MILITARY INTELLIGENCE PROFESSIONAL BULLETIN

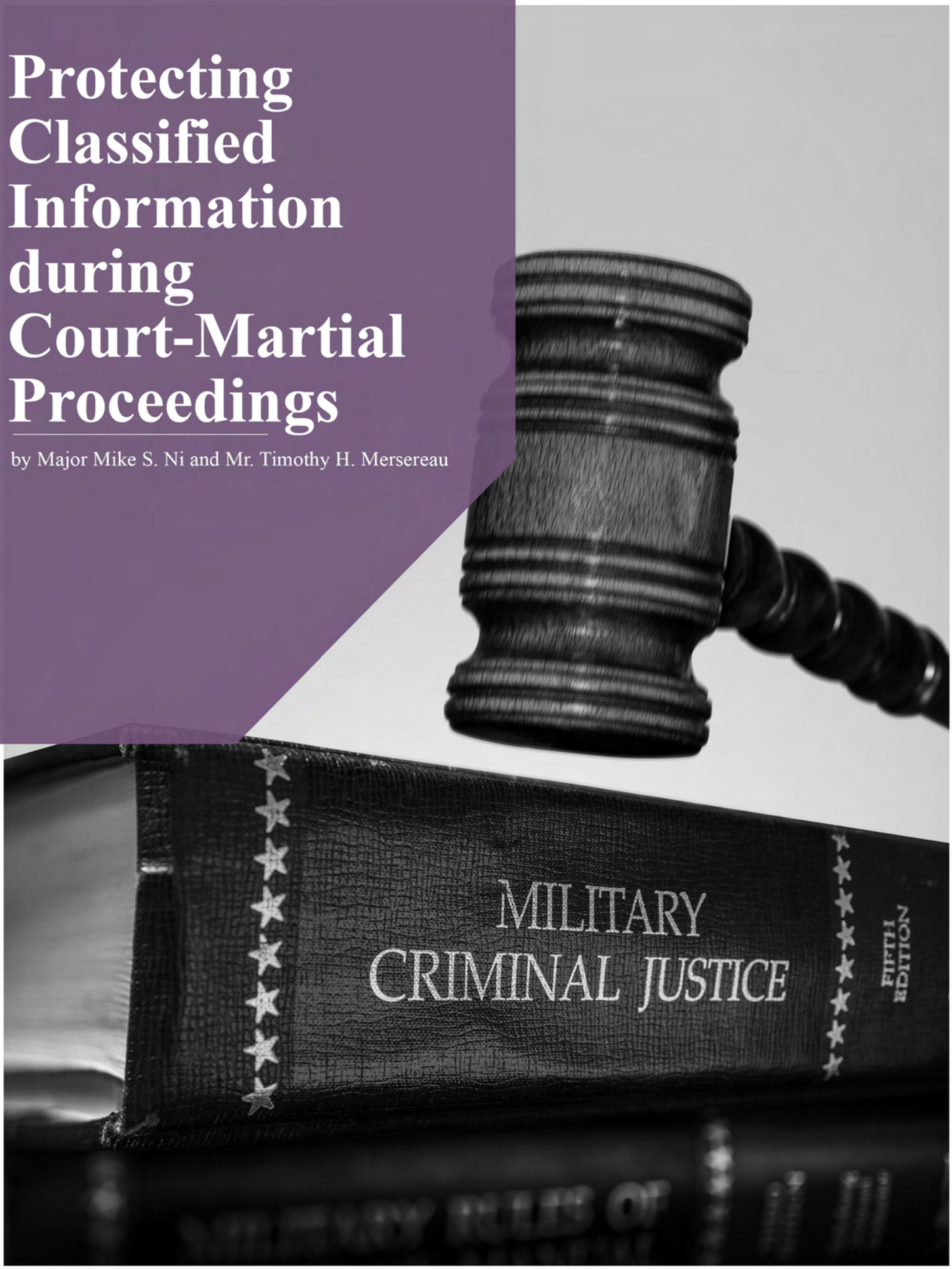
JULY – DECEMBER 2022 COLLECTION

MI PROFESSIONAL BULLETIN
July—December 2022

CONTENTS

Protecting Classified Information during Court-Martial Proceedings

by Major Mike S. Ni and Mr. Timothy H. Mersereau



United States* v. *Bergdahl

A U.S. Army judge is considering how to handle thousands of documents, many of them classified, that will be part of the case against a soldier who walked off an outpost in Afghanistan.

—CBS News, January 12, 2016

Lawyers for U.S. Army Sergeant Bowe Bergdahl…should have access to classified material to prepare his defense, a military appeals court has ruled….His defense asked for access to 300,000 pages of classified documents and on Feb. 2 a military judge ruled that the defense should have access to all classified information that the government may offer into evidence at trial. The U.S. government appealed the ruling saying the judge had abused his discretion….The Army Court of Criminal Appeals said in its ruling that the military judge had not granted the defense unfettered access to classified information, but only to material in the context of trial discovery.

—Reuters, May 1, 2016

Introduction

On 30 June 2009, United States Army SGT Robert B. Bergdahl walked away from his observation post in Paktika Province, Afghanistan. He was subsequently captured by the Taliban and held until his release on 31 May 2014.[1] What followed was a near 2-year court-martial in which SGT Bergdahl pled guilty to desertion with intent to shirk hazardous duty and misbehavior before the enemy. These were violations of Uniform Code of Military Justice Article 85, *Desertion*, and Article 99, *Misbehavior before the Enemy*.

Evidence in court hearings revealed that thousands of Soldiers, Sailors, Airmen, and Marines conducted an intensive 45-day search for SGT Bergdahl, which resulted in numerous U.S. casualties. Included in such evidence was a substantial amount of classified national security information (or classified information) which, if disclosed to the public, would reasonably cause serious or grave damage to our national security.

United States v. *Bergdahl* is just one example of the complexities of introducing classified information in the courtroom. The intent of this article is to assist military intelligence and security professionals in understanding and navigating the processes of disclosing, and especially protecting, classified information in court-martial proceedings. The article will describe court rules regarding classified information and will identify the roles of notable individuals in the court-martial process, including those with the authorization to determine disclosure.

> "Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information."

Overview of Military Rule of Evidence 505

Military Rule of Evidence 505 in the *Manual for Courts-Martial United States* is the primary reference concerning classified information in a military trial. It states, "Classified information must be protected from disclosure if disclosure would be detrimental to national security. Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information."[2] As such, people involved in a court-martial cannot request a waiver of Department of Defense rules that protect classified information. If these rules conflict with the rights of the defendant, the protection of classified information takes precedence. Neither the defense counsel nor the government prosecutors have the authority to disclose. Only the head of the executive or military department or government agency that produced the information can authorize the disclosure of classified information.[3]

Key Personnel in Protecting Classified Information in the Court-Martial Process

The following personnel are responsible for protecting classified information in the court-martial process:

- Article 32 hearing officer.
- Military judge.
- Government counsel.
- Defense counsel.
- Security managers.
- Court reporter.
- Sensitive compartmented information (SCI) program manager.
- Bailiffs and military police.

Article 32 Hearing Officer. When significant offenses are alleged against a Soldier, the court-martial process likely begins at an Article 32 preliminary hearing, which determines whether sufficient information exists to support the allegations for the government to proceed to a general court-martial.[4]

Military Judge. Following preferral of charges (i.e., when a Soldier is officially charged with a crime), the case is assigned to a military judge. Everyone in the courtroom can address the military judge as "sir" or "ma'am," consistent with traditional military courtesy, or as "Your Honor." As the head of the court proceedings, the military judge has the additional burden of ensuring that everyone involved upholds the responsibility of all military personnel to protect classified information.

Government Counsel. Government counsel, equivalent to prosecutors, consists of judge advocates from the Office of the Staff Judge Advocate servicing the court-martial convening authority, normally a commanding general. In addition to prosecuting the case, the government counsel is responsible for most administrative matters to bring the case to trial. This includes ensuring proper procedures are in place to present classified information consistent with AR 380-5, *Army Information Security Program*.

Defense Counsel. The defense counsel includes judge advocates from the Trial Defense Service and, at the defendant's expense, may include civilian counsel. Like the government counsel, the defense counsel also must adhere to all rules for accessing classified information and presenting classified evidence.

Security Managers. If it is likely that the court-martial process will involve classified information, the convening authority appoints three security managers—one to advise the military judge, one for the government counsel, and one for defense counsel. Security managers should be an integral part of their respective groups; however, the security managers' sole function is to protect classified information, not to give advice or participate in the trial's strategy in any way. The security managers will work together when necessary to protect classified information; however, they must never exchange any trial tactics, strategy, or other information they have observed about the case. To protect classified information, it is essential that security managers earn the trust of those they advise. This includes counsels' trust that security managers will not share any information that could harm the case in any way.

