MITRE | Intelligence After Next

Intelligence After Next

SERIES # 22

INTELLIGENCE ON THE BATTLEFIELDS OF TOMORROW: THE CHALLENGE TO REMAIN RELEVANT

by Joseph Convery

Evolve or Risk Extinction

Intelligence production and dissemination constructs as they exist today are insufficient to ensure critical and often perishable information can be delivered to battlefield decision makers in time to maintain the operational advantage. While the essential requirement for intelligence analysis to be accurate and timely is not new, the speed of warfare continues to accelerate, placing new emphasis on sharing intelligence at the speed of need.

How information collected by the full array of Intelligence Community (IC) capabilities is ingested by the analytic corps, analyzed, placed in context, and shared for the operational user must evolve, driven by an increasing need for timeliness. Barring this, any human-in-the-loop ability to determine accuracy or place that information in context will fail, as information is delivered too late to impact the decision cycle.

The lessons being learned in the ongoing conflict in Ukraine may shed additional light on the approach and solutions required to meet the challenge of rapid information analysis and intelligence dissemination. While approaches may differ on ways to improve timeliness, there is no doubt that we must hasten the pace of this evolution and be ready to fight at an intensity and speed previously unseen in conventional warfare. Intelligence must be prepared to deliver critical information at the speed of need, or risk placing our commanders in a position where they are constantly reacting to the threat vice maintaining the initiative—a position historically associated with defeat. It is time for a true common intelligence ecosystem, one that:

- Is enabled by artificial intelligence/machine learning (AI/ML) technology
- Is common to all Combatant Commands
- Can support multi-theater operations
- Provides intelligence rapidly to the decision maker from anywhere in the world and simultaneously to all in need

Learning from the Crisis in Ukraine

The ongoing war in Ukraine offers both our allies and our adversaries lessons on the conduct of intelligence in modern warfare. The Ukrainians realized early in the conflict that a heavily structured intelligence and targeting process would not enable their ability to maintain the advantage over a larger, albeit more ponderous foe. Their intelligence capabilities—including their targeting structure—had to evolve under pressure to enable a rapid decision cycle. This evolution would ultimately be realized by both a digital transformation underpinning the conduct of intelligence and a local adaptation of NATO's Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) approach.

ISTAR in Ukraine

The ISTAR construct is the integrated capacity to acquire, process, exploit, and disseminate intelligence with the necessary level of detail and with sufficient speed to enable operational decisions and planning. The Ukrainians' training relationship with U.S. and NATO partners enabled their study of Western military intelligence doctrine and tradecraft, generating a nodal, forward-based approach to information sharing based on this concept.[1] ISTAR helps sustain the initiative should vertical stovepipes fail under the pressure of the contested physical and electromagnetic environment. Horizontal sharing of information between units in contact with the enemy sustains the fight.

Ukrainian forces adapted their intelligence collection, analysis and, perhaps most importantly, dissemination to meet immediate operational need. Using every resource at their disposal, Ukrainian intelligence pieced together a capability that would become a critical element of staving off the much larger Russian force. This was "guerrilla" intelligence at its finest and offered critical insights that would not otherwise have been available at that point in the conflict. The actions of Ukrainian forces to share critical information horizontally took precedence, focusing on the current fight while leaving the future fight to higher headquarters to foresee and plan.

The core of this strategy was captured in a past interview with a military officer at the Ukrainian Defense Ministry's Center for Innovation: "The biggest differences between the Russian army and Ukrainian army are the horizontal links between the units. We are winning mainly because we Ukrainians are naturally horizontal communicators."[2] The ability to communicate horizontally, bolstered by the ability to share information vertically (and thus ingest information from their allies), has been an essential element of their success to date. Key to achieving this level of integration has been the Ukrainians' underlying digital transformation.

