Intelligence & Community Security

A Quick Start Guide to Understanding Intelligence

By Samuel Culper

FO
FORWARD
OBSERVER

Printed in the United States of America

First Printing, October 2018

CONTENTS

INTRODUCTION

Welcome to the Introduction of Intelligence and Community Security. This ebook is intended for those at all levels to become familiarized with the use of intelligence activities for community security. The first few pages will cover some basic concepts and then we'll get into a deeper dive of intelligence operations. It's my intention to have readers be familiar enough to begin teaching others about the value and utility of intelligence to improve community security.

America's trajectory is pointing towards another conflict. It's something many of us have suspected for a long time, and the question is What exactly will it look like? Perhaps a better question is Are we already in it? My answer is probably, and I'll describe what I believe could happen in the future. In short: empirical data shows that any potential domestic conflict is likely going to be driven by demographic and economic change. Amnesty and a return to liberal immigration policies are less than a decade away, and artificial intelligence, machine learning, and robotics are likely to create more job loss than jobs created. This disproportionately affects low skill, low wage workers, meaning higher youth unemployment, which is already an early warning indicator of civil unrest around the world; and amnesty and unlimited immigration is a vehicle to amass political dominance because of the voting preferences of those receiving the amnesty.

These two likely unstoppable trends are going to accelerate the adoption of identitarianism based on race (social justice) and class (economic justice) instead of civic nationality. Amnesty will overwhelmingly benefit the Democratic Party at a time when a pivot to left wing populism is perceived to be a much needed counter to the rise in right wing populism. The effects, centered on anti-capitalist, anti-American, pro-social "justice", and pro-international socialist policies, are going to permanently change the political landscape of America. If this is happens, as soon as five or ten years from now, then we should probably expect a culture war that moves from sporadic violence to routine violence, especially in regions where government is unable or unwilling to intervene.

This all sounds pretty pessimistic and, as we've seen with prognostications about financial and societal collapse (heaviest from 2007 to 2016), there's a tendency by many to overstate the conditions and shorten the timeline in anticipation of events that will likely happen much later than predicted. No one can predict the future with any certainty, but we can identify what could occur in the future, and this is one such possibility. Whether it happens in two years or twenty, very significant and persistent socio-economic conditions are a certainty, which are likely to result in some form of domestic conflict. Our next major hurdles are (1) the period between November's mid-terms and the 2020 general election, and (2) the next recession, which could rival 2008's in economic and financial terms, but with the toxic political and cultural climate of today.

With that as our starting point, the next question is Which systems will be disrupted and how will it affect our communities? We'll save that for later in this ebook, because for now we're focusing on intelligence and community security.

CHAPTER

1

A FRAMEWORK FOR UNDERSTANDING DECISION MAKING

We need a framework to understand how decisions are made, and we need to understand what's necessary for good decision-making. We can make decisions without any information, and unfortunately many people do. *Some* information may allow us to make better decisions, but ultimately we need *intelligence* to make good decisions. We need to understand our operating environment, the current and future conditions that will negatively and positively impact us, and realistic expectations of what may happen in the future. Intelligence allows us to anticipate what could happen in the future and it enables us to make better decisions about our security. Let's look at this decision-making process called the **OODA Loop** and what's required to feed it.

Let's say that you're driving up a small hill on the interstate with moderate traffic. You **Observe** brake lights ahead of you at the top of the hill. Is it a speed trap? Is there stuff in the road? Is there a wreck? We don't know, but brains jump into action as we consider a response. We immediately **Orient** ourselves to our relative speed and how near or far we are to those brake lights. Do we need to brake? Do we need to let off the accelerator a bit, or do we need to slam on the brakes and swerve off the road to avoid contributing to a massive pileup? Depending on how well we've oriented to the situation, we **Decide** on a course of action, our brains then tell our feet what to do and we **Act** on the decision. This is called the OODA Loop and it's a universal pathway for humans making decisions, from initial observation to final action.

Chances are good that if you've taken a professional tactical weapons course, your instructor has at least mentioned it in passing. U.S. Air Force Colonel John Boyd (1927-1997), who developed the concept, was a fighter pilot interested in how he could speed up the decision-making process for himself and his fellow pilots. He found that pilots who had fewer options when faced with a decision point made decisions faster than those who had a wide array of options. Additionally, he found that pilots who could more quickly observe and orient themselves to a fast-developing situation, like a dog fight, could also make faster decisions. This line of thinking is now a doctrinal part of military training because faster and better decisions are more likely to lead to successful and decisive outcomes. Understanding of the OODA Loop can also be applied to the enemy, which is why fighters seek to speed up their OODA Loops while simultaneously slowing down or disrupting the enemy's.

