MITRE | Center for Technology & National Security

SERIES Number 5

INTELLIGENCE AFTER NEXT

MISSION-BASED CHALLENGES FOR THE INTELLIGENCE COMMUNITY

By Eliahu Niewood

Prioritizing with Mission-based Challenges

Former Director of National Intelligence Daniel Coats in the 2019 National Intelligence Strategy (NIS), wrote "we have to become much more agile, more innovative, more creative." Given the dynamic nature of demands on the Intelligence Community (IC) and the rapid pace of emerging technology, it is hard to disagree with Director Coats' statement. At the same time, it is hard to look at the IC one year later and see real movement toward this goal or impact from the 2019 NIS. One could argue that it is not only the 2019 NIS that has failed in this way, but that the halls, safes, and hard drives of the National Capital Region are littered with failed strategies and initiatives to increase innovation or drive development of the favored technology of the day to support national security. For every document which has had lasting impact in shifting the focus of the problem set the IC addresses – there are dozens of others that have come and gone with no lasting and real impact.

As an alternative approach, this document proposes five mission-based challenges for the IC to take on in the next 3-5 years. They include:

- Countering adversary malign influence campaigns before they broadly impact our population.
- Mitigating insider threats rapidly and effectively through detection and protection.
- Enabling free flow of information and communication in 'smart' cities under authoritarian governments with exquisite surveillance capabilities.
- Finding peer high value relocatable targets (HVRTs) within the window when they are exposed for critical operations, thereby enabling traditional kinetic or non-kinetic attacks against them.
- Providing greater non-traditional and non-kinetic means for disabling critical targets.

Identifying measures of success and accompanying metrics for each of these will be key to achieving measurable progress in facing these challenges. Solving them, however, will not solve every problem the IC confronts today. No set of 5, 15, or even 50 challenges could do that. However, if the IC can solve even 2 or 3 of these challenges, it will have enhanced its impact while exercising its ability to identify the right emerging technologies needed for these specific challenges and the ability to adopt and adapt those technologies as needed for its problem set. Those behaviors will be critical enablers for addressing the other pressing problems the IC faces.

Introduction

The mission-based challenges identified in this paper strike a balance between the two core missions of the IC: helping the U.S. advance its geo-political aims while avoiding armed conflict; and helping the U.S. win in armed conflict when necessary. Increasingly, actions we and our adversaries take every day, whether to compete or prepare for conflict, are as or more important than the actions we would actually take in conflict. In the same way, the role of non-military industry, technology, resilience, and processes are as or more important than their military counterparts. These challenges reflect that.

These challenges also focus on the existential threats to the U.S. posed by our peer adversaries. Efforts underway today by both China and Russia fundamentally threaten the American way of life. Terrorists and insurgents threaten American lives, and we must do what we can to protect those lives, but we must also give primacy to protecting our core approach to government and society.

Perhaps most importantly, these challenges sit at the nexus between critical problems and emerging technology. Solving any one of them would have significant impact on improving our national security. Solving any one of them would also need to leverage one or more emerging technologies that are not today finding widespread applicability in the national security ecosystem. Each would provide the IC with game-changing capability relative to where it sits today.

Mission-based Challenges

Mission Challenge 1: Counter adversary malign influence campaigns before they broadly impact our population

Our adversaries have shown they can undermine our way of life through disinformation and misinformation campaigns without ever lifting a finger more than required for typing on a keyboard. They have used these campaigns to increase political divides within our country and undermine the general population's confidence in the election process and in our government. Such campaigns pose a dire threat to us, and they do it in a way that is relatively inexpensive to undertake and which we might not even know that they were occurring. They exploit existing weaknesses in our society or take advantage of the prevailing environment at a given moment in time.

SOLVING THESE CHALLENGES WILL REQUIRE THE IC TO BE INNOVATIVE AND TO FOCUS ON REAL AND MEASURED PROGRESS IN ITS PRACTICES AND TECHNOLOGIES.

While it is unlikely that we can eliminate these types of campaigns completely, the IC can play a critical role in minimizing their impact, including maintaining vigilant situational awareness around them and helping other elements of government respond effectively to them. Situational awareness should include:

- Understanding adversary intent
- Monitoring social media to know a foreign initiated campaign is underway
- Using that information to attribute that campaign to a specific country and actors within that country
- Understanding their objective or even predicting that they will mount a campaign
- Assessing the impact of the campaign

Responding to a campaign would include:

- Working with other elements of government to deter or take reprisal steps against the perpetrators. These steps could range from demarches or sanctions through the State Department to influence or counter influence campaigns that exploit adversary weakness mounted by appropriate government entities.
- Slowing or stopping progress of the campaign through social media
- Taking steps to mitigate the impact of the campaign on the public.

The IC could play an important role in attribution and prediction, in monitoring to understand that a campaign is underway, in enabling some forms of deterrence, and in partnering with commercial platforms. Relevant technologies include behavioral economics, artificial intelligence, and data analytics.

A useful metric in this challenge could be that the IC effectively counters malign influencers before they impact more than 5 percent of the U.S. population.

Mission Challenge 2: Mitigate insider threats rapidly and effectively through detection and protection.

Just as human sources remain a critical enabler for our intelligence operations, preventing insiders from serving as sources for our adversaries is critical for protecting our information. As unfortunately demonstrated time after time, from Chelsea Manning to Edward Snowden to Vault 7/8, computer networks and "soft" copies of documents make it all too easy for a trusted insider to steal large volumes of information at different security levels. The IC, including law enforcement, needs to take a significant step forward in how it uses a variety of tools to find insider threats.