Digital Transformation as a Component of Change

The need to share timely intelligence information under adverse conditions has driven a digital transformation of Ukrainian intelligence. This process would focus on AI/ML-based algorithms, leveraging both government and commercially available information to enable the fight. In their own words, "Our weapons are computers. Our bullets are information."[3] For the Ukrainians, a key element of this transformation has been the development of a common operational picture (COP) known as DELTA.[4]

The Ukrainian Center of Innovations and Defense Technology Development, under the leadership of Mykhailo Fedorov, currently Ukraine's Deputy Prime Minister for Innovation, Education, Science and Technology—Minister for Digital Transformation, grew out of Fedorov's prewar effort to move government functions across the civil sector to full digitalization. With the advent of the war, Fedorov's focus became evolving Ukrainian battlespace awareness capabilities. Improving situational awareness (including crowdsourced human intelligence and the exploitation of social media), developing AI/ML for identification and recognition of enemy targets, and strengthening intelligence capabilities through digital data analysis formed the core of this effort.

A conflict with China will press the limits of our ability to move intelligence fast enough into the right hands. We must adopt a new iteration of our own digital and cultural transformation to help analysis remain relevant.

The cloud-based DELTA COP facilitates the geospatial visualization and sharing of information across the multidomain battlespace. Accessible and distributed via a secure app, this tool simplifies critical battlespace awareness. It also integrates a wide range of information sources with the vertical and horizontal communications mediums necessary to connect intelligence from analyst to operator at all echelons of the fight, simultaneously. The benefit of crowdsourcing achieved by the Ukrainians could now be fully operationalized by crowd sharing.

Fedorov, in an August 9, 2022 interview with FRANCE 24, stated, "Delta provides a comprehensive real-time understanding of the battlefield and integrates information about the enemy from various sensors and sources, including intelligence on a digital map. Situational awareness tools, data centers, instant battlefield communication, cloud environments, and the massive use of drone armies instead of human armies are all investments in the army of the future. This will help to win on the battlefield and save the lives of Ukrainians."[5]

New Insights or Relearning Past Conclusions?

While certainly not a new lesson, the ability to see, understand, and act on the battlefield before your enemy can do so is an essential component of victory. For the Ukrainians, their digital transformation has, in part, made this possible. The deployment in 2022 of ISTAR units to eastern Ukraine, enabled with one product of their digital transformation (DELTA), is seen as an essential element of the success of Ukrainian intelligence.

As Western nations create constructs for sharing and rapidly accessing needed information via COPs, the lesson is clear. Data collected must be made rapidly available to those who would action that data, in a form they can use to quickly decide and act.[6] While simple in scope, this smart phone-based Ukrainian approach to a COP, born out of immediate operational need and enabled by constantly updated basic force disposition data, was enough when time was of the essence.

While many millions of dollars have been spent attempting to achieve lofty interoperability goals, sometimes a basic approach is the right approach on which to build. As we seek future interoperability with nontraditional mission partners, many with limited resources, a similar approach to information sharing might be in order. Could a variant of this approach be an answer as we seek nontraditional partnerships across the Indo-Pacific area of responsibility (AOR)?[7]

The success of Fedorov's approach has already been recognized around the world. It is easy to see how this construct could be employed in a potential China-Taiwan conflict. U.S. and allied engagement in this scenario will demand a similar approach to intelligence sharing across a range of disparate potential partners.[8] The key takeaway is that the need to "weaponize" intelligence rapidly and share this information across our partners, simultaneously at all levels of the fight, will be paramount to the success of future combat operations. However, as we adopt the construct of intelligence itself as a weapon, we must recognize the standards of quality and trustworthiness critical to sustain its effectiveness.

Understanding the Components of Change

Intelligence analysis is both art and science. Foundational to this process is the thoughtful review of multiple sources of information, separating fact from conjecture, and applying expert-level understanding to create a complete picture of the threat—normally from only a few pieces of the puzzle. All this must be accomplished with careful consideration, free of bias, and with the ever-present understanding that these findings may influence critical national security decisions. However, "careful consideration" often involves operationally significant periods of time—time that is critical at all levels of leadership and authority.

