RETHINKING THE INTELLIGENCE CYCLE FOR THE PRIVATE SECTOR

By: Daniil Davydoff

Author Bio: Daniil Davydoff is manager of global security intelligence at AT-RISK International and director of social media for the World Affairs Council of Palm Beach, Florida. Davydoff's work has been published by *Foreign Policy*, *Risk Management*, *The National Interest*, The Carnegie Council for Ethics in International Affairs, and RealClearWorld, among other outlets. His views do not necessarily reflect those of his company or of ASIS International.

What is the intelligence cycle and why do we use it?

Successful security risk management involves careful planning and preparedness rather than ad-hoc crisis response. Successful intelligence analysis requires something similar, and for specialists in this field the intelligence cycle serves as a planning and preparedness blueprint. But just as any set of guidelines must be regularly updated to be effective, the intelligence cycle needs to be reevaluated for its new life in corporate security. As a tool that has been perfected in the public sector, the cycle must adapt to private sector realities, including new consumers, new requirements, limited resources, and, at the core, a new mission.

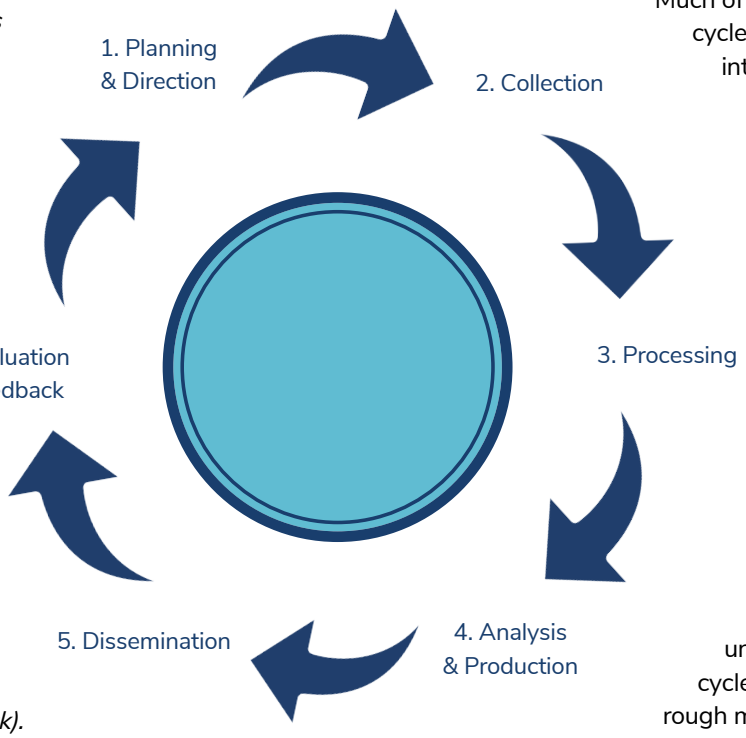
There are many ways to describe the intelligence cycle (or "the cycle" as it is sometimes referred to). In short, it is both a theoretical and practical model for conducting the intelligence process. Although there are many variations, the cycle usually consists of six steps: planning and direction; collection; processing; analysis and production; dissemination; and evaluation and feedback.

In one imagined scenario, these steps would be implemented in the following manner:

The head of corporate security reports from a meeting of executives that the company is planning to build a facility in another country. Senior leaders need intelligence on security risks around the planned site, and you agree to create a report on crime, terrorism, and natural disaster risks in two weeks (planning and direction). As head of the intelligence team, you

find raw information from local media reports, law enforcement records for the area, and credible disaster risk databases (collection). After considering the reliability of the sources and converting the raw data into easy-to-read graphs (processing), you decide which information to use. Now it's time to write the actual report (analysis and production), and submit it via email and hardcopy to the interested company's decision makers (dissemination). Via the head of corporate security, you check in two weeks later to find out how the report was received (evaluation and feedback).