There are several elements involved in solving this problem:

- Better monitoring of computer networks and how they are used could provide indicators when documents are being accessed or copied in anomalous ways.
- Taking steps to make anomalous behavior or improper use of information more detectable or attributable. For example, develop the analogue to a bank's use of "dye packs" against bank robbers.
- Monitoring of financial activity by cleared individuals or those with access to critical intellectual property is another example.
- Using historical data more effectively to understand what behaviors are typical of an insider threat and what behaviors are typically harmless, and how those indicators have varied over time.
- Establishing patterns of life in various modalities and looking for anomalies is another potential approach.
- Tracking connections and information in social media feeds is another potential data source.

None of these likely is sufficient on its own to solve this problem, but in aggregate they might make a real difference. Cyber resilience, artificial intelligence, social media, and data analytics could all potentially contribute to addressing this gap.

A useful metric in this challenge could be that the IC detects insider threats with an 80% probability of detection and a <1% probability of false alarm.

Mission Challenge 3: Enable free flow of information and communication in 'smart' cities under authoritarian governments with exquisite surveillance capabilities.

Free flow of information and the ability for people to communicate effectively is a strong counter to authoritarianism around the world. It also helps the Intelligence Community to better understand what is going on inside adversary governments and societies. However, the advent of smart cities, social credit scores, and ubiquitous surveillance all make the challenges of meeting and communicating freely under repressive governments more challenging. Whether in real time or forensically, there are many new ways a person's communications can be observed without them knowing it.

Some of those same technologies, however, also create new avenues for communicating effectively. Are there ways to communicate without face-to-face meetings or dead drops? Perhaps communication modalities can be hidden in plain sight by hiding a critical signal in millions or even billions of other communications. Perhaps information could be transmitted in innovative ways via social media or across other channels of the Internet. The new generation of proliferated low earth orbit satellites for communication might be another means. It might be possible to embed important signals in other non-intelligence communications. Encryption, 5G, social media, and microelectronics could all play a role in addressing this mission challenge.

A useful metric in this challenge could be to create covert communications technology that could be used without two people coming within 10 miles of each other in a 'smart' city.

Mission Challenge 4: Find peer high value relocatable targets (HVRTs) within the window when they are exposed for critical operations, thereby enabling traditional kinetic or not kinetic attacks against them.

One of the ways peer adversaries threaten us today is through their power projection capabilities. We cannot bring our forces as close to their territory as we have in the past because their air defense systems, anti-ship weapons, ballistic and cruise missiles put our forces at risk. To make it harder for us to target those power projection systems, they are often relocatable, meaning they move to an operating location, set up, operate for as short a period as possible to perform their mission, then tear down and move. While it is the DoD's responsibility to strike those targets, the IC (particularly NSA, NGA, NRO and DIA) plays a critical role in finding them or enabling the DoD to find them quickly.

There are several things the IC can do to help. These include:

- Conducting continuous monitoring to establish pattern of life, identifying non-traditional signals and modalities that serve as a location tip, and developing models for movement capability.
- Using its own sensors during conflict to contribute to both wide-area sensing for indications and warning or localization of the threat, and high-resolution sensing to geo-locate and identify threats.
- Providing a conduit to commercial sensing capabilities that could supplement national sensing or provide alternative modalities that help with detection, identification, and geo-location in novel ways.

Closing this gap is likely to incorporate emerging technologies such as non-traditional data, new space and commercial GEOINT, and artificial intelligence.

A useful metric in this challenge could be to find high value relocatable targets within the time they are exposed by their operational window some percentage of the time.

Mission Challenge 5: Provide greater non-traditional and non-kinetic means for disabling critical targets.

Even if mission challenge 4 is solved, the problem posed by the high value relocatable targets used for power projection is still significant. While traditional kinetic attacks are likely to remain the mainstay of conflict operations, the complexity and interdependence of the systems, their manufacturing and design, the communications and networks they rely on to operate, their reliance on human operators and networked command

and control, and the supply chains used for their production all need to be better understood. This information could help the US understand vulnerabilities that could potentially be exploited.

The IC should partner more rigorously with DoD and industry to do the work needed during peacetime to enable those non-traditional attacks. The IC could use a variety of intelligence sources, both traditional and non-traditional, to identify key systems, to understand potential vectors for gaining access to them, and to identify exploits of various types that could be implemented using those access vectors. That work will likely draw on new technology in microelectronics, non-traditional data, 5G, and data analytics.

A useful metric in this challenge could be to provide the non-traditional and non-kinetic means for disabling 10 classes of critical targets, growing the list by 20% each year.

Conclusion

There are, of course, many other mission challenges facing the IC today. Even for these mission challenges, the specific goals described may not exactly match the boundaries between too easy and too hard that would most effectively drive progress. What is most important, though, is to provide focus and prioritization, to drive progress through mission impact, and to move away from high level strategies and technology roadmaps that contribute little to real progress. Solving these challenges will require the IC to be innovative, rather than to talk about innovation or set up activities to admire and study it, and they will force the IC to focus on real and measured progress in its practices and technologies.

Authors

Eliahu Niewood, Sc.D. is vice president, intelligence programs and cross-cutting capabilities at MITRE. In this role, Niewood leads MITRE's efforts to identify national security problems that require joint and multi-agency solutions and shape MITRE and the nation's response to those problems. He also leads MITRE in applying systems engineering, technology expertise, and innovation to help the intelligence and federal law enforcement communities leverage cutting-edge technology for mission success, integrate across agencies, and operate effectively in a dynamic environment.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's analytical workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the IC's analytical community in the post-COVID-19 world.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.