Now imagine that you're the head of your community security or neighborhood watch team. There's been a disaster — a hurricane or tornado, an earthquake, maybe something worse — and the power is out. Your cell phone isn't working because the cell towers in the area are also down, and now you're concerned about second- and third-order effects: namely an increase in criminality because of this widespread systems disruption, and then maybe running out of food and water, and all the things that happen during prolonged periods of emergency. In this scenario, virtually *all* systems have been disrupted. What does your OODA Loop look like?

In short, it's the exact same process as a fighter pilot's. We **O**bserve what's going on, then we **O**rient ourselves to this new information, then we **D**ecide on a course of action or how to respond, and then we **A**ct. After that action, the OODA Loop starts all over again — in fact, it never really stops. We are always observing new information, and then orienting, deciding, and acting to changing situations. The greater access we have to accurate information, the better and faster our decisions can be. The less access we have to accurate information, the more likely we are to make poor decisions. And generally whoever can complete this OODA loop the fastest is going to stay the most secure or win the most engagements.

This concept is applicable to the tactical, operational, and strategic levels of decision-making. Gun fights are an example of using the OODA on the tactical level, but organizations on the operational and strategic levels can also make deliberate use the OODA Loop. A set of tactical observations can lead to a general understanding of what's going on in the area, and observations from several areas can give us an indication of the broader region. This is how we move from the tactical to the operational and to the strategic level. Additionally, with this understanding, we can inform decision-makers who can then make better operational or strategic decisions based on the ground intelligence.

For the purposes of community security, we're actually looking at two different functions: *intelligence* and *operations*. There are those responsible for intelligence and those responsible for operations, and the two work hand in hand. In fact, you may have heard the maxim "Intelligence Drives the Fight", and that's best described through the OODA Loop.

Observe and Orient (the **OO** in OODA) is the function of intelligence. *Observing* describes intelligence gathering and *Orienting* describes intelligence analysis. We have to be good at both of those things, and in later chapters we'll talk more about what it takes to Observe and Orient well in a time of conflict. After we Observe and Orient — in our case, after we gather intelligence information and produce finished intelligence — we pass it on to decision-makers.

Decide and Act (the **DA** in OODA) is a function of operations. As intelligence people, we advise the commander or decision-makers on what the situation is, but we don't make the decisions. We support planning, but we don't plan. And there's a very good reason for this: because as the intel guys, we're called to be experts on the enemy and operating environment. We alert the commander to where the enemy is, what they're doing, and what they might do next — something we refer to as the enemy situation — but only the commander knows his troops, time, and resources well enough to make decisions and issue orders.

Hopefully we've moved beyond the understanding of just the tactical use of the OODA and into how intelligence plays a vital role in an organization, like a community security or neighborhood watch team. Without the ability to observe and orient — that is to say, without the deliberate employment of intelligence activities — your organization will have a difficult time deciding and acting on security concerns in your community. I'm reminded of my absolute favorite quote. It's by Jack Welch, former CEO of General Electric, who says, "If the rate of change on the outside exceeds the rate of change on the inside, the end is near." He's talking about a multi-billion dollar corporation adapting to both the changing needs of the customer and product development by competitors. If GE isn't planning for 10 or 20 years into the future, then they're going to fail. It's the same for community security, but on a much smaller scale. If, during an emergency, we can't keep pace with security developments — if we don't have an adequate focus on intelligence gathering about threats in the area — then the end is near. It's only a matter of how near and how painful.

CHAPTER
2

WHAT INTELLIGENCE DOES FOR US

In the previous chapter, we covered that intelligence is the bedrock of decision-making. Military leaders use intelligence to make decisions for operations. Governments use intelligence for making decisions in foreign policy. Corporations use intelligence to make decisions on how to stay competitive. Every time you check the weather, the traffic, or the local news, you are receiving intelligence so that you can make better decisions, too. Everyone uses intelligence.

Here's one important distinction that you should know going forward: there's a difference between *intelligence* and *information*.

Information is usually raw and unverified. Studies show that the first reports after mass casualty events are almost always wrong. After a bombing, a school shooting, a plane crash, or any number of other events, media outlets report to the public whatever they come across so the channel can get higher ratings. What they're passing on is not intelligence — it's just information and it's usually wrong.