- ✦ Security managers ensure that everyone they advise has the correct security clearance to view needed classified information. Security managers may assist in obtaining the proper clearance and indoctrinations by coordinating with the appropriate personnel security manager or special security officer.
- ✦ Security managers should assist in obtaining access badges needed to enter the facilities where the relevant classified information is stored.
- ✦ Security managers should coordinate with the appropriate G-6/S-6 personnel to obtain access to the SECRET Internet Protocol Router Network and with the appropriate special security officer for access to the Joint Worldwide Intelligence Communications System.
- ✦ Security managers should coordinate with G-2/S-2 personnel to obtain a workspace for court members to view and analyze classified information. Government counsel may also assist. Security managers will ensure the workspace has the locks, safes, systems, and other features required for the classification level of the documents that court members will view.
- ✦ Although any court member with the proper clearance can obtain a courier card, the security manager should carry the classified information in order to limit the possibility of security violations or incidents.
- ✦ Security managers must be involved in each counsel's process of preparing witnesses for their testimony. They can provide valuable advice to lawyers and witnesses so that they avoid inadvertent disclosure of classified information in an open (unclassified) hearing. Security managers can advise how to keep presentations unclassified when closed classified hearings are not reasonably possible and how to instruct witnesses to ensure they provide relevant information without revealing the classified sources and methods used to obtain the

Glossary of Military Courtroom Terms

Article 32 Hearing. This is the Uniform Code of Military Justice equivalent of a grand jury. In the Article 32 hearing, the government makes its case on whether there should be a trial. The hearing officer of the Article 32 is not a judge. After listening to both sides of the argument, the hearing officer makes a recommendation to the convening authority on the type of court martial, if any.

Article 39A Hearing. Article 39A hearings are procedural hearings that occur before the trial in order to prepare for it. Among many other purposes, parties may agree how they will provide classified information to the defense or how they will present it in the trial.

Government Claim of Privilege. Government agencies are not required to release their classified information to the defense. They can withhold it if they deem it essential to protecting national security information.

Ex Parte Discussion. Typically, if the judge communicates with one side, he must include the other side in the communication. In limited instances, the judge may talk with one side without the other's knowledge. For example, if the government team notifies the court that an agency has claimed privilege (not to allow use of its classified information), that conversation should occur without the defense's knowledge in an ex parte discussion.

In Camera Review. In Latin, *in camera* means "in a chamber." When the judge reviews documents in his office (chambers), or in private, without discussion with the government or defense, he is conducting an in camera review.

information. *Such advice should NOT include telling counsel or witnesses to alter their testimony*. For example, the counsel might believe that a military map with detailed overlays is useful to describe the situation of the crime; however, if the overlays contain classified code words, route names, or other sensitive information, then the security manager should suggest ways to describe the situation without mentioning classified details that add nothing substantive to the testimony.

- ✦ Security managers assist the people they advise with reporting and mitigation if a spillage or unauthorized disclosure occurs.

Court Reporter. The court reporter is a key player in the information flow within the courtroom and therefore is exceedingly important to protect classified information. The court reporter will have a second recording apparatus for "red" proceedings (secret) and a third device for "yellow" proceedings (top secret). The court reporter ensures the audio and video feeds to the overflow spectator area are cut before any red or yellow proceedings.

SCI Program Manager. The SCI program manager approves the establishment of a temporary SCI facility (T–SCIF) at the courthouse if it is required.

Bailiffs and Military Police. Bailiffs are usually a member of the defendant's unit and senior in rank to the defendant (but not less than a sergeant first class). Their tasks are to call the court to attention, obtain witnesses when called to testify, attend to administrative errands during the trial, and maintain the general decorum of the courtroom.[5] Bailiffs are critical to managing access to the courtroom or the T–SCIF and must therefore have a security clearance that matches the classification of the information being presented. Bailiffs do not need to be in the courtroom during the presentation of classified information; instead, they should remain immediately outside the courtroom door to control access. The role of military police is to secure the outer perimeter of the court area and control access to the proceedings, if necessary.

Application of the Military Rule of Evidence 505

Military Rule of Evidence 505 is the government counsel's responsibility to contact any or all government agencies that may have information relevant to the case. The government counsel must segregate classified information and review it for relevancy. All government agencies are obligated to provide their information; however, they are not obligated to allow the information to be used in court or shown to the defense. When dealing with classified information originating from outside the Army, those individuals involved in the case must remember that merely having the appropriate security clearance does not give anyone carte blanche to see all the classified products, even if the products are relevant to the case.

The government counsel also has the responsibility to provide evidence to the defense. The defense counsel normally has access to any or all information relevant to the case to best represent their client and to ensure that due process is upheld. Before the release of information to the defense, Military Rule of Evidence 505 requires that the government review all classified information pertaining to the case to determine *only that information which directly applies* before its release to the defense counsel. The government counsel reports to the military judge what will not be released. While the defense counsel may not always agree with the government's decision to withhold certain classified information, it is essential to preserve the need-to-know principle of information security.

A gavel rests on the judge's bench in the courtroom of the 39th **Air Base Wing legal office, November 14, 2019, at Incirlik Air Base, Turkey. The defendant was being tried for sexual assault. The verdict was not guilty**[6] **(U.S. Air Force photo by SSgt. Joshua Magbanua)**

The release authority is the head of the executive or military department of the government agency concerned. This applies to the "right of originator to refuse presentation." The originator decides whether to allow the release of its classified information to the defense counsel or to allow its use in court. The originator might decide not to release the information at all. The originator makes its decision based on national security and is not required to defend its position. The originator's privilege is the "government claim of privilege." If an originator invokes the privilege, the government must notify the military judge. If the originator does not want the public or the defense counsel to know about its claim of privilege, the government does not have permission to notify them.

When invoking government claim of privilege, the originator may still allow the court to use a written summary of the classified information. For example, imagine the government counsel identified a top secret document produced by the Central Intelligence Agency (CIA). The CIA may preclude the document's release because it will reveal sources and methods to those with no need-to-know. The CIA and government counsel may collaborate to provide a secret document summarizing only those parts relevant to the case. Before the defense counsel receives the document, the military judge reviews the original document and the summary to ensure they only include relevant information.

It is also important for the government counsel to build and use a roster to track who has access to classified information in the court-martial process. This roster is useful to control entry in classified court proceedings.

Open and Classified Hearings

The general principle is for both the government and the defense to strive to make the hearings unclassified and accessible (open) to the public. Closed hearings should occur only when there is no alternative because of the need to present classified information. There are three types of hearings: open, secret, and top secret and SCI.

Open Hearings. An open hearing occurs at the unclassified level and is open to the public and the press. The court may provide overflow viewing areas, if necessary. During these hearings, security managers should sit in a place where they are readily accessible to those they support, i.e., military judge, government counsel, and defense counsel.

Secret Hearings. A secret hearing, also known as a "red" or collateral hearing, occurs after security managers have ensured the facility is adequate for secret discussions. If the hearing "goes red," it is necessary to cut all transmissions, such as the audio feed to the spectator overflow room. The court reporter should only record on a recording device authorized for secret information. Essential personnel identified ahead of time may remain present. Bailiffs will escort all nonessential personnel from the courtroom. For this type of hearing, the court should not provide overflow viewing areas in the event someone inadvertently leaves the audio or video feeds turned on. During the classified proceeding, bailiffs should stand outside the courtroom door and control all access, such as the calling of witnesses. These restrictions disrupt the transparency and flow of the proceeding; therefore, the use of secret hearings should be minimal and planned for ahead of time.

Top Secret and SCI Hearings. Hearings for top secret information and for SCI, known as "yellow," have similar procedures. (In some instances, the SCI information may have a classification lower than top secret.) However, courtrooms are rarely adequate to serve as a T–SCIF. Before the trial, the SCI program manager should work with the government counsel to identify an available T–SCIF. Again, it is important to identify authorized participants ahead of time and record their names on an access roster. Before the trial, it also important to ensure the lawyers and other court members have the relevant security clearances. In some instances, individuals may need to be "read on" for specific SCI programs. However, there will likely not be time to clear panel members (aka, jurors). Therefore, in addition to maintaining a fair and impartial panel, security clearances are an important consideration when selecting panel members if either side intends to introduce top secret information and/or SCI.

Best Practices

The primary best practices to protect classified information during a court-martial are—

- Rehearse.
- Be prepared to establish a T–SCIF.
- Prepare for inadvertent disclosure in an open hearing.

Rehearse. It is essential to practice the procedures for presenting classified information ahead of time, including a rehearsal for both "red" and "yellow" procedures. Key members of government and defense counsels, security managers, court reporter, bailiffs, and military police should all be present.

Be Prepared to Establish a T–SCIF. If it is not feasible to hold the hearing in an existing SCIF, it may be beneficial to establish a T–SCIF at or near the courthouse.

Prepare for Inadvertent Disclosure in an Open Hearing. If someone inadvertently divulges classified information in an open hearing, security managers should have a mechanism to notify their respective teams with a visual but discreet signal. We must be discreet so that we do not draw attention from the public and the press, indicating to them that they may have just heard sensitive information; this is part of the mitigation. When the military judge receives the signal, they should stop the proceeding, call a recess, permit the security managers to explain what occurred, and convert to a closed classified hearing, if necessary. The incident report should identify the unauthorized disclosure through normal reporting channels.

Conclusion

With our conditioning as military intelligence and security professionals, we are often quick to say, "You can't do that," or in the case of courts-martial, "You can't discuss classified testimony outside the SCIF." However, with the application of expert knowledge and some creativity, you can establish a secure environment for virtually any testimony. The real art of security is when we combine imagination with our extensive knowledge of the regulations. In our daily work, this

approach allows us to accomplish the operational mission without compromising security. In the courtroom, we have an inherent responsibility to national security to ensure everyone presents classified evidence securely and appropriately.

