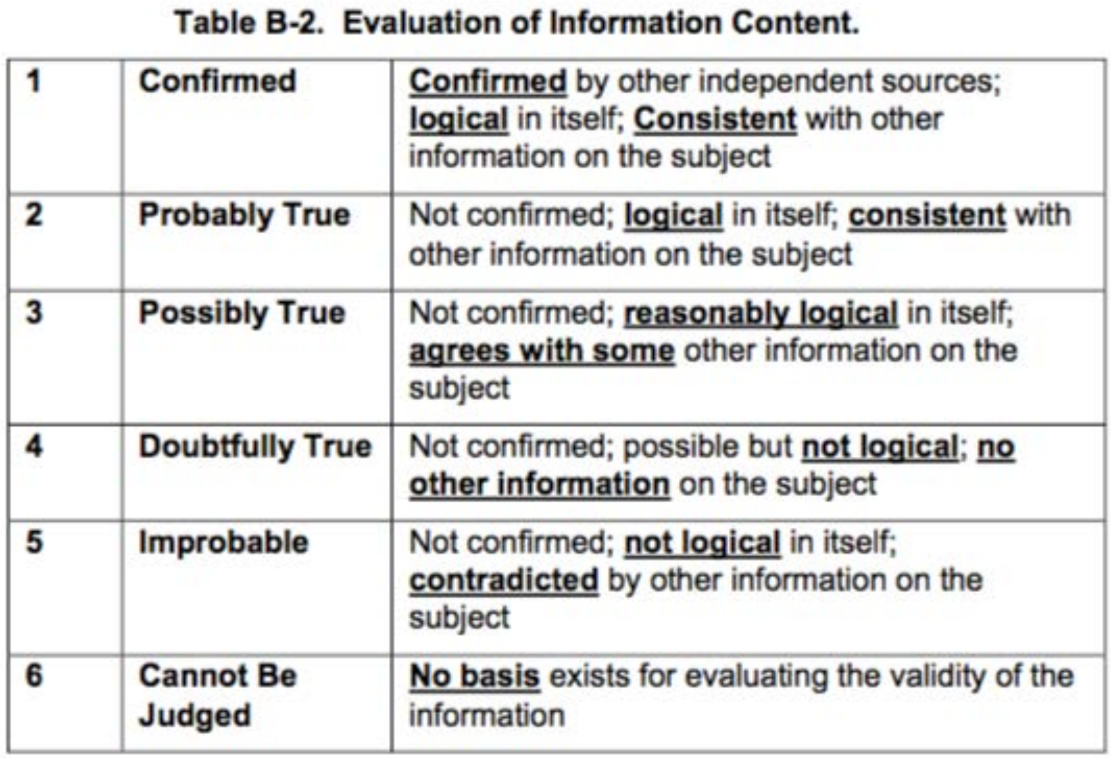


Table B-2. Evaluation of Information Content.

1	**Confirmed**	**Confirmed** by other independent sources; **logical** in itself; **Consistent** with other information on the subject
2	**Probably True**	Not confirmed; **logical** in itself; **consistent** with other information on the subject
3	**Possibly True**	Not confirmed; **reasonably logical** in itself; **agrees with some** other information on the subject
4	**Doubtfully True**	Not confirmed; possible but **not logical**; **no other information** on the subject
5	**Improbable**	Not confirmed; **not logical** in itself; **contradicted** by other information on the subject
6	**Cannot Be Judged**	**No basis** exists for evaluating the validity of the information

Together, this report would be graded as a B1 report. If an all-source analyst was to later reference this report in an intelligence product, he or she could say, "According to information rated as B1, the Plymouth County Sheriff's Department attempted to acquire an MRAP from the federal 1033 Program." That way, anyone who reads this finished intelligence product would have a better understanding of the intelligence: a usually reliable source produced information that was confirmed to be accurate.

There's one important caveat to grading sources and their content. We're likely to see a lot of F6 ratings, simply because we're unlikely to have a very robust HUMINT capability. A source rating of F does not necessarily reflect poorly on a source; it does *not* mean failing. The same can be said of a content rating of 6. It's not necessarily bad information, it's that it can't be judged.

These source reliability and content credibility ratings aren't just for human sources, however. The same rating system can and should be used for OSINT sources, too. We can grade websites, news stations and reporters, among other OSINT sources, in the same way.

BICC/E: Developing Potential Courses of Action

Once we have all our intelligence information, have combed through it to discard what untrue or likely to be untrue, and we're left with the remaining information that's true or likely to be true, what do we do with it? How can we be proactive and produce actionable intelligence? One of our jobs as analysts is to provide potential Courses of Action, or COA, to our command element. We understand the threat and we should have a good idea of what they'll continue doing, stop doing, or what they're going to do next. In order to provide this range of potential COAs, which helps our leaders to plan for the future, we must have a structured method of determine what's likely and what's less likely. We do that through BICC/E Analysis (pronounced 'bicky').

In Iraq, my section was having trouble determining the likely future plans of several insurgent/extremist groups. This was probably due to them not knowing themselves; not that it was ever a good excuse for us *not* to know. So I developed this structured analysis, which has a cascading effect; each step will affect the next. This analysis will help us to develop potential COAs. We not only need to identify several potential COAs, but also what we call the MLCOA and MDCOA. The Most Likely Course of Action, or MLCOA, is what believe a group is most likely to do. We may believe that multiple options are possible, so we rank each COA in relation: MLCOA #1, MLCOA #2, etc. The Most Dangerous Course of Action, or MDCOA, is the worst case scenario. For instance, if we in the intelligence section wanted to target an insurgent leader, then we'd most assuredly have to account for *second*- and *third-order effects*. If we kill or capture this insurgent leader, what happens next? Who's his replacement? How will the group respond?

Perhaps the group is likely to fracture due to in-fighting among the leader's lieutenants, represented by MLCOA #1. Or maybe the most senior lieutenant is able to wrestle control of the group by killing other rivals, represented by MLCOA #2. Or the MDCOA: the group is angry that their leader has been arrested, they band together to increase attacks against US/Coalition Forces as well as civilians, and begin infiltrating local police forces in an attempt to break him out of prison. These would all be examples of second-order effects, and the effects those events are of the third-order. BICC/E Analysis helps us to identify these potential COAs as well as their chain of effects.

Behavior — Judging behavior isn't always as simple as it sounds. If we know that the Leroy Jenkins Gang is our adversary, but we can't identify who they are (identities, names, nicknames, for instance), then we're less able to associate them with known events like criminal activity or attacks. If the culprits of these events remain anonymous — that is, if we can't attribute events to individuals or groups — then we really can't accurately judge a group's behavior. We know these people and groups 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.

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 active in 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 is 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 Leroy Jenkins Gang is robbing homes at gunpoint, and they enjoy relative safety and their goals are being met, then their MLCOA is that they 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 Leroy Jenkins Gang, 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 current level of 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't 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 — Understanding capabilities is highly dependent on the collection of intelligence information. What's our assessment as to the capabilities of the Leroy Jenkins Gang? 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 Gang 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.

Once we spell out their current capabilities, we 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 suspected intents are within the realm of possibility, regardless if the possibilities match their actual intent.

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 Leroy Jenkins Gang is to continue robbing area homes, what will the consequences and effects be? Increased household security, increased awareness, possible kinetic targeting of the Gang, and/or security patrols are all possibilities. 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 them could be detrimental to the Gang. 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, and it makes the area hostile or non-permissible for them. If it takes a month to spin up increased security or a community watch, then the robberies may last for a month.

Aftermath: Predictions and Outcomes

When I was a kid, my father was fond of telling me, "It's a good thing that you don't get paid to think." On several occasions, I would come home for dinner and leave the front door open, which prompted him to tell me to close the door.

"Well, I thought I did," I replied.

"Then it's a good thing that you don't get paid to think," was always his response. Some years later, after I enlisted and graduated from the intelligence schoolhouse at Fort Huachuca my first words to him were, "I get paid to think now." That, in and of itself, however, actually means very little. The government pays people lots more money to do less, after all.

In his book, *Expert Political Judgment: How Good Is It? How Can We Know?*, author Phillip Tetlock explains an experiment he conducted including more than 27,000 "expert" judgements. Just like in Burton Malkiel's *A Random Walk Down Wall Street*, that says professional stock pickers on Wall Street rarely outperform the randomly-selected stocks chosen by throwing darts at the paper's stocks section, Tetlock found that these 27,000 predictions weren't any more accurate than outcomes selected randomly. To make matters worse, he found that the more well-known the political pundit, the worse his or her accuracy was. Tetlock attributes this case of low accuracy to confidence levels.

In a separate survey of the educated class, researchers found that respondents with Master's degrees were more confident in their opinions and theories than those with PhDs. But what's even worse is that those with Associate's degrees and high school diplomas were more confident in their theories and opinions than those who held Bachelor's degrees.

Be cautious of predictions — both in making them and believing them — because those in the media aren't as interested in airing the cushioned opinions of a professional analyst as they are in airing the brash and bold predictions from celebrity personalities that drive up ratings. In other words, the more prominent the position, the more wary we should be of their predictions.

It reminds me of that Paul Krugman prediction from 1998: "By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's." And, here, Krugman is a Nobel-winning economist, professor, and *New York Times* columnist. Authority, even supposed expertise, is a very poor indicator of accuracy of predictions.

Airing some dirty laundry from my previous domain in the Intelligence Community, the National Intelligence Estimate (NIE) is an annual collaborative report involving input from the nation's 16 intelligence organizations — in other words, produced by people who get paid to think. A 20 year study of the NIE ending in the 1990s found that analytical judgments with the words, "will", "is" or "has" — very definitive words with zero wiggle room — were accurate only 57% of the time. That's a professional track record!

Predictions are outputs with variable inputs. It's akin to baking a pizza: if you leave out an ingredient, or use a wrong ingredient, then the pizza you bake won't be the pizza you necessarily want to eat. In addition, the farther off into the future your prediction is, the more time you're allowing for aberrations in current trends to occur that could cause your prediction to be wrong.

As far as predictions and your ACE are concerned, there are four types of information that you can produce: Facts, Findings, Forecasts, and Fortunetelling. We in intelligence are not in the business of fortunetelling — that includes telling your leadership what they want to hear or telling them what we want to come true. We can share our Findings, which are our opinions of Facts, and we can share our Forecasts, which are our opinions of the future based on Facts. But we can never, ever be Fortunetellers; which, in fact, would include producing baseless information.

If we, as an ACE, are going to produce forecasts, then we need to learn how to describe them properly. We do this by including either statements of probability or levels of confidence. One problem that the analysts who produced the NIE had is that they left themselves no room for small errors in their assessments. "This *is* happening," or "This *will* happen" are very definitive statements and we avoid making them for a good reason. Even if we're absolutely, positively sure that something is going to happen, we say, "This is *likely* to occur." In the event that we're wrong, we've built some room for error into our assessment. We never tell our commander that it *will* occur, only that it's *likely* to; or that it's *unlikely* to, or that it will *possibly* happen. You may be thinking that this is taking the 'easy way out' or that analysts sell themselves short when they don't display complete confidence in their work. Neither of these could be further from the truth! The truth is that we in intelligence can't know everything; in fact, we can only truly know whatever the gathered intelligence information tells us, in one way or another. If there's limited collection, then we remain in the dark, as well. Would you want to go into a gunfight with only half a magazine? Would you want to jump from an airplane with only three-quarters of a parachute? Neither would we and that's why we build in some room for error. Below is the breakdown of our statements of probability along with their corresponding likelihood.

Likely:	> 90%
Probably:	>75%
Possibly:	~ 50%
Unlikely:	< 25%

The alternative is that we assign levels of analytic confidence: HIGH, MEDIUM, or LOW. *We have a HIGH/MEDIUM/LOW analytic confidence that the Leroy Jenkins Gang will attempt to recruit teenagers from the local high school this week.* Which ever method you choose, be sure that your communication is clear and concise. Communicate exactly what you intend to. Our leadership is depending on us to inform them, and if we miscommunicate then we will negatively affect the mission.

Intelligence Tasks and Products

The ACE is the only organization capable of (and responsible for) producing intelligence products. (No one else is going to do them. If you don't do them, then they won't get done.) These products may be ad hoc and in response to a direct need for intelligence, or they may be prepared ahead of time before a need is even identified. Like the term 'product' implies, this is a final output that we call finished intelligence.

There are several intelligence products that you should begin work on immediately. Chapter Six details perhaps the most important of them all: Intelligence Preparation of the Community, or IPC. Your community's IPC product is absolutely the best use of your time right now (aside from reading the rest of this book). In the meantime, and like in the last chapter, I'm going to provide you with a menu of tasks and products that you might want to perform in your ACE.

Mission Analysis

The ACE conducts mission analysis for two reasons: first, to understand the mission, and second, to provide feedback to the commander that helps him better understand the enemy and terrain. (It's counterproductive to provide feedback if we don't understand the mission first.) Regardless of your AO or its conditions, in a SHTF scenario we may experience the need to bring security and stability to our community, through peacekeeping and/or law enforcement, humanitarian aid and disaster relief and other "civil affairs" tasks. Some Americans may even experience fighting in the streets in a worst case scenario; most typically those who live in built-up areas that already host significant levels of criminality. If you haven't already, begin thinking about the actions required to maintain community stability or what might be required to bring security back to the community. Knowing the potential actions and efforts beforehand will increase our readiness to conduct mission analysis.

To begin mission analysis, we need to answer four questions:

- What is the mission? (To degrade the Leroy Jenkins Gang ability to threaten the community.)

- What is the situation? (The Leroy Jenkins Gang, which is comprised of 15 members, is robbing neighbors and breaking into homes in the community, and is exhibiting a growing potential for violence.)

- What is the plan to accomplish the mission? (We will target members of the Leroy Jenkins Gang for arrest.)

- Where are we at risk? (Homes on the edge of our community are at most risk due to our inability to respond quickly. Soft targets such as the elderly are also at the greatest risk. In addition, Leroy Jenkins's cousin has a 50-member gang in an adjacent town.)

Answering these questions will help ensure that we understand the mission and the commander's intent. We may need clarification, especially if there is no mission statement or if it's poorly communicated. It's important that we're able to visualize the same concept that our commander is envisioning; after all, everything we do goes to support his plans. If he has a poor visualization or little conceptual understanding of his mission, then so will we. The mission is not our responsibility; it's the responsibility of our command or leadership. It's our job in the intelligence section, however, to assist our leaders by informing them about the battlespace. The more we understand our command's mission, the better we can foresee how his initial concept might work against the enemy. *We* are the expert on the enemy, not the commander, so it's important for us to be able to provide feedback where current planning might fall short. A plan to clear and hold an area where the Leroy Jenkins Gang is holed up might fail to account for Leroy's cousin, Bradley, who has his own gang several miles away in an adjacent town. What will Bradley Jenkins and his gang do in response to his cousin's problems? That's a great question for the ACE to answer, and it's now a new intelligence requirement. We need to inform the commander of the Bradley Jenkins Gang, and judge their potential for aiding Leroy, because that's a contingency for which our commander needs to plan. Our failure at anticipating — even a failure to know about or acknowledge — the effects of the the battlefield is one that greatly contributes to overall mission failure and strategic shock.

Understand that even with military leaders who have gone through, perhaps, the Army's Command and General Staff College, there are still failures among professional soldiers; and that goes both for command and intelligence elements. It's extremely unrealistic for us to expect any different for most of our community security teams - there will be hang ups, miscues and our peers might drop some balls. We can do our part with decreasing these failures by being proactive in understanding the mission, plan, and situation.

For most community security teams, mission analysis will likely be a luxury. I would expect that most of the time, community security teams are reacting to threats, not being proactive enough in being able to plan for them. This will largely be due to not having enough intelligence, or complete intelligence failures. But mission analysis is an important part of *doing things right the first time*. (Identifying that you don't even have a stated mission is something that can be fixed right now.)

The mission is based on something referred to as METT-TC - that's Mission, Enemy, Terrain & Weather, Troops & Support, Time, and Civil Considerations. In lieu of a formal process completed by our community security leadership, it's going to be helpful for the ACE to conduct an informal METT-TC analysis themselves. Part of our job as analysts, in fact, is contributing to our command's understanding of METT-TC; specifically Enemy, Terrain & Weather, Time, and Civil Considerations. Without our first understanding these factors, we will fail to inform our leadership and contribute to mission failure.

Just like with any analysis, we need data to analyze, so we may need to generate intelligence requirements in order to conduct accurate and specific METT-TC analysis. Here's an *example* METT-TC Analysis.

MISSION

The Community Security Team will secure, protect and defend the community from conventional and irregular threats. Our ability to target leadership and logistics of the Leroy Jenkins Gang is critical to mission success, and an emphasis on providing targeting support will be necessary.

ENEMY

Based on our current intelligence holdings, we expect the primary threat to be the Leroy Jenkins Gang. Secondary threats include individual criminals, with the strong possibility of other gangs and/or looters. Early warning of irregular threat activity may be possible through news stations (television and radio); ham band and other amateur radio traffic from others within the AO, county or greater area; and direct observation from within the AO. The likelihood of a conventional threat is diminished, however, mobilization of Army Reserve/National Guard units is possible. A secondary conventional threat could include law enforcement agencies enforcing unconstitutional laws. Military and law enforcement missions could potentially range from providing security for critical structure to targeting perceived threats throughout the region. We would expect those units to be based locally and likely receive support or direction from higher agencies.

TERRAIN & WEATHER

The AO's terrain is conducive to defense, however, our position off a major primary route could make our location more vulnerable against higher traffic. The terrain includes hills that separate the valley from outside areas, and will make ground ingress moderately difficult but not impossible. The only line of sight into the valley is from the surrounding ridges. Several open fields in the valley can, however, be used for rotary wing/helicopter landing zones (as shown by Targeted Areas of Interest HLZ1 and HLZ2 on the rotary wing overlay of our IPC product).

Weather from October to March can be unfavorable for enemy ground mobility, and can also affect air assets, including unmanned reconnaissance and surveillance aircraft. In the absence of equipment to maintain the roads, the accumulation of snow and ice will make road travel difficult, and passes within the region will potentially be impassible.

TROOPS & SUPPORT

There are local defense forces, namely a local militia, in the area. We have favorable relationships with local residents and will likely receive considerable support throughout our AO against irregular criminal threats.

TIME

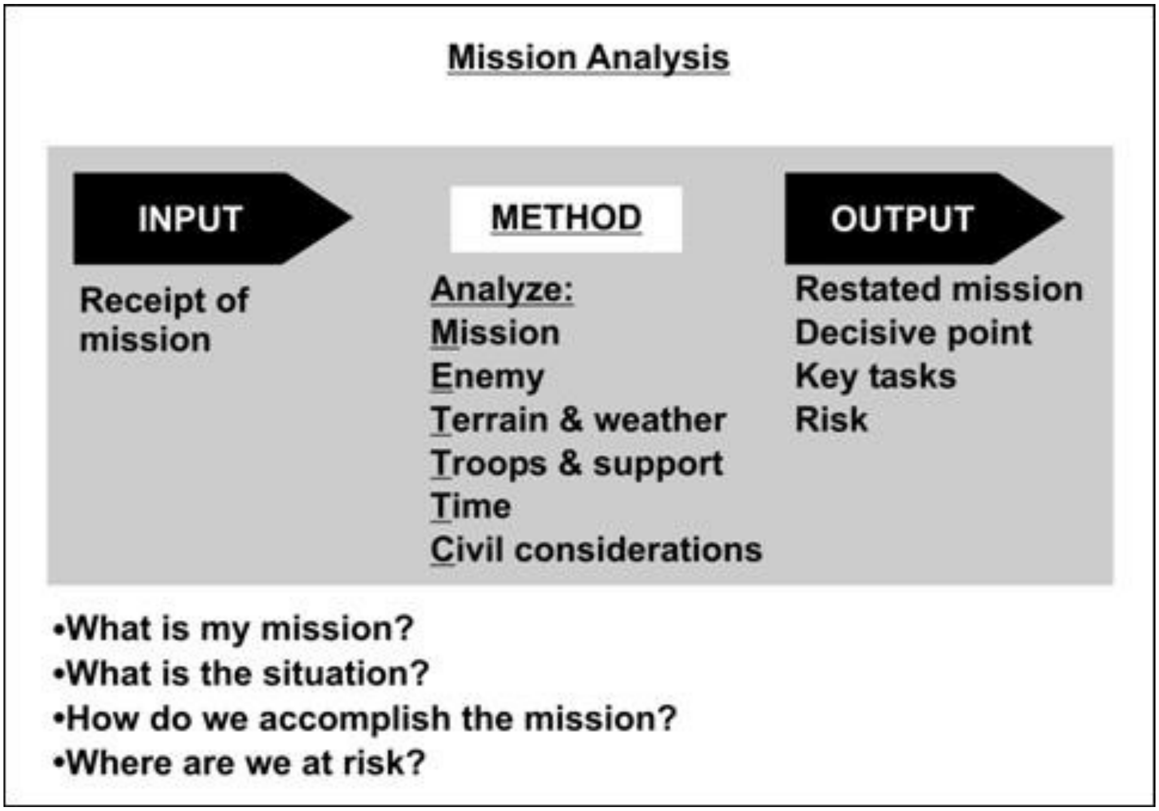
The latest estimate for restoring public services and utilities in the AO is five to six weeks, during which time we expect the needs of the community to increase and the Leroy Jenkins Gang to become more active.

CIVIL CONSIDERATIONS

Local governance is favorable towards the defense of traditional American values and the Constitution. There are, however, numerous local politicians and organizations who will likely seek to disrupt these opinions and activities. Local news media, as a whole, cannot be counted upon to provide pro-Constitution or pro-Liberty media coverage. There are stations more amenable to spinning positive stories about local defense forces, while others would easily provide pro-regime influence (these stations are named in the IPC product). Based on the capability of irregular threats, our ability to hold critical infrastructure within our AO is favorable. Our ability to hold critical infrastructure within the AI is questionable, based on the significant irregular threat.

As far as an introduction to the situation goes, one or more paragraphs for each of these six METT-TC topics will go a very long way in catching our teammates up to speed, as well as ensuring that we, ourselves, understand the mission and situation. Not every part of METT-TC will be easily answered by the ACE; Troops and Support, for instance, is information that we typically don't concern ourselves with as the intelligence element.

Understanding the mission is just the pre-requisite to mission analysis. Some of the feedback that an astute commander wants to know is, *What will the enemy do in response?* In order to answer that question, we have to ask a couple more: *How will the enemy perceive our actions?* and *What options does the enemy have based on his goals and capabilities?* Being the experts on the enemy, that'a question that only the ACE can answer. What the commander is specifically looking for is what's called a Course of Action, or COA. As the ACE, if we know the enemy well, then we should be able to provide our commander with a range of potential COAs. If the mission is to clear and hold the turf of the Leroy Jenkins Gang, then we must predict what they will do in response. (Additional information on COAs and COA development can be found in Chapter Six under the subsection on Determining Threat Courses of Action.)



Mission Analysis

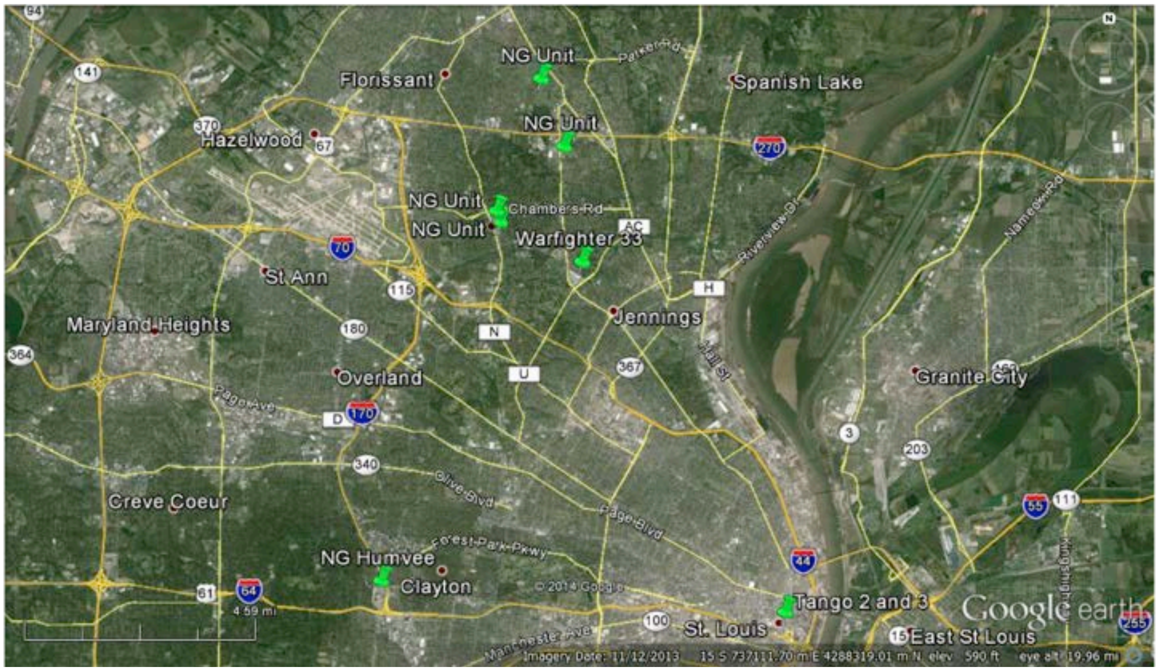
INPUT	METHOD	OUTPUT
Receipt of mission	Analyze: Mission Enemy Terrain & weather Troops & support Time Civil considerations	Restated mission Decisive point Key tasks Risk

- What is my mission?
- What is the situation?
- How do we accomplish the mission?
- Where are we at risk?

Battle Tracking

As the team saw during Operation Urban Charger (see Vignette: Operation Urban Charger, page 52), battle tracking is mission-critical for our own security because it allows us to visualize events in our AO. Imagine battle tracking like keeping up with a chess game that we can hear but not see. Each space on a chess board is named according to its row and column, (Rows A-H and Columns 1-8), much like home addresses (9811 Mulberry Lane, for instance). We hear that Player 1 moves his rook from space A2 to space C3, but that doesn't mean much to me, and probably not to you, either. If someone were to call out current locations of chess pieces, then we'd have a hard time keeping up with all that information in our head (we have very limited space up there). So instead we might break out our chess board and pieces and then move each of these pieces when its location is called out. We're visualizing information. (Admittedly, it may be a crude analogy, but it's the same concept.)

In our job as analysts, we can build visual representations of current locations throughout the AO in the same way, but we may be getting information like, "The police have set up a road block at the intersection of Oak Avenue and 15th Street."



In the screenshot above, an Urban Charger analyst used GoogleEarth to track the locations of roadblocks during the Ferguson, MO riots. While listening to just the police scanner, the analyst simply plotted events onto the map as they were reported. This allowed us to 'battle track' the current location of squad cars, shots fired, skirmish lines of riot police, burning buildings, and as well as the movement and activities of rioters and looters. Had we lived in Ferguson, we could have provided early warning intelligence to our neighbors and other residents.

Using GoogleEarth is a really great tool for several reasons. Not only do we have access to tons of data in the Maps Gallery, but we can also draw on these maps and overlays and export our work as .KMZ files. For instance, if I was to locate and add pins for all of our police, fire, and emergency services facilities throughout the AO and AI, then I could save and export the file, and distribute it to all my team members. They'd be able to open the file in GoogleEarth and see the same data I'm looking at. (Additional information can be found in the Chapter Six subsection on Imagery Intelligence).

Although GoogleEarth can be an invaluable tool, I highly suggest resorting to map board and overlays for two excellent reasons. First, they're not susceptible to electronic surveillance like your internet connection is, and second, we can use them regardless of the availability of electricity or the internet. Building a map board is easy and it's well worth your time. A map board is simply a map with a hard wood or cardboard backing with attached overlays, which are clear sheets of film, like mylar or acetate. We never want to draw on maps, so having numerous overlays allows us to record various physical elements of the battlespace.

In order to battle track, as well as to create additional overlays, your ACE will need the following items:

- 1:24,000 USGS Topographical Map of your AO (multiple copies; available from the USGS, mytopo.com, and numerous other websites). I recommend this map be somewhere in the range of 24"x36" or larger.

- Recent imagery photos of your AO (available from terraserver.com and other websites). I recommend this imagery be somewhere in the range of 24"x36" or larger.

- Street map of your community/AO (available in Google Earth). I recommend this map be somewhere in the range of 24"x36" or larger.

- Acetate, clear mylar or clear plastic for our overlays.[21] Order enough for at least ten overlays that fit over your imagery or map.

- A pack of small or medium binder clips (available from your average office supply store).

- Dry erase or wet erase markers in black, red, blue and green (available from your average office supply store).

- Tri-fold project cardboard or other hard backing material (available at crafts and general purpose stores). Purchase one for your topographical map, one for your imagery, and one for your community street map.

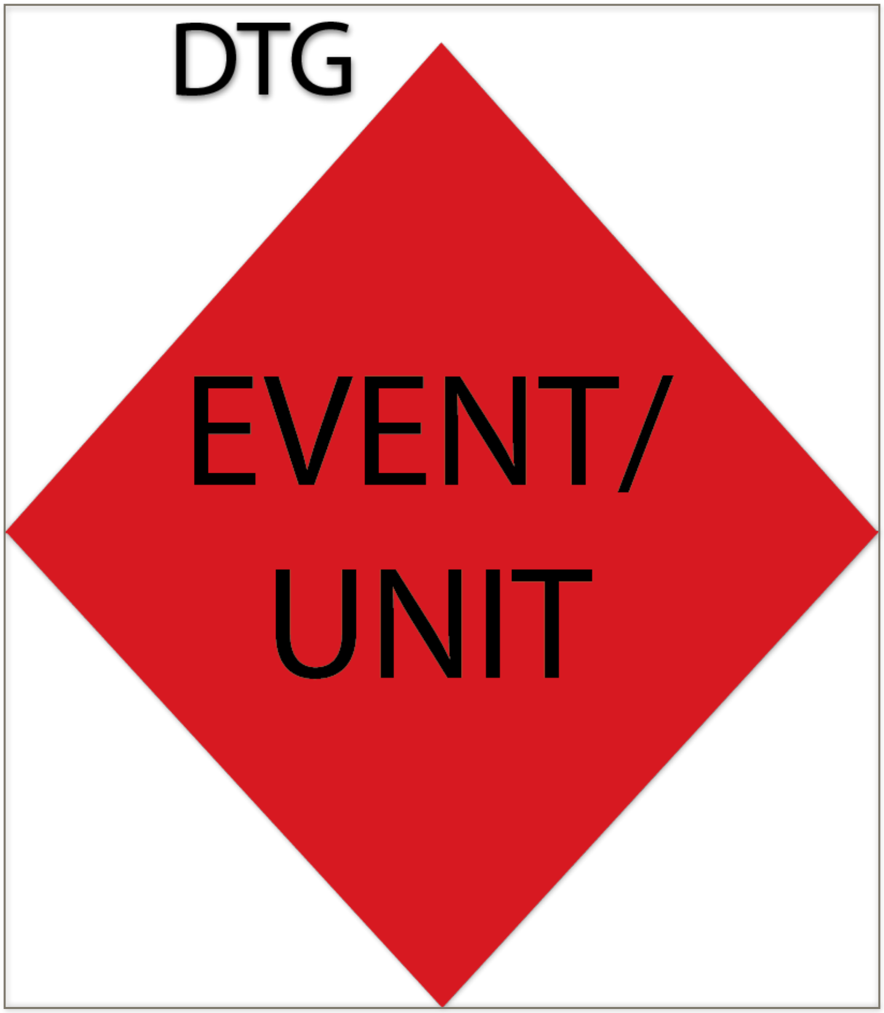
- Pins, clips

You'll use these items to create your map boards. Take your maps and either tape, pin, or staple each to their cardboard backing, ensuring that the maps won't slide around. This is your basic map board. Next, you'll want to affix your acetate, mylar, or clear plastic sheeting over your map, by using your binder clips. (We never want to write or draw on our map; that's what the clear plastic sheets are for.)

