Chapter 5 Intelligence & Red Teaming

This Chapter will introduce the basic concepts in intelligence and build upon these concepts to explore their role in attack/defend scenarios.

Student learning objectives. Upon completion of this chapter, students should be able to:

- Identify, describe, and explain the intelligence cycle.
- Identify common problems in intelligence data collection.
- Distinguish between reputation, reliability, and quality of intelligence sources.
- Describe the types of sources for intelligence data.
- Identify distinct types of open sources.
- Describe how open sources can be used to develop intelligence assessments.
- Describe the concept of attack/defend scenarios in intelligence requirements terms.
- Develop attack/defend scenarios for UAS.

Basic Concepts in Intelligence

The word intelligence can have several meanings. In one instance, it is an estimate of how capably a person can reason and think. In another, it refers to the data that has been collected for purposes of divining purpose, capability, or meaning. In yet another, it refers to the process by which information is collected and processed. In this chapter, intelligence refers to processes by which intelligence data are collected, processed, and analyzed.

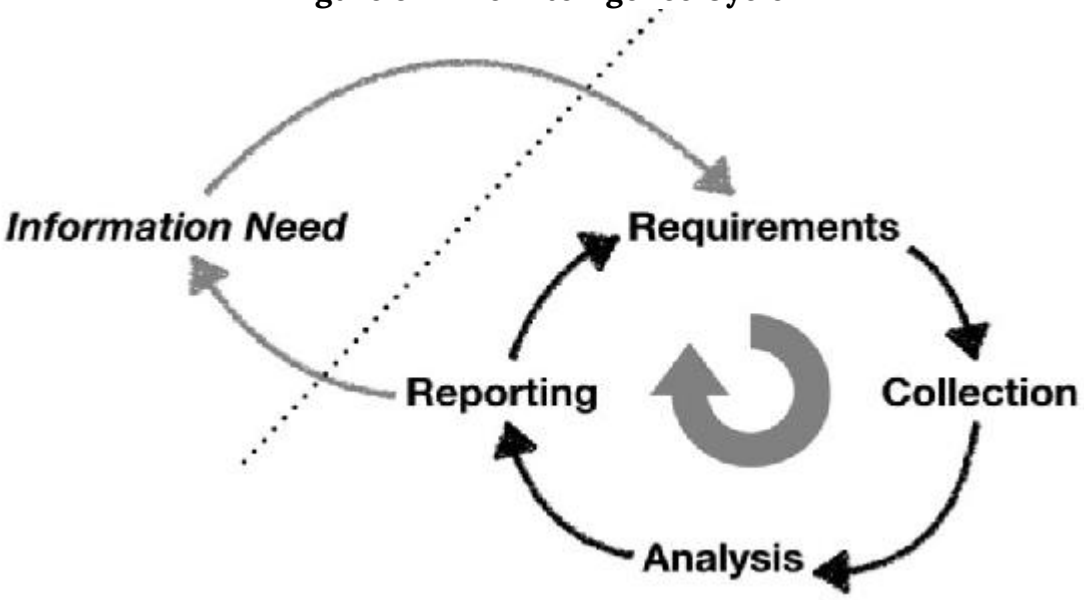
The fundamental reason for having an intelligence process is to collect and evaluate information that informs personnel about the operating environment. Governments have intelligence functions to make better informed decisions. Businesses have intelligence functions to be more effective and competitive. This is nothing new; intelligence functions are as old as mankind itself. As expected, they have grown more sophisticated and capable, with the advances in both product and process technologies. By integrating such technologies into intelligence processes, the timeliness and the scale of the data collected is greatly improved. Further, the integration of information processing technologies into everyday life has vastly increased the opportunities for data collection.

The Intelligence Cycle

The functions related to intelligence occur in phases known as the intelligence cycle. In simple terms the cycle consists of four phases: **requirements**, **collection**, **analysis**, and **reporting**. This

section will describe the phases general terms. Note that some organizations have specific terms for the functions that are addressed here.[1]

Figure 5-1 The Intelligence Cycle



Source: Ryan, J.J.C.H. (summer, 2018). Intelligence Cycle Decisions Collage.