American jurisprudence requires a transparent justice system. However, it must maintain a balance between ensuring a defendant's due process and protecting national security by not allowing the unauthorized disclosure of classified information. *United States* v. *Bergdahl* is a prime example of the defense counsel seeking thousands of pages of classified documents, arguing that they were necessary to satisfactorily defend their client and ultimately obtain a fair trial. While not every case may be as high profile as the Bergdahl case, scrutiny and caution are paramount when classified information is present.

Epigraph

"Classified documents prompt debate in Bowe Bergdahl case," CBS News, January 12, 2016, https://www.cbsnews.com/news/bowe-bergdahl-case-classified-documents-prompt-debate/.

"Bergdahl defense can access classified information, court rules," Reuters, May 1, 2016, https://www.reuters.com/article/uk-usa-defense-bergdahl-idUKKCN0XS1I9.

Endnotes

1. *United States* v. *Bergdahl*, No. 19-0406 (C.A.A.F. 27 August 2020).

2. Joint Service Committee on Military Justice, *Manual for Courts-Martial United States* (Washington, DC, 2019), III-24.

3. Ibid., III-24–III-29.

4. Article 32, Uniform Code of Military Justice, and Rule for Courts-Martial 405.

5. Rule for Courts-Martial 501(c) and U.S. Army Trial Judiciary, *Rules of Practice before Army Courts-Martial* (1 January 2019), 24, 30–31.

6. SSgt Joshua Magbanua, "Back in session: courts-martial return to Incirlik," Incirlik Air Base website, November 15, 2019, https://www.incirlik.af.mil/News/Article-Display/Article/2017423/back-in-session-courts-martial-return-to-incirlik/.

References

Department of Defense (DoD). DoD Manual 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*. Washington, DC, February 24, 2012, incorporating change 2, July 28, 2020.

Department of the Army. Army Regulation (AR) 380-5, *Army Information Security Program*. Washington, DC: U.S. Government Publishing Office (GPO), 22 October 2019.

Department of the Army. AR 380-28, *Army Sensitive Compartmented Information Security Program*. Washington, DC: U.S. GPO, 13 August 2018.

MAJ Mike Ni is an administrative law attorney in the Office of the Staff Judge Advocate for the U.S. Army Intelligence and Security Command (INSCOM).

Mr. Tim Mersereau is the Deputy G-2 at INSCOM, and he served as security advisor to the judge during the court-martial hearings and trial of the United States *v.* Bergdahl.

Paratroopers of the 82nd Airborne Division and other airborne units drift toward the drop zone near La Fière Bridge in Normandy, France, June 9, 2019. The paratroopers conducted the airborne operation as a way of honoring the paratroopers who jumped on June 6, 1944.
(U.S. Army photo by SFC Daneil Wallace)

Tactical Counterintelligence in Support of Large-Scale Combat Operations

by a contributor from the Southwest Region,
U.S. Army Counterintelligence Command

Company E, 16th Infantry, 1st Infantry Division, lands on Omaha Beach, Normandy, France, during one of the first waves to assault, 6–7 June 1944.
(Photo courtesy of Center of Military History)

How can I fight worth a damn without counterintelligence people around me?

—COL (later GEN) John. H. Michaelis
Commander, 27th Infantry, at the Pusan perimeter, Korean War

Introduction

For the greater part of the past two decades, the U.S. military has engaged in counterinsurgency and counterterrorism operations. This is transitioning to a greater strategic approach that focuses on large-scale combat operations against a peer or near-peer threat. The significant shift in priorities has created a need to update Army doctrine, education, training, and other areas, including tactical Army counterintelligence (CI) and its mission to detect, identify, assess, counter, exploit, and/or neutralize foreign intelligence entities at home and abroad.

By looking at the successes and challenges of the U.S. Army's Counter Intelligence Corps (CIC) during World War II, we can learn how to reform present-day Army CI in anticipation of operating as part of a broader joint force. Army CI will need to conduct CI activities that enable the Army to help penetrate and dis-integrate enemy antiaccess and area denial systems during large-scale combat operations, as described in Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2038*.[1]

This article will describe various tactical tasks that the CIC conducted during World War II and will recommend ways to reform present-day Army CI when preparing for large-scale combat operations.

The Beginnings of Modern Counterintelligence

Modern counterintelligence began in World War I when the Army established a corps of counterintelligence specialists, the Corps of Intelligence Police (CIP). In 1942, the CIP became the Counter Intelligence Corps. Counterintelligence units deployed worldwide to protect U.S. and Allied forces fighting on foreign soil and operating in an environment exploited by saboteurs and collaborators.[2]

Historical Tasks of the Counter Intelligence Corps

Formed in 1942, the CIC played a significant role during World War II, in both the European and Pacific theaters. CIC agents provided tactical intelligence about the enemy from captured documents, interrogations of captured troops, and civilian sources. They also protected military installations and staging areas, located enemy agents, and acted to counter stay-behind networks. The following are eight examples of their tactical tasks:

- Screening.
- Document exploitation (DOCEX).
- Raids against adversarial intelligence officers and their agents.
- Counter-espionage with indigenous resistance groups.
- CI collections.
- Counter-subversion.
- Counter-sabotage.
- CI threat awareness.

Screening. During World War II, commanders required CIC special agents to screen refugees, internally displaced persons, U.S. citizens (as requested), and local national hires to both protect U.S. forces and acquire information of CI value. Individual screening played a significant role in the identification of Axis intelligence and Axis powers' "stay-behind agents."[3]

One of the most important screening operations occurred in 1945 during the CIC's deployment in the Pacific theater during the Luzon Campaign in the Philippines.[4] Individuals of Japanese descent easily blended into the local populace, thus providing opportunities to remain undetected in a foreign country. Japanese intelligence would employ agents from a variety of demographics to conduct espionage, sabotage, and subversive operations. This resulted in an increased CI threat throughout the archipelago. In response, the CIC established screening points to identify those working on behalf of the Japanese or their ally (Axis) intelligence services. Throughout the Luzon Campaign, the CIC apprehended more than 1,200 "collaborators, puppet officials, enemy nationals, and Kempeitai agents [Japanese secret police comparable to the German Gestapo]."[5]

Document Exploitation. During World War II, the CIC played an important role in DOCEX. The most significant and influential task the CIC conducted during their assignment to the Western Task Force, North Africa Campaign, was capturing personnel and records from the German Armistice Commission. The commission was a commercial entity with the clandestine responsibility to ship raw materials to Nazi war industries.[6] Throughout World War II, Allied forces primarily controlled Casablanca, Morocco, but at one time, Axis forces occupied the city. This provided a rich environment for "stay-behind" agents and a wide spectrum of intelligence activities. In 1942, Allied troops deployed to Casablanca, where CIC agents conducted a series of DOCEX operations. This effort identified local nationals who were providing support or resources to the Axis intelligence services. The buildings that the German Armistice Commission had occupied were a primary target for DOCEX. Two CIC agents uncovered an intelligence windfall that led to the identification of several Italian and German intelligence sources in Morocco.[7]

Raids against Adversarial Intelligence Officers and Their Agents. Although CIC agents conducted raids against adversarial foreign intelligence service officers and their agents at all levels of war, including the notable arrests of the "Butcher of Dachau" and "Axis Sally," it was at the tactical level that the CIC's raids provided a direct advantage to U.S. forces. During the Allied campaign in Italy, just south of the Apennine Mountains, the 305th CIC captured more than 200 German

agents, numerous subversive Italians, clandestine equipment, and explosives traversing what the CIC had dubbed the "Spy Highway." These efforts ensured that Axis forces did not return from their deployment to the U.S. Fifth Army's area of responsibility, making it difficult for the Axis powers to defend Italy from an Allied liberation.[8]

Counter-Espionage with Indigenous Resistance Groups. The CIC's work with indigenous resistance groups in France, Italy, Belgium, and Hungary proved to be invaluable because the resistance groups had a far better understanding of the culture and threat unique to those locations.

One notable example of the CIC's important role occurred before the commencement of D-Day when CIC elements from the 101st and 82nd Airborne Divisions landed by parachute and glider at Normandy.[9] After initially securing their objective, a nearby communications tower, the surviving CIC agents linked up with members of the French Resistance who conducted combined raids against many of the Nazis' stay-behind agents, including those who were on the CIC's most wanted list.[10] The French Resistance also provided the CIC with "the location of an ammunition dump, names of other resistance members in the area, and disposition of enemy troops within the vicinity."[11] The CIC's actions against Axis intelligence undoubtedly provided a tactical advantage to Allied troops who would later liberate France and continue eastward toward Germany.