Having these ready to go on a table or hung on a wall in your ACE shop will greatly increase your ability to be immediately productive. Whether you're tracking flood lines and high water marks, wild fires, riots, or attacks from gangs, in most cases, you're going to be head and shoulders ahead of the competition.

At this point, we have our map board set up, along with an overlay, so let's talk about what we're going to put on this map. We call it military symbology; a set of icons used universally to represent units and events. Although standard symbology can be quite complex, we're going to stick with a very simple version. We should have four colors of markers: black, red, green and blue. Black will be used for boundaries (like our AO and AI) and obstacles. Red is always used for the enemy. Green is used for what we call "host-nation"; that is, local security units who aren't "friendly" but also not an adversary. And although we won't use blue very often, it represent friendly units.

In our simplified symbology, we're going to use one basic shape: red diamonds represent enemy units or activities (if you have trouble drawing diamonds, you can use triangles instead, as pictured below). Before we get into the symbols, understand that the irregular threat is more difficult to track that the conventional threat. An enemy infantry company or tank battalion is in plain sight; we can identify their location and plot the unit on the map. It's relatively simple to move the position of the enemy tank battalion; just erase its previous position and redraw the unit to reflect its current position. Irregular threats on the other hand — say, a group of three criminals — are harder to track, so we end up plotting their activities, instead.

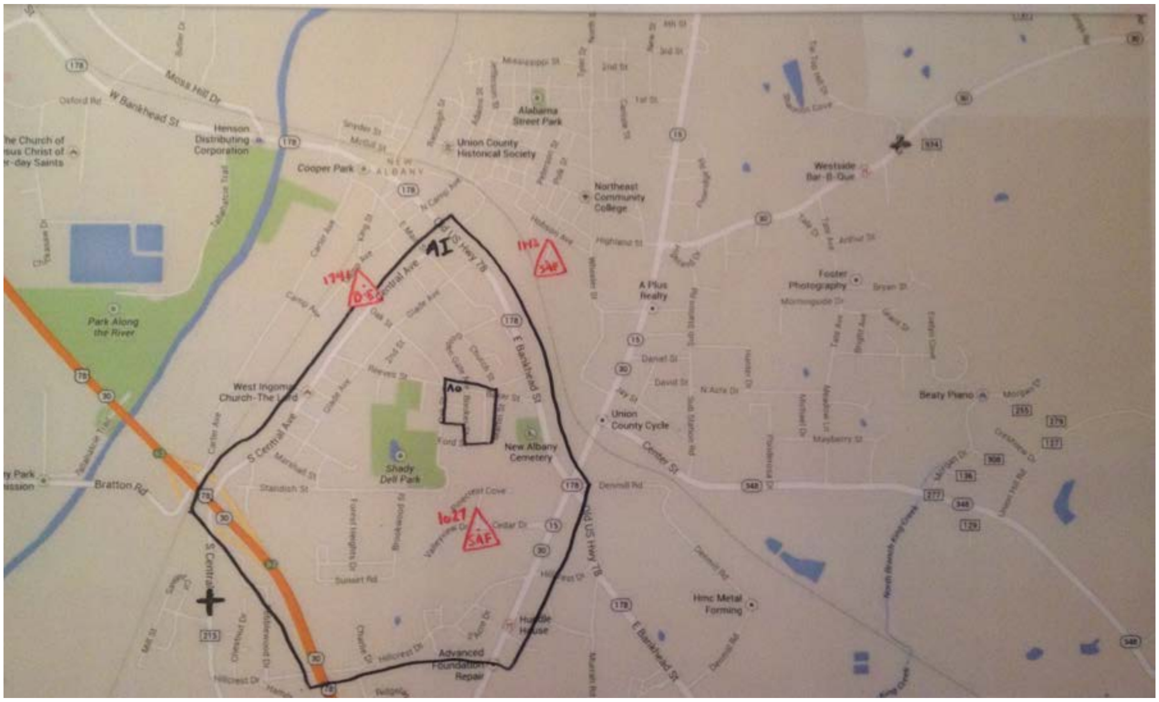


The diamond symbol is our template for plotting these irregular threat activities on our map overlays. In the center of the diamond is the event type; typically in abbreviated form. For us, there is no master list of activities and their abbreviations, but I can get you started with what's likely to be some more common activities. Shootings, for instance, we might call SAF, or Small Arms Fire. Robberies could be abbreviated to ROB. Kidnappings might be KID. Murder could be MDR. You get the idea.

One other issue we might have is that of attribution. If we're plotting these events, then who's committing them and how can we tell one irregular threat group's activities from another? Let's say that we have two named gangs in the area and countless other criminals. We might begin attaching LJG to the events, representing Leroy Jenkins Gang activity. We might write BDC for the Bill Davis Clan, and CRIM for common criminals. We might use a question mark (?) for unattributed events that are reported. You may opt for a separate color scheme: red is one group, green is another, and blue is yet another group.

On the top left-hand corner of the diamond is our Date Time Group, or DTG. That's the date and time that the event occurred, which is not necessarily when it was reported to us. The format of the DTG is up to you. Typically, we use the four digit time and time zone, then year, month and day. It looks something like this: 1724L20150621. This jumbled mess means, 5:24pm, Local time, on the 15th of June, 2015. I find that it's rather a lot of information, especially considering how full our map overlay might get. So we have some options. Option One is that we just put the four digit military time (e.g., 1724 or 0537) and we use a new, clean overlay for each day. Pursuing this option will allow us to "flip" through days and potentially recognize patterns in enemy operations. Let's say, for instance, that the Leroy Jenkins Gang's robberies have been slowly moving eastward over the past week. Option Two is that we keep a running event log, assigning each event a number. That way, instead of writing out a long DTG, we can put #17. If we want more information about that event, we look up Event #17 in our log book and find what we need. We must remember, however, the 'trash in, trash out' concept. If we plot #17 on the map and fail to record it, or fail to write down relevant data about the event, then it's might be very difficult to dig that information back out from our memory. Still, keeping an event log has its own advantages; you may find that a mix of both works best.

This is your ACE. It's yours to run however efficiently and smoothly that you can run it. Whatever you choose for your map symbology and the events you encounter, ensure that everyone knows the correct terms so that everyone can read — and plot — these events in the same way.



INTSUM

The Intelligence Summary, or INTSUM, is usually a daily product that includes the significant intelligence reporting and events from each day. This report is a great way to provide a quick intelligence brief to our leadership, or new analysts, and it also acts as a daily summary that can we can archive for later use. Are you trying to remember which day of the previous month that the local grocery store was robbed? Go flip through last month's INTSUMs where you can find it.

If no significant information was reported or no significant events occurred, then there's simply nothing to report. All significant reports and events, however, should be included in the INTSUM. Typically, this summary is compiled at the end of each shift change. If you're providing 24/7 support, then be sure to get each analyst's or team's input during the shift change meeting. Explain what, if anything, happened and then be sure to record that information in the daily report. The purpose is to facilitate the communication of relevant information so that nothing falls through the cracks. Here's an example of a daily INTSUM.

Intelligence Summary (INTSUM)
07 JUN 15

Conventional Threats Team

Nothing to report.

Irregular Threats Team

Two sources reported that the Leroy Jenkins Gang is suffering from a lack of ammunition. This comes after the death of one of its members, and the arrest of another. (Analyst Comment: Anthony 'Shady' Johnson was killed in a shoot out with local law enforcement on the night of Monday, 01 JUN 15. Johnson has long been suspected as a facilitator who coordinates the shipment of arms and munitions for the gang. His death will likely have a large impact on the gang's activities. At this time, there is no suitable replacement for Johnson as a facilitator, and the gang's lack of ammunition will continue indefinitely.)

Civil Affairs Team

Our engineer reported the completion of the well project that will provide clean water for our community. Several community members approached the volunteers to give their thanks, and asked how they could support our community security/stability efforts.

Politics Team

According to an intelligence source, the City Mayor was upset that our community had dug a well. Specifically, he was concerned that this accomplishment undermined his authority. No further information is available. (Analyst Comment: The Mayor has a history of seeking reprisal against his perceived political enemies. In the past three years, he's ordered the arrest of two citizens and revoked the permits for several businesses as a result of open opposition against his policies and efforts.)

// END INTSUM

Enemy SITTEMP

The daily Enemy Situational Template, or Enemy SITTEMP, is a map of the latest or last known disposition of enemy forces in the AO. We're going to use the same exact symbology from our battle tracking efforts to produce an overlay of the known or suspected locations of enemy forces. We can provide this map each day to our leadership so they can have an understanding of how the enemy is arrayed, and what's changed from the previous days or weeks. Through plotting these units and keeping a daily tally, we can identify patterns in movement or activity. Patterns are exploitable. The more patterns we as analysts identify, the better we may be able to exploit and more quickly defeat our adversaries.

Order of Battle

Order of Battle (OB), sometimes referred to as OrBat, is an intelligence product detailing the command, strength, disposition, and equipment of conventional military units. Building and maintaining these OB products for adversary and neutral forces is a very traditional task of the intelligence analyst. Sitting in the Pentagon right now, there's a likely an OB product for every military in the world, and each is updated periodically to reflect the most current design and health of the force. The OB is one of the most important of all intelligence products when facing a known adversary, and it costs nothing but time, collection and analysis to produce.

Typically, military intelligence analysts are assigned to a particular country or region, just as you are assigned to your own AO. If I was in a unit at Southern Command (SOUTCHOM), maybe I'd be looking at a nation's military, or perhaps focusing on terrorist groups or drug cartels. Either way, one of my first tasks would be to become intimately familiar with those forces. I would become the subject matter expert, and when there was a flashpoint or an event that required expertise, I would be called on to answer the questions of senior-level military or political leaders. A typical responsibility would be to provide periodic intelligence products to support operational or contingency planning.

We build OB products because they allow us to authoritatively estimate the capabilities of adversaries. The more we know about an adversary's organization and capabilities, the better we can identify the unit's future course of action, or COA. For instance, we can examine a military force and determine its capabilities. At the same time, we're identifying their limitations and vulnerabilities, which both affect their future operations. We can begin to remove potential COAs because the force is too small or too large to pursue that course of action; or the force is too technologically limited to pursue a particular COA; or the force is too vulnerable to pursue yet another potential COA. We're narrowing down a long list of potential scenarios in order to identify what's more likely and what's less likely.

One of the most critical parts of intelligence is being actionable or predictive. Using our completed and up to date OB products, intelligence analysts are able to determine which potential courses of action a military or adversarial force will take on the battlefield because we know their capabilities, and, therefore, we know what they're most likely to do. In this way, the OB product is a fundamental requirement for intelligence analysts to produce.

Although slightly different for our needs, OB intelligence products should be a mainstay for us, as well. We're going to want to look at security forces such as local law enforcement and any state or federal agencies in our area. That's the conventional side. We don't do this in order to fight them; on the contrary, our best case scenario is providing support to local authorities in order to bring security to an area. We complete an OB product on these organizations to see what they're capabilities are. For instance, how many emergency and law enforcement personnel would be required during a 100-year flood in the area? If we know that our local agencies don't have the capability to respond, then we not only know that these types of events will require outside support, but we'll also know that there are going to be people whose needs won't be met. That's predictive intelligence that may allow us to better provide support.

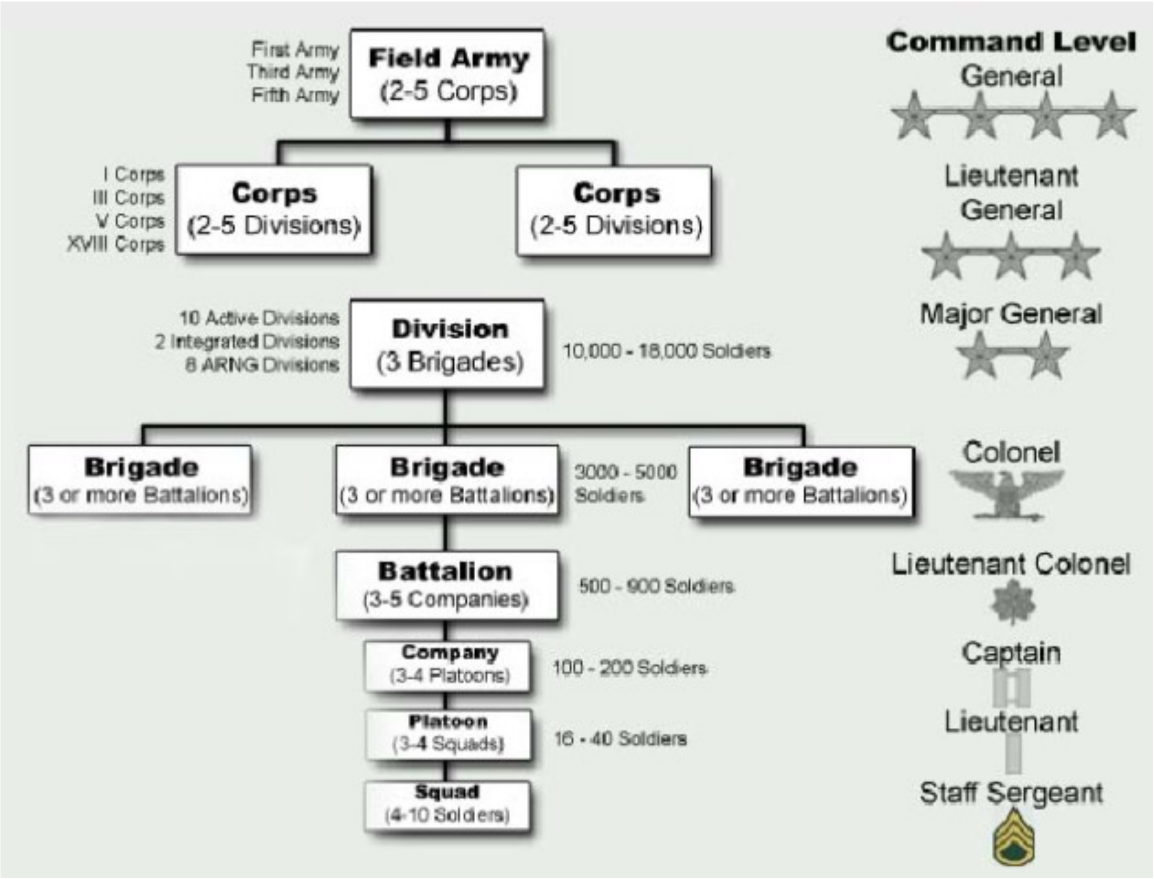
On the irregular side, we're going to look at organized crime, gangs, or other organizations that potentially pose a threat to us. We're going to approach the OB product in the same way, identifying leadership, strength, disposition, and capabilities, among other things. If we determine that there are, or will likely be, more criminals than law enforcement in our AO during a SHTF situation, then that's now predictive intelligence. Next we get even more predictive by identifying what kinds of activities these criminals be involved in, what level of violence can we expect from the various groups, how many of them there will be, etc. We can't definitively answer those until we understand the threat's structure and organization, which is the strength of our OB intelligence products.

As we look at potential adversaries from around the region, whether it's the Leroy Jenkins Gang coming to relieve you of your beans, bullets and band-aids, or a Military Police Company bringing some form of martial law to the area, we need to become experts on any group that will affect our AO. Building out an OB intelligence product is a very, very good place to start.

Our OB product is going to include two sections: 1) a Table of Organization & Equipment, what referred to as TO&E, and 2) a nine paragraph threat estimate. These two products make our larger finished Order of Battle for each potential conventional threat in our AO.

There are a lot of great resources to gather intelligence information; chief among them is the unit or organization's website itself. I'm not overly concerned with the Idaho National Guard's intent to confiscate our weapons, partly because I see on their website a mission "to protect, preserve and defend the lives, property and individual liberties of the citizens of Idaho…" Am I still going to build out an OB of the local units? You bet. These products will greatly aid me in determining their ability to provide stability and support operations in the area.

Go to your state's National Guard and Reserve unit websites. Typically, all your combat arms units are going to be National Guard. Reserve units are going to be combat support and combat service support classes (i.e., not combat arms units). Take a look around and find a list of state-wide units, then start drilling down on each unit in order to identify their proximity to you. We're going to start our OB products on the combat arms unit nearest you, whether it's six miles away or sixty miles away.



Write down the unit name – something like 2/116th Armored Cavalry or 65th MP Company. Army units, in order of small to large, go like this: company, battalion, brigade, division, corps, army (see diagram above).

Once you've written down the unit name, head over to Global Security's National Guard page[22]. Click on your state and examine the units listed there. I went to the Idaho page and drilled down on the 116th Armored Cavalry Brigade. These pages give some information on the mission, size and scope of these units. Familiarize yourself with the unit nearest you.

Here's the information you'll need – our Intelligence Requirements – to complete your OB product (this is not a complete list):

– What is the unit's disposition in the region? (In other words, what are all the unit's locations?)

– What is the unit's deployment history?

– What mission(s) was assigned to the unit while deployed?

– What is the force strength of the unit?

– What type of support is required for the unit to operate in any given 30-day period? (What will the unit need?)

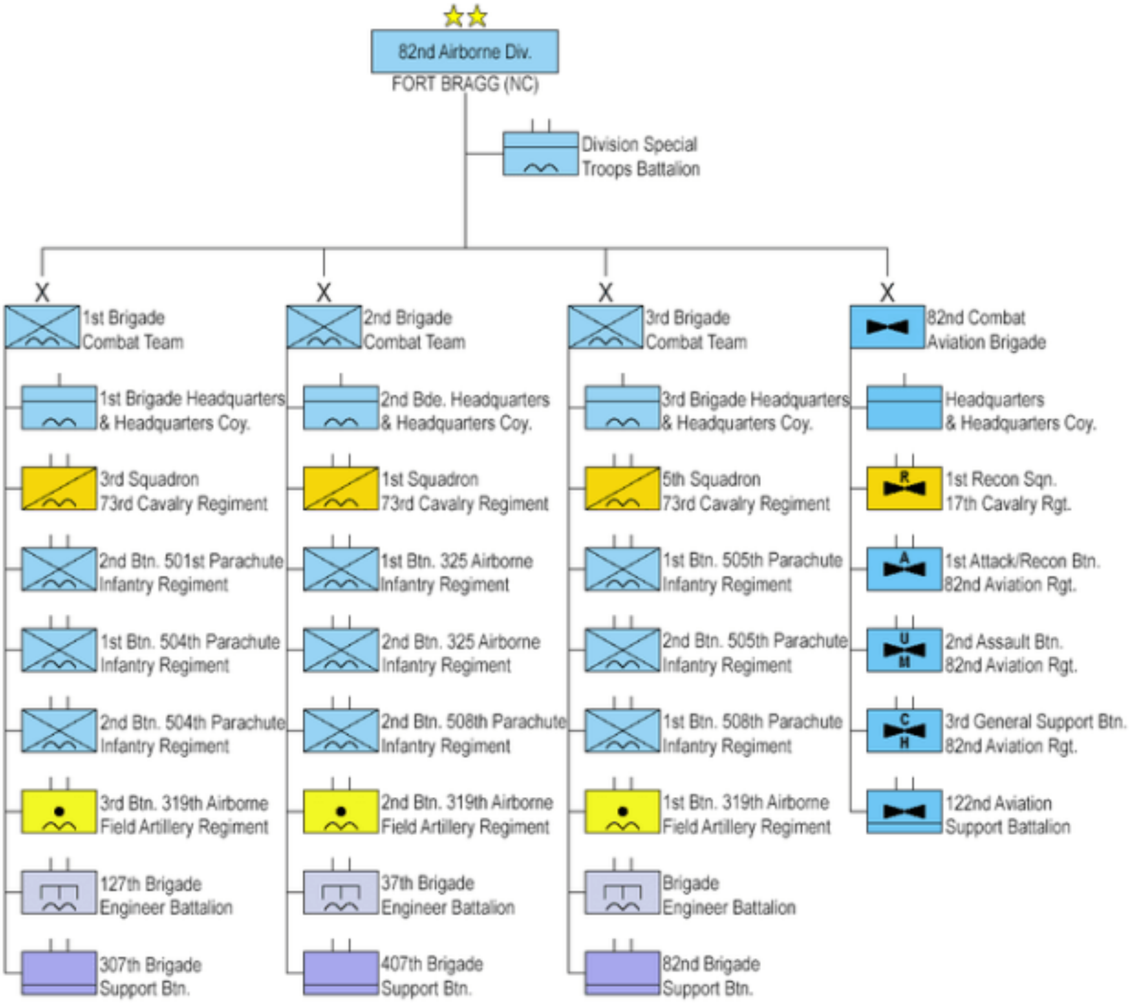
– What equipment, by subordinate unit type, does the unit have?

– What is the established doctrine of parent and subordinate units?

– What types and levels of training does the unit participate in?

– What are the logistical requirements for the unit? (How will it be re-supplied?)

– What communications systems are available to the unit?


82nd Airborne Div.
FORT BRAGG (NC)
Division Special Troops Battalion
X
1st Brigade Combat Team
1st Brigade Headquarters & Headquarters Coy.
3rd Squadron 73rd Cavalry Regiment
2nd Btn. 501st Parachute Infantry Regiment
1st Btn. 504th Parachute Infantry Regiment
2nd Btn. 504th Parachute Infantry Regiment
3rd Btn. 319th Airborne Field Artillery Regiment
127th Brigade Engineer Battalion
307th Brigade Support Btn.
X
2nd Brigade Combat Team
2nd Bde. Headquarters & Headquarters Coy.
1st Squadron 73rd Cavalry Regiment
1st Btn. 325 Airborne Infantry Regiment
2nd Btn. 325 Airborne Infantry Regiment
2nd Btn. 508th Parachute Infantry Regiment
2nd Btn. 319th Airborne Field Artillery Regiment
37th Brigade Engineer Battalion
407th Brigade Support Btn.
X
3rd Brigade Combat Team
3rd Brigade Headquarters & Headquarters Coy.
5th Squadron 73rd Cavalry Regiment
1st Btn. 505th Parachute Infantry Regiment
2nd Btn. 505th Parachute Infantry Regiment
1st Btn. 508th Parachute Infantry Regiment
1st Btn. 319th Airborne Field Artillery Regiment
Brigade Engineer Battalion
82nd Brigade Support Btn.
X
82nd Combat Aviation Brigade
Headquarters & Headquarters Coy.
R
1st Recon Sqn. 17th Cavalry Rgt.
A
1st Attack/Recon Btn. 82nd Aviation Rgt.
U
M
2nd Assault Btn. 82nd Aviation Rgt.
C
H
3rd General Support Btn. 82nd Aviation Rgt.
122nd Aviation Support Battalion

Included in our OB product is going to be a Table of Organization & Equipment (TO&E). The chart above is a division line and block chart. Chances are excellent that you don't have a division in your backyard, but most Americans will have a battalion headquarters, company or company headquarters, or a company detachment at a local National Guard or Reserve base within a couple hours of their location. All the chart above is missing is the equipment, which to simplify the process, I would just add under each unit, i.e. Armor Platoon: 16x personnel, 4x M1A1 Abrams tanks (4x personnel each). (I use 'x' to denote a specific number; 40x or 4x or 1x.) A division is a huge organization, so it's best to start at the company or battalion level. Your local reserve/national guard units will likely be a company or battalion.

Global Security is a great source of information for military units. I typed in each unit number and name (145th BSB and 1-183rd Aviation, for example) and arrived at each of their pages. At the 1-183 page, I learned that the Combat Aviation battalion has AH-64 attack helicopters. (Good to know!)

Knowing this information, I then generated new IRs:

1. How many AH-64s does a Combat Aviation Battalion have?

2. How many personnel is in each troop/company of 1-183 Aviation?

3. How many personnel does it take to maintain each aircraft? (Tooth to tail ratio, for instance.)

That starts a new collection phase, and I document the information along with the source for each IR. If I identify new intelligence gaps, then I create a new IRs and add them to the list.

Another great place to learn about exact TO&E is the Federation of American Scientists (FAS)[23]. Here we can find typical TO&Es for all the unit types (Combat Aviation Attack Company, for instance). Do a search for each unit type and look at a typical make up. Think about each unit's ability to project force. Think about their operational requirements for logistics, including supply and transportation. Think about which routes they would use in your county or AO. These are the types of questions that good intelligence analysts ask.

The second part of our OB product is a nine paragraph threat estimate. Start a text document and copy down these nine paragraphs, generating your intelligence requirements for each. Then begin collection and include relevant information under each topical heading. When you're done collecting information, next fuse this information together. Now you have an intelligence product. Here are our nine OB sections:

1. Composition

2. Disposition

3. Strength

4. Tactics

5. Training

6. Logistics

7. Combat Effectiveness

8. Electronic Technical Data

9. Miscellaneous Data

1. Composition — Let's start with identifying the composition of your local law enforcement; specifically the County Sheriff's Department. Why is this information good to know? Because as an intelligence analyst in a SHTF scenario, I'd like to be able to tell my group whether or not the Sheriff's Department will be able to provide security during the emergency. If they're unable, then there will be threats that remain unaccounted for and that will require extra effort on our part. Composition is its organization; what elements or units is the agency composed of?

We're going to identify the composition of all security and threat forces in our area. So, by necessity, we're going to be building several OB products; one for each agency, department, or group.

2. Disposition — By 'Disposition,' we mean location. Where are the headquarters, stations, or sub-stations of the agencies or departments? Are there regular patrols, and, if so, what areas get regularly patrolled and when? Our intent here is nothing nefarious, but answering these questions will give us a much better idea of the security picture for our AO. It's important to know what a regular law enforcement presence looks like, so we can determine spikes or lulls in traffic or activity. These indicators may signal that a critical event is occurring or about to occur.

3. Strength — We've already identified the structure of the Sheriff's Department, and now it's time to start answering questions about strength. How many full-time, part-time, and volunteer deputies are employed? How many deputies are on duty at any given time? If necessary, how many additional officers can be recruited and put in the field during an emergency? What vehicles, including war/combat vehicles, does the department have, and how many? What types of weapons are available, and how many?

4. Tactics — Perhaps the best way to learn about an organization's tactics is to look at its previous activities and current doctrine. In the schoolhouse, we learned intelligence on a Soviet-style adversary. Everything we expected to see from our adversary was based on doctrine and their OB – in other words, the recorded history of the way they did things in previous conflicts and engagements. Everything our adversaries expect of the US military are based on our doctrine; they expect us to act in a similar fashion in future conflicts as we have in recent conflicts of the same type.

So let's begin by looking at the most common tasks of an organization. In the military, we call it the Mission Essential Task List (METL). These are the handful of skills that we need to master in order to accomplish our mission.

So when completing OB, we ask, 'What's the mission?' How do they accomplish that mission? What are the things they do, and how do they do them? We need to take a long look at their tactics because we can know what to expect in the future based on that history.

The last thing we want to consider is, ‘Are their tactics effective?’ What was the outcome of their last engagements? If their tactics aren’t effective, then we as intelligence analysts can examine what they might change. In that case, we can tell our leaders that we expect the enemy to change X or Y about their operations. Knowing that those changes are expected, or could occur in the future, will help our leaders plan.

5. Training — When I went to my own county’s SWAT page, I learned a bit about the team’s strength, and also about the training hours each month. In my case, this county doesn’t have a full time SWAT/Tactical Response Unit, so they provide some special training to a few county sheriff’s deputies. What can we learn from these two pieces of information (training hours and strength)? What are they training for? Who are they bringing out to train them, or is the trainer already an employee? What are their training requirements or goals?

Once we have a good idea of a potential adversary’s training plan, we can begin drawing some conclusions. What’s the quality of their training? Are they going to be well-prepared for their next engagement?

6. Logistics — They say that amateurs argue tactics, and professionals argue logistics. If you have 100 troops out on mission, but have no way of supplying them with the things they need then your organization won’t be as effective. Same goes for all units, military or civilian. So we ask, ‘How does this organization get re-supplied?’ Where are the supply depots? What routes or channels does supply come from? Logistics is more than just supplies; it’s how those supplies are delivered. In many conflicts, adversaries sought to fracture supply lines in order to make adversarial forces less effective. A rifle, when out of rounds, becomes a blunt force object. So including Logistical and supply line information in the OB is very important. If we can provide intelligence that can be exploited to weaken our adversary’s ability to fight, then we are doing our jobs in intelligence. And that’s why we do our homework and create an OB product before we get into a fight.

7. Combat Effectiveness — In order to judge the combat effectiveness, we have to know a good bit about the history of the unit. We need to utilize intelligence sources to understand previous operations or engagements. From a previous component, we would analyze their training in comparison with potential threats or defensive preparations. If a unit has been preparing for a conventional war, they they may perform poorly in an unconventional war. If an adversary doesn’t train for dynamic entry and room clearing, then they may not be very good at it. We can look at another component — Logistics — and judge potential combat effectiveness if there’s limited re-supply. We could do some analysis and, as an example, say that after the fourth day of operations, combat efficiency will decrease due to poor logistical support. We always want to provide predictive or actionable intelligence, and judging an adversary’s combat effectiveness is a good way to do that.

8. Electronic/Communication Technical Data — In this section of the OB, we'll want to provide information about communications and other technical equipment. What frequencies does an adversary use to communicate? What type of communications equipment is used? What are the observed call signs? Where are static communications posts? What type of Signals Intelligence (SIGINT) equipment is available (if any)?

9. Miscellaneous Data — Finally, we arrive at a catch-all section. And example of information we might include is that the adversary commander has a secret family or a drinking problem or gambling debt. We might include information about previous attempts to reform or re-organize a unit or organization. Maybe the current leader is not respected or poorly liked by his troops, or other morale information. We'd include any pertinent data that could be good to know.