Intelligence, on the other hand, is the accumulation of this information that's been triaged, corroborated, assessed for accuracy, and synthesized with other information to meet the needs of timely-decision making. This is often referred to as *finished* intelligence.

"Intelligence gathering" is really a misnomer because you can't gather intelligence, only information. Information is *gathered*, intelligence is *produced*. Our goal for community security is to gather information, but to act on intelligence.

Intelligence for community security is going to be five things:

- Timely – we need intelligence by a certain point in time to make a decision. Intelligence that arrives after the decision has been made is often useless.
- Relevant – intelligence aids decision-making. If the intelligence doesn't help a leader to make a decision, then it is often useless.
- Accurate – Intelligence is not always spot-on. The more accurate the intelligence, the better the decisions.
- Specific – Intelligence is unfortunately sometimes vague. Saying that there are "a bunch of tanks" in the area is not the same as saying there

are seven tanks in the area.

- Predictive or Actionable – Intelligence that is predictive in nature helps us make better decisions about the future. Intelligence that is actionable in nature helps us to make better decisions now.

Regardless of your role or mission, we seek out intelligence because we have blind spots. In this chapter, we're talking a little more in-depth about those blind spots, and identifying some considerations for our own intelligence needs before getting further into the weeds later this week and next.

At the heart of intelligence is the ability to reduce uncertainty about the future. If we're expecting an event that causes systems disruption — that is, if our key assumption is that the event is not a matter of *if*, but of *when* — then how can we begin to reduce uncertainty about the immediate effects of that event? How about reducing uncertainty for the second- and third-order effects of the event as well? Intelligence is the only thing in the entire world that helps us to solve the problem of uncertainty about the future.

"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

So what are some questions we might have in the aftermath of an event that disrupts systems like the distribution of food, water, fuel, electricity, and public services? Close your eyes and imagine yourself suddenly without power, without a cell phone, without access to information. What are the first questions you want answered? *Should I stay or should I go? Are the roads navigable or are they clogged with traffic? Is it safe to hit the local grocery store or CVS and stock up just in case this emergency lasts more than a few days?* What are the questions you might start to ask yourself?

Congratulations: you're already involved in the very first steps of performing the work of intelligence. You are identifying *intelligence gaps* — literally gaps in the working knowledge of our operating environment. Once you identify an intelligence gap, it's important to write it down, where it becomes an intelligence requirement. This list becomes a collection of questions or statements describing information that we need to know, but don't. Here's a short list of requirements you might consider:

- Which neighbors will be willing to cooperate with a neighborhood watch?
- Who are the known criminals in the area?
- Which individuals in the area are likely to resort to criminality in the future?
- How is local law enforcement responding to this emergency?
- What's the security situation immediately outside of our neighborhood?

These are just a handful of questions that the work of intelligence can answer for us. If you're concerned about a grid-down event or financial collapse or the Golden Horde or an EMP or some other event or threat, then some basic intelligence work should be at the top of your To Do list.

Ultimately, what intelligence brings to the table is the ability to make well-informed, time-sensitive decisions because we're bringing in a constant flow of real-time intelligence information. That's going to take some work up front to build up that capacity, so I encourage you to do the work. It's going to be worth it. In future posts, I'll describe what that process looks like.

Two Major Responsibilities

One thing that will separate you from your peers is knowledge of what intelligence tasks and responsibilities will be required during an emergency. You and your community are going to find yourselves in one of two situations:

1. You're not going to have enough information to make timely, informed decisions; or
1. You're going to have so much information that you can't keep up, and will be forced to make a decision, anyway.

If I were a betting man, my money would be on the former for many in the preparedness community, and this is after *over a decade* of a very active preparedness industry. *An entire decade* later, most individuals who considered themselves prepared may have tons of gear and equipment, but if they're lacking the ability to gather intelligence information in real-time to aid their decision-making, are they truly prepared for an emergency?

In any emergency, whether it's local or national, we have two immediate tasks where it concerns intelligence. The first responsibility is to produce **Early Warning**, and the second is to produce **Threat Intelligence**. Early Warning is advanced knowledge of a threat's intent or activities.Threat Intelligence is an understanding of the intent, capabilities, manpower, equipment, and other factors available to, or employed by, a threat.