The **requirements** phase defines/identifies data of interest to the organization. For example, a business executive may identify the pricing strategy of competitors as desirable data. The executive would create a requirement statement for the business intelligence function, which would have the responsibility to try to meet the requirement. Similarly, a government leader may want to understand the military readiness of an adversary. That leader would, through established processes, require a statement of requirement to be generated and entered the intelligence community processes.

The aggregated set of requirements statements are the tasking for the intelligence process: and determines what data needs to be collected. When a requirement is generated, it is categorized in three ways; *importance*, *transience*, and *complexity*. These three categories help prioritize resource allocation to meet requirements. Obviously, the *importance* of the required data is something that should impact collection priority. Critical data needs should be met before a low priority data requirement. The *transience* of data is also a principal factor. Transience refers to how long the data will be available. The data may be fleeting in nature, like a radioactive emission, or may be available for collection only during a limited window. Finally, the *complexity* of the data needed affects how much planning must be done to assure successful data

1. The Intelligence cycle is important and is covered in various degrees in more than one chapter of this book. Chapter 14 also covers the intelligence process in terms of vulnerabilities of UAS and EW.

collection. Table 5-1 illustrates how these three characteristics can inform the prioritization of requirements. Please note: these are hypothetical examples for illustrative purposes only.

Table 5-1 Prioritizing Requirements Example

Requirement	Importance	Transience	Complexity	Priority
Competitor's pricing strategy for a contract	High	Medium	Low	1
Names of scientists on research effort	Medium	Low	Low	2
Amount of reserve cash on hand for investment	Low	Low	Medium	3

Source: Ryan, J.J.C.H. (2018)

Once requirements are prioritized, they are transferred to the **collection** function. The job of the collection function is just that, to collect data. Several types of data can be collected in diverse ways. To specify how the data will be collected, appropriate mechanisms need to be identified and allocated to the collection effort. I.E., *sources* of data and *methods* for data collection must be considered.

For example, collecting the data associated with a competitor's pricing strategy for a contract can be tricky. One strategy would be to infiltrate the organization and steal the strategy. This approach has obvious legal implications that make it less attractive option. Another method would be to go dumpster diving, sift through the garbage thrown out by the competitor, to extract clues and hints. This approach would only work if the garbage was both accessible and not shredded. A third alternative would be to send people to the local establishments to eavesdrop on conversations. Each of these approaches requires different collection strategies and resources.

The data collected may or may not, fully or partially, fulfill the stated requirement. Collected data that fully meets the requirement is complete and unambiguous. Data that only partially meets requirement may have some ambiguity or be missing some aspects. Data that does not meet any requirements is found to be useless; lacking in specificity and/or trustworthiness. The collected data is adjudicated during the **analysis** phase of the cycle. There are three steps in the analysis phase are *structural analysis*, *content analysis*, and *fusion*. Structural analysis consists mostly of describing the data. The descriptions can contain identifiers, such as index numbers and metadata, as well as actual descriptive data, such as statistical information. Structural analysis is important for both administration (record keeping) and post hoc studies conducted on the aggregated data. *Content analysis* is what most people think of as analysis, examining the actual data to derive meaning and insight. *Fusion* occurs when multiple types or

multiple source data are analyzed together. The benefit of fusion is that increased nuance can be parsed out of the data.

Once the analysis is completed, the results of the analysis is reported. The **reporting** phase consists of several several types of reporting efforts. First, and most obviously, there is *results* reporting, the delivery of the analyzed data to the required personnel. Results reports can include more than the data itself. The results can also include ancillary information discovered that relates to the original need, an assessment of the implications of the data, and caveats associated with the estimated reliability of the information. A second type of reporting is *feedback* reporting. Feedback reporting provides information to the other phases of the cycle. Types of reports that might be included are work product flow rates, percentage of needs met, identification of derived data needs based on the analytical process, and quality assessments. Finally, *strategic intelligence* reports can be generated based on aggregated analysis of many different results reports over a significant portion of an area of interest. Figure 5-1 shows the intelligence cycle in graphic form.