Today's continuum of warfare is more entangled than the distinct layers of action that previously framed our planning process. Now, the lines between what constitutes tactical, operational, and strategic intelligence begin to blur. What once mvy have been considered a tactical element of warfare may have strategic impact.[9] For example, intelligence collection detecting the launch of a theater ballistic missile—placed in context by analysis indicating it is associated with a unit and missile garrison that maintains hypersonic capabilities—quickly gains the attention of leaders at all levels. The information required must be accurate and rapidly disseminated. This begs the question of how intelligence analysis can rapidly meet critical demands while still adding to the value of expert human insight, when decisions must be made at various levels of authority and across the globe in minutes vice hours?

Preserving the impact of human-in-the-loop analysis may still be possible, but this will require an evolution in analysis and dissemination. Such evolution must be based on the rapid adoption of technology, analytic trust, and a degree of commonality necessary to create an ecosystem capable of breaking down the walls between the intelligence and operational communities. New tradecraft, methods, and tools must be created, adopted, and put into trusted use by the analytic corps across the common structure. Survivable communications mediums also will be necessary to simultaneously deliver intelligence to a broad spectrum of users, at the appropriate classification levels, to sites around the world. Leadership must then focus available funding and ensure sustainability for the common ecosystem.

Cultural Change

To address operational needs faster, analysts must think like the decision makers they intend to support. They must understand how to deliver information with just enough context to make their point, balancing their deeper insight with speed. The standard must not be what is potentially discernable over time, but what is operationally relevant and required at that moment in time. One way to help may be how a commander shares their intelligence requirements—or essential elements of information (EEI). The concept of crowd sharing could help.

Imagine a scenario where a commander and their operations officer, formulating their information needs, simply articulate the needs to an automated assistant (perhaps an ML-trained BOT). This specific request is machine translated into an EEI and posted to an intelligence dashboard, instantly accessible by the commander's intelligence staff (J2) as well as every lateral and higher intelligence organization focused on the fight. That EEI immediately becomes crowd shared. Specific organizations with production responsibility (RESPROD) for any element of that data are alerted to react. The results of their efforts are funneled back through an automated response queue for rapid review and "posting". Such an automated alert would share the information with the requestor while it simultaneously updates the common intelligence picture (CIP), where the information is visible across hierarchical boundaries. While this sounds wishful, the technology exists. Similar concepts are already being considered as developers wrestle with executive dashboards and CIP/ COP modernization constructs.

No small part of this paradigm shift will be fundamental change in the culture of analysis itself. Analysts are sometimes resistant to change. It is also true, to some degree, that the IC itself rewards this resistance. In today's culture, an analyst who briefs a senior military commander via PowerPoint presentation, or who has their position shared with the President via the Presidential Daily Brief process, will find their efforts lauded and likely rewarded. The culture must change to meet the modern demands of the consumer for rapid, succinct intelligence products that are quickly ingestible into the CIP and rapidly digestible by its human consumers.[10]

Where Can Technology Help?

At its core, the technical component of this evolution must start by helping to address the information challenge. Data (either too much or too little), "sense making" of that information, pairing the key elements of perishable data with essential context, and putting that information quickly in the hands of a decision maker is vital to maintain a commander's freedom of action. Again, this is not a new challenge for the IC, and one it has been working to improve consistent with advances in information technology. Conversely, limited resources, competing priorities, and lack of a long-term/program of record–level focus have challenged real progress in delivering on a common vision.

The element that technology must help solve today is time. Well-executed intelligence collection, strong analytic tradecraft, and well-managed information technology resources to manage and share that information can, with sufficient time, enable the IC to meet most information challenges. That time may no longer be available.