Counterintelligence Collections. The CIC conducted a variety of activities known as CI collections. Historically, a clear delineation between CI collection and human intelligence (HUMINT) collection did not exist during World War II. There was only CI collection. Collection requirements that addressed both adversarial perception and how foreign intelligence services collect information from U.S. forces were within the realm of CI collections. Today, this is not the case. In the years following World War II and the Cold War Era, the Army codified the collection of adversarial information from human sources into the military occupational specialty for HUMINT collector operations.[12]

During World War II, CIC agents ran internal networks throughout Army formations, primarily driven by fear rather than valid CI collection requirements. CI informants were positioned in almost every Army unit. The ratio of informants to a CIC agent totaled 1 per every 30 Soldiers, which was a massive undertaking. The emplacement of CI informants was most effective as a means of deterrence, dissuading Soldiers from succumbing to recruitment attempts by Axis intelligence agents.[13]

The overall efficacy of the CIC in this area was negligible. The causes were a lack of valid collection requirements, an inability to collect because of ongoing open investigations and the lack of deconfliction, the vast scope of sources-to-agent ratio within the program, and known collection activities of foreign intelligence services against friendly forces. The resulting criticism of the CIC's informant networks was substantial and nearly led to the disbandment of the CIC.[14]

Counter-Subversion. The Axis powers, primarily Germany, intended to use subversion for strategic objectives. This was evident through the Axis powers' denial of the Allied powers' use of a neutral power infrastructure. Routinely, American tactical commanders tasked their respective CIC detachments to counter Axis subversion of an established government. Iceland, while historically neutral, was concerned about its participation in the war. This hesitation stemmed from the citizens' fear of mandatory requirements to participate with, or at least identify with, either Axis or Allied partners.[15]

The British and American presence in Iceland was to establish and protect logistical lines of effort through the Atlantic region. Despite this presence, the Nazis increased their already considerable efforts to cultivate support among Icelanders and form a potential fifth column as they had done in Norway. Upon learning of this information, the CIC took action by emplacing more than 100 CI agents in Iceland, a country with a population then of only 120,000. This facilitated counter-subversion efforts, thereby ensuring Allied access to the strategically important

Axis Sally

Axis Sally's real name was Mildred Gillars. In 1935, she moved from the United States to Berlin, Germany, and took a job as an English teacher. Soon thereafter, she accepted a job as an announcer with Radio Berlin and signed an oath of allegiance to Nazi Germany. During the war, Radio Berlin broadcast her program "Home Sweet Home" throughout the European theater and the United States with a goal to undermine the morale of American Soldiers.

The Federal Bureau of Investigation and U.S. Department of Justice classified her broadcasts as psychological warfare but could not apprehend Gillars until the war ended. She managed to evade authorities until March 1946, when agents of the 970th CIC located and arrested her. In 1949, she finally went to trial in the United States and was sentenced to 10 to 30 years in prison and fined $10,000. After 12 years, she was paroled.[16]

Counter Intelligence Corps arrests Axis Sally, 14 March 1946. (U.S. Army photo)

island en route to the European continent. This effort came with many challenges, such as language barriers, a lack of cultural awareness, and a significant equipment deficiency, until the intervention of U.S. Army MG Charles Bonesteel, Commanding General of Iceland Base Command. Once the CIC leveraged the familial ties of their Icelandic agents, the CIC was able to identify covert Nazi operatives working throughout the island. These actions resulted in basing agreements for tactical Allied units, which later proved instrumental in the liberation of Europe.[17]

Counter-Sabotage. Aside from enemy agents engaging in espionage or subversion, the CIC had to counter foreign intelligence services' attempts to sabotage both the U.S. Army operations and the stability of the newly established Allied government in areas liberated from Axis forces.[18]

In March 1945, Soldiers from GEN George Patton's Third Army were planning to cross the Rhine River near the German town of Oppenheim. CIC detachments throughout the region garnered intelligence information that outlined the Germans' plan to use underwater swimmers to sabotage bridge crossings. Using information collaboration and CIC reporting, infantry, engineer, and military police units were able to ensure freedom of maneuver for the Third Army. They identified and captured the German underwater swimmers and transferred them to the CIC for interrogation. Effective CIC operations contributed to the success of GEN Patton and the Third Army's push into Germany.[19]

Counterintelligence Threat Awareness. The Battle of the Bulge was perhaps the most notable instance of CIC's threat awareness efforts. In 1944, German Lieutenant Colonel Otto Skorzeny, a noted German commando leader, orchestrated the training of 150 German soldiers. This training provided information on United States culture, language, and military customs in order to prepare these German soldiers for undetected infiltration into United States Army units. The intent of the operation was to collect information, incite confusion, and conduct sabotage within Allied units throughout the region of Ardennes.[20]

Skorzeny's commando unit, the *Einheit Stielau*, was not successful thanks to the CI threat awareness program, which was educating U.S. Soldiers on indicators for the possibility of enemy infiltration in an area of CI interest. The 9th Army's CIC detachment apprehended 35 German Soldiers during the first 15 days of December 1944. During an interrogation, one German soldier revealed information about Operation Greif, also known as Skorzeny's plan for infiltration. The CIC quickly placed additional emphasis on their CI threat awareness efforts, resulting in the detection of all but 10 to 12 members of Skorzeny's unit.[21]

Operation Greif

After the discovery of Operation Greif and the infiltration of English-speaking German commandos, American Soldiers devised security questions for checkpoint guards to ask, questions that they thought only a fellow American could answer. Categories included state capitals, baseball, and movie stars, and could be as specific as, "What's the name of the President's dog?" The goal was to avoid accidentally detaining American Soldiers and, of course, to capture enemy spies. High-level American officers were not immune to mistakes. BG Bruce Clark was once arrested for a half hour after he gave a wrong answer about the Chicago Cubs.[22]

Learning from the Past to Prepare for the Future

Based on the CIC's experiences in World War II, we can reform present-day Army CI to prepare for large-scale combat operations. For these recommendations, the following assumptions apply:

- All Army CI units will be realigned under a central CI command—the Army CI Command.
- Maneuver elements may be unable to assist Army CI in completion of their duties during large-scale combat operations because of competing mission requirements and resource constraints.

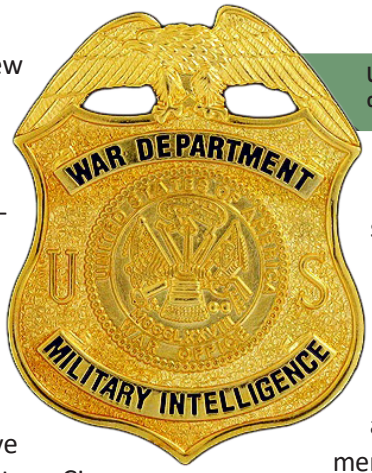
Underdeveloped tactical CI doctrine significantly affected CIC operations. The lack of doctrine delayed the implementation of an effective CI organization by at least a year and a half. The CIC units within this region also faced challenges with insufficiently trained personnel and no supporting tactical CI units. Currently, peer and near-peer threats pursue any means to reduce or impair the U.S. military's reaction time.[23]

Recommendation: Developing and implementing tactical CI doctrine are imperative to retaining the tactical CI advantage. Based on historical CI information and disparities in current CI doctrine, the Army should—

- Revise and disseminate tactical CI doctrine across classified and unclassified mediums.
- Develop and disseminate a comprehensive guideline to assist agents throughout the process of counter-espionage, counter-subversion, counter-sabotage, DOCEX, CI screening, insider threat identification and incident processing, and CI awareness training.
- Ensure the U.S. Army Intelligence Center of Excellence (USAICoE) collaborates with the Army CI Command when developing and revising tactical CI doctrine.
- Establish training courses, as resources and bandwidth allow, that implement updated information, concepts, or processes.

CIC agents received insufficient linguistic, cultural, and combat training before deployment. The areas most affected were CI screening, DOCEX, CI collections, and counter-espionage in coordination with the host nation. After the CIC's

campaign in North Africa, an after-action review revealed substantial gaps in training and overall understanding of the host nation's language and culture. The CIC realized this training was integral to mission success and sought to improve agents' overall understanding by sending agents to the Berlitz language schools for 13 weeks of intensive training before deployment.[24]



U.S. Army War Department military intelligence badge carried by CIC agents in World War II.

Recommendation: As a consolidated and modernized command, Army CI could improve language capabilities among current and future CI agents through an established pipeline, coded billets, or inclusion of language in institutional or functional training venues. Army CI agents fluent in common Eastern European languages, including Russian, would enable an Army CI Command to effectively liaise and communicate with allied and/or coalition partners during shaping operations of a campaign plan.

Combat arms basic training would provide advanced skills to engage in close combat with enemy forces. This would augment CI agents' basic combat training. Possessing both advanced combat training and proficient CI skills, Army CI units would be better suited to work in concert with combat arms units, rather than rely on combat arms units for mission success.

The CIC ran informant networks throughout many Army units without the use of validated CI collection requirements.[25] Army CI operates using validated CI collection requirements in accordance with Executive Order 12333, *United States Intelligence Activities*, dated 1981. Although Executive Order 12333 bans internal informant networks, in order to protect the rights of U.S. citizens, Army CI agents have the potential to identify sources of information through refugees and internally displaced persons.

Recommendation: CI agents could accomplish the identification of source information through CI screenings or debriefings, as demonstrated during U.S. Army operations in the Middle East. CI agents could also ask individuals with valuable intelligence information to return to areas of tactical CI importance to obtain and covertly relay information of CI value. This approach would provide real-time information and actionable intelligence to tactical commanders.