Common Problems in Intelligence

The motto for an intelligence analyst should be to believe nothing fully until it verified through multiple and distinctly dissimilar sources. There are too many people trying to obfuscate and too many challenges in interpreting the actual meaning from many different scraps of data. There are also many challenges associated with collecting and analyzing intelligence that go beyond simple access to the information. In general, there are three primary problems that must be considered. These are *quality* of data, *bias* in data interpretation, and *circular reporting*.

Data quality is an obvious issue for intelligence processes. This general problem set includes counter-intelligence activities, such as deception. When estimating the quality of the collected data, both the source and any methods that the data has been subject to must be weighed. Sources of data should be rated for truthfulness and informativeness. This discussion includes all types of sources, from instruments to people.

Truthfulness is an estimate of how close the data is to actuality. This can be an interesting measure, in that the data may be a complete falsehood but an accurate replica of actual data. For example, a business may be setting a pricing strategy based on wildly inaccurate material cost estimates. Thus, the data collected that reveal the inaccurate cost estimates is a truthful set of data, even though it reveals false information. A better example would be sending out info on false target knowing signal interception is a certainty.

A source may be rated as having a reputation for providing truthful data, sometimes truthful data, or mostly untruthful data. While sources that have a reputation for providing truthful data are obviously prized, a source that is known for repeatedly providing untruthful data can also

be useful for understanding the nature of the competitive landscape. Consider the repeated provision of untruthful data can hardly be considered an accident or coincidence. Ergo, the type and content of the untruthful data can provide insight into the adversary. All data is useful, just for different purposes.

Informativeness is the measure of how much added value the source provides to the intelligence process. High informative data sources provide a significant added value, while low informative sources provide little. Low informative sources are not necessarily bad; sometimes gathering a lot of low informative data sets can be extremely revealing in the aggregate. For example, a highly informative data source could provide you with the actual pricing strategy document for a company. Alternatively, low informative data sources could provide you with all the component elements that feed into a pricing strategy; salaries, qualifications, etc.

Combining truthfulness and informativeness provide a way of rating data sources. For scientific instruments, this is generally couched in terms like type 1 and type 2 error rates, as well as calibration. For publication sources, this might be discussed in terms of media bias, peer review, and impact factor. For human sources, terms such as reliability and reputation might be used.

Bias is a challenge for both human and algorithmic interpretation of data. Why algorithmic? Because humans write the algorithms. There are conscious and unconscious forms of bias, all of which must be addressed. A personal preference for uniformity of data may lead an analyst to treat various kinds of data differently, inadvertently skewing the results. Another type of bias may arise from a desire to see data that confirms suspicions. When such data is seen, it may be treated with more gravity than other data. Sufficiency introduces another type of bias, when analysts are satisfied that the data is complete, they may stop looking, even though they have only a small percentage of available data. Yet another form of bias can arise from the analyst overlooking subtle clues in favor of obvious data. Over-reliance of single source information also leads to interpretative bias. The bottom line is that data interpretation is a subtle art that must be approached carefully.

Circular reporting can sneak into intelligence processes in ways that make it difficult to recognize and manage. A circular reporting problem occurs when data that is collected and analyzed by one component of an intelligence function serves as input to another component, masquerading as new data. To the uninitiated, this may seem like a bizarre problem, but it happens too frequently in both very large intelligence functions and in news reporting. Examine a hypothetical news report. News service A reports that seven civilians have been killed in a suicide bomb attack. The wire services pick this up this report and publicize it. News service B then republishes the material but alters some of the wording. The wire services pick up this second report and repeat the process. News service A sees that report and takes it as confirmation of its original report, even though it is nothing more than its original report repackaged. This problem of circular reporting compounds the problems of bias in the analysis of intelligence data significantly and must be addressed.

Sources of Intelligence Data

Intelligence data has many diverse sources. Some of the more common sources are described in this section.

The earliest form of intelligence source is also the most easily understood. Human intelligence, or HUMINT, is intelligence data that is collected by human beings. HUMINT includes collectable information: stolen papers, intercepted letters, overheard conversations, observations, and physical artifacts. HUMINT need not be collected by specially trained agents, although that is a key role for them. HUMINT can come from travelers returning from a vacation, from chance encounters at conferences, or from interactions at parties. Because of the power of the human brain as a general processing system, HUMINT can be an amazingly important source of information.