A peer-level conflict with China, which also is developing its own AI-enabled sense-making capabilities, will press the limits of our ability to move intelligence fast enough into the right hands.[11] We must adopt a new iteration of our own digital and cultural transformation to help analysis remain relevant. We must get faster, and AI-enabled intelligence processes must play a role. AI must fuel advanced analytic techniques to derive the full benefit of the ever-increasing amounts of raw data harvested for potential intelligence insights.

For example, foundational data sets maintained via arduous hours of expert level analytic update, could be supported by automated harvesting of basic data elements from traditionally trustworthy information sources, saving precious analytic time. AI-based tools lend themselves well to this function, and processes like this example could be readily adopted into analytic tradecraft.

While AI may offer a cultural challenge to some analysts reluctant to trust a machine overwriting their past inputs, a less time consuming quality control protocol may offer a relief to their concerns and prevent adversarial "data spoofing" from corrupting related data sets.

While there will never be enough time or analysts to perform complete quality control of every data element in the vast data sets maintained by the IC, AI can help maintain the overall soundness of these critical data sets. The need for the analytic corps to trust AI will be essential.

The element that technology must help solve today is time. We must get faster, and AI-enabled intelligence processes must play a role.

The imperative to make both structured data and unstructured data (e.g., the unstructured text of social media) rapidly accessible to the analyst has driven many companies to develop various opensource tools and big data analytics, many duplicative with separate resourcing and sustainment demands. Enabling analysts, through a range of select, common, and sustainable automated analytic tools, to derive conclusions from large amounts of information (often from disparate sources) will save time and potentially increase quality, but these conclusions must then be made rapidly available to a decision maker or targeting staff. To solve this problem, at least in part, we must fix the CIP.

The Common Intelligence Picture

A true CIP has been a long sought-after capability by both the IC and the operational consumer. Many combatant commands are now pursuing their own somewhat unique theater-oriented CIP capabilities, as the Joint Staff J2 continues to try and shape a more common outcome. A true CIP, one common to all commands and capable of supporting multi-theater operations, must be the bridge to carry intelligence rapidly to the decision maker (and into the COP), from anywhere in the world, and simultaneously to all in need. The individual activities of each Combatant Command J2 must be harnessed effectively to deliver one true CIP for all, with the necessary information to support the fight in any domain and across AOR boundaries.

AI/ML-based "smart" displays drawn from the CIP, at the immediate, round-the-clock disposal of military and national-level leadership, will play an important role as both analytic tradecraft and the IC's interface with its consumers evolve. Enabled by a true, holistic U.S. and allied CIP, a commander's smart display, tailored to the mission, AOR, and their personal priorities, can offer a way for that leader to receive what is most important, dig deeper if desired, and drive actions.

The complexity of the IC, various levels of classification, an 11 Combatant Command structure, Service equities, numerous independent development programs, and the costs associated with sustaining true commonality are often unsurmountable difficulties in fielding a common solution. The fundamental leadership required to direct commonality is split between the Director of National Intelligence and the Department of Defense (DoD) Under Secretary of Defense for Intelligence and Security (USDI&S). While efforts are underway within USDI&S to design the necessary information ecosystem, bringing all to the table for a common solution will be difficult—yet crucial—to our future warfighting capability.

Train Like You Fight, Just Fight Smarter

This well-proven concept must be a core element in the evolution of intelligence. We must condition both consumer and intelligence producer to a new way of doing business. However, the penchant to reward an analytic culture for PowerPoint presentations to senior leaders will make it difficult to drive this change.