TO DO LIST:

- Become a subject matter expert
- Get topographical and street maps of your area
- Get overlay materials for battle tracking
- Build a map board
- Practice plotting events on your map board

Section Two - Collection

Chapter Five - Developing Intelligence Collection

Learning Objectives:

- Understand the available types and methods of intelligence collection
- Learn where to find and how to develop sources of intelligence information

Intelligence collection provides the lifeblood of the ACE. Access to timely and relevant information is absolutely crucial for the mission. Its importance really can't be overstated. We get into a bit of the *chicken and the egg* syndrome when we discuss which is more important: collection or analysis? On the one hand, without collection there can be no good analysis. Without a stream of reporting, analysts can do little other than twiddle their thumbs (or perhaps try to collect information themselves). On the other hand, having lots of information but no one to process and analyze it does us little good. In fact, it may cause more harm because we may be acting on inaccurate or incomplete information without the trained eye of an analyst to gauge its veracity. Further, while intelligence collectors report their information, they don't report intelligence, nor do they make intelligence products. Without analysts, there can be no finished intelligence, which is what our command element needs. Our collection assets, therefore, and the information they collect can either be an enabler of or a hindrance to good intelligence.

Intelligence collectors are not analysts and should not be involved in the work of analyzing their own gathered information. Remember that your ACE is an "all-source" effort; that means that your analysts are looking at potentially lots of information from many different sources. A human intelligence collector, for example, is only seeing a small sliver of the total amount of information going into the ACE. Similarly, a collector who's monitoring communications intelligence from radio traffic only sees his small slice of information. These collectors can't possibly begin to analyze their own collected information because each only knows what he's collected. A collector may be completely oblivious to another source who's reporting conflicting information. It's up to the analyst alone to deconflict the information from these two sources. The analyst is the only individual capable of fully understanding the importance or relevance of any piece of information in the broader scheme of an all-source intelligence effort.

And this is why the ACE drives collection. The ACE is in the drivers seat because they see both the road and the map; they know the organization's current location and where they need to go in order to get to the commander's intelligence destination. Each intelligence requirement identified by the ACE in Phase One of the Intelligence Cycle is an instruction. Our collection assets are tasked; that is, they are instructed or directed to collect based on the informational needs of the ACE. This isn't an abusive or dictatorial relationship between collectors and analysts, however, our collectors should understand that they are a cog in the intelligence wheel. To achieve maximum efficacy, they absolutely must be responsive to tasking and collect the information prescribed in the ACE's intelligence requirements.

At the community level, we're likely to be dealing with our four primary intelligence disciplines: Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Signals Intelligence (SIGINT). (For a refresher on each of these types of intelligence, see page X.) The rest of this chapter is dedicated to helping you stand up collection in these four areas.

A Word on Security

In his article entitled, *73 Rules of Spycraft*[24], former CIA Director Allen Dulles's first and second rules were about security in the profession. He wrote, "There are many virtues to be striven after in the job. The greatest of them all is security. All else must be subordinated to that." I like to the think that he included security as the first two rules because they are among the most important of all lessons for the intelligence collector. Simply stated, if you don't have security, then you don't have anything. In fact, the more time and training you dedicate to becoming a better intelligence collector, the more valuable you become. Your compromise will more greatly affect the organization's intelligence effort. Before venturing out to collect intelligence information, or setting up collection networks, we must be deliberate and thorough in our analysis and understanding of the threats in our operating environment. If we don't understand these threats and their relation to our environment, then our efforts could be exploited[25].

Open Source Intelligence

Several factors make Open Source Intelligence, or OSINT, our most important source of intelligence information. For starters, the U.S. Intelligence Community estimates that 80 percent of all intelligence information around the world comes from open sources. The same could probably be said of many of our own AOs. Second, OSINT information is so widely available. Every blog, social media post and check-in, television and radio news report, newspaper, transcript, directory, web and magazine article, speech, and live event produces OSINT information. Third, OSINT collection requires no sensitive equipment, technical know-how, or rigorous training. If you can operate a computer, and watch and listen, then you can be an OSINT collector.

In his book *Fixing the Spy Machine*, author and CIA veteran Arthur Hulnick writes of OSINT: "Neither glamorous nor adventurous, open sources are nonetheless the basic building block for secret intelligence."[26] In short, there's just too much free and open intelligence information out there to neglect this avenue of collection. An analyst's ability to associate or fuse together seemingly disparate pieces of information make news sources and the internet prime hunting grounds for collectors. Every reporter is, in essence, an intelligence collector. They have access to people and events that we do not, and therefore are invaluable assets. It's time that we start viewing media outlets as part of our intelligence collection; cautiously in many cases, but we should always be monitoring the multitude of reporting streams. And that's why we cover it first: it absolutely should be our first effort.

There are two ways that we can collect OSINT information: passive and active. Because we will always be limited by our finite time and resources, passive intelligence collection is preferred where possible. Removing much of the effort required to go and find this information, passive collection allows us to simply monitor updates and determine what, if anything, is of value to us. News aggregators and other online tools that automatically procure information or links to articles are already doing much of the work for us. GoogleAlerts is perhaps the best of them all.

GoogleAlerts[27] is a free service that monitors the keywords we tell it to monitor. For instance, I can sign up to receive alerts whenever the keywords "Harris County" and "drugs" are found in the same article. We can replace the keyword "drugs" with "gang", "murder", "shooting", "robbery" and any other search terms, and GoogleAlerts will send us an email whenever the keywords are mentioned in the same article.

GoogleAlerts and services like it are automated, saving us a great deal of time and effort. Most of the time, these services do exactly what we ask of it: they email us alerts based on our search strings. So that means that our search strings have to be accurate, and we have to ask for the information we're looking for. The search string "Harris County AND drugs" will give us articles containing those keywords, regardless of state. Because we could be getting alerts from any state with a Harris County, we may have to refine our search to include "AND Texas" or "AND [insert state here]."

Although you can select near-real-time alerts, potentially receiving dozens of emails throughout the day, I prefer receiving one email each day that lists all the articles and blog posts matching each of my search strings. This keeps my inbox lean, and at the beginning or end of each day, I can open the emails, search through the article titles and read the ones that might be relevant, while not wasting time reading any article that is irrelevant. This saves me a significant amount of time each day by allowing me to monitor news and blog articles for only the things in which I'm interested. What would have taken me an hour or two now takes a matter of minutes.

Another great online tool that I recommend is called If This, Then That[28], or IFTTT. This tool allows you to create 'recipes' and then it delivers you the information you ask for when it becomes available. For instance, let's say that I want to be alerted by email or text every time someone checks into a local gun store (or National Guard armory, or just about any other place) using a social media platform like Facebook or Instagram. I can create fake accounts on these social media platforms, and then IFTTT will monitor each of these location's profiles for any post about someone visiting the store (or whatever location I tell it to monitor for me).

Although 'check-ins' are a great way to identify individuals and monitor the comings and goings of places of interest over social media, it's by far not the only avenue available to us. The IFTTT website also monitors news agencies, along with other websites and social media, and its creation of new features is increasing, so our ability to leverage IFTTT to monitor potentially important events for us — for free — is virtually always increasing, as well. (As a caveat to security, I highly recommend using fake names and profiles while using these services. Further, we can use software like Tor to better mask our true identities. It's for your privacy, if not for your protection.)

Another tool I recommend is called 80Legs.[29] 80Legs will "scrape" a website, allowing you to download the data from each post, page, and link. It's the best way available for an average web browser to download an entire website. We can then take that data and search through years of posts, which could reveal important information we may not have otherwise found.

Along those same lines, it's been said that the internet is forever, and it's true. The Way Back Machine has catalogued over 434 billion webpages.[30] When something is published on the web — an article for instance — it can still be changed. If you hadn't read the article prior to the update, then all you will see is the latest version of that article. But the Way Back Machine, may have catalogued the original or previous versions of that updated article, which could allow us to see information that was edited out. Looking at previous versions of articles or blog posts could reveal some important information that was later removed.

On the flip side of passive collection, also known as monitoring, we have active collection. This is where we must actively search out a specific piece of information in order to answer an intelligence requirement. As much as Google is a competitor with NSA when it comes to violations of privacy, the Google search engine is probably still the best available. (I often use Tor while practicing my Google-Fu.) I've found the best strategy for searching information is to begin with a very narrow search, and then broaden my search until I find what I'm looking for. One great feature that Google has is that visited links show up in purple, and unvisited links show up in blue. That tells me which sites I've already been to during a previous, narrow search.

So let's say that we're looking for the additional information of an Operations Manager of an some company. We've already been to the company's website and read this individual's biography, which provided us some information to start our search. I might next go to Google and search "Operations Manager AND [organization name] AND [state, county, city, etc.]". That's a very narrow search. If I can't find what I'm looking for, then I'll remove the location keyword, which broadens my search and should return me more links. The inclusion or exclusion of certain words, called 'operators', is referred to as Boolean Logic. There some great resources that will teach you Boolean Logic (and they're just a Google away).

The obvious problem with searching for something specific on the web is that we may spend hours or days searching and trying to find it, when it either doesn't exist on the web or is not searchable. There's no end to the number of databases online with data that doesn't show up in search engines.

One of my favorite databases for looking up additional information on a person is called Open Secrets.[31] Open Secrets is a database of political campaign contributions. If you know the name and city/state or zip code of your subject, then you have access to any political donations he or she may have made. Identifying political ideology, along with which candidates were supported and how frequently contributions were made, may be a good indicator of an individual's willingness to cooperate in a SHTF situation. And in community intelligence, we are in the business of identifying these people ahead of time.

There are a few other open source databases that I highly recommend. The first two are RAIDS Online[32] and Crime Reports[33]. Both of these websites map available crime data and can provide for you a baseline of criminal activity. You can search by city and zoom into your neighborhood and surrounding area. You're also able to manipulate the map to show only certain crimes. This is useful for narrowing down violent crimes, as opposed to property crimes like graffiti. At RAIDS Online, you can also view a heat map of criminal activity, showing you the worst and potentially best neighborhoods in a given area. Be sure to print these maps out for inclusion into your IPC binder, as they are an invaluable at-a-glance resource.

There are a few limitations to these two websites. Not every law enforcement organization makes publicly available their criminal data. You'll typically find this to be the case where law enforcement has very little administrative support. The second limitation is that not all crimes are necessarily classified properly. Rape or sexual assault, for instance, could just be reported as an assault. The data may also not be complete. No law enforcement organization dealing with high levels of crime wants the public to know how poor a handle they have on area criminality. Lastly, the locations of crimes that are shown on the map aren't exact locations. In order to protect the privacy of victims, it's very common to have the location markers off by a short distance.

Another place to get really good information about an area is USA.com (formerly known as City Data).[34] Understanding demographics and culture is an important piece of our intelligence picture. The better we understand the communities and surrounding areas in which we live, the clearer picture we'll have of our operating environment and the better we can provide intelligence support.

Human Intelligence

Human Intelligence, or HUMINT, is perhaps the most unwieldy discipline of them all. It's the most dynamic and exciting way to collect intelligence information. When I mention HUMINT, you may have conjured up scenes of interrogations from HBO's *Homeland* or the latest James Bond film, or British and American intelligence officers working with the French resistance and conducting espionage. While you're not incorrectly associating these things, I'd like to talk about having realistic expectations for your community intelligence section.

There are several different types of HUMINT, ranging from interviewing and debriefing, which are the least intrusive, to interrogation and source operations, which are the most intrusive. This section is not about interrogation and source operations. The bad news is that, considering the amount of time and resources (and not to mention training) required, not only are interrogation and high risk source operations unrealistic goals for most groups, but they're probably not even the most productive for us, either. The good news is that we have several great options still available to us to collect HUMINT information. They are:

Interviewing / Debriefing - This type of HUMINT collection is most frequently associated with "friendly forces". We might interview a witness at a crime scene, someone who wants to cooperate with us to help catch the bad guy; or debrief a patrol leader returning from a firefight, who's noticed a change in enemy tactics. These sources have the benefit of direct observation, which is why it's critical that we ask them questions. Collecting the most basic information - who, what, when, where and why - is our top priority for establishing a sequence and/or description of events. In interviewing and debriefing, we're using "direct" questioning; that is, asking simply stated questions that will give us the specific responses we need to better understand the event or security conditions. Questioning in interviewing and debriefing is based on our intelligence requirements, so consider what knowledge your subject has and then ask questions that can fill in our intelligence gaps.

Liaison - We want to establish formal or informal relationships with authorities in the area. Collection through liaison can happen by way of ride-alongs with local law enforcement, which give us a level of "cover" to ask questions; volunteering at the local fire department or emergency medical services to learn how emergencies are managed; becoming an ambassador to a local civic or charitable organization; or establishing relationships with local security groups. A word of caution: our main focus in adopting liaison roles is to help, not collect intelligence. The more productive and useful we are, the more access we are likely to gain. Volunteer with these organizations, work smart, work hard, and the intelligence collection will follow.

Tactical Questioning - Often referred to as "TQ", tactical questioning allows us to collect intelligence information from humans in the battlespace. In Iraq and Afghanistan, it most frequently occurred after a firefight or IED strike, where smart leaders ensured that information was collected from any bystanders (e.g., "Who were the fighters, how long had they been here, which way did they escape?"). The goal of TQ is obtain potentially actionable information in a tactical scenario. Given the nature of tactical environments, TQ should be conducted quickly and only after security has been established. The longer you're standing around talking to people, the greater the risk you potentially create for becoming a target again.

There are some tips to consider if you expect to conduct TQ:

1. Keep a list of basic questions. Chances are good that those who question individuals will be untrained or have a low level of training. One of the best ways to direct good questioning is to prepare questions in advance. Write out on an index card, or print out and laminate, five questions. They might be, "Who is threatening you in this area?", "When is the last time you saw this threat in the area?", "What are the activities of this threat?", and "What are your major concerns for this area?". Always refer back to your intelligence requirements. It's good to ask questions and collect information, but it's great to fill in gaps in our intelligence.

2. Develop roles before you need them. One of the best ways to miss opportunities to collect intelligence information is not designating a member of a patrol

or security team as a tactical questioner. Give the opportunity to speak to a community member or witness, who will ask the questions? Ensure that these individuals receive training on how to question, and how to report collected information. If you don't designate the role of tactical questioner, then you're decreasing the likelihood that HUMINT information is collected at all.

3. Learn indicators of deception. One of the most difficult parts of a HUMINT analyst's job is understanding the context of how HUMINT information was collected. With the exception of recorded interrogation, analysts don't have the benefit of being able to observe the subject's mood or body language while providing information. Therefore it's incumbent on a tactical questioner to learn some of the most common indicators of deception. Some contextual information that analysts can really use is the subject's mental and physical state while providing information. (Additional information will be provided in the next subsection, *Understanding Non-Verbal Communication.*)

Screening - Screening gives us the ability to ask questions and collect information in making a determination, and has two purposes: to identify threat level and intelligence value. In Iraq and Afghanistan, for instance, potential detainees are screened as best as possible. Those with a high threat level Thus, there are four type of screening: tactical, checkpoint, local population, and pre-interrogation.

Tactical screening is similar to tactical questioning, in that they both are conducted in a tactical environment. The difference is that tactical questioning is conducted to gain intelligence information, while tactical screening is to determine threat level and intelligence value. For instance, if a SHTF security team responded to a home invasion in your community, the team would tactically question the elderly home owner, but would tactically screen a suspicious individual found outside the home.

Checkpoint screening can occur at static checkpoints, such as in a gated or fortified community, or at roving or "snap" checkpoints. ("Snap" refers to the ad hoc and temporary nature of the checkpoint.) In a SHTF scenario, a security team can use checkpoint screening to speak with individuals attempting to come in the community or neighborhood (primarily those who don't live in the area). Asking questions about identity, reason for travel, and who they're going to visit can be helpful in determining an individual's intent. It may be the case that before allowing them into the community, the destination can be confirmed (or perhaps community members can work that out with the "gate guards" ahead of time). Think of the bouncer at a nightclub who asks for name or identification and then says, "You're not on the list." That bouncer is basically a checkpoint screener, albeit in a lower risk environment.

Local population screenings are conducted to gauge the opinions and needs of those who surround you. In Iraq and Afghanistan, these screenings took place in order to identify the needs of the populace and to build familiarity and trust with US/Coalition forces. If I was a community leader in a SHTF situation, I would want to know what my neighbors thought the situation and how they felt. An added benefit of local populace screening is the opportunity to collect information directly from a community member who would not have otherwise approached you in order to tell you. We can't always expect individuals with relevant information to come to us; sometimes we have to go to them. And being there to check in provides us great cover to ask about threat information as well.

Pre-interrogation screening occurs as soon and as safely as possible after a criminal has been arrested. (Consider this law enforcement's "booking" phase.) Typically, a screener is attempting to gather biographical and historical information in order to determine threat level and intelligence value. Ultimately, if a detainee has a threat level or intelligence value that meets the threshold for prolonged detention, then he will be arrested until a trial and/or interrogated until he's been exhausted of intelligence value (which may not be very long at all). The benefit of doing a pre-interrogation screening, which is just direct questioning, is that we have information that can later be confirmed or denied during interrogation. For instance, if a detainee says one name or other piece of information during pre-interrogation screening, yet gives another name or different information during interrogation, then the interrogator and analyst have something to unravel.

The last word on screening: in Appendix G, there's an example screening sheet. Use what's relevant to you, and create new blocks of information, if necessary. If you're going to screen individuals, ensure that you create and print some screening sheets before you need them. In the military, screening sheets are unclassified when blank, but become classified when filled out. It's a great idea to protect completed screening sheets in the same way.

Source Operations - Low level source operations (LLSO) describes the utilization of human sources to collect intelligence information. Unlike traditional espionage, where agents are recruited to sabotage, influence, or gain access to sensitive or classified information (and where legality is of little or no concern), LLSO takes a much safer (not to mention more legal) route to collect intelligence information. Instead of recruiting highly placed sources, we're expanding the network of individuals we know and using simple techniques to collect information. Each of the previous types of HUMINT covered above can be considered forms of LLSO. Although a later subsection discusses the source recruitment cycle, your primary focus as human intelligence collector is to use the safest yet most effective (and legal) means to collect intelligence information.

There are likely those in our groups and communities who are more than willing to share with us information they already know, which is why our ability to simply ask questions and keep a conversation going is so vital. There are a few factors that go into asking appropriate questions the right way, whether we're having an innocuous conversation or actively asking questions in order to collect specific information. In fact, our ability to collect HUMINT information largely hinges upon how skilled we are at getting our subjects to speak freely. Before we get into each of the methods of conducting HUMINT, there are a few very important topics we need to cover. Let's talk about the critical skills of understanding communication and building rapport.

Understanding Non-Verbal Communication

In some cases, what's said is not nearly as important as how it's said. Our ability to pick up on these nonverbal communications, such as body language and facial expressions, can make the difference in our understanding of what's being communicated. For instance, how should we interpret a subject who has his arms crossed, and how might that change the value or significance of what he's saying? Is the subject's body language open or closed? What should we make of a subject who fails to maintain eye contact with us? What does it mean if a subject looks to the left while speaking, and then looks to the right for the next sentence? Skilled HUMINT collectors learn to recognize these changes and, given the context of the situation, may gain better insight as to what these changes in body language mean. While no single piece of body language is a dead ringer for indicating deception, there are some tips and tricks to help us out along the way.

One of my favorite tricks consists of three questions. Try it out on some friends or strangers and see what differences you can identify. The first two questions need to have answers that are recited from memory. "What's your wife's name?" or "What's your telephone number?" "Who was the last person you spoke with on the phone? What did you eat for lunch?" The exact questions don't matter so much as what they're asking. What happens is that our subject will recollect from direct experience and memory, which causes him or her to access a specific part of the brain. We ask two of these questions to form what's called a 'baseline'. Chances are good that as long as we're asking questions that our subject can answer from memory, he or she will continue to access that same part of the brain. Pay particular attention to where the subject's eyes go. Is it to the left or right? The next question needs to be answered by the creative side of the brain. We can ask, "If you won a million dollars, how would you spend it?" Or "If you had unlimited funds for a one week vacation, where would you go?" As opposed to recalling from memory, our subject now needs to think and create an answer. This is essentially what happens when someone tells an unrehearsed lie. Instead of recalling from memory, he or she accesses the creative part of the brain and can indicate that thought pattern though a shift of the eyes.

We can also detect whether or not smiles, a form on nonverbal communication, are genuine. We can illustrate this by asking a friend to smile, as he or she might for a photo. Next, tell a funny joke and see if there's a difference between a forced smile and a genuine one. A standard smile, which engages only the muscles around the mouth, are most typically forced smiles. Duchenne smiles, on the other hand, better indicate true happiness by engaging muscles around the eyes as well. The wider and fuller the smile, and the more contraction around the eyes, the more genuine a smile may be.

If you intend on actively collecting HUMINT information, I recommend a book called *Spy the Lie*.[35] Alternatively, researcher and psychologist Dr. Paul Eckman runs a website with invaluable free information about micro-expressions.[36] Understanding non-verbal body language and basic psychology is a must for reading human communication.

Building Rapport

The second preface to this HUMINT section is understanding the importance of rapport. If you were to approach a complete stranger on the street and begin asking questions about his job, home and family, then he's probably not going to be very interested in answering your questions. Not only does he not know you, but he also might think that you pose a threat to him. Even if he was open to answering your questions, what's in it for him? If he spends five minutes answering your questions, what does he get in return? If the answer is nothing, then he's much less likely to waste his time.

What's just been described is a lack of rapport. Simply put, rapport is a sympathetic relationship. Rapport is not just familiarity, but trust. It's an establishment of good will or similar interests. The purpose of building rapport is to make the subject comfortable speaking with us. When a car salesman approaches and introduces himself, he's building familiarity. But when he tells you that the dealership has been in business for 40 years, and exhibits interest in helping you solve a problem by selling you a car for the lowest prices in town with a five-year-no-questions-asked warranty, he's building trust.

If you want to master the art of building rapport, then Dale Carnegie's oft-cited *How to Win Friends and Influence People*[37] provides the best start. Short of that, here's a primer on rapport, how to build it, and how to exploit it.

In HUMINT, the more trust we gain, the more information we may be able to collect. Because rapport is the bridge between *our* questions and *their* answers, the more rapport we develop with the subject, the more likely it is that he or she will be open to answering our questions.

In his book, Social Engineering[38], author and social engineer Chris Hadnagy describes the interrogation of a peeping tom. During the interrogation, instead of castigating the criminal, who was arrested after being discovered spying on a woman wearing a pink cowboy hat through her bedroom windows, the interrogator empathized with him. Would the interrogator have gotten a confession and the information he was looking for had he simply attacked the man for being a sick pervert? Probably not by that method alone, so instead the interrogator told the criminal that secretly he, too, found women in cowboy hats attractive, and then began describing a woman he'd seen the previous week. Because the interrogator had built some rapport by being nice and empathizing with the man, the peeping tom admitted to being irresistibly attracted to the woman and following her home. Yes, the interrogator lied — that happens from time to time. But the interrogator used the situation to de-escalate the tension of being caught in the act, and built some rapport with the man in order to get the needed information.

It may be that we're able develop rapport under false or accidental pretenses. We need to use that to our benefit, too. How many times have you participated in or overheard a conversation containing personal information while waiting for an airplane to take-off or taxi? You or the other individual probably wouldn't have been so open had you been on a busy street, instead. But being travelers who have the same origin and destination, in a situation where disclosing personal information with strangers is acceptable, is rapport that we didn't develop but can still use. Having on apparel from the same sports team may be an accident (although it also may not be). We didn't intend to but by recognizing another fan, we've established the beginnings of a sympathetic relationship because we support the same team (or the same cause). If your code of conduct allows you, we can attend a meeting full of democrats, during which time we will be a democrat in order to build rapport. If we're speaking with an electrician, your father may have been one, or perhaps your son aspires to be one. We can use some gentle ego stroking about how important electricians are to our society, painting the picture that without them, most people would die. Whether purposeful or not, even small things (including sincere, well-placed compliments) can develop rapport in big ways.

One book that I consider required reading for understanding rapport and what kills it (as well as for interpersonal relationships in every day life) is *Choice Theory*[39], by Bill Glasser, M.D. In this book (and, by the way, I recommend reading each of his books), Glasser describes the four fundamental psychological needs of humans: belonging, connection and love; power, significance and competence; freedom and responsibility; and fun and learning. One of the best ways we can build rapport is to find a need and meet it. We'll cover that again in the subsection on motivating sources to work with us, however, these four areas of psychological need describe the avenues to building vast amounts of rapport. The better we get to know an individual, the better we can determine which, if any, needs aren't being met. Once we start meeting a need and providing real value in an individual's life, then we begin wielding more influence. If you want to influence, first be influential.

Rapport truly is quality of time over quantity of time. It's not the quantity of time that necessarily matters. Have you ever met someone and, after one conversation, you thought to yourself, "I really like that person!" When former president Bill Clinton was in college, he began writing down on index cards the names and biographical information of the people he met. Before he went to an event where he was likely to see someone again, he would review the cards and better recall spouses' or children's names, and other life and work information. And when this young man remembered their names and asked about the people in their family, what was he doing? He was telling these people that they're important enough to remember. He was very effectively building rapport with them.

There are some simple rules to follow that help us to build rapport. The first is that we should be genuine in our caring for the subject. Some people intuitively read body language and can tell if you're being disingenuous. Before approaching someone, take a moment and tell yourself that you care for this person as a human being… and then care. Studies show that when we smile for up to twenty seconds, we're telling our brain that we're in a good mood, and we can actually alleviate stress and feel better![40] The connection between our psychology and physiology is real, so if you want to build rapport, first put yourself in the right frame of mind.

When our subject begins speaking, actively listen. Include both verbal and nonverbal signs that you're listening. Verbal cues let speakers know that you're actively engaged with what they're saying, and these cues encourage speakers to continue speaking. Verbal cues may be words (*interesting* or *tell me more*) or interjections of understanding or amazement (*mhmm*, *wow* or *huh!*). Nonverbal cues include having an open body language by facing the speaker, maintaining eye contact and nodding your head. When developing rapport during a conversation, remember the old adage: b*e interested, not interesting*. When we show interest, we give the speaker another reason to continue speaking. We're showing that person respect through our undivided attention. And the subject may go into greater detail, providing us with more information if he knows that we're not zoning out on him.

Are there ways around having to invest and develop rapport? Sure. On the other end of the spectrum, coercion makes people talk, too. Fear of a credible threat may gain you someone's unlimited cooperation, or the appearance thereof. But that often comes at the cost of anger and resentment, and potentially worse problems down the road. When dealing with how to gain information from human sources, what we're really discussing is motivation. Therefore, in addition to building rapper, we also need to develop sufficient motivation for our potential sources to cooperate with what we want them to do.

Motivating Sources

If we don't understand motivation, then we won't be effect HUMINT collectors. For our purposes, there are three types of human motivation. The first is survival. Paleolithic man woke up and killed an animal in order to eat and survive. Individuals who run afoul of the law strike plea bargains and trade information on worse criminals in order to save themselves. Survival and self-preservation are the most basic and primal of motivators. The second type is extrinsic motivation. We do things because we expect to be rewarded. Why do some people work so hard at a job they hate? Because they have the expectation that the hard work will pay off. Why does Joe stay late at the office after his boss asks him? Because even though Joe doesn't want to stay late, he's seeking some kind of reward for it. Extrinsic motivation can also be psychological. Some people brag in order to be acknowledged. Some people 'go the extra mile' in order to be publicly praised. Most people will do anything if the reward is good enough. The last type of motivation — the motivation we as HUMINT collectors want to lean on — is intrinsic motivation. We as human beings do things we enjoy and that make us feel good, whether or not we're going to be rewarded for it. The feeling we get is our reward. When we do nice things for people we love because we want to; that's intrinsic motivation. It's our job as HUMINT collectors to intrinsically motivate sources to give us information. It's our job as psychologist, counselor, and friend to guide a potential source to the conclusion that not only is it in his best interest to give us information, but convince him that he's doing good by doing so. If our potential source feels as if he's doing the right thing, then he's much more likely to give us information. In the opening scenes of spy-thriller *A Most Wanted Man*, the protagonist, Gunther Bachmann, a German intelligence officer, receives a phone call from his Muslim agent. After a brief conversation pointing to the agent's unwillingness to carry on his work, Bachmann tell his agent, "You're doing the right thing." The agent hangs a couple seconds later up and presumably continues the mission. It's a great example of encouraging an individual to continue on with work, sometimes at great personal sacrifice, because it's the right thing to do.

Here's another example of intrinsic motivation. Chinese espionage directed at America is primarily industrial and economic in scope (including military-industrial). The communist Chinese government's rationale is, "Why spend billions of dollars in research and development when we can just steal technology?" And that's exactly what they do. One of the popular methods of Chinese intelligence when dealing with Chinese nationals who work in sensitive industries abroad (America and Europe, especially) is to exploit the love of their people back home. In essence, these Chinese scientists and developers working abroad are told, "Give us the technology and information. You're not hurting anyone in America by giving us what you know about this technology. America is rich, and many people in China are still very poor. You will be helping the Chinese people and making their lives better." And why is this approach so effective? Because Chinese intelligence convinces these people that they are doing good by conducting espionage, thus leveraging their intrinsic motivation. After all, it's human nature to want to help people in obvious need.

No matter if we offer external rewards to our potential sources or inculcate intrinsic motivation in them, we can use elements of MICE/RC as a guideline to specific motivators. MICE/RC factors are specifically associated with 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 heavily consider the motivating factors of our sources. 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 in order to gain information we want (source operations), we will do so in light of MICE/RC. 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/or solutions. MICE/RC stands for:

- Money/Material
- Ideology
- Compromise
- Ego
- Revenge
- Coercion

Everyone has needs. They may be physical or emotional/psychological, but there are needs that we as HUMINT collectors need to identify. And we go about identifying needs in one of two ways: either indirectly through social media or speaking to family, friends or colleagues of our potential source, or directly by listening to what these potential sources are telling us. Once we develop rapport and are able to ask questions more freely, then we can start covering more conversational ground. Nearly everyone talks about their problems at some point, and some people will open up to practical strangers if given the opportunity. We need to become that opportunity. If we can become a person in whom our potential sources can confide (in other words, trust), then we will get to the root of their issues. And once we understand what might motivate them, we can begin providing solutions to problems along the lines of MICE/RC.

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

As a caveat, understand that MICE/RC describes methods used by collectors, and they may not all be legal. In fact, some of them are explicitly illegal, but they're included anyway for your own knowledge. Remember that HUMINT is often a two-way street and, depending on the threat, collectors may be targeting you, as well.

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. A common theme throughout motivation is finding a need and meeting it. If we can meet their needs, then they're more likely to meet ours.

As an example of how we can use material goods to motivate potential sources to cooperate, identify the individual who has placement and access to information we want, and also has a need. A bag of groceries might go a long way in helping a father to feed his family. A couple in the neighborhood are very concerned about their safety, so some firearms training and a box of pistol rounds may be the key to anything you want to know. Ensuring that each family in your neighborhood equates their safety with providing us information is an invaluable step. Their not having to worry about looters or gang members moving through their community and by their house is a great motivator.

One downside to the Material motivator is that individuals may fabricate information in return for reward or payment. As was often the case with "walk-ins", or strangers with information who approached US bases inAfghanistan, villagers knew that providing information about the Taliban would earn them money. So there was incentive to make up information about a non-existent Taliban fighters residing in or traveling through the area.

Ideology

It's 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. 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 relevant information. We want this information, so we as HUMINT collectors 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 potential 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 people with whom he's ideologically associated.