Early Warning usually means that we have collection platforms, human and machine, in areas where early warning indicators can be observed. A long range reconnaissance team sitting in a hide site and observing the movement of enemy equipment could be one example. Signals Intelligence equipment that tracks the location of a cell phone is another. For us, we probably need to work on getting "eyes on" the entry ways of our neighborhood, at a minimum. If we expect looters or out-of-area criminals, then one of the best ways to produce early warning is to simply get beyond the boundaries of our neighborhood and scout out potential threats in the greater area. With a couple of radios and a decent vantage point, this could be a very effective way of producing early warning intelligence. There are others, which we can cover in future posts.

Threat Intelligence could come in many forms, usually as what's called an Order of Battle which details the manpower and equipment of a military unit. A police report on the members and activities of a local gang is an example of threat intelligence. Threat intelligence is usually cumulative and describes the strength, capabilities, activities, resources, and intent of a specific individual or group.

If we can take steps now to produce threat intelligence on potential threats, and develop ways that we can observe early warning indicators of these potential threats, then we can reap the benefits later. The work of intelligence is a lot like exercise; you won't be in shape for the emergency unless you get in shape now.

In the next chapter, we're going to pick back up with the difference between intelligence collection and intelligence analysis, and begin talking about why these two things are supremely relevant to community security.

CHAPTER
3

INTELLIGENCE COLLECTION & ANALYSIS

In previous chapters, we've discussed a good foundation for understanding the value and utility of intelligence for community security. We talked about the OODA Loop — the pathway for decision-making — and how intelligence is the first half of that loop: Observing and Orienting. In this chapter, we're talking about what intelligence collection and intelligence analysis actually look like for the purposes of community security.

We can't Decide and Act unless we Observe (intelligence collection) and Orient (intelligence analysis), which is why collection and analysis are so crucial for community security, emergency preparedness, warfighting, or anything in between.

We have blind spots; we have a fundamental need for real-time intelligence to support real-time decision-making, therefore, our mission requires collectors and analysts.

Traditionally, as with the military and civilian intelligence agencies, collectors and analysts are different roles. Collectors don't analyze and analysts don't collect, and there's a good reason for this. Let's think of intelligence as the process of baking a pie. Intelligence collectors are trying to collect the ingredients for the pie, while the analysts are sorting through everything that's been collected to find only the best quality ingredients. Collectors aren't that concerned with the quality of the ingredients they're finding; they job is just to collect and pass on the ingredients. Furthermore, each collector has access only to the ingredients he's collected, and doesn't know what other collectors have gathered. How can a collector, then, analyze what's best for the pie if he doesn't know what other ingredients are available? That's where the analysts come in, because they're pouring through everything that's being collected in real-time until they have everything required to bake the pie. That's how you get finished intelligence, as opposed to raw information. Collectors are reporting raw information, while the analysts are putting it together, using only the best and highest quality information, and then producing intelligence. We make decisions based on the finished intelligence.

Another way to look at this is using the previous puzzle analogy. Let's say that we're putting together a puzzle, so the analysts dump the puzzle box onto a table, sort through the available pieces, and find that some are missing. So the analysts tell the collectors what puzzle pieces are required to put together the puzzle, and then the collectors go look for the missing pieces. The collectors begin looking around the house for puzzle pieces, and give any puzzle piece they find to the analysts. Only the analyst can compare each new piece to the needs of the puzzle and determine if the puzzle can be completed.

Aside from these two analogies, there's training and specialization. Signals Intelligence (SIGINT) collectors are not Human Intelligence (HUMINT) collectors. Why? Because each of these jobs require very specific training for very specific missions. Additionally, neither SIGINT nor HUMINT collector would be good all-source analyst because he lacks the training and experience in intelligence analysis. This is also true for other professions: heart surgeons aren't brain surgeons, wide receivers aren't safeties, civil engineers aren't electrical engineers, and so on.

Unfortunately, we at the community level probably aren't going to have the luxury of having a well-staffed, well-trained, and specialized intelligence section. That means we're going to have to wear multiple hats, both of the collector and the analyst. Let's go ahead and break down what this all looks like.

First, our analyst — that's probably going to be you — is what's referred to as all-source. The all-source analyst is responsible for combining all the different sources of intelligence (called disciplines) into his analysis.

Next, our collector — that's probably going to be you, too — is responsible for gathering information from sources. There are numerous intelligence disciplines, however, for the purposes of community security, we're going to focus on four.