Much like the CIC during World War II, today's Army CI missions are misunderstood. During World War II, commanders and their respective G-2s did not fully understand the mission, responsibilities, and capability of the CIC. A commander's or staff's lack of understanding and underutilization of CI capabilities placed the unit at a considerable disadvantage.[26]

Recommendation: Establishing a clearly defined command and support relationship between a newly formed Army CI Command and U.S. Army Forces Command (FORSCOM) would be a critical step for ensuring tactical forces employ CI agents in a mutually beneficial capacity.

While assigned to tactical units, CI agents in a garrison environment should belong to the Army CI Command. This would provide the ability to receive tactical CI training and augment strategic CI missions before deploying in support of FORSCOM units. Using this approach, agents would receive training to execute tactical CI functions and possess the knowledge to leverage strategic CI assets to counter the activities of a foreign intelligence entity on the battlefield.

As a part of the newly established Army CI Command, deploying units would request a CI support team from a hypothetical expeditionary CI battalion. A memorandum of agreement with the Army CI Command would identify details of this support, outlining a direct support relationship. This would mitigate concerns FORSCOM units may have regarding their ability to assign priorities to tactical CI agents, while enabling the CI agents to operate under the legal authority and technical control of the Army CI Command. This would minimize risk to tactical commanders, ensure tactical CI agents are producing quality work on behalf of their supported commands, and enable the Army CI Command to shift strategic CI assets efficiently to foreign intelligence entity threats identified at the tactical level. Army CI units, in direct support to Special Forces units, would have the ability to conduct CI activities with host-nation resistance groups, which would be permitted as part of Special Forces' unconventional warfare core tasks.

Tactical commanders were not educated on how the CIC could enhance their operations. This included how the CIC could enable target acquisition, identify targets within the area of operations, and answer priority intelligence requirements. Initial reporting indicated that some unit commanders did not understand the CIC mission.[27]

Recommendation: As a means to bridge the gap in understanding CI mission and capabilities, a hypothetical expeditionary CI battalion, subordinate to the Army CI Command, could provide a CI officer to serve as the supported FORSCOM unit's CI coordinating authority or S/G-2X. Additionally, the Army CI Command could—

- Establish a website designed to educate the force on the differences between the Army CI Command, Criminal Investigations Command, and HUMINT as a specialty.
- Serve as a repository for annual Threat Awareness and Reporting Program training.

- ✦ Publish press releases to dissuade foreign intelligence entities, terrorist organizations, and insider threats while reassuring friendly forces of Army CI's ability to protect them.
- ✦ Provide vignettes detailing historical Army CI successes.
- ✦ Educate the force on how CI could enable the success of tactical operations.

Official after-action reviews concluded that CIC units' training and equipment were inadequate and their missions ill defined. Unlike most of the conventional Army, the CIC did not have an established organization and table of equipment. Tactical Army CI experiences in Afghanistan and Iraq have shown CI agents to be almost completely reliant on the support of combat arms patrols in order to conduct their CI operations. In the event of large-scale combat operations, this framework may not allow for a collaborative approach unless it is included in doctrine or codified before the engagement.[28]

Recommendation: An additional approach to tactical CI's current dependency on external organizations would be the creation of an organic tactical CI element subordinate to the Army CI Command (previously referred to as an expeditionary CI battalion). This element would have adequate resources, equipment, and training to conduct tactical CI operations without completely relying on combat support and combat services.

CIC agents assigned to the field armies lacked a clear delineation of responsibilities between strategic and tactical CI tasks. This led to the agents frequently being overwhelmed and overworked. The agents were responsible for national security investigations and tactical counter-subversion operations in support of forward-moving forces. This oversaturation was apparent during Operation Cobra in Northern France, when the rapid pace of the war forced CIC agents to leave investigations partially completed in order to focus on more pressing tactical CI tasks, such as counter-sabotage.[29]

Recommendation: The Army CI Command should be responsible for the full spectrum of CI activities and be obligated to delineate strategic and tactical tasks of subordinate units/commands. This would enable the augmentation of tactical CI agents to those fulfilling tactical CI activities. This would also apply to those agents fulfilling strategic CI activities requiring augmentation.

Way Ahead

As the U.S. Army continues to shift focus from counterterrorism and counterinsurgency to large-scale combat operations, Army CI needs to transition efficiently to the changing demands of conflict. This analysis of the CIC's successes and challenges during World War II demonstrates the need to establish a contemporary Army CI Command capable of—

- ✦ Organically providing training, equipment, management, and oversight of all Army CI special agents.
- ✦ Providing FORSCOM and Special Operations Command CI agents in a direct support role.
- ✦ Enabling Army CI units to work autonomously to accomplish their assigned CI tasks.
- ✦ Developing readily accessible, current tactical CI doctrine in coordination with USAICoE and TRADOC.

This approach would ensure both tactical and strategic leaders have the necessary CI support to accomplish their unique mission throughout operations and when countering peer and near-peer adversarial foreign intelligence services.

Epigraph

James L. Gilbert, John Patrick Finnegan, and Ann Bray, *In the Shadow of the Sphinx: A History of Army Counterintelligence* (Washington, DC: Department of the Army, 2005), 112.

Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2038 (Fort Eustis, VA: TRADOC, 6 October 2018), vi–viii.

2. "History of Army Counterintelligence," National Capital Region Field Office, accessed December 13, 2021, https://www.nec.belvoir.army.mil/902dNCRFO/history.asp.

3. James L. Gilbert, John Patrick Finnegan, and Ann Bray, *In the Shadow of the Sphinx: A History of Army Counterintelligence* (Washington, DC: Department of the Army, 2005), 54.

4. Ibid., 66.

5. Ibid.

6. Ian Sayer and Douglas Botting, *America's Secret Army: The Untold Story of the Counter Intelligence Corps* (London: Franklin Watts, 1989), 103.

7. Ibid., 106.

8. Department of the Army, *Counter Intelligence Corps, History and Mission in World War II* (Fort Holabird, MD: Counter Intelligence Corps School, 1951), 32.

9. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 42.

10. Ibid., 43.

11. Ibid.

12. Department of the Army, *Counter Intelligence Corps*, 58.

13. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 26.

14.Ibid., 32.

15. Sayer and Botting, *America's Secret Army*, 51.

16. Lori S. Tagg, "Counter Intelligence Corps Arrests Axis Sally, 14 march 1946," U.S. Army Worldwide News, March 13, 2015, https://www.army.mil/article/144444/counter_intelligence_corps_arrests_axis_sally_14_march_1946.

17. Sayer and Botting, *America's Secret Army*, 49–51, 54–56.

18. Department of the Army, *Counter Intelligence Corps*, 33.

19. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 52.

20. Ibid., 49–53.

21. Ibid.

22. Gina Dimuro, "Operation Greif: When German Commandos Were Trained to Act American and Wreak Total Havoc behind Enemy Lines," All That's Interesting, March 11, 2019, https://allthatsinteresting.com/operation-greif.

23. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 60.

24. Ibid., 30–32.

25. Ibid., 26.

26. Sayer and Botting, *America's Secret Army*, 23–24.

27. Ibid.

28. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 75–77; and Department of the Army, *Counter Intelligence Corps*, 21.

29. Gilbert, Finnegan, and Bray, *Shadow of the Sphinx*, 43–44.

The Army Counterintelligence Command conducts proactive counterintelligence activities to detect, identify, assess, and counter, neutralize or exploit foreign intelligence entities and insider threats in order to protect Army and designated Department of Defense forces, information and technologies worldwide.

BATTLE DAMAGE ASSESSMENT: IT DOESN'T HAVE TO BE THAT HARD

by
Captain
Justin R.
Beverly

U.S. Army Soldiers of C Company, 2-28th Infantry Regiment, 172nd Infantry Brigade, Task Force Black Hawk, prepare to move to another location, November 9, 2011, outside Combat Outpost (COP) Margah, Paktika province, Afghanistan. The Soldiers are evaluating the damage after a failed attack to COP Margah, November 8. (U.S. Army photo by SPC David Barnes)

Introduction

In the *FY20 Mission Command Training in Large-Scale Combat Operations Mission Command Training Program (MCTP) Key Observations*, the Center for Army Lessons Learned staff identified a number of consistent issues across the divisions and corps that had conducted warfighter exercises throughout the year. One key intelligence observation was that the intelligence staff had failed to effectively obtain and evaluate battle damage assessment (BDA) in order to influence the commander's understanding of the battlefield. The comments in the report were direct and to the point:

> ***Observation: The G-2 process for obtaining and evaluating BDA did not effectively influence the commander's understanding or ability to visualize the battlespace, which resulted in subordinate brigades' inability to maintain momentum.[1]***
>
> ***Discussion: The G-2 targeting section did not have an effective process for collecting BDA reports from data sources or tracking the number of destroyed systems across the battlespace. The BDA was not effective in delivering an assessment of relative combat effective strength to inform the commander, planners, or targeting cycle. The lack of a combat-effective strength assessment of enemy forces in the briefings and targeting working group resulted in an incomplete understanding of the enemy's remaining capability and intent.[2]***

These comments are likely not surprising to anyone who has been in an intelligence (G-2) section for a warfighter exercise, especially those who have been in the analysis and control element (ACE). However, it is disheartening to see that the Army as an institution still struggles with this problem, and it is particularly disheartening for those who have seen a G-2 section succeed at this task. For that reason, this article offers an effective and proven methodology for conducting BDA in a warfighter exercise.