Security can also be used as an ideology. Why do people volunteer for community watch programs? The safety of the community is a shared goal and therefore a shared responsibility. We can use trends in crime rates or types of crime to start a community watch program. In fact, I think developing regular town halls or community meetings is a great first step in identifying who shares the same ideology — not only of our safety, but more importantly our liberty. Organizing events like these provides us the perfect opportunity to identify like-minded individuals that we may have never met.

Compromise

Think of compromise in this case as leverage. It's the businessman who tells a politician, "We know you're having an affair, so vote No at the next meeting or we'll tell your wife." A foreign intelligence agency who says, "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 or extortion but it's an ugly reality of the spy world. HUMINT collectors and those involved in source operations find good reasons to motivate individuals who are otherwise 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.

Ego

Pride and ego are universal feelings, and we can 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 or at home, and will continue to collect for us because we enable that emotion of happiness or accomplishment.

Alternatively, we can play down pride and ego as well. These people might be willing to collect for us in order 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 your organization… but if you can prove to us that you have that amount of power then we can provide you with this.”

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 or hatred to achieve a positive development for us. Assessing the potential source who’s out for revenge is a critical part in planning his collection.

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 mistake, with coercion we are creating a justified physical 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. This is very illegal and I don’t recommend it, but understand that it’s used, especially by nefarious actors. It might even be used against you.

Developing Sources

Not only do we need to motivate sources to provide us with intelligence information, but we also need to sufficiently influence them to continue their work. Professor and social psychologist Robert Cialdini, PhD wrote an excellent book entitled *Influence*.[41] In this book, he cites six principles that guide human behavior, referred to as RASCLS, and we need to become very familiar with each of them. They are:

- Reciprocation
- Authority
- Scarcity
- Commitment and Consistency
- Liking
- Social Proof

Reciprocation

Reciprocation occurs when we do something nice for others because they did something nice for us. One good turn deserves another. According to Dr. Cialdini, human nature dictates that we seek out reciprocal behavior. It goes both ways: our natural inclination is to respond to nice gestures with nice gestures, and we desire to repay insults and affronts with those of our own. If someone opens a door for you, then you are more likely to open the next door for them. If someone is driving like a jerk, then you're more likely to drive like a jerk, as well.

Why do salespeople buy gifts or drinks or dinners for their clients? Because their clients are spending lots of money on their products, and the salespeople want to ensure that relationship continues. They are providing some reciprocation and showing appreciation. By fostering their personal relationship, the salespeople are ensuring that the business relationship continues.

So when we're meeting with a source, one of the best ways to set ourselves up for reciprocation is to make the first move. Because we know everything about our source before we start the recruiting process, we should know their wants and needs. Whether we're buying dinner, drinks, a pack of nice golf balls, or some other material or action, we ought to make it deliberate. As long as we're doing the small things, we're setting ourselves up for future success. Our source might just reciprocate by offering a small but important or difficult-to-collect piece of information.

Authority

Authority is a critical part of our persona that we need to project. No one wants to risk his job, life, or family's security in order to report sensitive information to someone who is weak, from a weak organization, or who lacks the authority to provide security or materiel support for him while he collects.

Part of our job is to be the guy that our sources believe they're working with, even if we're not that person. One particularly effective persona is the smart, competent, man-in-the-field doing the work of his very powerful bosses. This provides us a multitude of benefits, and allows us to exercise their authority, or the authority of our powerful organization.

For one, it allows us to save face. If we can't deliver something that our source wants or needs, then it's because our bosses won't agree to it, and never because we can't or won't. Even if we're calling all the shots, pawning off difficult decisions on our 'boss' is one way for us to maintain a good rapport on a very personal level, even when telling our source difficult or discouraging news.

Two, it provides us some leverage. One of the most useful negotiation tactics is to act as though a minor concession is, in reality, really important to us. Maybe our source is asking for $50 per week, or a bag of groceries per week, and it's well within our organization's means to make that happen. We can convince our source that it's a really, really big deal in the eyes of our supervisors. It's not because our supervisors can't provide it, but because they want our source to prove himself before they provide him with that material. "My boss want you to prove that you have access to the information (or he wants you to collect a specific piece of information) before he's willing to provide that amount of support."

Three, it allows us to build rapport by going to bat for 'our guy'. I noticed one example of this when I bought my last vehicle at a used car lot. I made an offer on a truck that was significantly below the sticker price. The salesman told me that he didn't have the authority to make that decision (he may not have, but he probably did). He said he needed to speak with his supervisor, and then came back ten minutes later after getting coffee and smoking a cigarette. He said that if he could, then he'd sell me the truck at that price, but his supervisor wouldn't take that offer. What he really did is decline my offer while saving the relationship. I ended up buying that truck after his supervisor accepted another offer under the sticker price.

In our HUMINT collection activities, if our source makes a request for money or material, then we can put our supervisor in charge, too. We might report back initially that our supervisors said, "No." Or maybe we need some time to examine the consequences if our source acquires this material; maybe he wants a weapon or some other sensitive item. In either scenario, we can report to him that we've been lobbying our bosses, promising to them that 'our guy is worth it' (or some other positive, affirming, and encouraging description), and that they've finally come through for us. You should probably re-iterate that you've been fighting for your source in the office, so your source needs to fight for you and be responsive to future takings.

In these situations, we can be whomever we want as long as we're consistent (covered later) and building rapport with our sources. It may seem counterproductive to not appear like you're not 100 percent in charge, however, I recommend having a scapegoat (i.e., your boss) that you're able to use very, very sparingly.

Scarcity

Scarcer things are generally more valuable. Look at gold and silver: they're only mining so much out of the earth, and there's only so much above ground in circulation. It's a limited amount and for that reason it's valuable. In the case of diamonds, that value is largely a created value. Because most of the world's diamonds aren't available, diamonds are made artificially more valuable. It all comes down to scarcity… supply and demand.

Likewise, the information we need is often scarce, and therefore so valuable to us that we're willing to risk our lives or well-being to recruit and task individuals to risk their lives or well-being to collect that information for us. If there comes a time when our source is unwilling or reluctant to collect, depending on the cause of those feelings, we should look at introducing him to the concept of scarcity.

Why do furniture stores and car dealerships celebrate Memorial Day with sales? Why do television advertisements promote limited time offers? Because they work. The sale is ending soon, so if you want the savings, then you'd better buy now. Remember that our source is meeting our need of information and that we're meeting his needs, too. "We can work with anyone, but we choose to work with you," or "This opportunity is going to be available for a limited amount of time before we have to move on to someone else." Even if there aren't, there are always other people willing to work for us; always. There's one job and several people who are willing to fill it. The work is scare and therefore valuable to our sources. Their inaction or unwillingness to cooperate is going to threaten the opportunity they have, or the need that we're meeting for them.

Commitment and Consistency

No one wants to work with or depend on the guy who only sometimes comes through. The guy who's continually late, lacks commitment to the cause, or is inconsistent is generally not employed for very long. Source handlers will find themselves in similar unemployment situations if they aren't committed to their sources and don't stay consistent with them. If your sources lack commitment or are inconsistent in their efforts, then they're either likely not being properly motivated or questioning our commitment or their trust with us.

It's critical for us to make abundantly clear our commitment to our source. Not only are we committed to his safety and well-being (and probably the safety and well-being of his family), but also we must always be consistent in our dealing with him. If we make a promise, then we must follow through. If we schedule a meeting, then we must show up (unless it becomes a security risk). We must make a commitment to being consistent, and be consistent in our commitment.

Liking

Cialdini and others have pointed out that we like others who like us, and vice versa. People like being liked, and we form relationships with those who like us, and who are like us. We can build better rapport by liking our sources and if our sources like us. Even if we don't like our sources, it's imperative that they like us. We have to be the guy who's interested in or who shares the interests of our sources. If our source is motivated by ideology, then we have to emphasize that his ideology is also important to us. If he's motivated by his ego, then we must be interested in him or his exploits. If he's motivated by the security of his family, then me must make the security of his family important to us. The concept of liking builds rapport and enables more efficient collection.

Social Proof

Why are authors and manufacturers so interested in having 5-star reviews on Amazon? Eighty percent of online shoppers read reviews of products before they make a purchase, and 72% of them trust online reviews just as much as word-of-mouth reviews. That's social proof. It's proof that society is accepting of a product, or likes a product, which makes us more likely to make a purchase.

So how do we exhibit social proof? We might mention that our organization has worked with many different people in the past — people of a high profile or significance; people who couldn't afford to be identified as cooperators, or having their cooperation made public – and if those people can trust us then so can our source. We do this around the clock with many other people, so we can be trusted. Social proof builds trust.

Source Recruitment

As we consider placement, access and exposure in our own communities, review your intelligence requirements and determine who knows or may be able to collect that information. After you develop a list of potential sources, we need to confirm their suspected placement and access. If we're going to invest the time and resources into befriending an individual to collect intelligence information, then we need to know that this person actually has access to the information we need. Next we need to determine how we should go about collecting that information; that is, whether these potential sources should be informal or formal sources.

To keep things simple and effective, there are collectors and sources. We are collectors. It's our job to put ourselves into positions to collect information. Our sources are those individuals who have information that we want. These sources can be *informal* or *formal*. Informal sources are those who provide us information from knowledge. We may be friends or associates with these informal sources, but we're not tasking them to go and collect specific information. A sheriff's deputy who provides us with information about crime trends and threats in the area is an informal source. We're not tasking him to collect; he's just telling us what he knows. A formal source, on the other hand, is a source that we've recruited and trained, and are tasking to collect information. For instance, if we wanted to know what phone numbers another sheriff's deputy called from his work phone, then we might task our formal source to collect that information. To recap, the major difference between informal and formal sources are whether or not we've recruited them to work for us.

Furthermore, informal sources can wittingly or unwittingly provide us information. Witting sources know that we're a member of a community security organization. Unwitting sources provide us with information without knowing its use or value. These unwitting sources aren't aware that you are collecting information. While they're speaking, you're making mental notes to report on later.

Everyone in our organization capable of keeping a secret should collect HUMINT information passively. It's incumbent on every person in our organization to be a sensor. The more eyes and ears we have, the better off we are when it comes to intelligence information. The opposite of passive collection is active. Not everyone should be an active intelligence collector. The more active collectors we have, the more chances we create to cross our lines and make other mistakes. As opposed to passive collectors, active collectors deliberately speak with and/or befriend individuals who are considered potential sources.

So who is a potential source? Remember that all collection is based off our intelligence requirements. We shouldn't be collecting unnecessary information. Our objective is to collect the intelligence information we need from someone who has it, so what we're looking for initially is placement and access, or exposure. Once we develop and/or receive an intelligence requirement, we begin surveying potential sources.

If a potential source has 'placement' then he or she has physical proximity to the target information. Let's say, for instance, that we're trying to get information about a corporate Chief Technical Officer's schedule. Maybe we can befriend a janitor who works in the company's building. He has placement. Through the course of his official duties, this janitor has physical placement in the building, however, he doesn't have access to the CTO's schedule. He can't approach the CTO in order to gain the information; that would be an example of 'access'.

But the CTO's executive assistant has both placement and access. The assistant not only has placement because he works in the same building and floor, but is much more likely to have in-depth knowledge (or access to that knowledge) about the CTO's schedule and whereabouts. So when we're ranking potential sources by placement and access, the assistance would be first, followed by the janitor.

Although the janitor may not have access to the CTO's schedule, he may have what's called exposure. As the janitor empties the trash each night, he may come across travel information. The janitor, while not having access, is being exposed to so some potentially important information.

The source recruitment cycle describes the steps taken in order to recruit a formal source. When we get into talking about source recruitment, we're talking about source operations. Source recruiting takes a lot of planning and expertise. We know this because it can be dangerous work and because recruitment still fails, even when properly prepared. The source recruitment cycle is a methodical and rational way to approach sources.

Step One - Survey potential sources based on intelligence requirements

Everything about collection always comes back to one thing: intelligence requirements. All collection is directed and need-based. The first step of source recruitment is a combination of a) knowing and understanding your requirements and b) identifying specific individuals (or types of individuals) who may have placement and access to satisfy our requirements In other words, we need specific information so we find people who have access to that specific information.

In order to identify these potential sources, make a list of of individuals who could potentially answer our requirements. For instance, if you needed to know how many sheriff's deputies are on duty at any given time, who could you ask? The sheriff, the deputies, sheriff's department administrators, retired deputies, county politicians. Can you think of any others?

Step Two - Assess placement and access for these potential sources

When we're assessing placement and access for potential sources, we're not immediately concerned with whether or not they'll cooperate. We just want to know if they can provide us the information we need to know. So in assessing our list of potential sources, identify whether they a) directly know the information or b) can acquire the information.

Approaching and recruiting sources carries some risk, so we always want to justify the risk for the reward. Along with ranking our potential sources by level of placement and access, we'll also want to rank these potential sources in terms of risk. Approaching the sheriff directly for certain information might be riskier than approaching a retired deputy.

The next question is how do we gain access, ourselves, to these potential sources? In intelligence lingo, a "bump" is an engineered meeting that appears coincidental.

Becoming a member at a local country club might allow you to “bump” anyone from a politician to a doctor or lawyer. Identifying where a potential source does his grocery shopping, and then shopping there after he gets off work, might allow you to “bump” this potential source.

We want to focus on building familiarity and rapport and gaining trust in these bumps. Have something of value to offer (reciprocity), whether it’s the fandom of your potential source’s favorite team or tickets to a game or some useful information. Just focus on becoming a friend and you’ll be well on your way to better assessing placement and access of this potential source.

Step Three - Judge responsiveness to tasking

We learn about individuals from interacting with them and listening to what they’re saying and how they’re saying it, along with reading the messages of their body language. Get to know as much as you can about a potential source before working with him or her. That includes biographical information, familial ties, education, religion, politics, hobbies, and any other topics of personal interest. Knowing as much as you can about this person will make your job of recruitment much easier. When approaching a potential source, you could either introduce yourself or get a mutual friend or acquaintance to introduce you. If you choose to introduce yourself, it can be as simple as, “Hello, I’m so-and-so. I see you work for the sheriff’s department.” Once we’ve made contact with our potential source, we begin building rapport and probing for responsiveness. The truth is that this process is not only ongoing, but it can also take weeks or months.

Take a short survey of yourself and your job. If a practical stranger came up to you and started asking about your company’s security policies, or biographical information on your boss, what would you do? You’d probably become extremely suspicious and defensive. But what if someone you’ve been in contact with a couple times a week and gotten to know, maybe had a beer, played golf, or hung out at the same business convention, asked you the same questions? You’d probably be more willing to open up about the answers to those questions. And if provided the right motivation – money or promotion, for instance – you might even be willing to go collect specific information. Do your research and find what motivates your potential source.

In judging responsiveness to tasking, we need to identify the potential source’s suitability, motivations, and vulnerabilities. Is this person suitable for the task of collecting information for us? Is he mentally able to deal with the added stress; is he competent enough to acquire and deliver the information; and is he trustworthy enough to justify the risk of our meeting?

The important thing is that you’ve identified what makes your source tick, and many sources will be willing to collect as long as you provide purpose, motivation, and direction.

Also consider the downsides related to dealing with this individual. If he’s caught or gets into trouble for collecting information, is he likely to open up about what he’s been doing and for whom? How dangerous might he be as the adversary’s asset? What are the second- and third-order consequences? When the source's usefulness has come to an end and it's time to terminate the relationship, what will he do or what will he want?

We have to survey each of the source's motivations and identify any vulnerabilities, in addition to spotting flaws in personality, morality, or ethics. (To reiterate, this is done over the course of days or weeks, not hours.) It may be the case that those flaws and vulnerabilities don't pose a risk to the mission. On the other hand, I would recommend that if you have any reason to suspect that an individual may be detrimental to the mission, don't use him. Bad sources waste your time, or worse, compromise your mission or organization.

Step Four - Recruit the potential source by selling him the opportunity

There are fundamentally two ways to approach source recruitment – soft and hard. The soft approach is to lay out the problems, hint at the solution, and then have the potential source offer the solution. Paint a picture and allow the potential source to describe it. Have him come up with an idea to help you. Rarely do we ever want to offer something concrete. The hard is approach is much more direct but is rarely recommended. Just like you'd approach your boss to ask for or demand a raise, you have to convince a source that it's in his best interest to cooperate. In pursuing a raise, you might tell your boss that you raised revenue by 20% this year. If I'm your boss, I won't want to let you go! That's the same point we need to get across to our potential sources. We need them to feel like we're presenting them an opportunity that they can't refuse.

Step Five - Meeting with and developing your source

After the potential source has agreed to collect information comes the much harder part: tasking him to collect, developing his tradecraft and security skills, and ensuring security (both for him and you). It's your duty not only to protect and support the relationship, but also to protect your source's identity.

You also have to keep your new formal source motivated and cooperative. Elie Cohen[42], the Israeli master spy who infiltrated Syria's Ba'ath Party is a good example of a motivated source. Posing as a Syrian businessman in Argentina, Cohen befriended members of the then-illegal Syrian Ba'ath Party and slowly worked (and paid) his way into positions of greater access. After being showed the location of Syrian artillery pieces and staging locations to be used against Israeli kibbutzes in the 1960's, Cohen had accomplished his last mission. Mossad, the Israeli intelligence agency and Cohen's employer, warned him against going back to Syria, citing the increased risk of compromise. But Cohen, who had a wife and child, went back to Syria with expanded access to begin clandestinely reporting on Syria's planned attacks against Israel, until he was caught and executed in 1965.

HUMINT Tradecraft

Up to now, we've discussed the avenues to collect HUMINT information and how we develop relationships that hopefully lead to intelligence gathering. This subsection covers questioning and elicitation, two of the most important skills a HUMINT collect possesses. Unless you practice asking appropriate questions and eliciting information today, you will not be effective tomorrow.

The types of questions we have at our disposal are myriad, but they do come with one word of caution. When we ask questions, we may be telegraphing our intelligence gaps, which could be working against us. For instance, if I were to begin asking a series of questions to a detained gang member about his leader, Leroy Jenkins, then that gang member may well identify that Leroy is of serious concern to us because we want to know so much about him. Keep that in mind when questioning someone, and use a combination of the following question types to hide your true collection goals.

Direct - We use simple, straightforward and concise questions, which should be easily answered. Examples: *Who gave the weapons? Where does Leroy Jenkins live?*

Follow-up - We expand or complete information, or clarify a previous statement. Use words like "how" and "why" to identify additional information, or elicit a more in-depth explanation. We can also repeat the answer back to begin a clarification. Examples: *How did Leroy Jenkins acquire the weapons? So Leroy Jenkins dropped off the weapons on your back porch… Why did he leave them there?*

Chronological - These questions are used to establish timeframes and allow us to break down events step by step or minute by minute. They also can be used to determine a subject's knowledge of events. Examples: *What time did you find the weapons on your back porch? What did you do after you took to Tony's house?*

Non-pertinent - We can build rapport with a subject by inquiring about topics that don't pertain to our mission through non-pertinent questions. We also use non-pertinent questions to conceal our collection objectives. For instance, if you're questioning a childhood friend of Leroy Jenkins, you might begin asking about where the subject went to school and who his friends were. Asking information about each of his friends, which may include Leroy Jenkins, is an example of a non-pertinent line of questioning. Examples: *How are you feeling right now? You said that you grew up in Pittsburgh; do you miss your family?*

Repeat - We use repeat questions to test a subject's consistency about a given topic. Questions are typically spaced out by a matter of minutes, hours, or days, and each question, although asking the same question, is stated differently. Our intent is to compare both answers to the repeat question to see if they differ. For instance, if we were questioning a Leroy Jenkins gang member about the source of a weapons shipment, then we might begin by asking, *Who gave you the weapons?* After some time has passed and we've begun talking about other topics, we can come back and bring up the repeat question by asking, *Who did you get the weapons from?*

Control - Control questions are developed from information we already know to be true. They're a way that we can confirm or deny the likelihood that a subject is being truthful with us. For instance, if I begin a series of questions about Leroy Jenkins, and obtain information that I don't already know, then I may want to ask a control question next. If the subject answers accurately, then I have more reason to believe his previous answers. But if the subject answers the control question inaccurately, then I have more reason to suspect that his previous answers have also been dishonest.

Presumptive - Using presumptive questions, we presume that a question has already been answered. For instance, instead of asking a subject, *Are you in the Leroy Jenkins Gang?*, we ask, *How long have you been in the Leroy Jenkins Gang?* If the subject begins to recollect the number of years, but then tells you that he's not, in fact, in a gang, then our presumptive questioning has worked. Presumptive questioning also gives us routes around obtaining a simple *yes* or *no* answer. We can combine presumptive questionings with an a *We Know All* approach, and give the subject the impression that we already know about his gang activity, even if we don't.

Prepared - Prepared questions are planned ahead of time. They can be organized topically and then used as a reference in case you get stuck. Our preplanned tactical questioning cards are examples of prepared questions. Before we begin to question a suspect, we should have done some homework to learn more about him or her, as well as the circumstances surrounding the event. It's a good idea to write down your questions as you think through biographical information or the event, and then use them during questioning.

No section on questioning is complete without charting the differences between open-ended questions and closed-ended questions. Consider attempts to get information from an annoyed teenager. He or she is all too happy to provide simple yet sufficient *yes* or *no* answers to your close-ended, *yes* or *no* questions, even though you may want more information. Open-ended questions, on the other hand, allow for longer answers. Instead of asking, *Did you have fun at school today?* try *What was your favorite part of school today?* The teenager may still be annoyed, but he can't escape the question with a simple *yes* or *no*.

Although there are many questioning pitfalls that you should avoid, perhaps the worst of them all is asking a vague question, or one that's too open-ended. I remember coming home from school and my parents asking me about what I learned in school that day. Well, I learned a lot; so much that it was difficult for me to mentally re-cap everything and then choose an answer. So instead of having to spend time thinking about it, it was usually more convenient to just say, "Stuff." But when they began asking me what I learned in economics or government or field ecology, I was able to give more specific answers. Instead of asking me for the whole puzzle, they asked me for one puzzle piece and they usually got it.

Questions are great. Understanding how to craft a question to your target audience can carry you a long way in getting the information you're looking for. In some situations, however, asking questions is impractical. It may be because we don't want show our interest in a particular subject (asking for a price, for instance) or give the appearance of prying, or it may be because we haven't built enough rapport (familiarity and trust) with an individual to begin asking questions. In these situations, we can attempt to elicit our answers from statements instead of asking questions.

Elicitation

The National Security Agency, whose employees are top targets of foreign elicitation, defines elicitation as "[t]he subtle extraction of information during an apparently and innocent conversation." Elicitation is low risk and non-threatening because we're not asking questions, and therefore it's also difficult to detect and prove. Our goal is to guide a conversation from innocuous chatter to our target information.

Elicitation works because it exploits human characteristics of wanting to help or be polite, or because humans enjoy talking about themselves. In fact, that's typically everyone's favorite subject — themselves. A great rule of thumb during elicitation is that the more you listen, the more you will learn. The more you speak, the more time you're taking away from your target to speak. Look for a happy medium around the 80/20 mark; listening 80 percent of the time and speaking 20 percent of the time. It's also very important to keep in mind that your motivation for conversation is just that; don't try to force the conversation to fit your collect requirements. Keep the flow natural and moving, and consider how you can leave breadcrumbs for your target to pick up. It's always a better idea to let him naturally move into your target topic than to push him into it.

One of the best methods of elicitation is taking a question and turning it into a statement. For instance, instead of coming right out and asking a police officer about crime in the area, I can make a statement and prompt him to give me an answer. *Is crime bad in this area?* becomes *Crime must be bad in this area.* If crime is bad, then human nature would have him want to elaborate on just how bad crime is, or perhaps crime trends or common crimes in the area. If crime is not bad, then he may let us know that it's not as bad as we think. Either way, we've prompted him to give us an answer based on our statement instead of a question that he might be more reluctant to answer.

If you've elicited answer based on your statement, congratulations, but it doesn't stop there. What you've just done is started a conversation and now you need to keep it going. There are a few techniques we can use to keep our subject talking.

Asking for an opinion is a really good option, especially if we can combine it with an Ego Up approach. *Hey, you've obviously been on the force for a good while. I imagine you've been around the block a time or two. You probably really know what's going on with crime in the area.* We haven't asked him a question, but the odds are good that, after stroking his ego a bit, he'll continue the dialogue.

If he doesn't bite on giving his personal opinion, we still have a few other options without having to ask questions. Refer to a newspaper article or tv news story about a robbery or some other crime and say that you imagine those crimes happen a lot (or don't happen very often). Or you can reference his safety. Thank him for what he does as a law enforcement officer and say that it must be difficult going to work everyday and having a heightened sense of awareness. Maybe he'll start talking about how difficult or dangerous it is being an officer (or how safe it is), and give you some more information about criminality in the area. To reiterate, we're not asking *How do you feel being a police officer?* or *Do you feel in danger as a police officer?* We're merely providing a statement and letting the subject continue with the talking, while we listen.

Feel free to play dumb, too. Most humans want to help others in need, and if the officer wants to help you by educating you about police work in the area, by all means let him. Another way we can get our subject to bite is by making a deliberately false statement. How many times have you heard someone being corrected about an inaccurate fact or event? It seems like human nature for us to jump on the urge if we know someone is incorrect, and we can exploit that. It may be in our best interest (our own ego aside) to make a factually incorrect statement with the hopes that our subject jumps on the chance to correct us. For instance, we can say that we know that robberies are the top crime in the area. If they're not, then there's a good chance that your subject will correct you and let you know what actually is the top crime in the area. We might say that we heard that MS-13 has a large presence in the area. If they don't, then the officer may say so, correcting us and giving us valuable information.

With enough practice, elicitation is very powerful. Begin practicing some of these techniques at work or at home, and be amazed at just how much more information you can get by exploiting human nature.

Closing Advice on HUMINT

Earlier in this chapter, I advised to keep your HUMINT collection at a low level; that is to say, focus on building rapport and trust in relationships instead of trying to pay your way into highly-placed sources and agents in what's typically considered espionage. Remember risk versus reward: the higher the access, the more risk there is in working with the source. Because you are a non-renewable resource, it behooves you to limit your exposure to risk, except where necessary. You are not a dime a dozen, so keep it simple and effective.

Imagery & Geospatial Intelligence

Whether it's satellite photos of target locations, full motion video from a drone feed, or the terrain data from a topographical map, imagery intelligence (IMINT) and geospatial intelligence (GEOINT) play an undeniable roll in successful operations. While we certainly don't have access to satellites, we do have access to some startlingly good imagery and geospatial intelligence information.

But first, why do we need imagery, maps and map data? For the simple reason that imagery allows us to safely see places without a physical presence, maps enable us to identify roadways and lines of drift that might be used for enemy mobility, and geospatial data allows us to understand the characteristics of the environment and physical terrain. Our operating environment includes this terrain, and if we don't understand it, then we're setting ourselves up for failure.

Let's first identify something that's absolutely mandatory: 1:24,000-scale topographical maps from the United States Geological Survey (USGS). These maps are available online to purchase[43], and I recommend having the quadrangle for your AO, as well as the quadrangles surrounding your AO. You can also download them, in which case you can print them off at your local print store. I recommend having these maps in at least 11"X17", up to 24"x36" and maybe larger. I've had them printed off in 11"x17" and laminated at a national printing chain for around six dollars per map. (For additional information on map board and how to build them, refer to Chapter Four, subsection on Battletracking).

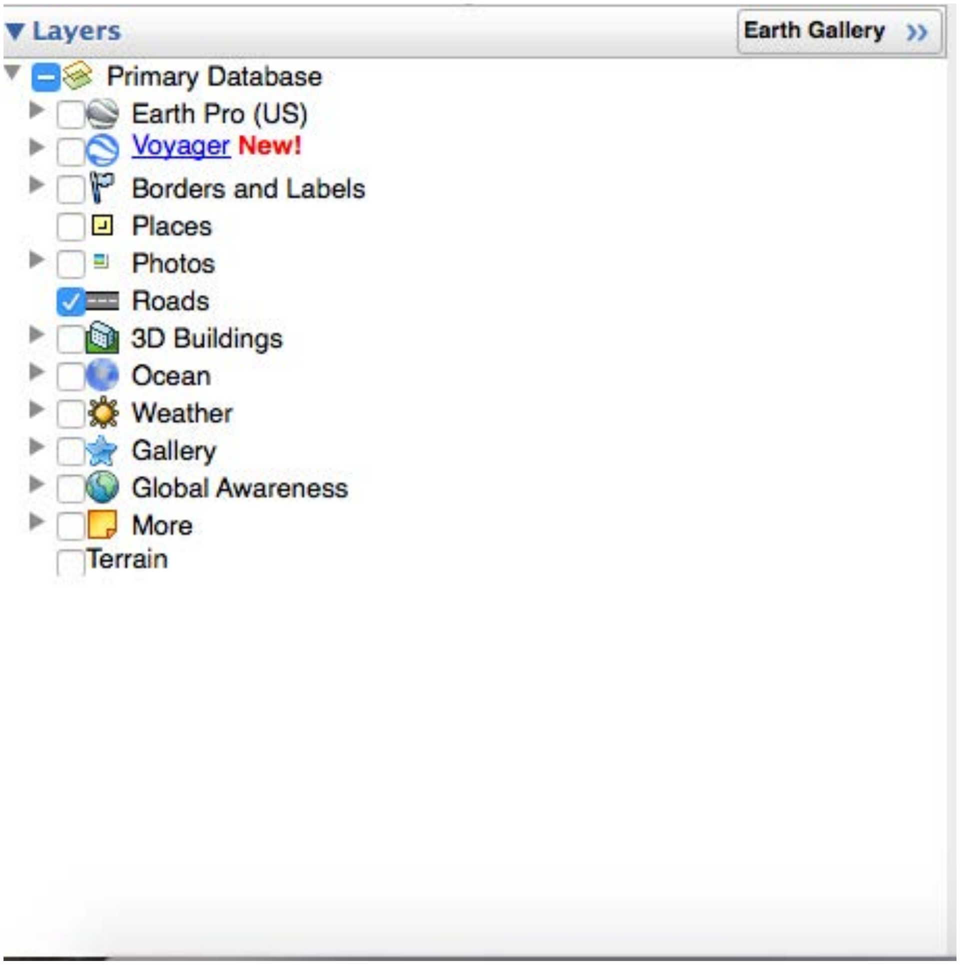
Not only are satellite imagery and street maps available to us (IMINT), but also terrain, demographic, flood, fire, climate, and event data (GEOINT). And therein lies the difference between IMINT and GEOINT. IMINT is just imagery; GEOINT is raw data plotted on maps, as well as environmental data.

Imagery Intelligence

GoogleEarth Pro is "free"[44], and I consider it to be the civilian gold standard for IMINT collection and reference. In addition to having those USGS topographical maps printed, I also highly recommend getting similar size and resolution prints of the imagery of your AO. You'll need to take screenshots (PC: Print Screen key; Mac: Shift +Command+3) of the area around your home and/or bugout location. Be sure to print them off in at least 11"x17" and have them laminated (for protection) so you can use them for a reference later on. Here are the steps to accomplish that.