Automation of basic tasks, a focus on rapid delivery of EEI vice "finished" intelligence products, the use of BOT-based intelligence agents to accept intelligence requirements and deliver EEI, and the continuous improvement of a truly common CIP may all be components of enabling intelligence at the speed of need. Technology could help enable needed cultural change while reducing analytic burden. In this scenario:

- Analysts would no longer be required to spend hours preparing briefings. They would continue to create foundational data, aided by algorithms constantly reviewing both commercial and classified data to discover updates to specific data fields essential to their area of responsibility. These data fields would be automatically updated, saving analysts thousands of hours to maintain an overwhelming number of facility-centric records. Order of Battle records, force disposition movements, and other transient data requirements could also be automatically updated and set up for rapid analytic review, ensuring currency with appropriate but rapid analytic oversight. This would allow analysts to concentrate their limited hours on drawing valuable context from changes that would otherwise go unseen.
- AI-based algorithms would constantly scour open-source intelligence threads, looking for key words and phrases, correlating similar data, topic clustering, and prioritizing data sets for analytic review. They also could create open-source intelligence reports, quickly appraised by an analyst, and rapidly consumed into the CIP, further amplifying intelligence being presented to a consumer in crisis mode.
- Intelligence feeds into the Watch and simultaneously the CIP could be dissected and prioritized, broken into geospatially correlated data bites, compared against a commander's evolving set of EEI, and cued up for the commander's review based on the need for immediate warning. That information could be pushed as a specific alert or made available for presentation via the leader's BOT, with this same information rapidly ingested into the CIP for consideration by the complete staff.
- There would be less frequent briefings and fewer finished intelligence analysis products. Need would drive information access, and audible feedback to the BOT would drive additional intelligence requirements or operational intelligence direction. The intelligence analyst would begin to think like their consumer, build indirect relationships with each key consumer via automated feedback mechanisms, and improve the speed, quality, and relevance of information sharing.

While some of this may seem fanciful, it is not the limits of technology but rather vision, leadership commitment, and resource management that pose the greatest challenge to making it a reality.

Stop Admiring the Problem and Evolve

Time is of the essence. We must be ready to fight at an intensity and speed previously unseen in conventional warfare. Intelligence must be prepared to deliver critical information at the speed of need, or we risk placing our commanders in a position where they are constantly reacting to the threat, vice exploiting initiative. From this position, it is difficult to win.

For the IC to be ready, it will be imperative for DoD and IC leadership to:

- **Settle on the common intelligence ecosystem required to meet this challenge.** While intelligence technology modernization will be a key foundation for this ecosystem, the effort must go much further,

directing the common tools, architecture, and even the basic changes in analytic tradecraft and culture required to ensure success. The essential philosophy must be to enforce commonality and interoperability. We must share a true CIP or risk moving to war with commanders viewing the battlefield with different sight pictures.

- **Enforce the common intelligence ecosystem across the defense intelligence enterprise through swift budgetary decisions, fiscal oversight, and—if required—budgetary penalty.** The IC's most senior leaders, with the authority to direct and enforce commonality, must take responsibility for these actions. Debating tool after tool and spending limited research and development dollars on competing tools for different consumers with common needs, are time and resource sinks we can no longer afford.

Both analyst and operator must trust that the intelligence provided, and acted on, is the best possible in both the time and information constraints of each situation. While failures based on information inaccuracies can never be completely avoided in the "fog of war", victories will far outweigh failure if intelligence can be delivered with the speed necessary to enable a commander's freedom of action. This challenge must be met by the intelligence resources of the United States and our allies before our potential enemies can benefit from this same paradigm.

You May Say I'm a Dreamer, But I'm Not the Only One …

Change is hard; overcoming culturally entrenched processes is harder. We must be driven from our comfort zone to evolve or risk extinction of the value offered by human analytic insight in understanding enemy actions in war. We need a well-structured, comprehensive program to speed intelligence dissemination, one that reaches across the IC and our operational consumers. If we don't, we will remain locked in a piecemeal, uncoordinated, and resource draining approach that will continuously evade our primary objective —that of getting the information to commanders with sufficient time to allow them to stay one step ahead of the adversary.