Battle Damage Assessment Management during Warfighter Exercise 18-04

During warfighter exercise 18-04, the 1st Infantry Division G-2 targeting cell was responsible for tracking and reporting BDA to the commander and the rest of the division staff. The cell was understaffed because of manning shortfalls and other training requirements—with one captain, the officer in charge, and one specialist (military occupational specialty [MOS] 35F, Intelligence Analyst). Another specialist (MOS 35F) from outside the organization augmented the cell during the exercise but was not available to train on processes and procedures before the warfighter exercise. As a result, the cell needed a simple, easily trainable and maintainable method to conduct this critical task. This would allow all members of the cell to maintain the system while not detracting from the cell's other critical task—identifying targets for the division's shaping efforts.

Effective BDA management involves three tasks that are interconnected but require their own specific considerations:

- The cell's reporting must be accurate, accessible, and sufficient without being overwhelming.
- The cell must conduct effective analysis, requiring an advanced knowledge of the battlefield.
- The cell must disseminate the information effectively across the staff and to the commander in order to facilitate effective planning and decision making.

However, this all begins in the planning process, with an understanding of the enemy and a method to track BDA.

Planning

Before any operation and during the military decision-making process, the targeting cell has a number of duties, the primary one being development of the high-value target list (HVTL) for approval and development into the high-payoff target list. However, the key task relating to BDA is developing an understanding of enemy forces and a method for tracking enemy forces as they are destroyed or damaged.

An understanding of the enemy is important both in HVTL development and in BDA planning. Targeting analysts work with the fusion cell during intelligence preparation of the battlefield, especially during step 3, evaluate the threat, and step 4, determine threat courses of action. Targeting analysts should focus their efforts on understanding the threat characteristic factors, including weapon systems capabilities. This will help them to understand both what forces the enemy has on the battlefield and how those forces can accomplish enemy objectives. They should also understand the enemy courses of action that the fusion cell develops. This will feed into an understanding of the battlefield that allows them to make the assessments required during the engagement.

In order to track BDA, the 1st Infantry Division G-2 targeting cell developed a Microsoft Excel spreadsheet to organize enemy force information in an orderly manner and to maintain a running estimate of their strength. Figure 1, on the next page, shows a sample section of this spreadsheet.

The BDA spreadsheet is a data-centric representation of the fusion cell's development of the enemy's most likely course of action. It is displayed by doctrinal enemy zones—disruption zone, battle zone, and support zone—each with its own tab. As the fusion cell develops and refines the most likely course of action, the targeting cell arrays the forces in their zones within the spreadsheet. The enemy order of battle provides the unit types and associated equipment and strengths. When the analyst updates the number destroyed, the formulas in the spreadsheet automatically update the Remaining column and the CE% column (combat effectiveness percentage), along with the Battle Zone Total section at the bottom of the spreadsheet. In this way, the targeting cell always has access

to an up-to-the-second estimate of enemy strength by zone, unit, and equipment type. The spreadsheet also populates a final tab, which displays the overall totals for the battlefield. (Additional details about the spreadsheet are in the Analysis section of this article.)

Key Recommendations for Planning:

- Develop a BDA-tracking spreadsheet that displays enemy key equipment by number, unit, and zone.
- Ensure that the spreadsheet incorporates formulas to auto-update all numbers when the analyst updates the number destroyed.

BATTLE ZONE

		SYSTEM	STARTING STRENGTH	DESTROYED	REMAINING	CE%
831st AR BDE	1st BN (AR)	T-62	31	27	4	13%
		BTR-60	5	2	3	60%
	2nd BN (AR)	T-62	31	4	27	87%
		BTR-60	5	0	5	100%
	3rd BN (MECH)	BMP-2	31	4	27	87%
		BTR-60	5	3	2	40%
	FA BN	2S3	18	4	14	78%
		Zoopark-1	2	0	2	100%
452nd FA RGT	1st BN	2S3	18	7	11	61%
		BTR-60	3	1	2	67%
	2nd BN	2S1	18	1	17	94%
		BTR-60	3	0	3	100%
	3rd BN	BM-21	18	5	13	72%
		BTR-60	3	2	1	33%
	TAB	Zoopark-1	2	0	2	100%

BATTLE ZONE TOTAL

SYSTEM	STARTING STRENGTH	DESTROYED	REMAINING	CE%
T-62	62	31	31	50%
BMP-2	31	4	27	87%
BTR-60	24	8	16	67%
2S3	18	7	11	61%
2S1	18	1	17	94%
BM-21	18	5	13	72%
Zoopark-1	4	0	4	100%

Graphic adapted from original provided by author

Figure 1. The BDA spreadsheet displays enemy forces equipment by unit and zone across the battlefield

Receiving Reports

Effective reporting requires coordination and guidance on exactly what the cell expects and where and when the cell expects to receive the information. This calls for a primary, alternate, contingency, and emergency (PACE) plan for reports, as well as reporting criteria. Effective reporting also requires a feedback loop from subordinate units to ensure that the picture of the enemy remains consistent across echelons.

The PACE plan can use whatever methodology suits the organization and its standard operating procedures. The 1st Infantry Division used a BDA chat group as the primary means for all BDA reporting. The G-2 targeting standard operating procedure for all subordinate and enabling elements published the name of the chat group. The cell also coordinated directly with the tactical air control party (TACP) to receive BDA reporting from all close air support (CAS), strike coordination and reconnaissance, and air interdiction missions. This led to some double reporting, as a ground unit would report a target destroyed by CAS, just to have the TACP report the same target later in their 24-hour rollup.

While the primary method of reporting was the observer or the shooter (as long as it was an observed or direct fire mission), the G-2 collection management and dissemination cell also provided reports. This called for specific information requirements aimed at identifying damaged or destroyed enemy targets on the battlefield. Even though collection management and dissemination reporting was generally the secondary method, it often confirmed prior reporting and occasionally provided BDA that had not been previously reported.

Reporting criteria will vary by mission type and echelon, but the standard operating procedure must publish this information. In early exercises, the G-2 targeting cell failed to develop criteria and was overwhelmed with reports of destroyed motorcycles, jeeps, and even individual rifles. While these are important at the platoon or company level, the division and corps are generally more concerned with tanks, air defense radars, and artillery systems. As a result, the cell developed reporting criteria that limited reporting to weapon systems annotated on the official BDA tracker and dictated a size, activity, location, and time format. If in doubt, subordinate elements should report any BDA not on the tracker and let the targeting cell make the decision whether to report it higher. This significantly reduced the "noise" in the reporting, allowing the cell to focus on what was important, but did not completely shut out the opportunity for judgment calls from subordinate elements.

The check on the reporting was in the daily intelligence synchronization meetings. The targeting cell would brief the latest BDA and always asked for feedback from participants. This allowed them to raise concerns, and at least once, this resulted in identifying an error in the targeting cell's analysis. This method ensured that all stakeholders had the opportunity to review the BDA before it was briefed to the commander and that every unit had a common understanding of the enemy's current strength.

Key Recommendations for Receiving Reports:

- Publish the standard operating procedure, as well as the PACE plan and reporting criteria, to subordinate units.
- Include BDA-specific information requirements in collection plans.
- Coordinate with the TACP for regular reporting from CAS, strike coordination and reconnaissance, and air interdiction missions.
- Include BDA feedback in regular intelligence synchronization meetings.

Analysis

Analysis is the step that transforms data from reports into information, and eventually intelligence. This is the key to enabling the staff planning and the commander's decision making, rather than reporting raw numbers that, alone, are meaningless. Using a detailed knowledge of the battlefield and both quantitative and qualitative assessments, analysts can provide the "so what" behind the reports they have collected from all sources.

The process begins by determining the accuracy of the report. This requires analysts who understand the battlefield. It is extremely important to have analysts with a well-developed situational understanding that allows them to make an accurate assessment of the report's veracity. For example, if a brigade combat team destroys five tanks with CAS, the brigade combat team will likely report the damage. However, the TACP will also likely make the same report in the next 24-hour rollup. A high-quality analyst can review the reports, including information on the time and location of the strike, and recognize the duplicate reporting. After making the decision to use a report, the analyst enters the information into the BDA tracking spreadsheet.

The spreadsheet does much of the quantitative analysis. For example, when the analyst updates the number in the Destroyed column (of a given vehicle), the spreadsheet automatically produces a combat effectiveness percentage for the unit and the zone. The analyst can conclude, "27 artillery tubes remain in the battle zone, leaving them at 31% strength on artillery pieces." This is a simple method to quantitatively describe the effects on the battlefield.

Putting these details into more qualitative terms requires a deeper understanding of the enemy equipment and its use. Analysts must be intimately familiar with enemy equipment

capabilities and the ways they affect the battlefield. One technique is to maintain a "smart book" that includes the Worldwide Equipment Guide pages for every high-value target as well as current versions of the BDA tracker and other targeting products, as required. This gives the analysts a quick reference to provide information on the impact and significance of the BDA. Most of the time this will not take much explanation because commanders inherently understand what enemy equipment is important and why, but sometimes it helps to clarify the importance of certain items.