Figure – Key Steps of the Intelligence Cycle



This approach is useful across most types of intelligence work, whether protective intelligence or global security intelligence. In recent years, even investigators have adapted the cycle to serve their needs. Of course, the intelligence cycle's usefulness is not the only reason that it is has become both the standard reference point for analysts and a framework for many private-sector analyst training programs. When government employees move into the private sector, they bring the cycle with them.

At the lower levels of the corporate intelligence ladder, intelligence analysts come from a diversity of backgrounds. One can find among them English and psychology graduates, young regional specialists, data-savvy social media analysts, and budding think-tankers. The middle and top sections of the ladder are starting to diversify, but it is well known that former military and three-letter-agency employees still are hired disproportionately within corporate security departments. Intelligence leaders, therefore, have been raised on the intelligence cycle, and whether or not they innovate in other areas, many consider the cycle a fundamental model to follow.

Challenges facing the intelligence cycle model

There's a degree of uncertainty regarding the origins of the intelligence cycle. Depending on whom you ask, it was conceived around the time of the French Revolution or during World War I. In any case, it seems to have become an intelligence community staple in the Cold War period, and during that time, there was no shortage of criticism of the model.

Much of the criticism has decried the cycle's oversimplification of the intelligence analysis process and its inaccuracy. Are there enough steps? Who actually drives the cycle? Is the cycle unidirectional or does it really flow both ways? These and many other questions are routinely discussed regarding the cycle's usefulness or need for revisions.

This begs the question of whether a reevaluation is needed. Some would make the case that rethinking the model is unnecessary. The intelligence cycle was always meant as a rough model with the key being the fluidity of its application to any environment, whether public or private. It is true that many of the current challenges facing the traditional intelligence cycle model can be resolved by adaptable analysts and good training. Having said that, considering the nature of these challenges is itself a needed exercise.

Although the cycle has faced myriad criticisms, the premise of this white paper is that private sector analysts have a special set of obstacles and considerations at each step of the model. This is due to some of the elements that distinguish the private sector from the public, including (but not limited to):

- **The wider variety of hierarchies and reporting line types**
- **Different rates and priorities concerning technology implementation**
- **Higher variation in workplaces**
- **Widely different organizational goals**
- **Potentially faster rates of change, growth, and organizational restructuring**
- **Limited resources for security in relation to other institutional focus areas**

There is an important caveat to these distinguishing characteristics, namely that they are trends rather than certainties. Regarding limited resources, for example, there are many government agencies that would dream of having the resources commanded by protective intelligence teams for some major companies.

Steps of the cycle and the private sector

To dig deeper into how the intelligence cycle may be affected by these factors, we can consider each phase of the cycle in turn.

Step: 1 - Planning and Direction

Establishing the recipient's intelligence requirements is one of the most critical steps, because understanding customer needs aids the team in structuring a project and pursuing certain types of intelligence. In the public sector, this step is fairly straightforward. A government institution or senior official has an "ask" on a security issue, and intelligence personnel pursue the information, whether the subject is government instability, terrorism, or another threat. In the private realm, intelligence consumers may have only elementary levels of knowledge on threats, requiring basic research from intelligence teams. Christopher Broomfield, a global security and threat analyst for Carnival Corporation, and former intelligence officer with the U.S. government, notes that:

> *. . . private sector analysts must uncover security issues and events which are not necessarily apparent but could impact business operations, and be able to quickly find and provide relevant findings for decision makers. In addition, they often need to address stakeholders who are not familiar with specific transnational issues and explain how these could present challenges to the business environment.*

In some cases, private sector consumers may not have a good notion of what is needed, so the process should be reversed, with the corporate analysts being more proactive to "push" their ideas in creating a research plan. This issue is not unique to the private sector, but is typically more pronounced. It is sometimes most apparent in the protective intelligence realm because evaluating individual threats requires specialized training in forensic psychology, among other disciplines. AT-RISK International was once working with an organization that was concerned about threats made by an employee and references made to "Allahu Akbar." While the client asked us to investigate the employee's dissatisfaction in the workplace and the Islam connection, our experience in threat assessment told us we needed to also pursue other directions. After digging through the subject's social media posts, we found that he had undergone recent changes in mood and behavior, and ultimately the focus of the assessment needed to be psychological in nature.