The shepherds of this process must be those bearing the leadership and resource responsibilities to select the best ideas, decide on a common approach, and enforce that approach across the entire enterprise. This must be the mandate of our most senior IC and DoD leadership, and it must have teeth. Technology is not the limiting factor to our success; rather it is a parochial approach to this evolution, lacking true unity of purpose, that remains our greatest challenge. Business as usual will not enable the transition quickly enough to meet the coming storm.

References

1. The Ukraine began development of its initial constructs for ISTAR early in their training relationship with NATO. IPLEMENTATION OF ISTAR IN UKRAINIAN ARMED FORCES, by Y. Pashchuk and Y. Salnyk, 4 May 2013. This paper directly discusses the need to implement NATO ISTAR concepts to modernize Ukrainian battlefield intelligence capabilities.
2. Julian Borger, 'Our Weapons are computers': Ukrainian Coders Aim to Gain Battlefield Advantage, The Guardian, December 18, 2022.
3. Julian Borger, 'Our Weapons are computers': Ukrainian Coders Aim to Gain Battlefield Advantage, The Guardian, December 18, 2022.
4. Under development since 2016, The Ministry of Defense of Ukraine first formally presented the DELTA situational awareness system to NATO's Consultation, Command and Control Organization in December 2022, stating that "DELTA is a vivid example of the success of the cooperation between NATO and the Ukraine." English translation of article from Ukrainska Pravda based on Ukrainian Government News Release, Undefined Author, 20 Dec 2022
5. France 24 Television Interview with Mykhailo Fedorov, Ukrainian Vice Prime Minister, December 18, 2022.
6. The core interoperability challenges between existing and new NATO partner nations were identified as, "technological disparities, command and control, doctrinal differences, and resource gaps". Enhancing Interoperability: The Foundation for effective NATO operations, Dr. James Darleth, 16 June 2015
7. A good example of U.S. regional Interoperability investment in this critical AOR has been the over $475 million invested since 2016 into Pacific Regional interoperability via the Maritime Security Initiative, which provides a maritime common operating picture and enhances the maritime operational capabilities of seven ASEAN member states. FACT SHEET, SECRETARY AUSTIN'S NINTH TRIP TO THE INDO-PACIFIC REGION, Defense.Gov, 2023
8. The Australian Army, for example, has already begun the process of integrating the lessons learned in Ukraine into their doctrine. This will impact how they fight as a key U.S. partner in the Pacific. Beyond Twitter: The Real Lessons from the Battle for Kyiv for the Australian Army. By Brad Gilbert, 26 May 2022
9. "Given that there are no fixed limits or boundaries between the levels of war, how does the student differentiate between them when strategic assets have tactical applications and when tactical actions have intended and unintended strategic consequences?". The Levels of War as Levels of Analysis, Military Review, Army University Press, Andrew S. Harvey, PhD, Dec 2021
10. "The dispersed battlefield will become ever harder to manage with humans who simply cannot make decisions fast enough. Military and political decisionmakers will not find it any easier to order humans into harm's way, especially as the range and lethality of weaponry increases. The United States will need to develop and deploy superior AI technology to keep up with great-power competitors and other potential adversaries who are investing heavily in the technology... If AI applications help the United States prevail, both the military and civilian culture will be forced to adapt." Considering Military Culture and Values When Adopting AI, Rand, Commentary by Marta Keep, 22 June 2020
11. "AI will be a force multiplier for the People's Liberation Army (PLA)…The widespread adoption of AI technology to enhance PLA decision-making appears to be realizable in the medium term rather than the short term (that is, within ten rather than five years)". How China Leverages Artificial Intelligence for Military Decision-making, The National Bureau of Asian Research, by Zi Yang 26 Sep 2023

Author

Joseph Convery is a senior intelligence advisor at MITRE and recently served as Chief Engineer for the MITRE Intelligence Center's Command Priorities Department. He is a former U.S. Army intelligence officer and a retired government civilian analyst and collector with over 40 years of experience across the Intelligence Community.

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 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 Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

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

MAY 2024