Some technical data requires special technologies for collection. Humans are great at observing information in the visual light spectrum and hearing things within normal hearing ranges but are not much good at collecting infrared or encoded digital signals. For these types of data, special sources are required. Imagery Intelligence, or IMINT, uses imaging capabilities to collect data. Signals Intelligence, or SIGINT, is a combination of different intelligence sources. SIGINT includes Communications Intelligence (COMINT) and Electronics Intelligence (ELINT). COMINT is the collection and analysis of communications through various channels. This includes the content of the communications (the internals) and the external routing information; the return address, the intended recipient, the content and time of the transmission, etc. Sometimes referred to as metadata; the data that describes the facts of the communication. ELINT is like COMINT, in that it is the collection of signals electronically transmitted.

As information technology expands and becomes incorporated into everyday life, specialized forms of intelligence data collection and analysis have been developed to focus on the material from special sources. Some of these are obvious, such as Financial and Geographic Intelligence. But other sources are sufficiently specialized to warrant designation. These include Measurement and Signature Intelligences (MASINT) and Cyber Intelligence.

Countering these extremely specialized technical sources is Open Source Intelligence (OSINT). OSINT takes advantage of the Internet and other open sources of information, to build robust analytical portraits of targets of interest. For example, consider an OSINT analysis of a competitive business. The types of open source information may include employment ads, floor plans, financial filings, and leadership profiles. Consider a business that is running employment ads for quantum computer specialists, whose floor plans include laboratories, whose financial filings include speculative notices regarding technological risk associated with research, and whose leadership includes people who have long histories in the communications business. Are they more likely to be developing a quantum communications capability or a space vehicle?

The fact of the matter is that the residue of an enterprise's operations are an incredibly rich source of information. Open source data can be extracted from social media, conventional media sources, scientific publications, press releases, public speeches, financial filings, legal filings, official documents, and administrative documents. With the availability of powerful datasets at local libraries, it can be quite cost effective to leverage open source intelligence.

Combining data from different sources can assist in intelligence analysis. One use is detecting deception. Another of use is building a more complete and sophisticated knowledge of capabilities. Combining static imagery, video, and signals data can provide a structured understanding of the control and capabilities of a smart munition.

Understanding Attack/Defend as a Tool

It is one thing to collect information and analyze the capabilities and intentions of an adversary. Using that intelligence to create attack/defend scenarios takes it to the next level. There is tremendous training experience gained from engaging in attack/defend exercises. Building attack/defend scenarios forces one to determine the extent of one's knowledge base, potentially identifying latest information requirements. Practicing attack/defend scenarios can reveal strengths and weaknesses on both sides, which can lead to strategy development, tactics refinements, and organizational changes.

Such scenarios can be conducted with varying levels of abstraction. At one end of the abstraction scale are simulations. At the other level are real world exercises, that use real equipment in actual conflict conditions, albeit with constraints. In between are many different combinations of games and exercises.

Simulations include table top games, computer programs that mimic real world interactions, or mathematical algorithms that generate outcomes based on input values. For attack/defend exercises, table top exercises are quite common and even have their own acronym, TTX. A benefit of table top exercises is that complex scenarios that require human decisions can be worked through and discussed as the game progresses. A limitation of table top exercises is that there is typically little fidelity to real world conditions.

Real world exercises are conducted using actual equipment in conflict conditions with limitations and constraints for safety and security. The benefit of real world exercises is that participants significantly advance their knowledge and experience. The downside of real world exercises is that they tend to be enormously expensive, expend resources, take significant time to plan, and require extensive safety and security protocols.

Attack/defend scenarios can be viewed as a series of activities conducted by teams. The red team acts as the adversary, attacking opponent's capabilities. The blue team acts as the defenders, detecting and countering red team activities. Because these are exercises, it is important to have safeguards and strictly delineated boundary conditions. For example, if the attack/

defend scenario includes cyber activities, a typical safeguard would be to ensure that there is no Internet connection. This prevents adversaries from spying on the exercise, but can also prevents accidents, such as the inadvertent penetration of a non-participatory network. While it may appear as if it could never happen in a well-managed system, the fact of the matter is humans make mistakes. Better safe than sorry.