1. Once you've downloaded, installed and started GoogleEarth Pro, in the top left-hand corner of the window, you'll find a "Search Google" box. If you put in an address and click "Search", then the program will automatically zoom into that location.

2. You'll notice in the lower left-hand corner of the window a box entitled "Layers". In this box, you're able toggle on and off elements like borders, public places and roads. For your printed imagery maps, I would include only roads, which are represented by the white lines on your screen. Turn everything else off until you have your screenshots.



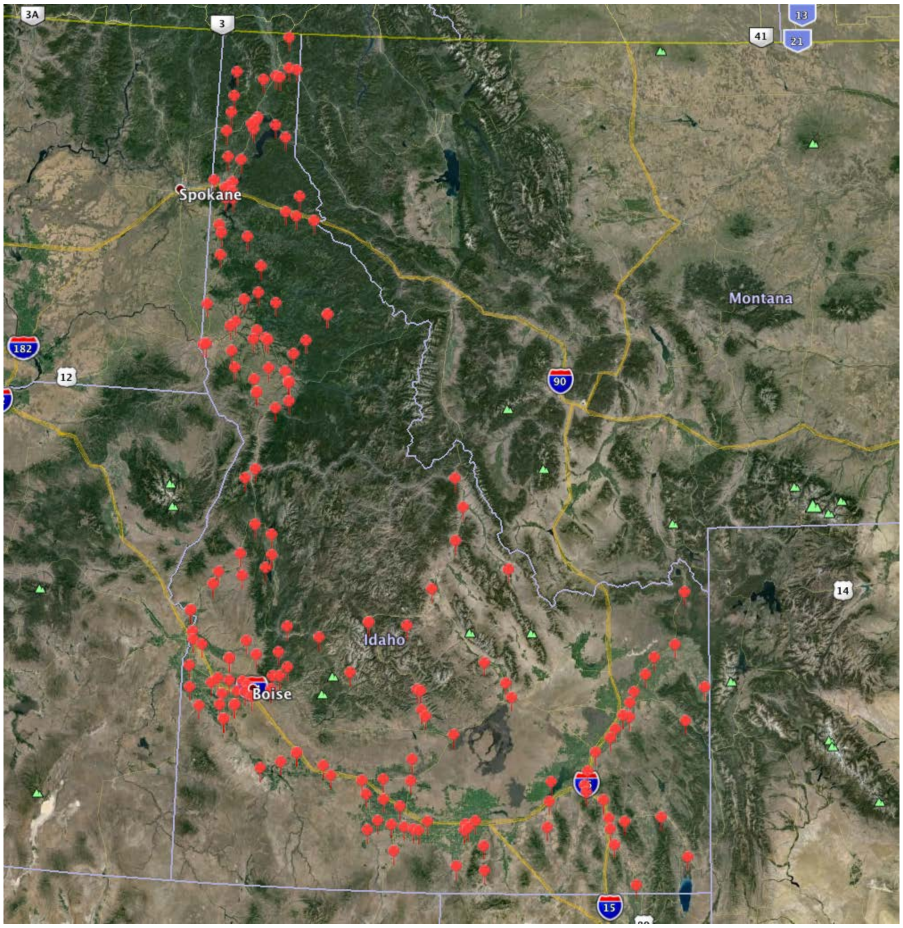
3. Center your home or bugout location on the screen. On the top menu bar, you'll see a ruler button about two thirds of the way to the right. Click on it to open the ruler. Ensure that the ruler is being measured in miles, and then draw out a tenth of a mile. That's your first screenshot. Now draw a half mile, re-center your screen on your home and take another screenshot. Next draw out one mile and take another screenshot. Be sure to edit these, if necessary, and print off multiple copies of each. These three imagery photos will provide you a great reference of your immediate area, and you'll need them again in the next chapter on Intelligence Preparation of the Community.

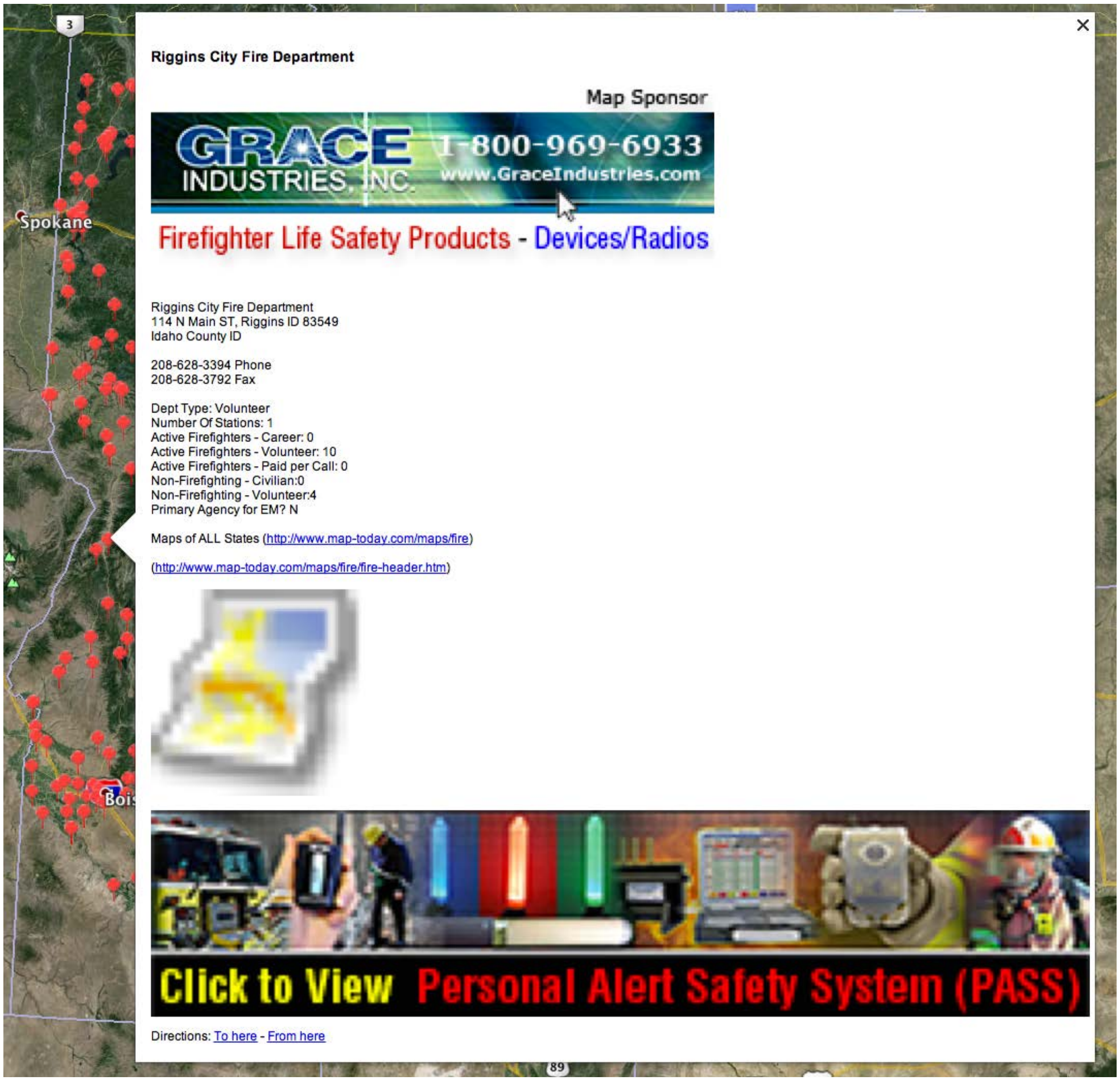
Geospatial Intelligence

While still in GoogleEarth Pro, on the top right-hand corner of the aforementioned Layers box (located in the bottom left of the window), you'll find a button that says "Earth Gallery". Open it up. Begin finding what's available for your state by searching for your state in the search bar. Check out what's available to you by clicking on the specific map data of interest and then View in GoogleEarth (bottom right-hand side of the map image).

Next, see what's available in your town or area. When I type in "Coeur D'Alene, Idaho", I get elementary school district maps and a couple road race and marathon maps, not that those are particularly useful. The area has hundreds of map options that you can scroll through (a thrift store map, marina/boat ramp locations on Coeur D'Alene Lake later, and self-storage locations later camp up, which are a little more useful.)

I searched for "Idaho Fire" next, which gives me a map of every fire station in the state, as well as a map of 2015 forest fires. (There were a lot of useless maps that also came back during the search.) I clicked on the map of fire stations and viewed it through GoogleEarth. Because this map data is of particular interest to me, I want to save it for later. So in the Places box, I right-click on the map overlay and then click on "Save To My Places". When I open GoogleEarth Pro next time, that map overlay will already be available in my Places box.





Spokane
Bois
3
89
Map Sponsor
GRACE INDUSTRIES, INC.
1-800-969-6933
www.GraceIndustries.com
Firefighter Life Safety Products - Devices/Radios
Click to View Personal Alert Safety System (PASS)

Riggins City Fire Department

Riggins City Fire Department
114 N Main ST, Riggins ID 83549
Idaho County ID

208-628-3394 Phone
208-628-3792 Fax

Dept Type: Volunteer
Number Of Stations: 1
Active Firefighters - Career: 0
Active Firefighters - Volunteer: 10
Active Firefighters - Paid per Call: 0
Non-Firefighting - Civilian:0
Non-Firefighting - Volunteer:4
Primary Agency for EM? N

Maps of ALL States (http://www.map-today.com/maps/fire)

(http://www.map-today.com/maps/fire/fire-header.htm)

Directions: To here - From here

What's even better is that I can click on each fire station location and get an information box like the one below. Not only does it give me contact information, but also the number of firefighters, and whether it's a career or volunteer fire department.

So let's say that we wanted to send this overlay to a friend. We can right-click on the overlay again, and then click on "Save Place As…" We can now name this file and save it to our desktop as a .KMZ file, then email it to the members of our prepper group, who can open and view it in GoogleEarth, too.

Earth Gallery is a great source for GEOINT information, so be sure to make good use of it. You can also search for census and demographic data, You may have to search your way to useful maps, but you'd be hard pressed to find this amount of data at your fingertips anywhere else.

ArcGIS[45] is another very useful geospatial software tool. The learning curve is a little higher, however there's plenty of documentation on how to use ArcGIS.[46] One problem you'll encounter with ArcGIS is finding ways to feed it. ArcGIS is just a tool; without data to plot of maps, it will be of limited use to you. Fortunately, there are a few good options to find shapefiles to view through the software.

The first is to simply search the internet for shape files for your state or area. A simple search for "Kootenai County shapefiles" returns the County's GIS page, which provides a large menu of links to download files like land plat information, airports, telephone lines, EMS and ambulance facilities, polling places, law offices, and a whole host of other data. Typically, counties with larger administrations make this data available through their website.

Keep in mind that there may be non-government organizations (such as corporations or non-profits) who have created and shared shapefiles online. You may have to dig a little deeper and get creative with your search queries, or maybe check shapefile databases online (the Census department also has shapefiles available for download[47]).

Another option is to purchase a one terabyte hard drive and head down to your county's agricultural extension office. Inquire about the county's GIS data, and then ask them to download it to your hard drive. My
county's extension office asked me why I needed the information (as if I needed justification for public data) and I said for real estate development. But I could have also just told them that I'm a tax payer who paid for it. (If you're in proximity to another county, it's a good idea to get their GIS data, too.)

Environmental effects are another factor of GEOINT. In the mountain west, every spring is runoff season. As temperatures become warmer, massive snow melt floods rivers, which flow a muddy, chocolate brown. In other areas of the nation, flash floods are a real problem, as are torrential rains brought by hurricanes and other potentially disastrous weather effects. If your AO is susceptible to these types of weather patterns, then we also need to look into collecting information about their environmental effects.

The Federal Emergency Management Agency (FEMA) has data about flood plains that may be of use to you.[48] The site allows you to type in an address and then view and download maps showing potential flood plains. It's a good idea to download these maps of your area, just in case you need them later.

Another resources for flood information is FloodTools.[49] Like the FEMA website, FloodTools allows you to type in address and view your area's risk assessment for flooding. If you give the website an email address, then they'll send you a flood risk assessment in PDF by email. Be sure to print that out and include it in your IPC binder.

One website I use to track wildfire information is InciWeb.[50] Not only does the website catalogue and track these events (including prescribed fires/controlled burns), but it also provides information on road closures. The Map tab also provides maps of the affected areas.

Signals Intelligence (SIGINT)

In an emergency situation, you're more likely to get up-to-the-second intelligence information through signals monitoring than by any other collection method. Listening in on a police scanner - hearing law enforcement officers and emergency first responders communicating over the radio waves - is going to be your best bet for intelligence gathering. We it communications intelligence (COMINT), which in this case is a subset of SIGINT.

At an absolute minimum, you'll need a police scanner. Although I recommend the Uniden Home Patrol[51], any police scanner will suffice. Unlike an ordinary police scanner, the Uniden Home Patrol allows you to type in your zip code (you can also select your city), and then it programs itself to monitor your local emergency frequencies. Not only does it monitor those frequencies, but it also shows on the screen which frequency is broadcasting and who that transmission belongs to. For instance, our local police department is broken into precincts, so the Home Patrol can distinguish between a transmission from the north precinct and the east precinct. Another nice feature is that you can tell it to ignore certain frequencies.

Attached to your ACE, you need a good COMINT section, whether it's one or more individuals monitoring the radio waves, picking up not just radio traffic over the police scanners, but also news reports from radio stations, amateur radio operators on the ham bands, and possibly even local VHF/UHF traffic. You really do need an experienced ham radio operator on your side, so seek one out and get some training yourself.

<u>TO DO LIST:</u>

1. Identify sources that can satisfy your intelligence requirements
2. Begin developing sources who have the information you need
3. Ensure that you have access to at least one collection asset for OSINT, HUMINT, IMINT and SIGINT/COMINT.

Section III - Intelligence Preparation of the Community

Chapter Six - Intelligence Preparation of the Community

What we're all concerned about is our survivability. The two questions we ask is, *What advantages can we create for ourselves over our adversaries?*, and *What adaptations can we make to our surroundings that will help us survive?* One definite advantage that we can create is information dominance, and that's where intelligence comes in. We just finished discussing intelligence collection; in the chapter previous to that we talked about how to direct collection and then how to analyze it. Now we're bringing both pieces together in order to build out finished intelligence.

Information is what I call a "conflict currency." The more information we have, the wealthier we are. It's the raw data that gets turned into intelligence that allows our commanders to make informed, time-sensitive decisions. Not having enough information when you need it is like fighting a boxing match blindfolded. Even if you knew a punch was coming, you wouldn't know which hand was throwing it, and once you were hit it would be too late to matter.

To really drive the point home, Napoleon Bonaparte once wrote that "War is ninety percent information." And the low intensity conflict for which many of us are preparing is going to be reliant on information as well. So one thing we need to achieve in order to be wealthier than our adversaries is called information dominance. What we need is a framework or foundation that allows us to anticipate our intelligence needs based on our operating environment, and that framework is called Intelligence Preparation of the Community, or IPC.

This IPC process is a modified version of the Army's Intelligence Preparation of the Battlefield (IPB). The Army prepares itself for operations and contingencies by studying each area of responsibility through the IPB process. But IPB is really not sufficient for our uses; first, it doesn't focus enough on the human terrain, and second, it's designed for large military units with deep combat support systems. The four step process is the same, however, the guts of IPB have been modified for community use. The IPC process helps communities in several ways.

First, it's a methodical process that helps us to identify what we need to know, what we already know, and what we don't. Intelligence without a focus is a bottomless pit that you will never fill. We task out what we don't know through intelligence requirements, and we begin analyzing the intelligence information we do have.

Second, IPC helps us break down an extraordinarily complex problem into four very manageable steps. What we're doing is examining our operating environment through the lens of all its different layers - physical terrain, human terrain, critical infrastructure, security/defense, and political/civil. And it's these five layers that comprise the information we'll need in order to gain an expert understanding of the risks and threats in our community. Knowing that these factors exist isn't enough; we must be able to describe how they will affect us and the community.

Third, IPC helps us develop actionable intelligence. Like a business plan to a corporation, IPC is going to enable us to diagnose the problems we expect to encounter.

And once we identify and understand those risks and threats through the IPC process, then we can begin working to mitigate risks and neutralize threats.

Without IPC, community security is aimless. Sure, you can set up guard posts around an area, but you won't know what to expect. It's like showing up to play a football game without having studied game film from the other team. We don't know the plays our opponents like to run, we won't recognize their formations and we won't be able to anticipate their play calling. In short, it's a game we're probably going to lose.

Now that we've covered intelligence collection and analysis, this your first and most important project. Without further ado, here are the four phases, including sub-tasks, of the IPC Process.

Phase One: Define the Community Environment

A. Establish the limits of your area of operations (AO)
B. Establish the limits of your area of interest (AI)
C. Identify the significant characteristics of the community
D. Identify current intelligence gaps

Phase Two: Describe the Community's Effects

A. Develop map overlays
B. Describe the effects of weather and terrain
C. Describe the effects of the five layers of the community

Phase Three: Evaluate the Threat

A. Identify, analyze and rank threats
B. Develop Order of Battle products
C. Develop Table of Organization & Equipment

Phase Four: Determine Threat Courses of Action

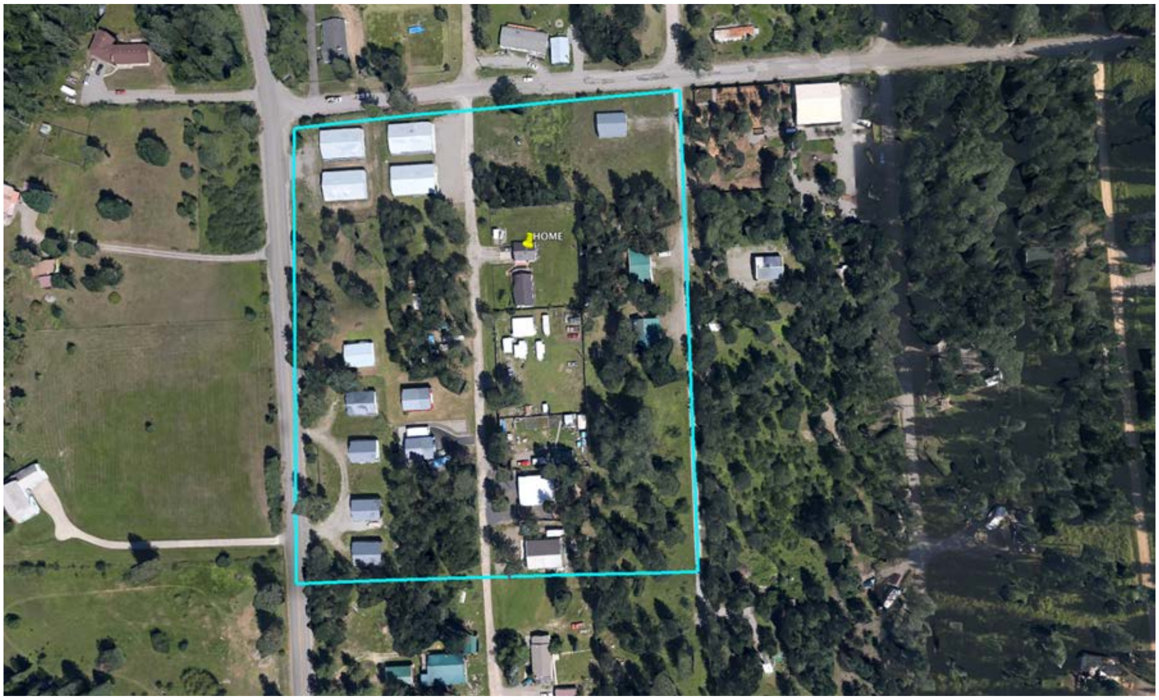
A. BICC/E Analysis
B. Identify and rank potential COAs
C. Identify MLCOA and MDCOA

The next four sections provide a step by step process to completing an IPC product. You will need a map of your area, a few sheets of acetate, and at least two dry or wet erase markers (black and red). You an also follow along on GoogleEarth and use their drawing tools.

<u>Phase One</u>: Define the Community Environment

A. Establish the limits of your area of operations (AO)
B. Establish the limits of your area of interest (AI)
C. Identify the significant characteristics of the community
D. Identify current intelligence gaps

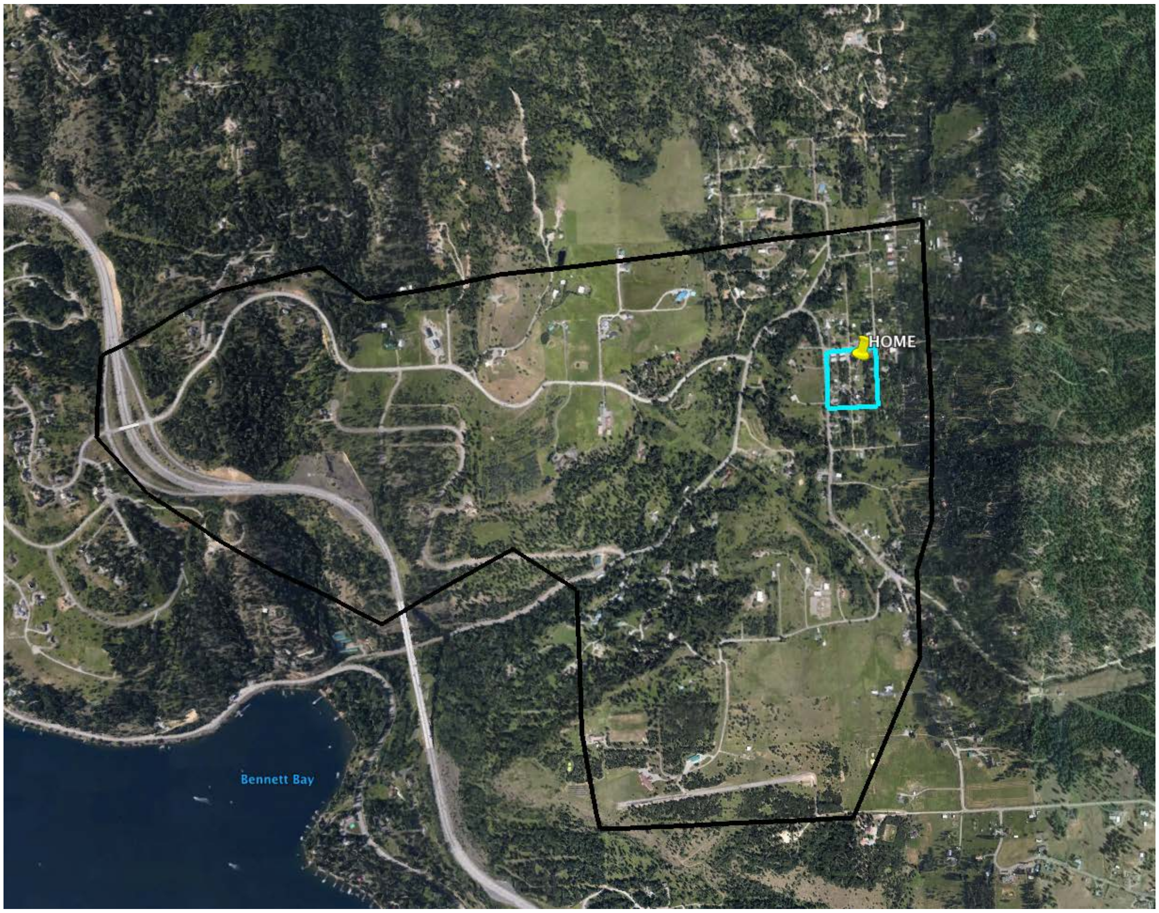
The first phase of work in the IPC process is understanding the mission, including the boundaries of our operations. This is our Area of Operations, or AO. The unit commander sets the boundaries of the AO based on where he intends to operate. Knowing that boundary helps us as the intelligence section to focus our collection. We're not worried about what's going on anywhere else other than in our AO because that's the mission area we're supporting.



The first step in Phase One is to establish the boundaries of our AO. Break out a map of your community and find your home. The size of your AO is mission dependent; consider the acronym METT-TC (Mission, Enemy, Terrain & weather, Troops, Time available, Civil Considerations). (For a refresher, refer to the Mission Analysis subsection located in Chapter Four.) Your AO is either the limits of your ability to project force, or the area where you expect to operate. It's the mission critical area for which you're responsible.

For a family of four in suburban America, an AO is not going to be very large. If that family of four begins working with their neighbors post-SHTF, then their AO expands because not only do they now have a greater capability but they also have a larger area to protect. It's difficult to provide a baseline size for an AO because I don't know the METT-TC factors for your area, however, consider this: it takes the average person about 15 to 20 minutes to walk a mile on flat terrain. That says to me that the AO for an average family should be much, much smaller than a mile radius. I might suggest starting with a quarter mile. An alternate way to measure the limits of your AO is to go out on your front porch and consider your line of sight. If you can see it or reach it with a rifle, then it should be in your AO.

Using a sheet of acetate placed over your map and a black marker, you'll need to draw out your AO. The AO can be a square, rectangle, circle, or polygon. It doesn't have to be uniform; it just needs to include the area for which your responsible for.



In the photo above, I've used GoogleEarth to make a place marker on my home, and using light blue (for visibility; you should generally be using black for these boundaries) I've drawn a line around my AO. Once you've drawn yours, in the top left hand corner write "AO" just beneath the line. If you show this to a member of your prepper group or security team, he should be able to determine that the line is the limits of your AO.

After determining the AO, we need to identify our Area of Interest, or AI. The Area of Interest is not our responsibility, but we are interested in what happens there. It may include a nearby school or a police station or electrical substation. Although they're not in your AO, they can affect you and your AO, and therefore should still be monitored. Using the same sheet of acetate, use the black marker to draw the limits of your AI. Keep in mind all the factors that could influence the people in your AO (churches, for instance) or affect the things in your AO (such as water treatment, electrical, or law enforcement facilities).

When we talk about information dominance, this is where we should be focusing our collection efforts. It's a lot more likely that people and things already in this area are going to more immediately and directly affect you than people and things outside this area. This is why we must achieve information dominance in this area.

In the photo on the next page, my AO is marked in light blue. The black line is the limits of my AI, and it includes the nearest interstate exit, the primary route from that interstate exit that runs close to my AO, and a private airstrip to the south of my AO. The interstate exit, the main highway, and the airstrip are all of interest to me, which is why they're included in my AI.

Before we move on, remember that as the METT-TC changes, so might our AO and AI. You're not married to these shapes; they can be changed to reflect area conditions or changes in the mission. If a new threat is identified outside your AO, but it becomes your responsibility, then your AO needs to expand, and that addition becomes an additional focus for intelligence collection and analysis.

The third step of Phase One is to identify significant characteristics of the community. These significant characteristics can influence or affect what happens in your AO. These influences or events may also cause second- or third-order consequences, which is why need to identify them in order to identify how they can affect us. Our community environment consists of five factors:

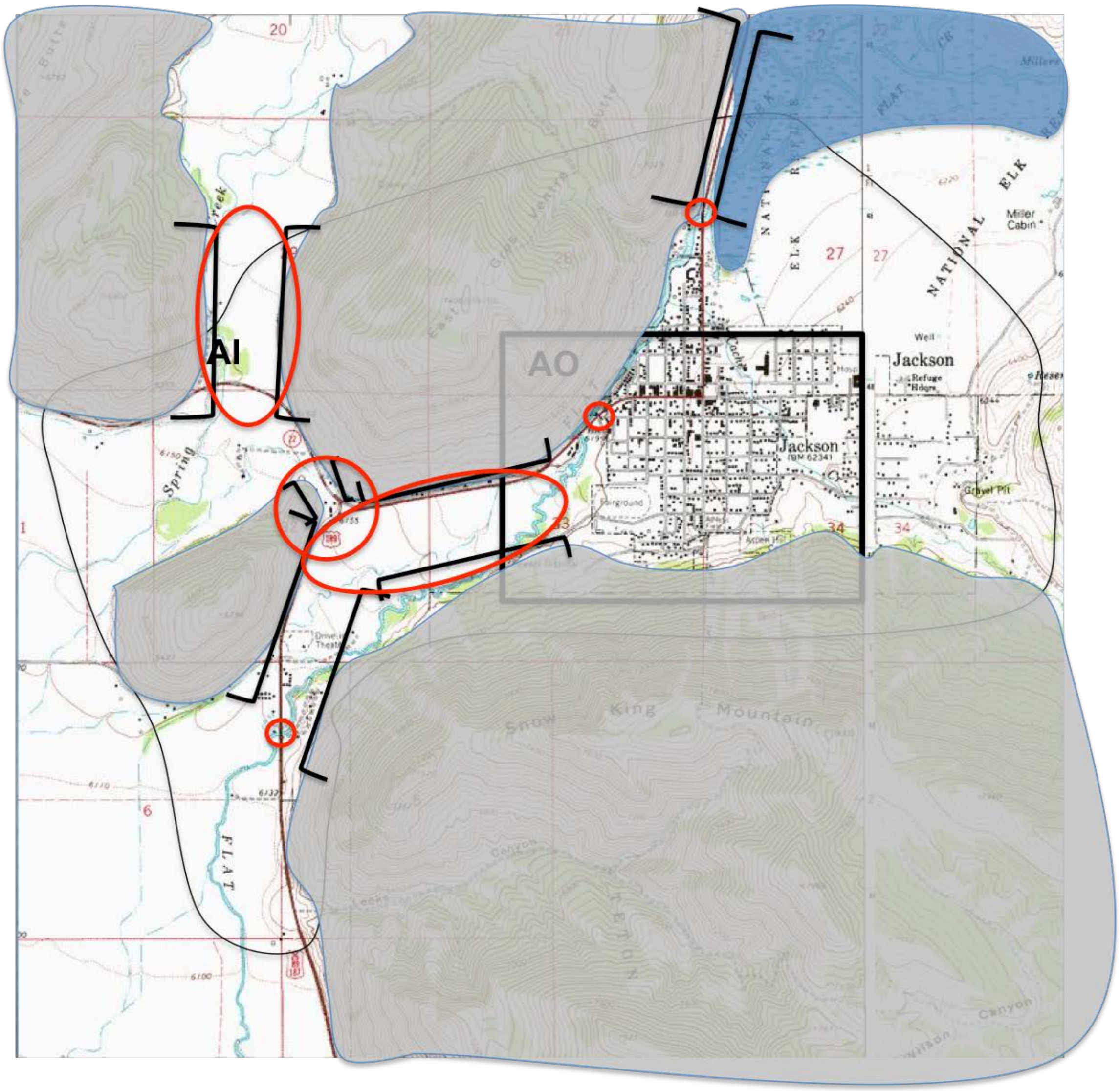
- Physical terrain
- Human terrain
- Critical infrastructure
- Security/defense
- Political/civil

We can use an acronym to help us identify significant terrain features. ASCOPE stands for:

- Areas - affluence, poverty, population density, cultural and ethnic
- Structures - military, security, defense, political, civic and community
- Capabilities - local security, military, law enforcement
- Organizations - civic, religious, criminals
- People - key figures, influencers, leaders
- Events - cultural, religious, community

Let's start with the physical terrain, which includes mountains, hills, valleys, depressions, hydrology like lakes and rivers, streams, swamps and marshes, irrigation ditches, and other natural or manmade barriers and obstacles. Examine your topographical map and use a blank sheet of acetate to identify these features.