Open Source Intelligence (OSINT), 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 percent of all intelligence information globally comes from open sources. That's probably 90 percent or more considering the ubiquitous adoption of social media. 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, easiest to collect, and provides us with some quick wins up front, OSINT should become one of our top collection priorities.

Imagery Intelligence (IMINT) is information derived from photographs and video, and we're going to rope GEOINT into this category, as well. 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, like the attributes of physical terrain (flood plain data, for example). 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 examples of the use of HUMINT. For our purposes, we'll focus more on localized collection about local threats. Friends and family, neighbors, convenience or grocery store clerks, peace enforcement officers, and city/county officials are all high value sources of information.

Signal Intelligence (SIGINT) is derived from signals, including from communication devices like cell phones and computers. 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), U.S. military and civilian intelligence agencies (to include law enforcement 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.

Utilizing all available disciplines, sources, and methods required for the mission, the task of intelligence is ultimately to reduce uncertainty about the future. Now that we have our feet with with the understanding the decision-making process, the difference between information and intelligence, and the practical difference between collection and analysis today, the next chapter will be about putting this all together and what the entire cycle of collection, reporting, analysis, and dissemination looks like.

CHAPTER
4

THE OPERATING ENVIRONMENT & YOU

The chapter is about understanding the layers of our surroundings — something we refer to as the "operating environment". Think about your community and it's characteristics: the houses up and down the street, the people who inhabit them, the width and condition of the roads, fences or ditches, and probably a whole lot of other things. These are all characteristics and it's up to us as intelligence analysts to identify and describe how these things might impact us and our security.

There are six layers of our operating environment, and we need to account for each of them:

1. Physical Terrain
2. Human Terrain
3. Critical Infrastructure
4. Politics and Governance
5. Law Enforcement/Military/Security
6. Economic/Financial

Practically, you'll need to go though each of the six layers of your community and identify the significant characteristics. This is a critical step, especially during a local or national emergency, and specifically for community security. Failure to complete this step is like building your house on sand, except your intelligence product will be built on sand.

Threats don't exist in a vacuum. The same layers of the operating environment — mountains, roads, neighbors, police, etc. — are going to affect threats in the area, too. And unless we understand what's positively and negatively affecting area threats, we're likely going to fail to arrive at an accurate estimation of what threats will do in the future. Yesterday, we discussed that actionable or predictive intelligence is our end goal for community security, and we certainly can't produce predictive intelligence unless we understand all the factors that weigh on a threat.

The **Physical Terrain** includes traditional terrain features — mountains, hills, valleys, lakes, rivers, etc. — and manmade features like roads, houses, buildings, fences, etc. Weather is often grouped in with physical terrain, so we'll cover weather and climate patterns, as well. Understanding how these factors could influence future conditions is an intelligence task.

The **Human Terrain** includes the people, along with their attitudes, beliefs, behaviors, and customs. From a community perspective, identifying all the elements of the Human Terrain helps us to identify security partners and potential threats and foes, especially if disaster were to strike.

Critical Infrastructure includes the facilities and people who provide access to food, water, fuel, electricity, transportation, commerce, communications, and the internet; all of which are critical to the average AO.

Politics and Governance includes elected officials, political appointees, government employees, their institutions and facilities, and their political and ideological beliefs. The better we understand how local political and governance works, the better informed we can be of their potential future decisions, especially during a protracted emergency.

Law Enforcement/Military/Security includes all aspects of public and private security personnel. Police departments, sheriffs' offices, National Guard and Reserve components of the military, and private security corporations all take part in security and emergency operations. Understanding these organizations or units, their personnel, and their capabilities goes a long way in staying informed of what they're likely to do in the future.

And finally, the **Economic and Financial** drivers of a community matter, especially if these systems are disrupted. Disruptions to economic and financial factors have very significant second- and third-order consequences, and understanding how these factors will affect the community is critical.

Once we identify the significant characteristics in each of these layers, our next job is to describe how they will affect us. How will terrain and weather affect our community security operations? Which roads flood? Which people in our community will help out with a neighborhood watch? Which people are going to be burden or try to impede our efforts? How will local governance respond to an emergency, and how could they worsen the situation? What might that look like? How can we expect law enforcement to respond? What will their presence look like? There are all sorts of factors we need to consider.

Two question you might ask: "How large of an area should I be looking at, when considering these layers, and how large is my operating environment?"