A colleague from a top global technology services firm recently noted an even more fundamental problem. After transitioning from several years in the intelligence community and starting her position as a lead threat and risk analyst in the commercial space, she realized that some of her company's stakeholders did not understand that they were consumers. Upon receiving her reports, at least one of them thought he needed to edit the report and give it back to her team. In the end, my colleague had to explain her role as advisor and inform the individual that his primary responsibility was to use the gathered intelligence to inform his decisions.

Step: 2 – Collection

For most intelligence analysts, the collection step will be the most obviously different between the public and private sectors. In short, the private sector analysts need to be more versatile to be effective. Whereas government analysts are often hyper-specialized, with some focusing on human intelligence (HUMINT) and others focused on signals intelligence (SIGINT), private sector teams are, in some sense, "any source any time." This is partially due to raw team size. Even the wealthiest corporations do not usually devote enough resources to security generally, and certainly not to maintaining large intelligence departments.

The leanness confers both advantages and disadvantages onto private sector intelligence gathering. On one hand, small teams mean risks on the intelligence continuity front. Should one analyst leave a three-letter agency in Washington, the impact will likely be less severe than the departure of one of four analysts for a large multinational. The latter probably has a greater amount of wide-ranging knowledge on critical sources the company needs to follow, as well as a better understanding of operations at the company.

On the plus side, having fewer resources encourages analysts to become experts in utilizing open-source intelligence (OSINT) to a greater degree than those in the public sector. It is commonly stated that 90 percent of critical intelligence is open-source, so this is a major strength. In fact, it is a strength even in areas where one would think that publicly available information is insufficient. As Audrey Villinger, a senior manager with the firm Security Industry Specialists, Inc., puts it, "Even in law enforcement and crime, open-source intelligence is a big deal. People don't call 911 anymore, they don't stick around for witness statements, they tweet about it." To be sure, law enforcement agencies (among others) are now relying on the Twitter feed themselves, both through their own resources and by working with the small industry of data-mining firms that have arisen. Yet as new open sources and feeds pop up, it is typically the private sector that still adapts to the new technology first.

Yet another opportunity (and to some degree a requirement) for private sector analysts is networking. Of course, filling out the Rolodex or connecting on LinkedIn is helpful to government employees, too. But using those contacts for the purposes of intelligence collection is something corporate analysts and consultants can do with more ease despite the greater individual effort necessary to expanding networks. Broomfield, of Carnival, points out that analysts must be "cognizant of proprietary issues, but these issues are nothing like the scrutiny or restrictions of the public sector's classified environment." Using

personal networks as sources is also more critical absent government agency resources. Some companies solve this problem by relying directly on government and law enforcement contacts to eliminate lag between the occurrence of a major incident and their intelligence feed. On the travel security front, networks of travel risk managers or even analysts themselves now voluntarily share information on travel warnings, achieving something similar.

Step: 3-4 – Processing, Analysis, and Production

The traditional intelligence cycle model is a step-by-step approach, with the production and analysis phase following processing, which in turn follows collection. Whether the analyst is working for the public or private sector, most would agree that this is a very naïve way of describing the process. In reality, the steps are fluid and production of analysis may run concurrently with information gathering or even start before intelligence is fully collected. In practice, then, steps three and four are frequently combined.

This is not unusual within the government or within the commercial space, though the private sector may create more pressure to "just start writing." The resource and specialization issue already mentioned is partially responsible. Small teams of corporate intelligence analysts often must cover more ground in less time. In one day, an analyst may have to jump from reputational risk in Latin America to terrorism risk in Europe to intellectual property risk in Asia. Furthermore, private sector consumers such as traveling employees sometimes are less knowledgeable on intelligence matters than government customers, so it can be easier for corporate security analysts to just start writing what they know and fill in the details later.