We'll also want to identify chokepoints and potentially hazardous areas. You'll need to identify canalizing terrain such as bridges, ditches, fences and canyons. When driving around your neighborhood, what are potential ambush locations? Roving traffic control points are common across Mexico, where bandits are able to sometimes use the physical terrain to block traffic and rob at gunpoint the vehicles that are stuck on the road way. These areas are an important part of the physical terrain, too.



In the photo above, the gray areas are steep hills, the blue area is a marsh, and the red circles identify chokepoints. I've also bracketed what are called "mobility corridors". That has more to do with where and how large units are able to maneuver, however, the map overlay above shows two very distinct ways to arrive in town.

Human terrain features include individuals and ethnic, cultural, religious, political and socioeconomic groups in the populace; their wants and needs; the problems they face; and the dates and events that are important to them. If we're going to be living and surviving among these people, then it's absolutely critical to know as much about them as possible. A large part of low intensity conflict is not making unnecessary enemies. The less we know about people, the more likely we are to treat them as a threat. But by identifying these features of the human terrain, we can identify groups who are more aligned with us, potentially gaining allies; and determine which groups or individuals more likely represent a threat.

Start with the individuals and groups in your AO, using this checklist:

- Identify the family relations, religious values, political views, and ethnic ties (tribes or clans, if any) of these individuals.
- Examine the problems your community faces: economic, political, religious, criminal.
- Identify key figures in your community: government/political, religious, criminal leaders.
- Evaluate the different parts of your community: high crime areas, poverty, affluence, high and low population density.
- Identify the local media, their bias, and how people get news information: print, radio, television, social media

Critical infrastructure is any facility, utility, or service that sustains life as we know it. If you have critical infrastructure in your AO - grocery stores, distribution centers, power plants, water treatment facilities, roads and bridges, etc. - then you'll need to identify on a new overlay. It may be the case that we have to provide support to the security of these places in order to keep the lid on community security. Knowing where these places are ahead of time will help us anticipate the level of support we may need to provide.

Security and defense includes military and law enforcement. Identify police stations and substations, National Guard or Reserve facilities, or active duty bases in your AO and AI.

Lastly, identify the political and civil facilities in the AO and AI. These include political buildings (at the local, state and federal level), and civil groups like the Rotary Club or the Shriners.

By now, you should be getting a feel for what you know about the area and what you don't know. Intelligence gaps reflect what we don't know, so we need to generate intelligence requirements. (For a refresher, refer to Chapter Two, subsection on Intelligence Requirements.) Unless you know everything there is to know about your community, then you're going to have to generate some Intelligence Requirements. (A starter list of Intelligence Requirements is located in Appendix B.)

<u>Phase Two</u>: Describe the Community's Effects

A. Develop map overlays
B. Describe the effects of weather and terrain
C. Describe the effects of the five layers of the community

In the last phase, we identified a lot of people, places, areas and things — these are the significant characteristics of our community. In this phase, we're going to describe how they'll affect the AO or the community. To do that, we'll start creating some map overlays.

When you can identify areas that face the same problems, experience a similar rate of crime, or have the same socioeconomic status, start with a blank sheet of acetate and create another overlay. You can create as many overlays as necessary. Think about identifying areas where it's safe to travel and areas that aren't. Identify the areas that are most likely to be looted during an SHTF event and create an overlay that illustrates these areas. When or if a catastrophic event occurs, break out your high danger areas overlay so you can better anticipate where the dangerous areas will be. Create something that you can show to others to brief them on the situation.

All the things we identified in the last phase are still on our plate for this phase. Let's say that you identified a minister of an area church who leads a congregation of 500 people. With a potential ability to influence 500 area residents, isn't it important to begin learning more about him? What will he do and how will he influence his congregation during a SHTF environment? Will he tell them to obey all political leaders and law enforcement, regardless of the lawfulness of their orders? Or will he encourage his flock to do what's right and help protect the community? Phase Two is all about describing how these characteristics might affect us.

Refer back to our ASCOPE factors. How will affluent, poverty, high population density, and high crime areas affect us? How will structures like nearby apartment buildings affect us? How will the capabilities of the local sheriff's department affect us? How will the charity organizations affect us? How will the people and influencers affect us? How will religious and cultural events like Christmas or sports games affect us?

In the last chapter, I gave you six blocks of Intelligence Requirements that need to be answered. Once those are answered, you can modify those Intelligence Requirements to ask, "How will [significant characteristic] affect my AO?"

Start a list of potential threats for the next phase. Once you determine that a significant characteristic will or could negatively affect your security in a SHTF environment, then add it to the list of potential threats.

<u>Phase Three</u>: Evaluate the Threat

A. Identify, analyze and rank threats
B. Develop Order of Battle products
C. Develop Table of Organization & Equipment

Threat analysis is such a critical part of intelligence that it deserves a lion's share of our time and attention. Our goal with Phase Three of the IPC Process is to provide actionable or predictive intelligence on our potential and known adversaries. Preparedness groups and security teams who fail to conduct a thorough assessment of the threats are going to be in a constant need of valuable intelligence — realistic expectations based on the enemy's capabilities — and are much more likely to find themselves in compromising situations when faced with threats they didn't know existed or threats with unknown capabilities. In a life or death situation, having "an idea" of an adversary's capabilities or being "vaguely familiar" with them may very well lead to some heartache. We have to put in the time and truly know the enemy we face.

Threats are broken down into four categories:

- Conventional
- Irregular
- Catastrophic
- Disruptive

The conventional threat includes foreign and domestic armies, the police state, and other forces of state tyranny. We call them conventional because, by and large, they wear uniforms that symbolize their de jure authority. They're acting within the authority of a recognized, legitimate government.

The irregular threat includes gangs, looters, insurgents, guerrillas and other criminals. More often than not, although they may wield de facto authority, they are not the nationally-recognized authority. The irregular threat typically doesn't represent a recognized, legitimate government. They typically don't wear uniforms and often aren't bothered with laws, either civilian or of land warfare.

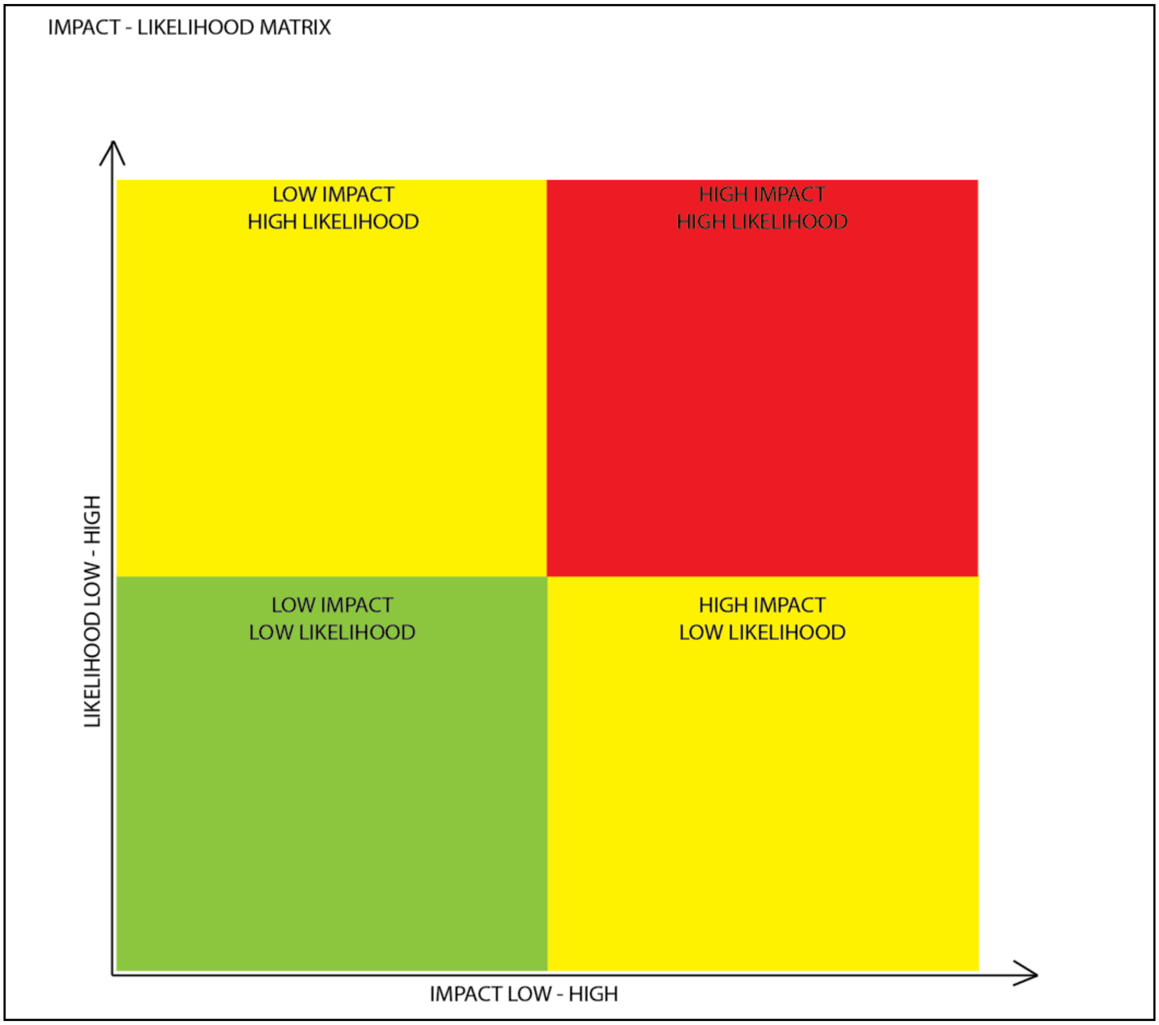
Catastrophic threats can be either natural or man-made disasters. Examples are hurricane, earthquakes, pandemics, and nuclear/biological/chemical weapons. These are mass casualty events and, through second- and third-order effects, can create conventional and irregular threats.

Finally, there are disruptive threats. A disruptive threat isn't going to kill you, although it will disrupt your operations. Things like power outages, identity theft, fuel shortages, and cyber attacks are all examples. Like catastrophic threats, these, too, can can result in conventional and irregular threats.

By now you should have compiled a list of potential threats in the area, however, it's unlikely that your list is complete. Before moving on with this chapter, I highly recommend getting together with your group and brainstorming all the potential threats in the area. Use the four types of threats to help brainstorm and add to your list. During brainstorming, we're not looking for perfect or the most likely answers, just realistic ones. A cyber attack that shuts down banks and electronic purchasing is realistic. An alien invasion is not.

One problem that we may encounter is the desire to prepare for everything. What we end up doing is wasting a lot of time and money on items we're unlikely to need. What we should be doing instead, is preparing for the threats that pose us the most likely and greatest risk. So what we need to do is draw out an X and Y axis, representing four quadrants. Our X axis is going to be Impact and our Y axis is going to be Likelihood.

What we're going to do is begin ranking each threat according to its likelihood and impact, so we can better prioritize not only our intelligence focus, but also our general preparation. Impact is the level of severity. A disaster would be considered a High Impact, while no noticeable event would be Low Impact. Likelihood, on the other hand, is the probability that an event occurs or threat exists, either High or Low.



For instance, if you lived in Kansas, a tornado might be a High Impact, High Likelihood event because tornadoes happen every year. So in the top right-hand quadrant, we'd include tornadoes because it's a High-High event, and therefore receives a higher priority.

Let's say that we want to rank the impact and likelihood of a nuclear strike in the area. That would definitely be high impact, but the likelihood is quite low, so we'd include nuclear strike on the bottom right-hand quadrant, which are the the High (Impact) - Low (Likelihood) events.

And finally, we're going to rank the impact and likelihood of a rabies outbreak among humans in our community. Its impact certainly is questionable, however, for my area I'm going to give it a low impact rating because although rabies will cause death, it's not a mass casualty event. And for its likelihood rating, I'm also going to assign it as low. Since it's overall score is Low-Low, we'll include human rabies outbreak in the bottom left-hand quadrant with all the other Low-Lows.

What we're attempting to do here is prioritize the threats for which we should prepare the most (High-Highs) and identify those threats for which we should dedicate the least amount of time preparing (Low-Lows). Starting at the top of your threats list, discuss each threat and assign it an impact and likelihood. There is a subjective quality to this, however, be rational about ranking each threat. One problem I see in groups is that they allow their fear of an event to overstate its impact or likelihood. Another problem is that being unfamiliar with certain threats, which is an overt bias, tends to negatively affect a threat's ranking as well. Do some homework, if you need to. We're mainly concerned with being accurate.

Once we've identified our high priority threats, we need to begin our assessment beyond impact and likelihood. We'll begin by producing a nine paragraph Order of Battle and threat assessment product. (Refer to the Order of Battle subsection located in Chapter Four.) Using topics of the nine paragraphs, determine your intelligence gaps and then task out collection to satisfy them. A Table of Organization & Equipment, which charts the unit composition and equipment, should be included under the Composition section.

You can also use the Threat Characteristics sheet. Use the categories to help you brainstorm the threat characteristics that apply to each of your high priority threats. Once you've completed an initial threat assessment for your high priority threats, continue on with the High-Low and Low-High threats, what we might refer to as medium priority threats. After completing threat assessments for the threats most likely to cause a high impact, you should have a much better idea of a threat's capabilities, which we'll use to develop their potential courses of action, providing you with some potentially actionable or predictive intelligence.

Table 3-1. Threat characteristics

Threat Characteristic	Examples		
Composition	Regular Army	Militia	Unit designation
	Unit history	Uniforms	Type of unit
Disposition	Historic	Current	Proposed future
Tactics	Method of operations	Intent	Propaganda
	Conventional	Unconventional	Asymmetric
	Terrorism		
Training	Individual	Team	Unit
	Source of training	Uniforms	Insignia
	Specialized training		
Sustainment	Food	Transportation	Fuel
	Spare parts	Water	Ammunition
	Maintenance status		
Finance	State-sponsored	Support from allies	Criminal activity
	Taxes	Donation	
Operational Effectiveness	Strength	Goals	Personnel
	Morale	Weapons	Leadership
	Equipment	Chain of command	Loyalty
Communications	Written	Internet	Signal
	Verbal and live drop	Emitter type	Frequency range
	Electronic		
Intelligence	Surveillance	Countersurveillance	Deception
	Reconnaissance	Electronic warfare (EW) capability	
Recruitment	Local	National	Regional
	International	Coercion	Volunteers
	Motivation		
Support	Financial	Media	Local
	National	Regional	Religious
	International	Popular	Tribal or ethnic
Intelligence Reach	Databases	Assets	Connectivity
	Architecture	Access	Informal networks
National Agencies	Loyalties	Agenda	Leadership
	Capabilities	Relationships	
Law Enforcement Agencies	Loyalties	Agenda	Leadership
	Capabilities	Relationships	
International Organizations and NGOs	Loyalties	Agenda	Leadership
	Capabilities	Relationships	Areas of operations
Personality	Key leaders	Education level	Idiosyncrasies
Other Threats	Natural diseases	Biohazards	Radiological
	Chemical hazards	Wildlife	Toxic industrial material
	Criminal activity		

Phase Four: Determine Threat Courses of Action

A. BICC/E Analysis
B. Identify and rank potential COAs
C. Identify MLCOA and MDCOA

Determining the potential courses of action (COA) for a given threat can be one of the most difficult steps of the IPC process. One reason being that we're likely to always be at a loss for critical information. Without tools that allow us to listen into phone calls and read the emails of our adversaries, it's going to be more difficult to discern their next course of action. But it's not impossible.

One of the greatest pieces of intelligence we can provide our commander is a list of potential COAs. There's no greater gift than being able to determine what's going to happen, before it happens. These potential COAs allow us to tell the commander the top few things that we believe could happen. These scenarios enable the commander to make better decisions based off what the enemy is likely or more likely to do next.

For instance, after reviewing the physical terrain and the enemy doctrine, the intelligence section is able to provide the commander with what's called an "avenue of approach," that is, where and how the adversary will move to their destination on the battlefield. Knowing that the enemy is likely to take a specific path while maneuvering allows the commander to dedicate resources to monitor that area until the enemy arrives, at which time the commander will call for an artillery strike, destroying the enemy forces. We are describing events yet to occur.

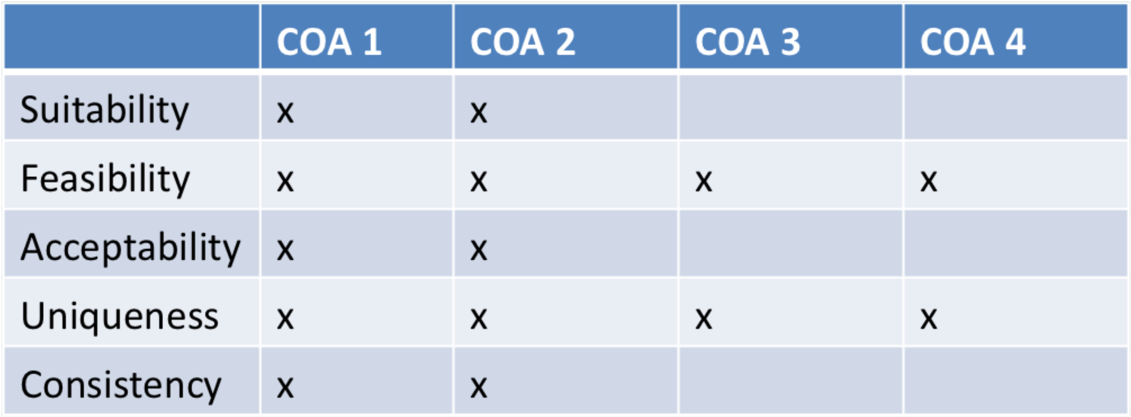
One of the things that enable us to do that is knowing threat capabilities. Once we know an adversary's capabilities, then we can begin ruling out potential courses of action if the requirements for that course of action are greater than the enemy capability. Without threat analysis — without knowing the enemy and his capabilities — that doesn't happen. So if we haven't done a threat assessment and determined an enemy's capabilities, then it's less likely that we can determine his COA.

The process we use for developing threat COAs is called BICC/E Analysis. (Refer to BICC/E: Developing Threat Courses of Action, located in Chapter Four.) Through identifying Behavior, Intent, Capabilities, Consequences and Effects, we can better determine which COAs are more likely and which are less likely.

Once we've developed a list of potential COAs, we need to rank them. We use the following metrics to do that:

- Suitability: Is it suitable for the enemy to pursue a particular course of action? Based on his known or suspected capabilities, does the COA fit his modus operandi?
- Feasibility. Is the potential COA feasible for him to accomplish? After examining his capabilities and the environmental conditions (physical and human terrain), is he capable of pursuing the COA?
- Acceptability. How much risk is involved in the potential COA? Is that level of risk, or the potential for casualties, acceptable to him?

- Consistency. Is the potential COA consistent with what we've see the enemy do in the past? Is it consistent with the intelligence information we've seen?
- Uniqueness. Is the potential COA unique? Is it a separate COA or a slight variation on another potential COA? If the COA is not unique, then it should be included with the one most like it.



	COA 1	COA 2	COA 3	COA 4
Suitability	x	x		
Feasibility	x	x	x	x
Acceptability	x	x		
Uniqueness	x	x	x	x
Consistency	x	x		

These five grading factors are what we use to determine the likelihood of each potential COA. This is a cumulative process and each COA should be judged based on all five factors. In the matrix above, each COA receives a check mark if it meets the grading requirements. Based on the results, which COA is most likely and which is least likely? Rank the COAs according to the results.

If you ranked COA 1 and COA 2 as the most likely, then you're correct. And COA 3 and COA 4 are the least likely. In this case, we'd want to alert our commander to the top two COAs because we've determined them to be the most likely. He can begin making informed decisions based on what we believe the enemy is most likely to do. Once we know what the enemy intends to do, or is likely to do, then we can begin effects-based targeting to ensure that he cannot accomplish his goals.

Section IV - Targeting

Chapter Seven: Targeting

Learning Objectives

- Understand the difference between kinetic and non-kinetic
- Understand how actionable intelligence aids targeting
- Understand the responsibilities of a targeting analyst
- Understand how to target for influence

There's been some catastrophic event - a stock market crash and bank holiday, or a declaration of war that results in major cyber attacks against the grid and financial institutions - and our once safe and peaceful community is threatened by small gangs and petty criminals also trying to survive. Not only are these groups successful in plundering soft targets, but the more success they have in looting and plundering, the larger and more dangerous they grow. If we do nothing today, then we could be at severe risk of defending against a much larger threat tomorrow. Frankly, this is where targeting becomes an option.

There are two primary drivers of targeting: intelligence and operations. Intelligence can provide targeting packages for every known bad guy in the AO, but with operations to project force, those targeting packages do us little good. The same can be said for operations: your team can have all the gunslingers you need, but without accurate target information, you're much less likely to be able to find those bad guys.

As long as we have the operations side that conducts targeting and the intelligence to support those activities, then we should seriously consider pursuing both in the scenario we just outlined.

And we have a couple good options that explain the 'how' of targeting. First, we can begin kinetic targeting, also referred to as lethal targeting, which is killing bad guys and breaking things. And second, there's non-kinetic targeting, or non-lethal targeting, which is targeting for influence. In either case, targeting exists to create desired effects. Targeting is not a task that happens independently of all other activities. It should be synchronized with all our other operations to decrease the chance that one activity negatively impacts another, and to increase the chance that targeting supports our other missions. For instance, if the source of the Leroy Jenkins Gang originates from the south end of town, and our commander's intent and mission planning consisted of clearing that area of known gang members, then how could targeting help and hinder that mission?

Kinetic Targeting

Let's say that by next Tuesday, we plan to have increased security patrolling in this Leroy Jenkins Gang area south of town in order to find gang members and kill or arrest them. But on Monday, we targeted and killed the leader of a rival group, which ends up being incorporated into the Leroy Jenkins Gang, doubling their size. Because that targeting mission wasn't synchronized to support our other mission, we ended up making security conditions worse for ourselves.

But when we use targeting to support our other missions, then we can exponentially increase our success. In Iraq and Afghanistan, U.S. Forces targeted bomb builders all day and twice on Sunday. Did it make a significant difference in the amount of bomb builders in our AO? Of course not, because IEDs aren't that difficult to make as long as you have the materials. (Aha!) But if there are no bomb making materials, then it doesn't matter if you have a thousand bomb builders in the AO. So we start seeking out facilitators, with the line of thinking that if we were to remove the logistical hub of IED cells, then we could greatly diminish the number of IEDs in the AO. That's effects-based targeting: we're not targeting something just because we can; we're choosing to target an individual because of how it will negatively affect the enemy's operations.

So if the commander was to need intelligence support for the Leroy Jenkins mission, then as an intelligence analyst, the first thing I would start thinking about is who or what we can target in order to degrade their will or ability to fight. But in order to do that, we need to produce good intelligence, preferably actionable in nature.

Developing Actionable Intelligence

Intelligence drives the fight. Our goal as collectors and analyzers of Intelligence — as members of the ACE — should be to discover and/or produce actionable intelligence; that is, intelligence that we can act on now (or in the near future). For instance, U.S. Forces raid a compound in the al-Rashid District of Baghdad. We find information that leads us to believe other known terrorists are at another known location, and so we raid a second compound on the same night. We found information that led to actionable intelligence, and then we 'actioned' it because it met other mission or targeting criteria.

Israeli jets bomb a convoy of trucks moving through Libya because Mossad received actionable Intelligence that the convoy was transporting weapons to Iranian proxy terrorist groups. Maybe that Intelligence came from SIGINT, perhaps HUMINT; either way, Intelligence information of value was collected, analyzed, and then actionable Intelligence was produced and actioned.

In Nazi-occupied Denmark, Danish resistance fighters storm a bar during a meeting of mid-level Nazi leaders and shoot them all because the resistance intelligence cell was able to produce actionable Intelligence that it passed on to the fighters. Maybe the Intelligence cell had recruited the bartender to alert them of future Nazi meetings; maybe a resistance element was conducting surveillance and watching for Nazi activity. Either way, actionable Intelligence was produced.

The best actionable Intelligence is described by three words: accurate, timely, and predictive. Your job as a member of the ACE is to produce actionable Intelligence on the back end, in order to disrupt enemy operations on the front end.

So how do we know that potentially actionable Intelligence is accurate? After all, if it's not accurate then it's not really actionable, and if we act on inaccurate intelligence, then bad things tend to happen. When I look at new information that appears to be actionable, I first view it through the lens of consistency. (Refer to the Judging Single Source Reliability in Chapter Four.) Is this Intelligence information consistent with what we currently believe to be true? Is it consistent with previous accurate source reporting (if any exists)? As a general rule, the more sources that independently confirm any given piece of information, the more credibility they lend to the veracity of that reporting. The exception is when those sources all believe as truthful something that is incorrect. Your job in that instance is to not be dead wrong.

If the potentially actionable information isn't consistent, then I have to resolve this new conflicting information. Why doesn't this new information line up with what I believe to be true? Have our assessments been wrong? Is this new information just inaccurate for any number of reasons? If the potentially actionable Intelligence is contradictory, then I may just pass on it. If my tin-foil-hat-wearing, HAARP tracking, lizard people investigator cousin Joe Bob screams bloody murder about UFOs and little green men invading the corn field, and I find it to be inconsistent with what I believe to be true, then I'm going to shrug off his claims. I'll pass.

If no other amplifying information is available then I move to feasibility. Is it even feasible that Leroy Jenkins works at IKEA as a furniture salesman? Sure, it's feasible, but it's unlikely based on what we know about Leroy. Is it appropriate for Leroy Jenkins to work at IKEA? Probably not.

The second criteria, timeliness, is also important. Intelligence value almost always diminishes over time. It has a shelf-life. What we were told 72 hours ago may no longer be true. What's important right now will be less important next week, even less important next month, and of zero use to me next year. Providing amplifying information on a firearms raid that happened last month could be important but not as important as information about the raid that happened yesterday, and definitely not as important as the raid happening right now.

The last criteria by which we can judge actionable information is whether or not it's actually predictive. If a source keys me in on an illegal firearms checkpoint that's going to be set up from Tuesday to Thursday on Highway 89 just past Thompson Farm Road, then it's going to be critically important from now until at least Thursday. On Friday, it will be less important, and maybe even useless except as an historical location (maybe they're rotating checkpoint locations and will come back around next week - that's an exploitable pattern). If we assign a name to each checkpoint location (A, B, C, and D) and after D they move back to A, then at what location can we expect them to be next? What can we prepare for B? As intelligence analysts in search of actionable intelligence, we always want to search for patterns because people get lazy and fall into routines. It's our job to make routines fatal. The next best thing to hearing about a checkpoint that went up today is hearing about the checkpoint that's going up tomorrow.

Target Selection

Alright, so what types of things should we target and how should we select these targets? Although what follows are military terms, they do have civilian/criminal equivalents. Here are the five main areas we as targeting analysts should identify:

- Command and Control

- Communications
- Intelligence
- Mobility
- Combat Support & Service Support

Command and Control is the most critical battlefield operating system. It's the leadership that coordinates activities and is ultimately responsible for mission success or failure. During the American Revolution, General Washington and other commanders would target British officers who exercised command and control over the Redcoat units. Without an officer telling them what to do, British soldiers would do nothing.

Communications is another critical area. During the Vietnam War, Radio Telephone Operators (RTO) were targeted extensively by the Viet Cong and North Vietnamese Army because without communications, a unit couldn't coordinate with other units, nor could it call for fire support or assistance.

Since Intelligence is the eyes and ears of the battlefield, removing the ability to see or hear is one of the greatest effects-based targeting there is. Irish Republican Army officer Michael Collins targeted British intelligence and constabulary forces in the fight for Irish independence. If you remove an organization's ability to observe, then you put them at a great disadvantage.

Mobility is enables movement and is necessary for operations. In Iraq and Afghanistan, IEDs inhibited mobility. Countless convoys and patrols were disrupted because soldiers couldn't drive down a route without striking an IED or having to stop while one was blown in place. If you can kill an organization's ease of movement, then you cause them to dedicate additional and scare resources to improve their ability to travel.

Combat Support and Combat Service Support functions are the elements that keep forces in the field. They include: logistics, supply, maintenance and transportation. In Afghanistan, re-supplying remote forward operating bases and combat outposts was already difficult enough. Include the effects of the environment like sand storms, which ground rotary aircraft; altitude, which makes air travel difficult; and the prevalence of Taliban fighters armed with RPGs, and sometimes logistics and re-supply by air are temporarily impossible. With a prolonged inability to re-supply, soldiers run out of things: food, water, ammunition, medical supplies.

There are two types of targets: deliberate (or planned) and dynamic (or targets of opportunity). Through deliberate targeting, we engage either scheduled targets, which are pre-planned and scheduled to occur on a certain date or within a certain window; or on-call targets, which are prepared ahead of time and can be targeted as desired or necessary. When we consider the scenario described in the beginning of this chapter, how can we use deliberate targeting against the Leroy Jenkins Gang to end his criminal rampage?

If you answered by developing targets ahead of time that can be actioned in response to his violent activities, then you are correct. These on-call targets can be useful because they may deter Leroy Jenkins' future violent, criminal activities. If you answered by targeting the Leroy Jenkins Gang headquarters while the gang is out committing crimes, then you're also correct. This is an example of a scheduled target, which can be actioned during the time that no one is home.

Aside from deliberate targeting, there's dynamic targeting, which include targets of opportunity. There are two types of those, too: unplanned and unanticipated. Unplanned targets represent bad actors we know exist in our AO, but haven't begun the targeting process on them. Unanticipated targets describe bad actors in our AO that previously didn't know about. We can still action these targets of opportunity, although we may be immediately unprepared for them.

Army Field Manual (FM) 3-60 describes the desired effects of targeting as follows: to deceive, degrade, delay, deny, destroy, disrupt, divert, exploit, interdict, neutralize, and suppress. While selecting targets, although it's more of an operations function, consider how each potential target can be engaged, and what effects you want to achieve through targeting.

It goes on to describe the desirable effects of targeting. Those include:

- Military - exploit an adversary's weakness or ability to fight; or enable friendly operations and/or hindering enemy operations

- Political/Diplomatic - improve the balance of friendly power or decrease the balance of the enemy's power

- Informational - result in positive media coverage for friendly forces, or enable information superiority

- Economic - degrade the enemy's ability to operate

For our purposes of targeting the violent criminals who threaten our families and neighborhood, the positive effects would include neutralizing leaders and facilitators of the criminal activity (military); diminishing the legitimacy and authority of the Leroy Jenkins Gang (political); improve our legitimacy and support as peacekeepers in the AO (informational); and decrease the opportunity of Leroy Jenkins to re-supply and sustain himself by plundering soft targets (economic).

