

Intelligence Surprise

by Kevin M. O'Connell [\[1\]](#)

Surprise. Intelligence services hate it, work tirelessly to avoid it, and know that they and their political masters inevitably will be burned by it. The two most lasting events in our national security psyche – the Japanese attack on Pearl Harbor and the Al Qaeda attacks on the World Trade Center and the Pentagon – stem from failures to recognize surprise, among others.

While we know this intuitively, let's look at the substantive challenges of warning. Since the beginning of the 20th century, the potential to recognize threats and provide warning to decision-makers in time for meaningful response has been declining. In any war with the Soviets, for example, we would have seen the mobilization of mechanized land units in Europe over weeks at a time, but would only have minutes had they launched an intercontinental ballistic missile barrage over the top of the earth.

Warning is more complex today in two important ways: first, for a number of topics, timelines to understand are severely shortened, like terrorism or cyberspace attacks. Here, experts talk about the need to extend collection and analysis back in time to identifying suspicious activities, or to be able to assess and respond to cyber attacks within microseconds. Threat is often harder to identify, and often so are potential responses.

Second, for a number of other emerging topics, we don't even understand the temporal or geospatial dimensions of warning. Environmental scientists now worry that the timelines for climate change are accelerating beyond our best analytic understanding, and biological attacks might appear only as an incidence of flu in a local area without any signal of where and when it could spread to something more severe, even deadly. Beyond the alerting problem, in some cases we may not even know how to respond.

Surprise. During Director of National Intelligence (DNI) Blair's first annual threat briefing to the Congress, he focused as much on non-traditional areas – economics, energy, and environment, to name a few – as he did on Al Qaeda, Pakistan and China. Why? Because developments in these areas are increasingly affecting political stability and can quickly become sources of conflict.

The problem with these issues – and even traditional ones, like the values of demographic segments in the Muslim world – is that they don't lend themselves to “secret” intelligence collection. Poorly understood issues rely overwhelmingly on the judgment of time-seasoned experts to provide “weak-signal” warning as the best indicators of threat. These realities prompt us to rely heavily on two of the more historically undervalued elements of U.S. intelligence – exploitation of open sources and analysis.

Wait – isn't intelligence about spies and satellites? Historically it was, but today's nexus of instantaneous communications and information technologies – combined with their widespread use – creates new opportunities to collect unique information, including the overarching context required to conduct good analysis. In fact, almost every one of the intelligence disciplines confronts a growing “seam” with the outside world that must be recognized: human intelligence (HUMINT) vies for insights with the open gathering of outside expertise, signals intelligence (SIGINT) has commercial rivals that mine cyberspace and other parts of the electronic spectrum with incredible efficiency and the data mining required to provide services in the market, and imagery and geospatial intelligence (GEOINT) operates in the context of commercial space imagery and the software that produces useful renderings of complex visual and mapping data. Beyond substance, any objective comparison of these sources should involve an understanding of the costs of regulatory burden – typically, classification, compartmentation, and controls— whether in dollars or in terms of U.S. decision advantage.

Traditionally, U.S. intelligence has seen these developments as pure competitors, and largely tried to slow them down, a long and complicated legacy best left to the historians. But in light of our warning challenges, an enlightened view would recognize the strong complementarity between closed and open sources of information and optimize their mix. Secrets still matter in this world, but should be reoriented, first and foremost, on what is not available credibly in the open world, and then only on the hardest aspects of our hardest intelligence problems.

Here's another way to look at it: for years, we've talked about “persistent surveillance” – the notion that, for any topic or target, U.S. intelligence could look at it all the time (or at least long enough to understand it). While this concept was largely developed in the classified realm, the potential elimination of boundaries between closed and open information sources for intelligence means that we are already there. But this creates a different challenge, namely, that analyst, politician, decision-maker, or ideologue can dip into this information ocean to find the data that proves virtually any point that he or she wants to make. Matters of national security, homeland security, and others are far too important to be left to such poorly developed positions. Analysis will rest harder than ever on its traditional hallmarks of questions asked, sources used, methods of logic and evidence, and critical peer review.

Yet analysis is also in renaissance, drawing upon collaborative tools, multi-disciplinary approaches to interpretation and a powerful set of emerging analytic methods from academia, business, social networks and elsewhere. U.S. intelligence analysis must continue to move boldly and confidently beyond characterizations of politics and failure, and embrace new ways of dealing with uncertainty, understanding complexity, and finding better ways to visualize analytic judgment. Certainly the Obama Administration has an appreciation for these kinds of things, having come to power on the backs of them.

Surprise. Intelligence used to be about collecting secrets and protecting them. While this remains partly true today, our post 9/11 experiences to share intelligence among federal, state, and local entities, and even CIA's recent brokering of crisis information between India and Pakistan reflect the growing importance of information sharing. Yet several years of intense

focus has not made the reality any easier as we continue to struggle with it in a way that a psychiatrist could only deem schizophrenic. For sure, more intelligence sharing will create a demand for innovation as sources and methods decay rapidly or perish. But planned obsolescence is a reality of the information world - use it and lose it.

For DNI Blair and the new intelligence leadership, there's much to be done. Rather than the suffocating paroxysm of intelligence reorganization, what is called for here is a rethinking of the entire enterprise. Security reform – a better understanding of what the U.S. government can and cannot meaningfully control – is also urgently necessary. By the way, both of these are entirely consistent with the Project on National Security Reform (which Admiral Blair helped direct), and which focused on security-related information and analysis much more in terms of getting it right than the boundaries within which they lie. Intelligence officers in large numbers are finally recognizing that the system that brought us through the Cold War may still have large imbalances for the way we need to approach the future.

Surprised? You shouldn't be. But there may be many more surprises with tragic consequences if we don't re-orient ourselves in the right direction, very soon. Yes, secrets still matter, but open sources and analysis need to be a mainstay of 21st century U.S. intelligence.

[1] Kevin O'Connell is the CEO of Innovative Analytics and Training, a "sources and methods" company that helps clients with analysis and decision-making. His previous assignments have included stints in the State Department, the National Security Council, the Office of the Vice President, and the Office of the Director of Central Intelligence. He was also the first Director of RAND's Intelligence Policy Center. He is adjunct faculty at Georgetown, where he teaches a course on comparing intelligence services.