Red Teaming

Red teams act as the adversary. What does that mean? One implication is that the red teams need to know technologically how to execute attacks on the target. If the red team mimicking a specific adversary, the members of the red team must also be knowledgeable about the strategies and tactics of the actual adversary. This can include methods of attack, cultural assumptions about how activities occur, and organizational constraints on command and control.

To technologically execute attacks on the target requires a set of activities. First, the target must be identified. In attack/defend scenarios, this might or might not be specified. Assuming it has not been specified, the first thing to do would be to conduct reconnaissance activities to identify potential targets. There are interesting implications here. Conducting reconnaissance is much more than simply a visual assessment. Depending on the type of target and its location, diverse types of intelligence sources might be needed to collect the information to identify potential targets. This challenge is particularly tricky when the potential targets are moving, such as airborne platforms.

Once the potential targets have been identified, then the capabilities and weaknesses need to be cataloged. This is done by probing and testing. For example, if the target of a red team exercise is a computer system on an unmanned aerial system, then one-way weaknesses can be potentially identified through analysis of attempts to connect to the system. Error messages can be useful, in that they can reveal information about why an error occurred.

After the capabilities and weaknesses of the targets are cataloged, an attack plan is created. This plan allocates resources in a prioritized pattern to execute a strategy to achieve a specified result. Resources include both human operators and tools, such as weapons. If the red team is mimicking an actual adversary, this plan must mirror the normal processes of the adversary. If not, then the red team is free to develop their own plan. Once the plan is in place, the red team executes the plan, possibly making real time adjustments in response to changes in conditions, discovery of new information, or to ward off defenses.

The most important result of the red team exercise is knowledge. It should be collected at every step of the exercise. All activities should be noted. This can accomplish through filming, recording, instrument readings, or taking notes. Generally, it is best to have one or more observers collecting the data. After the exercise has concluded, it is very important for the actual team members to immediately conduct a hot wash-up; a real time review of what was

successful, what as not, and lessons learned. Their individual impressions and observations can be extremely valuable to developing the knowledge and capabilities of the enterprise.

Blue Teaming

The blue team is the defending team. Their challenge is as complex, perhaps more so, than the red team. In order to defend a target, the blue team needs to have full knowledge of the target, including technical capabilities and weaknesses, vulnerabilities, and operational patterns. There should be detection mechanisms in place to alert the blue team to adversarial actions. Additionally, the blue team needs to be on the lookout for stealthy or unexpected adversarial activities. Finally, the blue team needs to be able to stop adversarial actions and remediate any harm done.

Having full knowledge of each potential target is a daunting task. Obviously, not any one person can full knowledge of a complex system. This is where team composition becomes important. The team must possess a variety of capabilities, spanning technical to operational knowledge sets. Running many exercises can assist in identifying areas that need additional expertise as well as broaden experience. One possible problem in some systems is that the knowledge of the vulnerabilities and remedies may be extremely sensitive. It may be necessary for some blue teams to have compartmentalized knowledge areas; a common set, a sensitive set, and a closely held set. This becomes a challenge for both constituting the team and managing the interactions of the team members.

The detection mechanisms the blue team relies on should be ubiquitous. It does no good to have special detection mechanisms simply for exercises. The blue team needs to be operating in as close to a real environment as possible. The conduct and result of the exercise should be a substantial input to planned improvements in the system. The feedback from the blue team is an important part of that.

Recall in Chapter 4 the author discussed the classes of events that needed to be detected. The blue team needs to address each detection challenge while planning their defenses, including detection of the unanticipated or exotic activities. The blue team cannot simply rely on detection capabilities but must be on the alert for any unusual activity and be prepared to react as necessary. The red team is motivated to overcome blue team defenses. The blue team needs to be on constant alert.