The Targeting Process

FM 3-60, the Army's FM on the Targeting Process, still uses what's referred to as D3A: Decide, Detect, Deliver, and Assess. That means that the commander Decides to target a person, place or thing; the target is Detected on the battlefield; the strike on target is Delivered; and then the damage Assessed and strike on target is confirmed or denied. It works, but I think there's a better way to describe that process.

F3EAD is version used by special operations units. There are a couple more components there and if it seems more complex, then it's because it is. F3EAD, however, is a more accurate, thorough way to describe what should happen. Here's what the acronym stands for:

- Find
- Fix
- Finish
- Exploit
- Analyze
- Disseminate

First, threats — potential targets — are discovered on the battlefield through. That's the Find part of the targeting process. It starts with intelligence; if there's no intelligence collection, then there's no finding threats on the battlefield (before it's too late, anyway). It may be through surveillance, either from drones or human beings, or it may be from SIGINT, or any number of other methods of collection. Once a threat is identified, we need to get a fix on his location.

No matter how a threat was discovered, we need to Fix is location, typically through continued surveillance. We need to identify what effects (both positive and negative) we will achieve, how we're going to action the target, and what's the potential collateral damage. The three requirements just mentioned are part of the target vetting process. We don't want to disrupt other missions by killing an intelligence source, or have our strike result in creating unnecessary enemies, for instance, which is why we need to vet each of our targets. Once a target has gone through the vetting process and the risks are acceptable, we finish the target.

Drone strikes have been the hot topic in the conflicts across the Middle East and southwest Asia. Many of those targets were being Finished. Drone warfare is seen as low risk and offers precision as good as the intelligence allows, but that's not going to be an option for community security. More than likely, you will need a physical presence "on the X" for the Finish mission, but it doesn't always have to be your team. If law enforcement is still available, you can still identify and confirm the location of a target, but have someone else action it. It all depends on our situation and capabilities.

Once we've Finished the target, we exploit it. We search the bodies for pocket litter and identification, and search the home or compound for electronics and documents. This is the Exploit phase where we're trying to gather as much information as possible because not only could it potentially yield intelligence information, but it could also yield actionable intelligence information. One the electronics and documents are collected, they need to be analyzed.

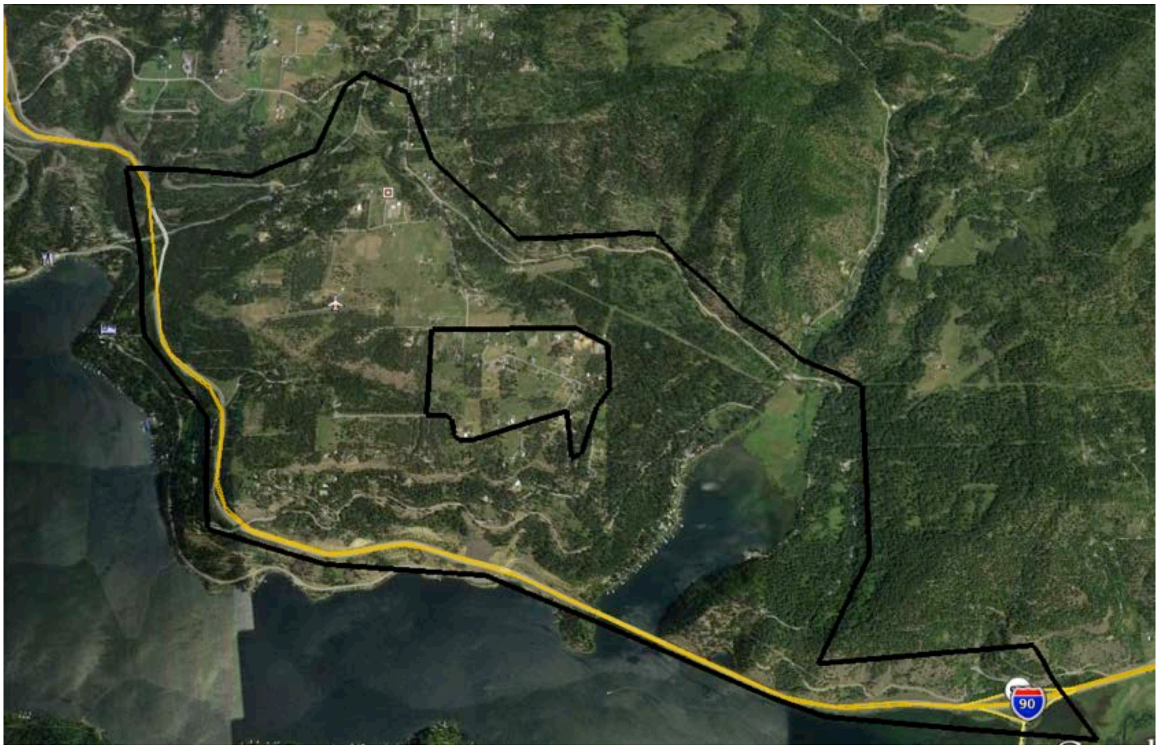
The Analyze phase of F3EAD tells commanders the results of the strike. Often, boots on the ground can confirm or deny that a target was killed or captured (that's still intelligence analysis, by the way), but the effects of the strike generally take more time. Before a target is finished, intelligence analysts describe the effects, whether the death or arrest of target will degrade his organization's ability to operate, deter future activity for fear of the same consequences, or delay the arrival of a specific capability for the enemy organization. This is where the rubber meets the road for analysis: did the strike achieve the intended effects, and what unforeseen effects (positive or negative) occurred?

After that analysis has been finished, it is Disseminated to commanders. From there, commanders make other decisions about mitigating a negative unintended consequence, planning a new operation to exploit the death or capture of enemy facilitation or leadership, or pursuing new targets. This completes the F3EAD targeting process.

Appendix A: IPC / Area Study Example

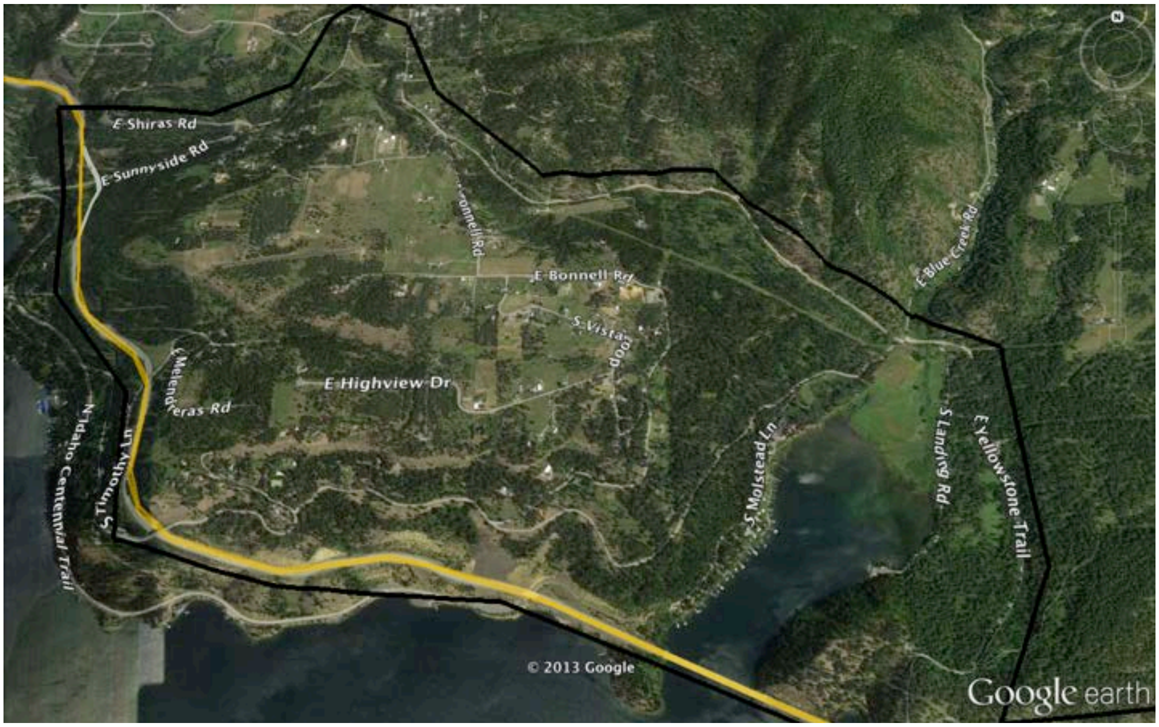
IPC for AO Moonraker
LOCATION, STATE
YYYYMMDD
ANALYST/TEAM

AREA OF OPERATIONS / AREA OF INTEREST



[DESCRIPTION HERE: The Area of Operations (AO) is x miles southeast of x town in x county. The Area of Interest (AI) includes x terrain features, x critical infrastructure, and x primary routes.]

ROUTE MAP OF AI

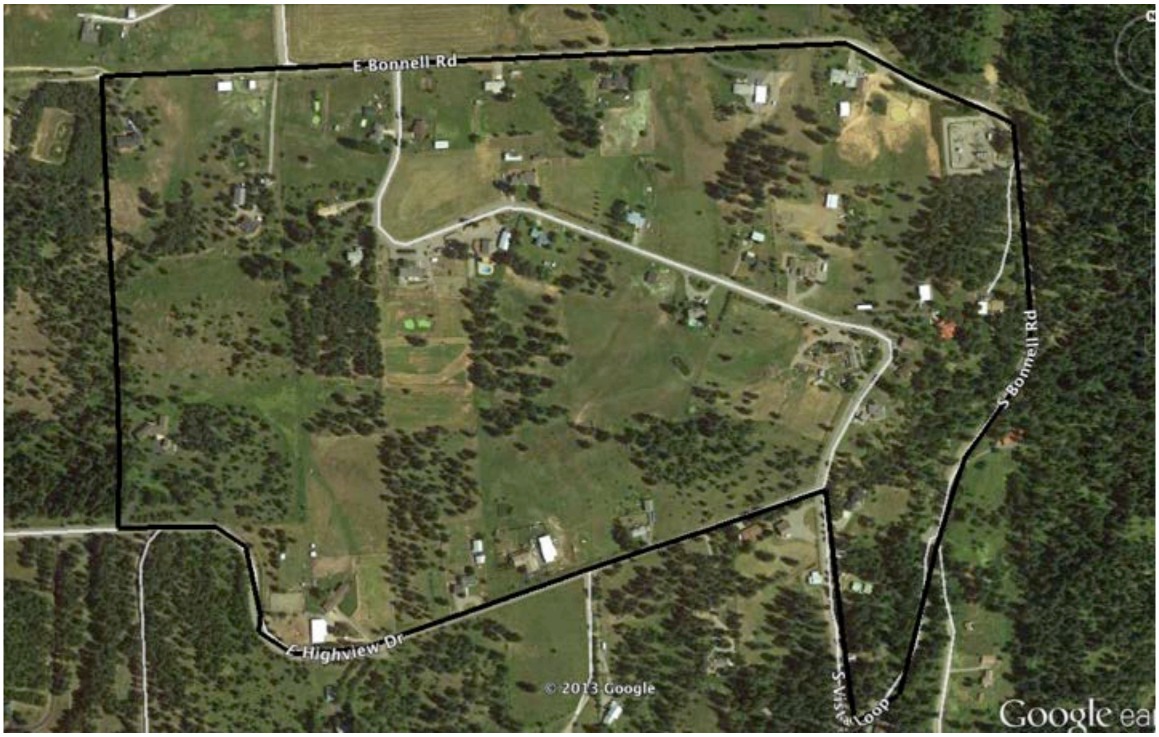


(Include road maps and any other layers you build.)

PRIMARY ROUTES WITHIN THE AI
Interstate 90

SECONDARY ROUTES WITHIN THE AI
East Shiraz Road
East Sunnyside Road
Bonnell Road
East Melenderas Road
South Molstead Lane
South Landing Road
East Yellowstone Trail
South Timothy Lane

ROUTE MAP OF AO



Include road maps and any other layers you build.

PRIMARY ROUTES WITHIN THE AO
N/A

SECONDARY ROUTES WITHIN THE AO
East Bonnell Road
South Bonnell Road
South Vista Loop
East Highview Drive

GEOGRAPHIC TERRAIN INTELLIGENCE REQUIREMENTS

1. What is the physical terrain that affects my area?

2. How does the physical terrain affect my area?

3. What physical terrain is the most likely to change?

4. What man-made obstacles will affect my area?

5. What seasonal climate factors affect my area?

6. What electrical infrastructure affects my area?

7. What hydrological features affect my area?

9. What are the primary transportation routes in my area?

10. What are the secondary transportation routes in my area?

HUMAN TERRAIN INTELLIGENCE REQUIREMENTS

1. What is the population density in my area?

2. Identify the areas of homogenous race, ethnicity, culture, and religion.

3. What is the socioeconomic breakdown in my area?

4. What are the crime patterns and high-crime sections in my area?

5. Identify the civic and social organizations in the area.

6. What media outlets affect my area?

7. Which groups or sub-groups are most aligned with our goals?

8. Which groups or sub-groups are least aligned with our goals?

9. Which groups or sub-groups will likely have a disposition towards violence during an emergency?

10. Which groups or sub-groups have the most in common with other groups or sub-groups?

11. Who are the leaders or individuals who hold influence over each group or sub-group?

POLITICAL TERRAIN INTELLIENCE REQUIREMENTS

1. Who is the political leadership in my county/AO?

2. Who are the civil servants who wield political influence?

3. Who are the civil servants who wield administrative influence?

4. Who are the known pro-Constitution politicians and civil servants?

5. Who are the known statist/anti-Constitution politicians and civil servants?

6. What is the organizational structure of county governance?

7. What are the perceived strengths of the county government?

8. What are the perceived weaknesses of the county government?

9. How effective at maintaining security will the county government during an emergency?

10. What is the overall quality of governance of the county government?

11. Where are the county and local government offices and buildings?

ECONOMIC INTELLIGENCE REQUIREMENTS

1. Who are the major job providers in the county?

2. What industries operate in the county?

3. What are the service industries dependent on industrial production?

4. What is the unemployment in the county?

5.What are the trends or indicators regarding economic stability?

6. What factors threaten future economic stability?

7. What is the distribution of socioeconomic levels?

8. What are the dual-use manufacturing companies?

9. Where are the manufacturing plants?

10. Which economic infrastructures are directly related to the political infrastructure?

SECURITY INTELLIGENCE REQUIREMENTS

1. Identify the state and local law enforcement organizations in the AO.

2. Identify the federal law enforcement organizations in the AO.

3. Identify the organizational structure of law enforcement organizations in the AO.

4. Identify the leadership of law enforcement organizations in the AO.

5. What is the strength and disposition of law enforcement organizations in the AO?

6. What are the attitudes of law enforcement leadership towards the Constitution/ Liberty in the AO?

7. Which law enforcement officers are pro-Statist/anti-Bill of Rights?

8. Identify the private security apparatus in the AO.

9. What is the quality of security in the AO?

10. What is the quality of justice in the AO?

11. How does the populace view law enforcement in the AO?

DEFENSE INTELLIGENCE REQUIREMENTS

1. What military installations are in the AO?

2. What is the strength and disposition of active duty forces in the AO?

3. What is the strength and disposition of Reserve/National Guard forces in the AO?

4. What are the capabilities of all federal and state military forces in the AO?

4. Which units are trained to provide security and/or force projection in the AO?

6. Identify the leadership of military units that could provide security in the AO.

7. What are the attitudes of military leaders towards the Constitution?

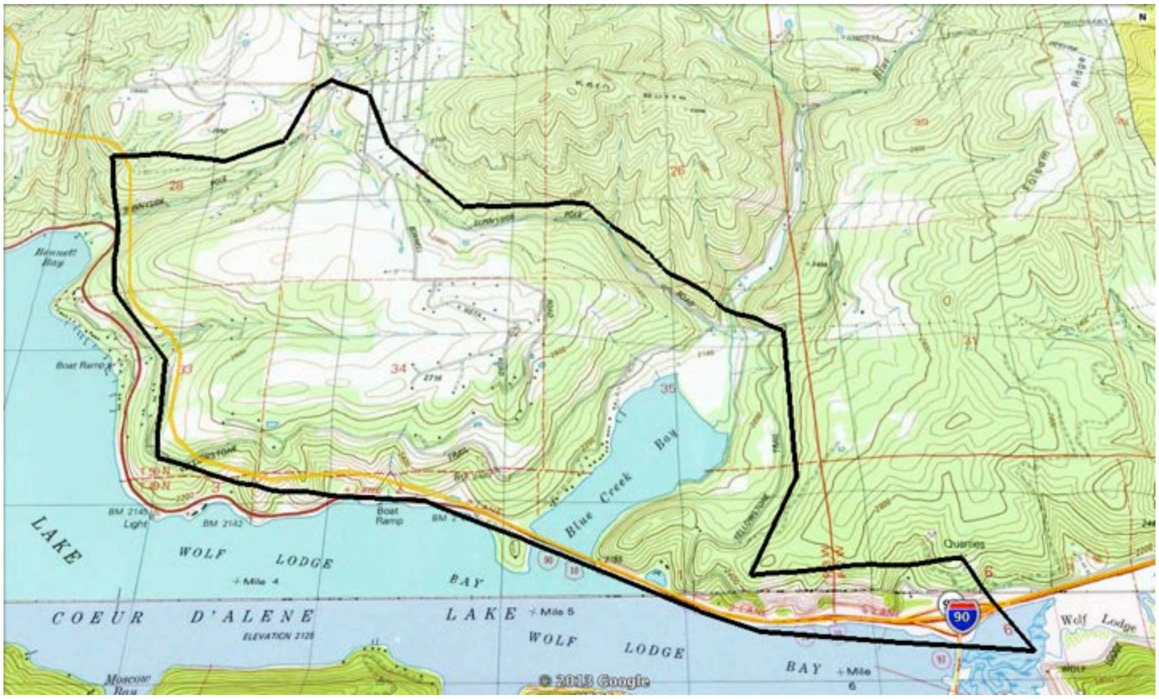
8. What is the strength and disposition of unorganized militia units in the AO?

9. What are the attitudes of the populace towards military forces in the AO?

10. What are the attitudes of the local government towards military forces in the AO?

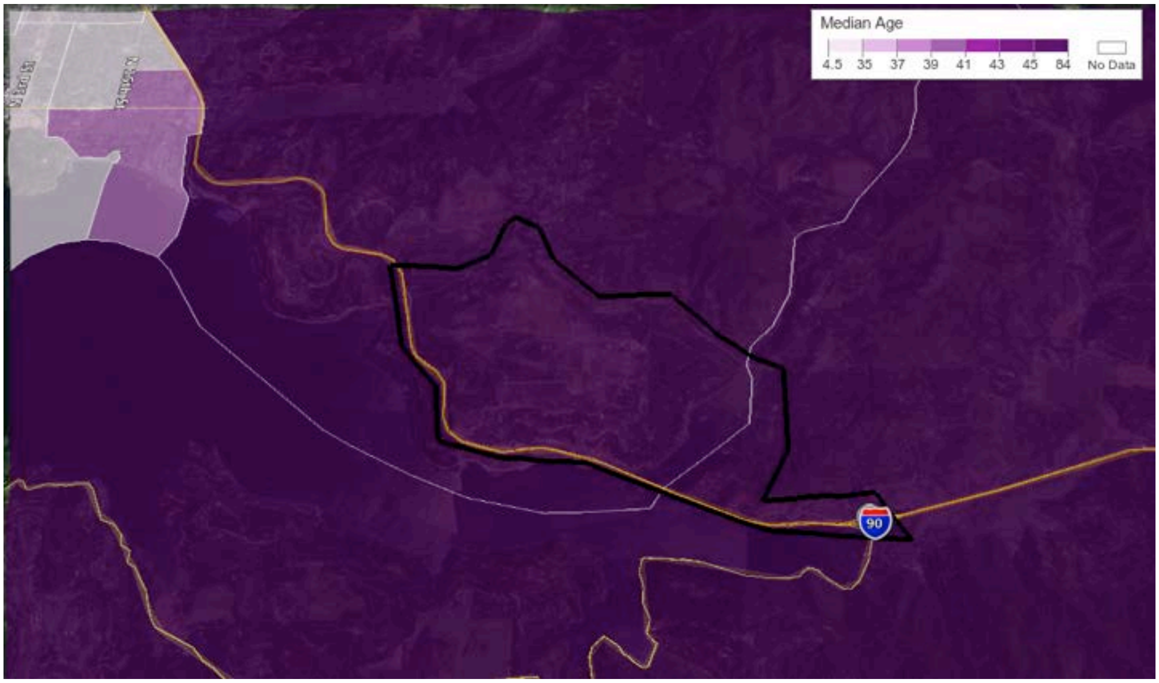
MAPS

Terrain

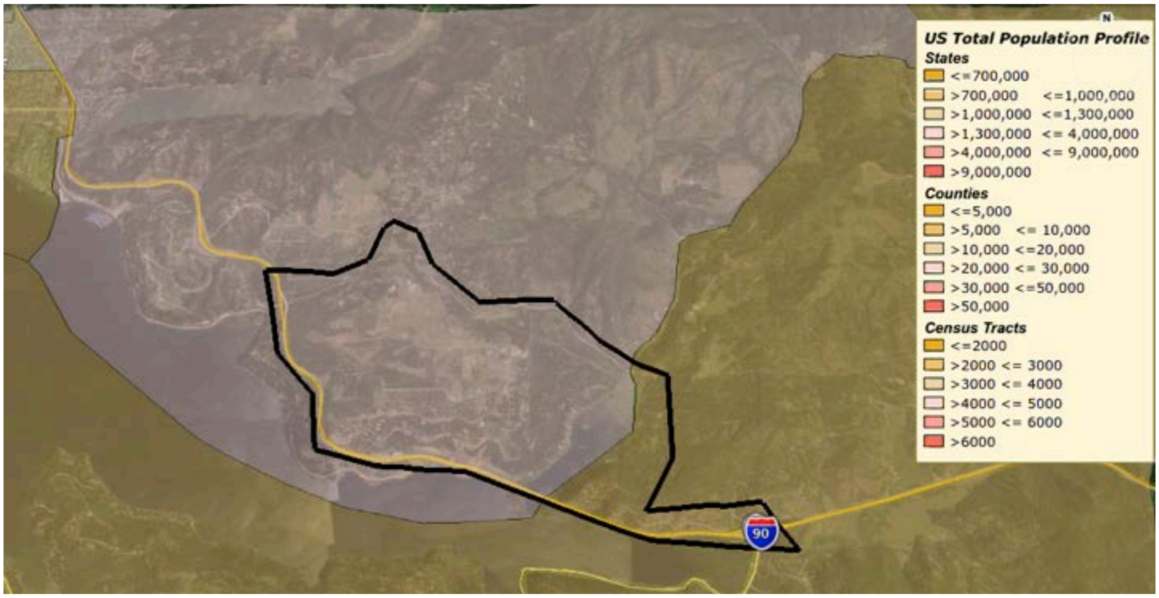


(Include your IPC Map Overlays here.)

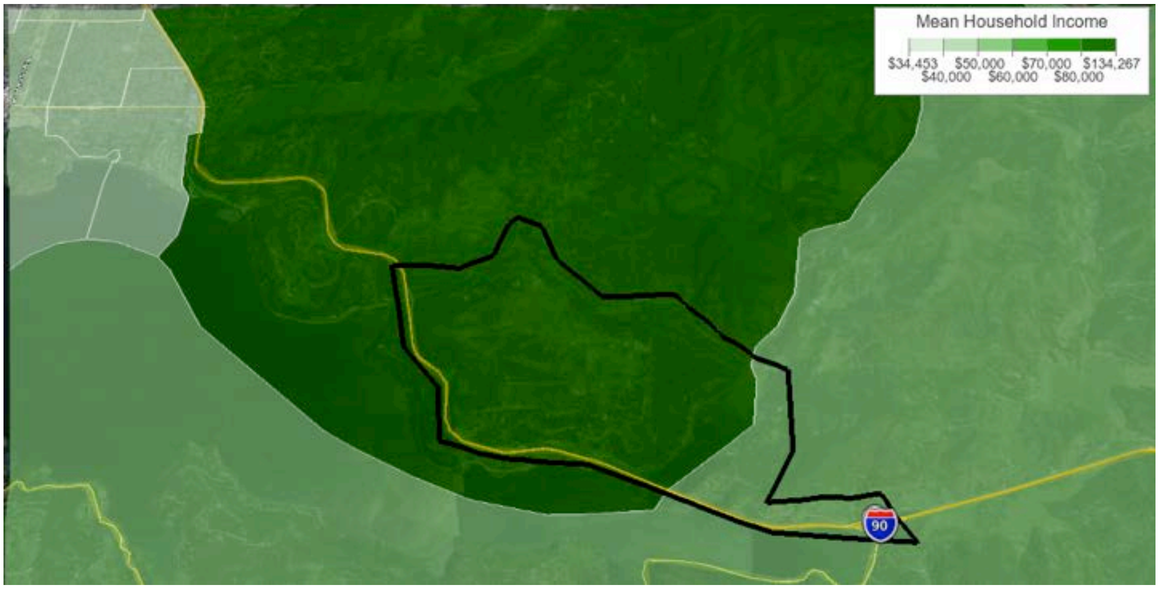
Median Age



Population Density

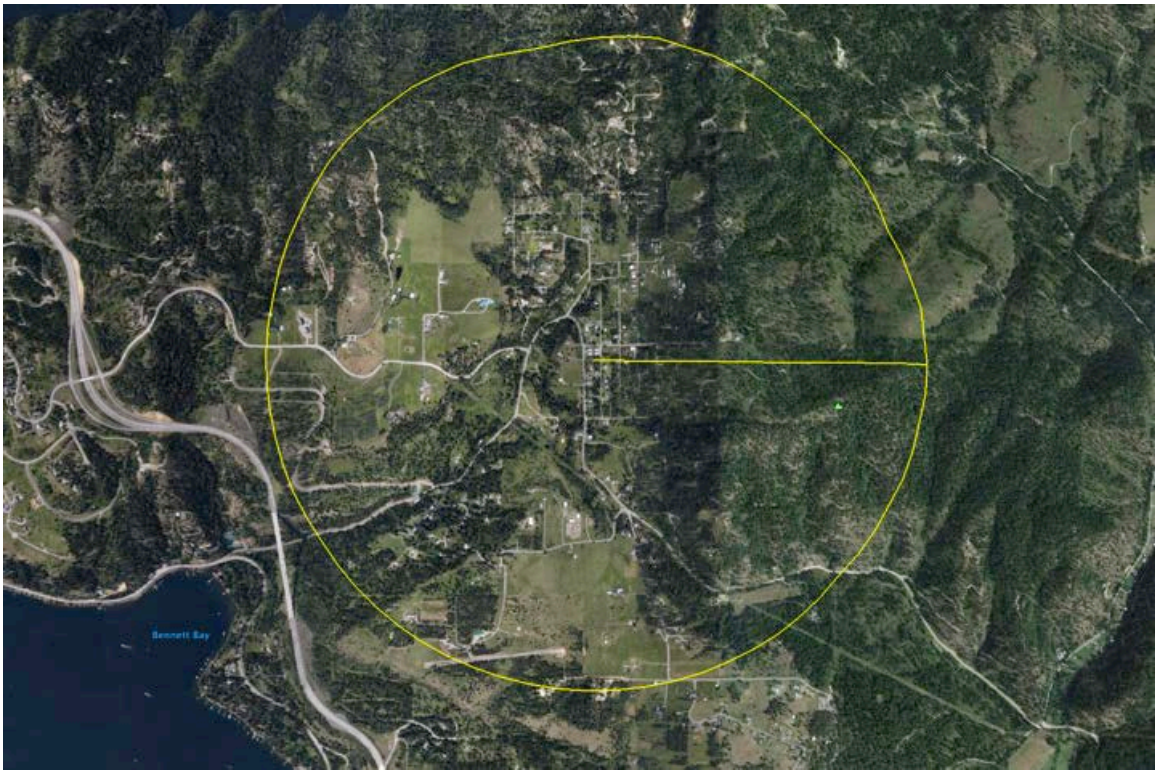


Household Income

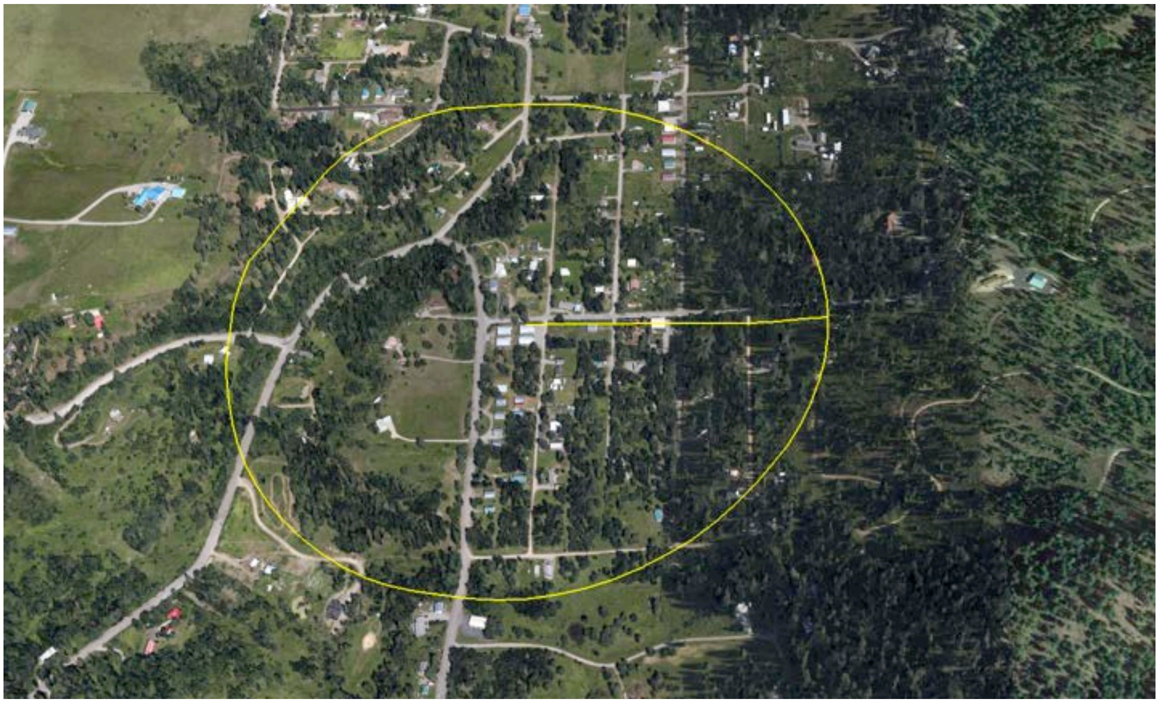


(INCLUDE ANY OTHER MAPS THAT ARE RELEVANT TO YOUR AO/AI.)

1 Mile Radius



¼ Mile Radius



METT-TC ANALYSIS

MISSION.