The next level of analysis comes from understanding how the equipment fits into the target system—for example, disabling an entire integrated air defense system by hitting a key command and control node or radar. That requires a target system analysis, which is a part of mission analysis and is used in developing the HVTL. Target system analysis is critical to both BDA and the broader targeting process but is beyond the scope of this article.

Key Recommendations for Analysis:

- Assign an analyst with an in-depth understanding of the battlefield and a keen situational awareness to track BDA.
- Use automated tools (spreadsheets) to perform quantitative analysis.
- Maintain references and conduct a thorough target system analysis and mission analysis to enable a qualitative analysis.
- Always focus on the "so what," rather than briefing simple numbers or percentages, to enable the commander's decision making.

Dissemination

Having all this data and analysis does no good if the information stays in the ACE, or worse, within the targeting cell. Dissemination is the critical step to getting the information into the hands of those who need to know—the broader targeting team, the plans section, the operations section, and the commander.

Ultimately, how the ACE distributes BDA will depend on the unit's standard operating procedures and battle rhythm. At a minimum, BDA must be included in the daily graphic intelligence summary (GRINTSUM), the intelligence synchronization, and the slide decks for the targeting working group and targeting decision board. It can also feed the assessments working group, and if the commander has a daily "fighting product" or "placemat," it should be in the intelligence section of that product.

Determining exactly what information and how much of it to display will also depend on the unit and the audience. Some will want a PowerPoint slide with enemy icons. Others may want the entire spreadsheet. At the 1st Infantry Division, the commander was happy with a summary page of the spreadsheet, which displayed enemy strengths and the combat effectiveness percentage by battalion-sized element and specialized equipment, and total numbers by zone (Figure 2).

The ACE published this product in the GRINTSUM and the commander's daily placemat. The ACE also published it in slide decks for the targeting working group, the targeting decision board, and the intelligence synchronization. At the targeting working group and targeting decision board, it was an important input to the meetings because it assessed the effectiveness of the previous day's shaping operations and it focused planners' and decision makers' efforts on the most significant units remaining.

BATTLE ZONE						
UNIT	LOCATION	INF BNs	AR BNs	FIRES SYSTEMS	AD SYSTEMS	CE%
862 MECH BDE	PL Betty	2	1	8	8	50%
844 REC BDE	PL Annie	2	1	9	9	50%
865 FA BDE	PL Betty	0	0	36	0	50%
384 FA BDE	PL Annie	0	0	36	0	50%
382 FA BDE	PL Betty	0	0	38	0	55%
802 MECH BDE	N of OBJ Denver	2	1	10	9	60%
803 MECH BDE	PL Annie	2	1	8	9	60%
804 AR BDE	PL Betty	1	2	12	5	65%

Graphic adapted from original provided by author

Figure 2. BDA rollup for the battle zones

Key Recommendations for Dissemination:

- ✦ Determine what battle rhythm events and products require BDA and the best way to present the information.
- ✦ Present enough information to enable decisions, without overwhelming the audience with data.
- ✦ Ensure that assessments, including BDA, are driving the targeting process.

Conclusion

As the Center for Army Lessons Learned identified in its FY20 report, tracking BDA requires a well-thought-out plan. There must be a tracking method, effective analysis, and an effective means of disseminating the critical information. All of these capabilities exist organically within an ACE and a targeting cell. The FY20 report's observation about collecting and evaluating BDA concluded that—

> ***This is a training issue. The Mission Command Training Program (MCTP) can provide training on ways to collect, report, and track BDA geospatially using analog and digital products.***[3]

This article attempts to remedy that training issue. While describing one of many effective techniques, and every situation will require nuanced methods, this proven methodology offers a baseline from which units can build their standard operating procedures. If they do that, they will be well on their way to providing information that the commander needs to effectively shape the battlefield and win our Nation's wars.

Endnotes

1. Department of the Army, *FY20 Mission Command Training in Large-Scale Combat Operations Mission Command Training Program (MCTP) Key Observations* (Fort Leavenworth, KS: Center for Army Lessons Learned, October 2020), 16.

2. Ibid.

3. Ibid.

CPT Justin Beverly is training as a foreign area officer. He has held leadership and staff positions at every level from platoon to division, including G-2 target officer in the 1st Infantry Division. He has published online articles with From the Green Notebook and The Field Grade Leader.

Intelligence Support to Protection: An Approach

by Major Paul Ward

Introduction

Across multiple division and theater-level exercises, the 2nd Infantry Division's intelligence warfighting function is called upon to provide intelligence support to both targeting and protection. Intelligence support to targeting is a mission essential task for the 2nd Infantry Division G-2; however, intelligence support to protection is not. G-2s need to adopt an approach that will help the commander to understand and visualize the operational environment, provide the required support to staff action across all time horizons, and drive the unit's targeting *and* protection processes. This article describes the 2nd Infantry Division G-2's approach to supporting both processes.

Background

Targeting and protection are operationalized through their respective working groups. They result in key outputs that enable staff action (in the case of targeting) and unit and staff action (in the case of protection) at the current operations, future operations, and future plans cells across the time horizons for multiple warfighting functions.

Targeting. Army doctrine provides that "a targeting methodology is a rational and iterative process that methodically analyzes, prioritizes, and assigns assets against targets systematically to create those effects that will contribute to achieving the commander's objectives."[1] The targeting process is operationalized through the targeting working group and decision boards and drives a unit's lethal and nonlethal operations. Two key outputs of the targeting process are the high-value target list (HVTL) and the high-payoff target list (HPTL).

Protection. Army doctrine states that "protection is an important contributor to operational reach. Commanders anticipate how enemy actions and environmental factors might disrupt operations and then determine the protection capabilities required to maintain sufficient reach….The protection warfighting function helps commanders maintain their force's integrity and combat power."[2] Protection is operationalized through the protection working group and helps the commander understand and visualize the risks to the mission and to the force. Key products that support and enable the commander's decision-making process are the critical asset list, defended asset list, and prioritized protection list.

Working Groups. The relationship between the targeting working group and protection working group is an important factor for leaders to understand. Through these two working groups, the staff aids the commander's understanding and visualization of the operational environment, generates decision space, and provides options to allocate and apportion combat power to achieve the end state. Outputs from the targeting working group support the commander's allocation of combat power and effects to remove adversary capabilities from the battlefield. Outputs from the protection working group support the commander's allocation of combat power and effects to mitigate risks to the mission and to the force.

The Role of the Situation Template

The 2nd Infantry Division G-2 relied on the situation template (SITEMP) as the primary product that supported visualization of the adversary and operational environment for the staff integrating elements (referred to as the boards, bureaus, centers, cells, and working groups, or B2C2WGs) for both targeting and protection. Using the division's operational framework, the SITEMP framed the adversary in the division's deep, close, and support areas. A standardized SITEMP that action officers could carry into the B2C2WGs, across multiple command nodes, enabled the G-2 to maintain a consistent analytic narrative and yielded efficiencies given the analytic and manpower constraints with which the 2nd Infantry Division G-2 was operating. Although the SITEMP was an effective product to frame the adversary and operational environment, it was also the responsibility of G-2 action officers to frame the adversary to enable a situational understanding for various staff sections and warfighting functions. Requirements to support the targeting process framed the primary model that the G-2 used across multiple exercises. However, it became apparent that the G-2 needed a slightly different model for intelligence support to protection.

Intelligence Support to Targeting: The Methodology

The 2nd Infantry Division G-2 supported division targeting by focusing on the nature of the adversary, what the adversary was doing, and why the adversary was doing it. How would the adversary employ combat power and lethal effects to accomplish its end state? Given the terrain and friendly combat power and effects, where would the adversary exploit opportunities? Those questions generally focused on the adversary in the division deep and close areas.

With the adversary executing offensive operations, we used the following framework: If the enemy wants to accomplish (end state), then where is the decisive point in the battle?