The more extensive use of OSINT in the private sector has also, paradoxically, introduced both greater certainty and greater uncertainty to analysis, depending on the case. Instead of weighing a "raw" diplomatic cable against local reporting as some government analysts can do, private sector employees whose remit is country risk might have to decide which of ten media stories and blog posts about a certain security incident have it right. Judging source reliability is just as critical within the government, and some would say that oversights in this area have been responsible for some of the most notable intelligence failures of recent years. Still, the reality for some small private sector intelligence teams is that they have few local sources at all, making accurate judgment tougher to some degree.

In other areas, private sector analysts who are used to leveraging OSINT due to the lack of other resources might have an analytical advantage. Social media monitoring allows protective intelligence analysts to have a much better idea of the risk that individuals may pose to threatened targets. When combined with threat assessment guidelines, social media posts serve as highly useful indicators for violence.

Step: 5 – Dissemination

The nature of the audience matters a great deal near the end of the intelligence cycle just as it does at the beginning, when the initial requirements are being discussed. At the dissemination step—when findings are finally given to the recipient—private sector intel teams must once again contend with consumers who are not used to typical intelligence deliverables. Innovation on delivery is essential.

There are differences among the typical public sector consumers on this front, with some requiring briefings or presentations, but it is safe to say that most are at least accustomed to the report format. This is not always so in the private realm. Outside of the corporate security department, many senior leaders with MBA degrees last read a long and detailed report in grad school. For key corporate decision makers, storytelling through PowerPoint—or similar presentation tools—is a necessity. And when it comes to this kind of storytelling, bullet points on slides are not enough. Intelligence findings need to be visual and interactive, and most of all emphasize the quantitative for maximum impact. In the private sector, there are variations among industries that may not be as significant in the public sector. According to Villinger, of Security Industry Specialists, Inc., tech firms, for example, tend to have very high aesthetic requirements.

It is worth noting that, generally, the government tends to invest more resources in technology for collection than technology for presentation, whereas the reverse is sometimes true in the private sector. It is, therefore, possible that the gap in what dissemination means between the two sectors will only expand over time, and the intelligence report will continue to be standard within the government even as private companies move to radical technology such as virtual or augmented reality for presentations.

Step: 6 – Evaluation and Feedback

Depending on whom you ask, the intelligence cycle has a sixth step—evaluation and feedback. At this juncture, the intelligence creators receive some sort of response to or comments on their work, at least in the ideal world. For many analysts, this step is frustratingly similar in the public and private sectors in the sense that they only hear back if something goes awry. If anything, this silence is more common in the private realm because intelligence consumers in business environments are busy creating revenue rather than taking pride in policy or tactical knowledge on a security issue. Sometimes, private sector consumers come back with additional requests, which means the job is being done right. Frequently, getting feedback requires intel teams to be proactive. Requests for feedback are necessary, but need to be as convenient and quick to fulfill as possible for intelligence recipients. An annual survey is the ideal approach, but follow-up calls on important products can also work in a pinch.

What's next for the intelligence cycle?

All these challenges—individually and taken together—are meant to remind us about the need for constant reevaluation of the cycle. This review, however, is not meant as a call to replace the model. If anything, thinking about the problems experienced by private sector intelligence can help improve efficiency of the analytical process outlined by the cycle. It can also aid in creating a more realistic and effective training program for new analysts. In that sense, each intelligence team should consider not just these issues but obstacles specific to their own organization.

That takes us to perhaps the most important difference between the public and private sectors, and the best reason for reevaluation of how we "do" intelligence: the difference in mission. Whereas government institutions are committed to the safety and security of citizens at virtually any cost, the core objectives of businesses revolve around profit. Security for personnel, assets, or the enterprise must be balanced against costs and revenue goals. Apart from improving methods or making their own lives easier, it is imperative that intelligence teams regularly assess how the cycle can better fit into these central corporate calculations. Only then can intelligence go from being a "cost center"—a fate often ascribed to corporate security broadly—to something that creates value.

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314
+1.703.519.6200
asisonline.org