The Neighborhood Security Team will secure, protect and defend the community from conventional and irregular threats.

ENEMY.

Based on our current intelligence holdings, we expect the primary threat to be irregular. Those irregular threats will likely include common individual criminals, and the possibility of gangs and/or roving looters. Early warning of irregular threat activity may be possible through news stations (television and radio) and through ham band contact from others within Kootenai County. The possibility of a conventional threat is diminished, however, mobilization of Army reserve/ national guard units is possible. A secondary conventional threat could include state law enforcement agencies. Their potential missions could range from providing security during an emergency to targeting 'extremist elements' and military members throughout the region. We would expect those units to be based locally and likely receive support or direction from regime agencies.

TERRAIN & WEATHER.

Our AO's terrain is conducive to defense, however, our position off a major primary route could make defense more vulnerable. The terrain includes hills that separate the valley from outside areas, and will make ingress moderately difficult but not impossible. The only line of sight into the valley is from the surrounding ridges.

Weather from October to March can be unfavorable for enemy mobility, with the exception to air assets. In the absence of equipment to maintain roads, the accumulation of snow and ice will make road travel difficult, and passes within the region potentially impassible.

TROOPS & SUPPORT.

There are indigenous defense forces, namely a local militia, in the area. We have favorable relationships with local residents and will likely receive considerable support throughout our AO.

TIME.

Our ability to be self-sustainable within the AO is favorable and improving. We estimate that we could be supplied for up to 12 months of heavy operations, and 18-24 months of low intensity operations.

CIVIL CONSIDERATIONS.

Local governance is favorable towards the defense of traditional American values and the Constitution. There are, however, numerous local politicians and organization who will likely seek to disrupt pro-FREEFOR activities. Local news media, as a whole, cannot be counted upon to provide pro-Constitution or pro-FREEFOR coverage. There are stations more amenable to spinning positive stories about local defense forces, while others would easily provide pro-regime influence. Based on the threat, our ability to hold critical infrastructure within our AO is favorable. Our ability to hold critical infrastructure within the AI is questionable, unless we develop similar groups throughout the region.

Appendix B - Intelligence Requirements

Physical Terrain

1. What is the physical terrain that affects my area?

2. How does the physical terrain affect my area?

3. What physical terrain is the most likely to change?

4. What man-made obstacles will affect my area?

5. What seasonal climate factors affect my area?

6. What electrical infrastructure affects my area?

7. What hydrological features affect my area?

9. What are the primary transportation routes in my area?

10. What are the secondary transportation routes in my area?

Human Terrain

1. What is the population density in my area?

2. Identify the areas of homogenous race, ethnicity, culture, and religion.

3. What is the socioeconomic breakdown in my area?

4. What are the crime patterns and high-crime sections in my area?

5. Identify the civic and social organizations in the area.

6. What media outlets affect my area?

7. Which groups or sub-groups are most aligned with our goals?

8. Which groups or sub-groups are least aligned with our goals?

9. Which groups or sub-groups will likely have a disposition towards violence during an emergency?

10. Which groups or sub-groups have the most in common with other groups or sub-groups?

11. Who are the leaders or individuals who hold influence over each group or sub-group?

Political

1. Who is the political leadership in my county/AO?

2. Who are the civil servants who wield political influence?

3. Who are the civil servants who wield administrative influence?

4. Who are the known pro-Constitution politicians and civil servants?

5. Who are the known statist/anti-Constitution politicians and civil servants?

6. What is the organizational structure of county governance?

7. What are the perceived strengths of the county government?

8. What are the perceived weaknesses of the county government?

9. How effective at maintaining security will the county government during an emergency?

10. What is the overall quality of governance of the county government?

11. Where are the county and local government offices and buildings?

Economic

1. Who are the major job providers in the county?

2. What industries operate in the county?

3. What are the service industries dependent on industrial production?

4. What is the unemployment in the county?

5.What are the trends or indicators regarding economic stability?

6. What factors threaten future economic stability?

7. What is the distribution of socioeconomic levels?

8. What are the dual-use manufacturing companies?

9. Where are the manufacturing plants?

10. Which economic infrastructures are directly related to the political infrastructure?

Security

1. Identify the state and local law enforcement organizations in the AO.

2. Identify the federal law enforcement organizations in the AO.

3. Identify the organizational structure of law enforcement organizations in the AO.

4. Identify the leadership of law enforcement organizations in the AO.

5. What is the strength and disposition of law enforcement organizations in the AO?

6. What are the attitudes of law enforcement leadership towards the Constitution/Liberty in the AO?

7. Which law enforcement officers are pro-Statist/anti-Bill of Rights?

8. Identify the private security apparatus in the AO.

9. What is the quality of security in the AO?

10. What is the quality of justice in the AO?

11. How does the populace view law enforcement in the AO?

Defense

1. What military installations are in the AO?

2. What is the strength and disposition of active duty forces in the AO?

3. What is the strength and disposition of Reserve/National Guard forces in the AO?

4. What are the capabilities of all federal and state military forces in the AO?

4. Which units are trained to provide security and/or force projection in the AO?

6. Identify the leadership of military units that could provide security in the AO.

7. What are the attitudes of military leaders towards the Constitution?

8. What is the strength and disposition of unorganized militia units in the AO?

9. What are the attitudes of the populace towards military forces in the AO?

10. What are the attitudes of the local government towards military forces in the AO?

Appendix C - Developing a Community Security Strategy

If there's one maxim of Intelligence, it's that *Intelligence Drives the Fight*. Without Intelligence, organizations are essentially blind to the battlefield, battlefield conditions, threats, civilians, infrastructure — all the things that make conflict so dynamic. It's our job in Intelligence, therefore, to be the eyes and ears that inform our command or leadership. But if Intelligence drives the fight, then it must be asked: *What drives Intelligence?*

Answer: the mission drives Intelligence. In the military, foreign and national policies drive the mission. (I would be remiss if I didn't point out that foreign and national policy should be decided on the basis of Intelligence, not necessarily ideology.) It's important to understand that everything we do in Intelligence goes to support mission.

I often ask my students about their mission. The routine, almost rote answer I get is, "To survive and protect my family." Chances are good that your simple mission statement is about the same. I then ask about the strategy; *How are you going to accomplish that?* "By storing up food, water, and other supplies to survive, and getting guns and ammo to protect my home and family." It's important to note that a mission statement without a sound strategy is nothing more than a wish or desire. Storing up "stuff" and purchasing guns and ammo are definitely the first step in being prepared; however, those alone will not necessarily guarantee survival or safety. That's why I'm including an introduction to the Four D's. They fall under mission planning, which is typically a chief task for Operations; the Intelligence section merely provides support.

The Four D's is a memnonic that describes the goals of counterinsurgency. What we're likely to face in post-SHTF community security is fragmented or tribalistic groups that make up a larger community or area. The more homogenous your community is, the less fragmented it may be; however, these potential fragments may be broken down along race, ethnicity, religion, sect, family or kin, socio-economic status, or a host of other fault lines.

In other words, there may well be small groups in our communities with competing interests, who have goals that are diametrically opposed to ours. The classic *haves-versus-the- have-nots* type of class warfare is a prime example; ethnic conflict is another that prioritizes special interests ahead of security and stability. Between criminal elements and special interest groups, not to mention the egos of seemingly well-meaning people, you very well may have your hands full with these human and interpersonal dynamics of your community. These people are, at the most basic level, insurgents; they are security vampires, drinking the blood of your community in order to satisfy themselves, and they pose a risk to community stability.

The key to counterinsurgency is maximizing the efforts and benefits of the human terrain; i.e. your neighbors and community members. These people may be of a different ethnicity, religion or class, but that in and of itself is immaterial to community security. What we really need, just as much as the supplies that sustain us, is a strategy to gain cooperation and work with these people, thereby increasing our Intelligence collection capabilities, manpower and authority. Most humans want to live in peace and prosperity. If the immediate goal of our neighbors is survival, and secondary goals are peace and security, then we all have something in common. If we can help them achieve their goals, then they're much more likely to help us achieve ours. We can achieve them together with a little planning, networking and forethought; but gaining their cooperation to these ends should be among our top priorities and may be among the most difficult.

We may find ourselves in a situation where our supplies fail to gain the cooperation of any of these people towards the ends of security because we have such limited resources. The use of firearms or our tendencies to use them coercively may even make community security matters worse. In order to ensure community security, we have to focus on the key word, which is *community*. We might alternatively called it *tribe*.

What follows is what we do with our tribe; it's the cumulative security strategy that we essentially have to sell to them and the one they must buy. Competing groups may be selling different solutions; perhaps ones that result in injustice and insecurity. The Four D's are how we can deal with these threats. Wise readers will seriously consider how each of these can fit into their security strategy.

Defend

The first of the Four D's is Defend. This is the absolute imperative for survival: we must defend ourselves and what we already have. That includes our lives, followed by our livelihoods. You are a non-renewable resource. If you're reading this book, then you have friends or family - *tribe* - to whom you are irreplaceable. And your neighbors are irreplaceable to their families as well. This is very first thing that we all have in common, therefore, it's a very good place to start when confronting our neighbors during an SHTF scenario.

Whether you're going to set up check points or otherwise monitor the traffic coming in and out of your community, your (probably unstated) mission is to defend the community. We're going to deter attacks against us by either being or appearing to be a hard target. Your AO, your battlespace, your home and community belong to you. Dominating your battlespace is your primary Defend mission. I recommend two books: *The Reluctant Partisan*, Volume I by John Mosby, and *A Failure of Civility* by Lawson and Garand.

Diminish

Threats in the community will have or will find support from somewhere; an individual or an ethnic, religious, or socio-economic group. Our adversaries have support somewhere, so it's our job, in providing security and bringing stability to the community, to identify and remove this support to our threats.

In Afghanistan, for instance, the Taliban rob or tax the populace for funds, and find moral and materiel support from their ideological peers. The question, then, is how do we diminish support for the Taliban? The presence of U.S. soldiers may diminish the Taliban's ability to coerce tax collection from villages, but soldiers can't be everywhere at once. Then it becomes a game of cat and mouse. So Army's solution is to build up a competent, local police force to deter the Taliban, and empower the villages to defend themselves. Great plan in theory.

The mythical Leroy Jenkins Gang robs and loots, and gives part of that loot back to their community. Leroy Jenkins and his gang, therefore, now find support among this community. As long as Leroy Jenkins maintains this support, he'll have increased Intelligence collection and places to hide. Through Intelligence, we find out that the only reason the community support Jenkins is because he provides for their security. It may not be easy, maybe not even possible for us, but we have to figure out a way to wrestle that support away from the Leroy Jenkins Gang. How might it be done?

If Leroy Jenkins robs homes in a wealthy community in order to finance his survival, then we may have to defend that community; otherwise, he'll continue financing himself, he may grow larger and more dangerous, and he may eventually begin attacking our community. If we can end the robberies and looting, threaten his survival and diminish his ability to operate; if we can, in essence, convince him that his goals are unachievable, then he may stop trying long enough for us to gain the initiative and remove him from the area. If the Leroy Jenkins and his gang are encouraged to plunder by a former civic figure, then we influence (or remove) that former civic figure.

In any case, we find the enabler of bad behavior and we remove it. In the Diminish mission, we seek the end of anything that enables our adversary to conduct operations against us. And you will not find their facilitation and logistical nodes unless you have an active and robust intelligence element.

Deny

What are U.S. operations in Yemen, across the Middle East, North Africa and Wouthwest Asia designed to do? Deny safe haven to al-Qaeda and their affiliates. Let's say that you're in Iraq, and your Forward Operating Base (FOB) is under the constant deluge of mortars, rockets and improvised artillery rounds. Your attackers have their own Area of Operations where they're active, and they have bed down locations where they rest and sleep. When those al-Qaeda fighters get done launching rockets at you, they go back home. Therefore we need to find their homes – their bed down locations – and deny them a safe haven. They have hide outs. They have places where they feel safe. Therefore our job is to start kicking in doors and making them feel very unsafe. They need to know that if they're going to attack us, then they're going to pay for it.

Similarly, if Leroy Jenkins is going to come into our community to rape and pillage — any community to rape and pillage — then he ought to know that he won't be safe in his safe place. As long as he remains a threat to my community, I'm going to deny them safe haven because that's where he builds and plans. The Deny mission is all about disrupting our adversary's down time in the places he feels the safest. We find those areas and we deny them those safe havens. *You will not find those areas unless you* *have an active and robust intelligence element.*

Defeat

If we're doing the first three things (defending, diminishing and denying) then we should be well on our way to defeating our adversary. If we're staying secure and choking off the supplies and safety of our adversary, then we will eventually cause his defeat. The more kinetic we are in targeting our adversary's leadership and facilitation, the more quickly we will defeat him. The Defeat mission is offensive: separating the proverbial head from the body (targeting leadership) while removing the legs and arms (logistics and operations, respectively). *You will not defeat your adversary unless you have an active and robust intelligence element.*

Seven Lines of Effort for a Community Security Strategy

One threat that many preppers are likely to face post-SHTF is that of the criminal insurgent, or groups of criminals, gangs, mobs, and looters. This criminal threat will manifest for a few reasons; namely out of the criminal's need to survive, the availability of unprepared, soft targets, and the community's inability to enforce laws in a Without Rule of Law scenario.

"Learn all you can about your Ashraf and Bedu. Get to know their families, clans and tribes, friends and enemies, wells, hills and roads." – T. E. Lawrence

One question that ought to be answered is, "How long after SHTF, and under what conditions, will the criminal threat become active in my area?" That's a question best answered by the intelligence element. This article assumes that many communities will eventually encounter the conditions that support a criminal insurgent threat, and that the best way to fight against the criminal insurgent threat is through Counterinsurgency (COIN). The criminal insurgent defined is the individual, or group of individuals, who are not only actively engaging in common criminality, but also actively working against the re-establishment of the rule of law. In other words, it's in the criminal insurgent's best interest to work against any system that attempts to bring security back to the area.

COIN is and has always been, even before being named Counterinsurgency, about the people. There are wars that involve tanks and planes fighting for domination, and then there are wars of the people. In COIN, the populace is the center of attention; every plan is viewed through the lens of the populace, and every action is put through the paces of the populace. In short, as the populace goes, so goes the war.

The worst case scenario is that the criminal insurgent receives support from any segment of the populace. Let's look at Ferguson, Missouri briefly. Are there members of that community who don't support the rioters? Yes. But are there members of that community who like the police and perceived injustice less? Are there members of that community who believe, as much as they may be against it, that violent protests are the only way to effect change? Yes, there are, which is why those rioters are finding cover from the protestors and the community. If there wasn't a significant part of the population who supported violent protests, then there would be very little violence and it wouldn't last very long. Where there's smoke, there's fire, as the saying goes; and in this case, there is some level of support for the activities that go on there.

When considering a COIN plan for your community, first ask yourself, "What does this community want? What will this community want in a post-SHTF scenario?" To be honest, you may have a segment of the population who will tolerate criminality as long as it benefits them. As long as they benefit, they will tolerate it, and you may even find that they begin actively supporting that criminality if it helps them achieve their goals, i.e., survival.

To start COIN planning, we need to look at the seven lines of effort (slightly modified from its traditional form in FM 3-24.2 Tactics in COIN):

1. Establish Local Security – What will your community want? They'll want what nearly all humans want: to be secure without the threat of violence against them and their family. If the criminal insurgent gives that to the populace, then the populace will find a very good reason to support the criminal insurgent. It's therefore incumbent on you to be prepared before the SHTF and be ready to step in to provide this fundamental service to your community. If you can bring and/or maintain security without losing the trust of the people, then you will be successful. Lose the trust of the people, though, by having your volunteers loot, rape, or plunder, and the populace may seek, or form, a viable alternative.

2. Establish Local 'Control' – By control, I mean positive control of the situation. Bringing security must be the first step, but security is not governance. And I'm not talking about taxes or legislation, here. Establishing local control means establishing legitimacy by forming a judicial system, enforcing Constitutional laws, and generally protecting the citizenry against internal and external threats — the very basic tenets of limited government. Ask yourself, To whom will this community lend their support, and why? Answer that question, and you'll be well on your way to establishing local control. Your community may support warlordism or the law of the jungle. I'm sorry if that's the case, but it's probably time to move if you find yourself in that situation. For all others, you can prevent warlordism and 'might makes right' by making these plans beforehand.

3. Support for Local Security – Once you've provided security for the community, are enforcing laws, and generally keeping the peace, then you'll need to continue to keep the support for your efforts. That means doing everything above board and allowing the populace to have some skin in the game. It also means training up at least a semi-professional security staff who are effective at solving problems the least intrusively (to the populace) as possible and who make good decisions.

4. Support for Governance – How will you build support for local governance? If things

get bad enough, building support for governance is going to be a huge problem for a lot of people. How do you get the average citizen to "buy-in" to your plan? Starting at the community-level, you could simply form an agreement that all disputes will be taken up by a third party, like a judicial system. However you decide to solve problems, disputes could arise that may negatively impact your legitimacy in the eyes of the populace. Maintain that support by being fair.

5. Restore Essential Services – Creature comforts come down to water and electricity. Both of these may be disrupted; in fact, it's probably in the criminal insurgent's best interest to keep essential services out of commission. So once essential services are restored, how are you going to protect and maintain them?

6. Support Economic/Infrastructure Development – Three words: Intelligence Preparation of the Community. How can you create meaningful work as soon as possible? What are the demands in your area? What goods and services can your area supply to others? Other things to consider are transportation and telecommunications. Being able to communicate easily, i.e., the restoration of phone lines, for instance, will make commerce much easier. Safe roads capable of supporting commerce is another piece of this puzzle.

7. Conduct Information Engagement – Simultaneously, we need a way to 'exploit' all the positive contributions we're making in the community. How are we going to get out this information to the public? How are we going to shame criminals and continue to turn the public's opinion against these criminal insurgents? How are we going to publicize attacks against the community and frame them in a way so that the populace will continue to turn against these threats? On the flip side, we need to keep our ears to the ground and learn how the populace feels and what they think. If they think we're doing a good job, then they'll continue their support. If they think we're doing poorly, then they may find a good reason to support someone else.

Appendix D - Military Intelligence Creed

I am a Soldier first, but an intelligence professional second to none;
With pride in my heritage, but focused on the future,
Performing the first task of an Army:
To find, know, and never lose the enemy.
With a sense of urgency and of tenacity, professional and physical fitness,
and above all, Integrity, for in truth lies victory.
Always at silent war, while ready for a shooting war,
The silent warrior of the Army team.

Appendix E - Screening Sheet

SCREENING SHEET

BIO

Last Name:
First Name:
Middle Name:
SVC/ID No:
DOB:
Unit:
Duty:
Location:
Skills:
Experience:

ASSESSMENT

Mental Condition:
Education:
Intelligence:
Cooperation: H M L
Intel Value: H M L

APPROACH:

EVENT DATA

Date:
Time:
Location:
Circumstances:
Documents:
Weapons:
Equipment:

NOTES:

SVC/ID No - Service ID Number
DOB: Date of Birth
HML: High Medium or Low; circle the corresponding level.

Appendix F - Operation Urban Charger Data

Raw Data
PIR1: What are the observed TTPs of Local, State and/or Federal Law Enforcement?
– IR1: What is the LE:Protester ratio in the AO?
– IR2: What LE vehicles are on scene?
2001L: Confirmed Air unit back over Ferguson at this time.
– IR3: What LE lethal/less lethal weapons are being used?
– IR4: What is the strength and disposition of the LE Agencies?
1927L: Early radio transmission confirmed the use of two choppers over Ferguson. "Air2 returning for fuel." (AC: Air asset. STL Metro PD has three aircraft, two rotary wing helo's and one fixed wing Cessna 172.)
2023L: Responding PD Unit: Team 231
2033L: Team 228 on Adams street
2033L: Police with helmets and riot shields (no body gear) pulling protestors out of the crowd
2034L: 3268 on site at Miramac
2036L: 52 south central, sending units. "large group moving to backpacks"

PIR2: What are the observed TTPs of the National Guard?
– IR1: What is the responding NG unit?
– IR2: What is the strength and disposition of the NG unit?
1900L: (T-90 minutes before the announcement), National Guard units began to forward stage. (AC: This is an example of an indicator.) Locations included fire stations, electrical substations, and static strategic posts.
1900L: "Arrived at Fire Station, just unloaded our troops," was transmitted over the local police frequency.
1900L: National Guard command post/tactical operations center (TOC) was situated at the Target on West Flourissant. Observed call signs included Tang1, Tango2, Tango5 and Warfighter33. (AC: Warfighter33 is the Call Sign for the NG Command Element.)
1921L: "Tango 5 enroute back to base with three (pax) on board." (AC: 'Pax' is a code word for personnel.)
1927L: National Guard unit at Galleria Mall, thin skinned HMV, 3 Guardsmen visible.
1931L: 2-4 man NG elements posted at substations and firestations, all sound to be static posts to stop damage. Unarmored humvees observed so far, but some elements appear to be dropped off without transport.
1950L: National Guard are making secured pickups of personnel and bringing them back to the TOC. (AC: Unclear as to who.)
1956L: "Tango 2, Tango 3 made it to St Louis Justice Center, on station now."
1957L: "Tango 5 arrive back at base with 3 packs." (AC: Three passengers.)
2003L: Multiple new units coming online performing radio checks.
2004L: At least on new Guard unit "Regulator____" and a Medic Unit
2019L: Tow truck was trying to make entry into secured area and NG and Ferg PD called

to check if it had been requested. They denied request.
2020L: Defender27, new unit on comms.
2021L: NG unit also using cell phones to communicate.
2022L: Tango 2 on base with 2 packs.
2024L: Warfighter11, new unit on comms.
2026L: "unit on station at verdue (spelling) shopping center"
2027L: Castle1 new unit. Medic902 new unit.
2051L: Squad 238 being advised to move due to shots fired.
– IR3: What NG vehicles are present in the AO?
1927L: National Guard unit at Galleria Mall, thin skinned HMV, 3 Guardsmen visible.
1940L: Armored HMMV with turret mount located outside court building in St Louis proper (AC: NFI on weapon system. Based on current TTPs, likely a M240B or M249.) No weapon mounted in the turret * in Ferguson.

– IR4: What LE lethal/less lethal weapons are being used?
1940L: Armored HMMV with turret mount located outside court building in St Louis proper (AC: NFI on weapon system. Based on current TTPs, likely a M240B or M249.)

PIR3: What are the observed TTPs of the protestors/rioters?
– IR1: How are the protestors/rioters coordinating command and control?
– IR2: How are the protestors/rioters communicating?
– IR3: What weapons/improvised weapons are being used in the AO?
1922L: Ferguson police department is reporting a black male with a long gun (NFI) at the Little Caesar's showing off for the crowd.
1950L: Armed robbery being reported at the corner of Kingman Dr and MLK Blvd. 2 black males, fled in vehicle one armed with handgun (NFI.)
2037L: Lancer occupied by Black male with grey hoody throwing ammo at police line
2037L: Shots fired! 7343 Jennwood (sp)_
2037L: Multiple shoots fired calls now
2038L: 4659 Mattis Rd Explosion reported
2039L: Windows broken out by protestors on S. Florrsent
2050L: Squad 238 at Florissant and Paul have had several shots discharged at their location.
2054L: Shots fired were from Harrison (st/rd).
– IR4: What is the strength and disposition of the rioters?
1924L: North Florissant Rd shut off by protestors. Using persons and vehicles.
1949L: Crowd estimated 350+ outside Ferguson PD
2032L: Large crowd moving down Adams.

PART 2 ———— 2045L +

Front line officers at pd reporting objects being thrown at them

Com unit is separate from Command post. They just reported looting at 145 S Fl. At Boost mobile store

White car and SUV coming into

238 relocate
Ordered to relocate per command post, shots from a block away
1 block NW Florrsent and Paul
238 maintaining post

Car 200 heading toward Ferguson PD

Shots fired near post office

All 200's teams forming skirmish line and moving North

shots fired near 215 across from ferguson PD
tactical A + B responding to 215 location across from PD

200 is getting rocks thrown at it requesting back up tactical
240 going to 200, tactical on scene at PD

marked county sheriff vehicle on fire
9:00 PM
shots fired at pd

200 sounds like their position is going south

9:03 PM
Second Precint on Emergency status

241, 242, 243 out of Ferguson PD

Family Dollar being looted something and parker?

9:06 PM
Bellfont and PArker

9:08 PM
Air 4 helo down to 15 min of gas

9:11 PM
car 200 has several prisoners requesting transport

1032 s. florrsent BP looting and “destroyed”

Looters next to McDs w floorsent and furgeson 9;12

Gas in front of PD 9:14

three police APC in wedge formation driving down Florissant in attempt to push protestors down street 9:16

5 APCs pushing back, protestors moving N.

More gas N of PD 9:21
Crowd moving north and east

They are launching Tear Gas from the tops of the APC

9:23 PM
shots fired at fire dept

205, 206 207 208 are all platoons heading to its floorsent and paul

200 sounds like local command at PD, 200 series units are platoons (tac?) smaller units are adam boston, etc

Sounds like possible kidnapping on Airport road near area. Requesting Ferg PD respond

9:30 PM
Kidnapping was a women reported a van pulled up beat her husband and threw him into the van sped away

9:33 PM
LArge group looting business 2 doors north of adams on S florrsant 73 responding on foot
N of PD gas thrown canisters?

9:35 PM
Squad 236 abandoned post due to large number of protestors
409 S Florrsant fully engulfed PD car

9:36 PM
220 retreating to Solway
tac vehicle being surrounded, nobody in it

AR near or to rear of meineke

9:38 PM
AR-15

9:42 PM
220 is asking to shut down road behind them

9:44 PM
PD reporting rifle stolen from their car (219)

Looters at chambers and N floorsent at walgreens. too large for one squad

9:49 PM
3 damaged PD cars relocated to Ferg PD lot

9:51 PM
200 protesters at shop and save

9:56 PM
Air 2 cant confirm fire at Walgreens but 30 to 40 looters

9:56 PM
smoke coming from mcdonalds
9:56 PM
and strip mall next to it with metro PCS

10:01 PM
Had a report early on of a crowd near the Brewing company looks like it expanded and got violent

9:56 PM
swat team en route to paul see above
platoons there too at 9:23

10:03 PM
Tac D going to W Floorsent tollway

10:06 PM
OK, sounds like Tac D is going to I-44

10:13 PM
Code 3000 at TrU at Ferguson?

10:14 PM
requesting air unit at toys r us
10:14 PM
en route

10:14 PM
15 vehicles and 40-50 subjects at TrU

10:16 PM
crowd going from TrU to walmart. I44 blocked and lots of units going. We need units on the I44 job. Unit 321 Westfield (?) going to sonic

10:16 PM
sonic in westfalls center, 321 responding to sonic

10:17 PM
Chesterfield for 321

10:20 PM
Public Storage lot now has fire started

10:21 PM
I do not think its the same location as the Beauty salon. Small building

10:21 PM
2nd fire, molatov cocktails

10:21 PM
Off the tops of buildings

10:22 PM
Air 2 reports there is a second fire near public storage started by Molitov Cocktails thrown from a vehicle behind building.

10:23 PM
3rd fire reported

10:23 PM
Storage facility on fire and building S on fire

10:24 PM
Squad 321 secure lot at Sonic for Staging

[1] Napoleon: A Life; Andrew Roberts (2014)

[2] Lee; Douglas Southhall Freeman (1935)

[3] On Guerrilla Warfare – Mao Tse Tung

[4] Leatherneck Magazine, May 1997, "Equipping the Man… Not Manning the Equipment.

[5] Reducing Uncertainty: Intelligence Analysis and National Security. https://www.youtube.com/watch?v=CkQvRKRRcLY

[6] https://www.dmdc.osd.mil/appj/dwp/reports.do?category=reports&subCat=milActDutReg

[7] http://www.nleomf.org/facts/enforcement/

[8] Lord Cameron of Dillington, UK. http://www.dailymail.co.uk/news/article-1024833/Nine-meals-anarchy--Britain-facing-real-food-crisis.html

[9] http://www.pewresearch.org/daily-number/do-you-know-your-neighbors/

[10] http://www.macleans.ca/society/the-end-of-neighbours/

[11] National Spy Museum, Spycast, Eavesdropping in Vietnam: One Man's Experience; http://feeds.spymuseum.org/spycast/media/2012_03_28_Tom_Glenn.mp3

[12] Secrets of Signals Intelligence During the Cold War and Beyond; Matthew M. Aid, Cees Wiebes.

[13] For additional information, refer to Army Doctrinal Publication (ADP) 5-0: The Operations Process, May 2012.

[14] National Commission on Terrorism, Report to the 105th Congress, *Countering the Changing Threat of International Terrorism*, 7 June 2000.

[15] Kent, S. 1949, Strategic intelligence for American world policy, Princeton University Press, Princeton, NJ.

[16] http://www.dispositionservices.dla.mil/leso/pages/1033programfaqs.aspx

[17] Kent, S. 1949, Strategic Intelligence for American World Policy. Princeton University Press, Princeton, NJ.

[18] http://www.nytimes.com/interactive/2014/12/03/world/middleeast/chemical-weapons-iraq-pentagon-secrets.html

[19] Thinking, Fast and Slow; Daniel Kahneman

[20] http://www.brookings.edu/~/media/research/files/papers/2007/10/intelligence%20kuperwasser/10_intelligence_kuperwasser.pdf

[21] A company called Grafix manufactures acetate overlays, as well as rolls of Duralar while will fit larger maps like 11"x17" and greater.

[22] http://www.globalsecurity.org/military/agency/army/arng.htm

[23] http://www.fas.org/man/dod-101/army/unit/toe/

[24] Direct download: URL

[25] In 2013, I wrote a short security manual…

[26] Arthur S. Hulnick, Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century (Westport, CT: Praeger, 1999), 8, 40-41.

[27] https://google.com/alerts

[28] https://ifttt.com

[29] http://80legs.com

[30] https://archive.org/web/

[31] http://opensecrets.org

[32] http://raidsonline.com

[33] http://crimereports.com

[34] http://usa.com

[35] Houston, Spy the Lie (St. Martin's Griffin, 2013).

[36] https://www.paulekman.com/research/

[37] Carnegie, How to Win Friends.

[38] Hadnagy, Social Engineering.

[39] Glasser, Choice Theory.

[40] Kraft & Pressman, University of Kansas, 2012

[41] Robert Cialdini, Influence (Harper Business, 2006).

[42] Eli Ben-Hanan, Our Man in Damascus: Elie Cohn (Steimatzky House, 1969).

[43] http://http://store.usgs.gov

[44] "Free": http://www.google.com/earth/download/gep/agree.html

[45] ArcGIS Home Edition is only $100/ year. http://www.esri.com/software/arcgis/arcgis-for-home

[46] YouTube has a several good ArcGIS tutorials. This is a good one. https://www.youtube.com/watch?v=ekmyWkAP4eI

[47] https://www.census.gov/geo/maps-data/data/tiger.html

[48] https://msc.fema.gov/portal

[49] http://floodtools.com/Home.aspx

[50] http://inciweb.nwcg.gov/

[51] http://www.homepatrol.com/