We need boundaries for intelligence collection. We need to be able to tell our neighborhood watch or community security group how far away is too far. At what point do potential threats become irrelevant? A mile away? Two miles away? 10 or 20 miles away?

In the Army, we had Intelligence Preparation of the Battlefield, or IPB. There's an IPB product for every contingency operation in the world, and before an operation is planned, military commanders and their staff are looking over the latest intelligence contained in the IPB. I've taken that IPB process and modified into Intelligence Preparation of the Community; something we refer to as IPC. Instead of dealing with tanks on a battlefield, we're dealing with people in a community. The benefit of using a methodical and systematic process like this is that we have a framework for everything we do.

To answer those two questions above, we want to identify some boundaries that we call the Area of Operations and the Area of Interest.

Area of Operations (AO) is the he area around our home or neighborhood where we expect to conduct security operations. For most, this is a small area; it's the boundary of your property or perhaps just beyond your property. Others might determine their AO by the range of their rifle scope. If you don't foresee yourself venturing farther than a mile from your home, then your AO should be less than a mile radius. If, during an emergency, you don't see yourself venturing more than 100 yards from your home, then your AO should be less than a 100 yard radius.

The **Area of Interest** (AI) is a boundary around our AO that we'd like to monitor. We don't expect to operate here, but we may still be interested in what happens here. For instance, my AO doesn't include the nearest police or fire station, nor does it include the nearest school or Walmart; however, I'm still very interested in what happens at these locations. The AI is the area that we're going to monitor because what occurs there could indirectly affect us.

This is an important step because it's going to focus our planning and intelligence gathering within these specific boundaries. Threats are a game of proximity; the father away they are, the less relevant they are to us. But at some point, threats become very relevant because they enter our AI or AO. That's why we need to identify these boundaries. In the next chapter, we'll discuss threats and how they fit into the operating environment.

CHAPTER
5

FINAL THOUGHTS ON THREAT INTELLIGENCE

In the last chapter, we talked about the Operating Environment that is your community, and the boundaries that help our intelligence efforts focus on where and what to collect. In the final chapter of this ebook, I'm leaving you with some final thoughts on threat intelligence.

Now that we have a good grip on some basics of intelligence and the area in which threats exist, let's start to break down the threat environment. The are four categories of potential threats we're concerned about. They are:

- 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. For instance, U.S. Forces in Iraq and Afghanistan represented a *conventional* threat to insurgent groups there.

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. Insurgents posed an *irregular* threat to U.S. Forces in Iraq and Afghanistan.

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 result in conventional and irregular threats.

Think about your community and what types of threats may exist, either potential or active. Snowstorms and tornadoes are examples of potential threats, thieves and gang members pose active threats.

Get out a sheet of paper and think through your community; imagine that you are at the beginning of a national emergency that has local effects, and write down all the active and potential threats that you may face. Keep this list and discuss it with your neighborhood watch, community security team, or preparedness group. Use a group approach to ensuring that we have as complete a list as is realistic.

The next step is to audit this list and determine the actual risk of each threat. Specifically, we want to look at the threat's likelihood of threatening us and the impact if we're threatened. Sort the items on your list according to HIGH and LOW likelihood, and HIGH and LOW impact.

For instance, looting in your neighborhood after a natural disaster may be a HIGH likelihood and HIGH impact threat. A nuclear meltdown or a cyber attack that causes bank holidays are examples of LOW likelihood but HIGH impact threats.

Ultimately, we want to determine what our HIGH/HIGH threats are because they're the most likely to affect us and impose the greatest impact. Once you complete this step, I highly recommend you review the next page and begin incorporating your previous thoughts into a cumulative approach to intelligence and community security. Bring this all together and use it to aid in security planning for the next emergency.

If you treat these exercises seriously and get this far either by yourself or with your group, you're going to be head and shoulders over your peers, and in a good position to teach others about this approach to threat intelligence and community security.

Major Learning Points:

- The OODA Loop
- Early Warning
- Threat Intelligence
- Open Source Intelligence (OSINT)
- Imagery Intelligence (IMINT)
- Signals Intelligence (SIGINT)
- Human Intelligence (HUMINT)
- Six Layers of the Operating Environment
- Four Types of Threats

If you feel confident that you understand each of these Learning Points, then you're probably ready to begin the next steps...

Ready to get started?

Join the Forward Observer Schoolhouse and continue your journey with our online training on each of the topics and a lot more.

Get Started