When the blue team detects red team activities, they need to have plans and procedures on how to mitigate these actions. This implies that the blue team has considered and practiced reacting to various activities. Part of that practice should include command and control of actions. Clean lines of communications with fail-over procedures, if a link in the chain of command is disabled or unavailable, is critical to effective team action. Ad hoc responses may be necessary, particularly in the case of unexpected red team activity, but the command and con-

trol of the ad hoc response execution is just as important as it is to preplanned activity execution.

Blue team experiences are just as important to knowledge development as red team experiences. During exercises, all activities should be logged, just like red team activities. Again, this can be done through filming, recording, instrument readings, or through taking notes. Observers should be responsible for collecting data. The blue team should also conduct a hot wash-up of their experiences. Both the team members' individual impressions and observations are extremely valuable to developing the knowledge and capabilities of the enterprise.

Benefits

An obvious benefit of attack/defend exercises is building expertise. Another obvious benefit is testing the target system and developing improvements to its defenses. Less obvious benefits include developing new tactics and techniques, discovering innovations, and creating stronger team relationships.

Operator expertise is an important benefit. While marginal improvements for individuals can be achieved simply by working through a scenario, improving how the team interacts is also a desired outcome. When teamwork improves, sharing of knowledge is an added benefit. Teammates who trust and value each other share information, ideas, and techniques, improving both individuals and the team. Leveraging this synergy during team activity reviews can result in powerful advances. The secret is to truly value each person's contribution; no person should be marginalized or made to be a scapegoat for any real or perceived failure. The value of exercises is in learning and improving. There should be no penalties for making mistakes. Learning occurs from making mistakes and seeing the consequences.

Testing the target system in not simply a matter of seeing what the red team accomplish. The target system is comprised of technologies, people, and organizational constructs. Each of these can potentially be improved and refined through probing, testing, and attacking. Improvements that are discovered through attack/defend exercises can be as trivial as improving the chain of command. Table top exercises in disaster recovery scenarios often reveal that there are few plans for replacing people who fall ill or are unable to communicate with the rest of the team. In fact, one of the best stress tests for organizations is to do a table top exercise of a common operational scenario and then randomly remove players how the organization reacts without them. Simple insights can lead to easy improvements that greatly benefit the organization as a whole. Individual interactions with technologies during exercises can also reveal needed changes. Reviewing all the collected material from the exercise should be done with these types of insights in mind.

While attack/defend scenarios tend to focus on how well the defense is conducted, one of the more powerful outcomes could benefit the offense; the development of new tactics, tech-

niques, and procedures in adversarial situations. Careful recording of red team activities and enabling members to test innovative approaches can be very important benefits to the entirety of operational needs.

Discussion Questions

Test your understanding of the material by thinking through the following questions. Discuss them with other people. Can you think of more questions that would be useful?

1. Devise a table top exercise for a kinetic attack on a surveillance drone. Identify an adversary, select a kinetic attack, and lay out the attack scenario in phases. Who should participate in this exercise? What questions and decisions should be considered at each step in the exercise? Consider all the elements of national power while creating this exercise; diplomacy, information, military, and economy.
2. What kind of intelligence would be needed to set the stage for such a table top exercise? What sources would need to be used?
3. Imagine that you have been asked to command a blue team for a UAS ground station attack/defend exercise. What types of people would you want on your team? How would you organize your team?
4. Imagine instead that you have been asked to command a red team for a UAS ground station attack/defend exercise. What types of people would you want on your team? How would you organize your team?
5. For the attack/defend scenario imagined in challenges 3 and 4, how would you organize the observation aspects? What types of technology would you want to use? How would you collate and curate the information collected? What kinds of reports would you want to develop at the end of the exercise?

Sources for more information

O'Neil, Cathy. (2016) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown. ISBN 978-0553418811

Mudd. Philip. (2015) The HEAD Game: High-Efficiency Analytic Decision Making and the Art of Solving Complex Problems Quickly. Liveright. ISBN 978-0871407887

Heuer, Richards J. Jr. (1999) Psychology of Intelligence Analysis. Central Intelligence Agency Center for the Study of Intelligence. Available online at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Red Team Journal. https://redteamjournal.com/about/