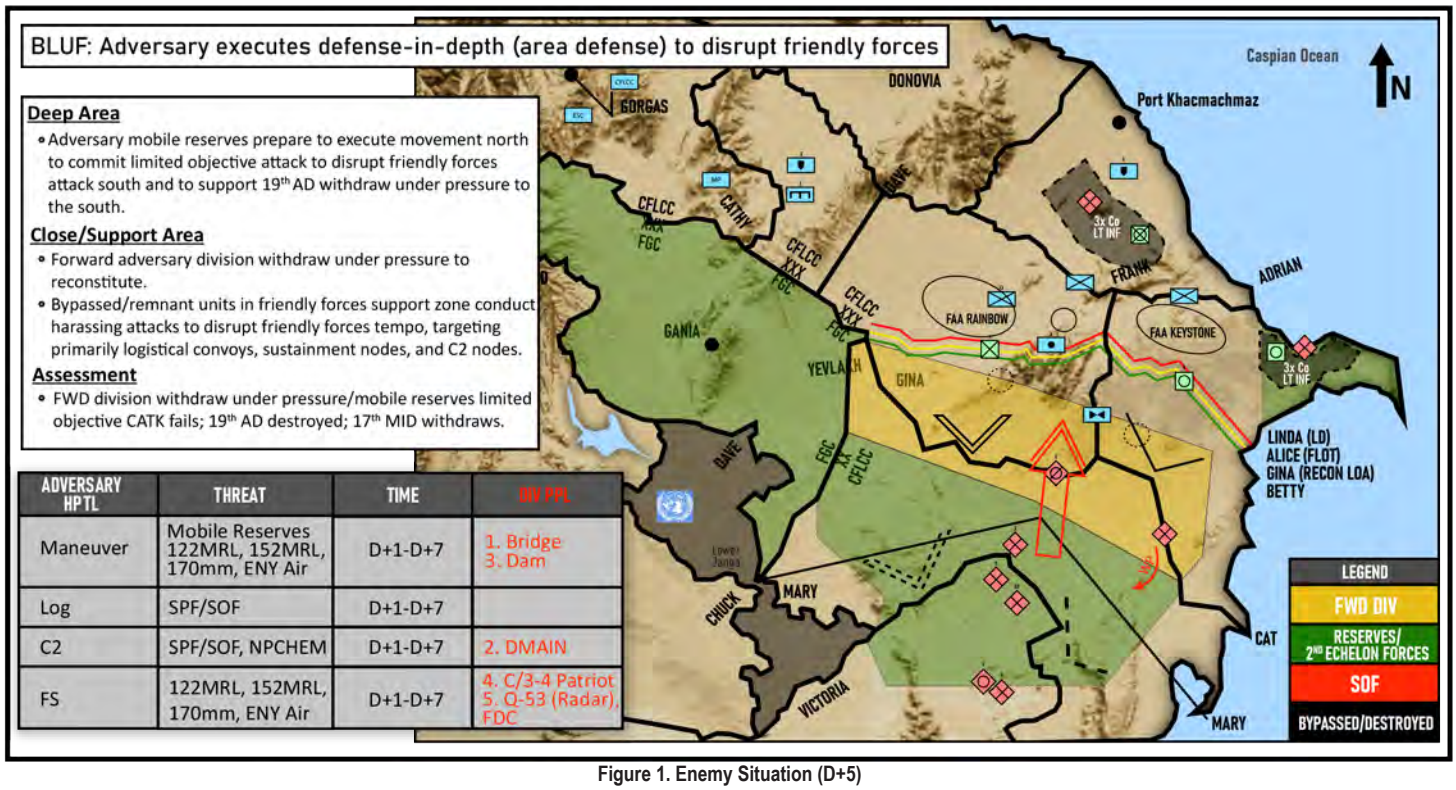


Figure 1. Enemy Situation (D+5)

With the adversary executing defensive operations, we used a different framework: If friendly forces execute (end state), then where will the enemy apply combat power and effects to counter? The answer to those questions drove where the adversary would employ its combat power. Using a threat model, we obtained an initial understanding of how the enemy would organize itself and, when overlaid on terrain, this yielded our SITEMP.

To support the targeting process, our starting point to frame the adversary was to identify what the adversary wanted to accomplish, either to achieve its end state or to prevent friendly forces from achieving theirs. This enabled the targeting team to—

- ✦ Identify key capabilities the enemy needed to accomplish its mission.
- ✦ Support the development of the HVTL.
- ✦ Identify the capabilities that the division needed to target to accomplish its mission.
- ✦ Support the development of the HPTL.

Additionally, these questions supported the development of the division's information collection plan and the tasking of the division's organic information collection assets and requests for support from higher headquarters.

Intelligence Support to Protection: The Methodology

The 2nd Infantry Division G-2 supported the division protection cell by focusing on the following questions:

- ✦ What the division was doing and why it was doing it?
- ✦ What combat power and effects did the adversary possess that could counter what the division was doing?
- ✦ Given operational variables, did the adversary possess the ability to deploy those effects against division assets?
- ✦ Where were the operational seams, and did the adversary retain sufficient combat power and effects to exploit?
- ✦ Did those actions, or effects, nest with the adversary's intent and end state?

Those questions generally focused on the adersary in the division close and support areas.

To support protection, our starting point to frame the adversary was to understand and visualize what the division was doing and then to determine if friendly actions overlapped with the adversary's intent, end state, and capabilities. In practice, this meant we built on our understanding of the adversary's composition, disposition, and intent, and we then created an estimated adversary HVTL and HPTL. We overlaid the adversary HVTL and HPTL with the current assessed adversary collection capabilites, combat power, and other capabilities that could be leveraged to engage the friendly targets. We then identified the time horizon that was available for the enemy to prosecute the targets (Figure 1). These actions—

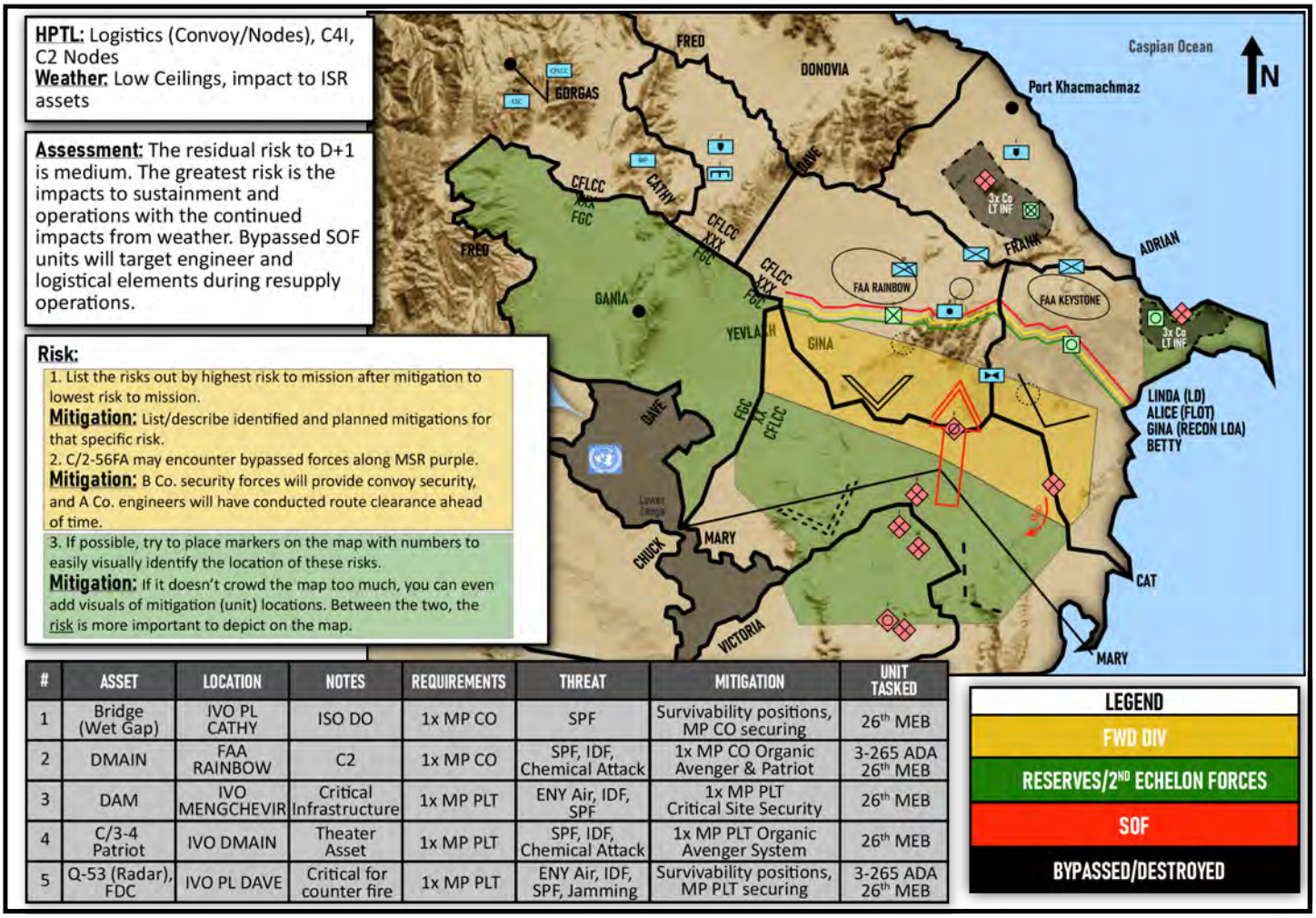
- ✦ Resulted in the creation of a refined and detailed prioritized protection list (Figure 2, on the next page).
- ✦ Provided the commander and staff with a greater understanding of risks to the mission and to the force.

Assessment:
- What happened?
- By who/what (enemy, friendly, weather, etc.)?
- What was the effect?
- Were mitigations in place?
- Were they effective?
- Why or why not?

Mitigation:
- What can be done to prevent or lessen negative effects to the mission?

RECOMMENDED PRIORITY	ASSET	LOCATION	NOTES	REQUIREMENTS	THREAT	MITIGATION	UNIT TASKED
1	Bridge (Wet Gap)	IVO PL CATHY	ISO DO	1x MP CO	SPF	Survivability positions, MP CO securing	26th MEB
2	DMAIN	FAA RAINBOW	C2	1x MP CO	SPF, IDF, Chemical Attack	1x MP CO Organic Avenger & Patriot	3-265 ADA 26th MEB
3	DAM	IVO MENGCHEVIR	Critical Infrastructure	1x MP PLT	ENY Air, IDF, SPF	1x MP PLT Critical Site Security	26th MEB
4	C/3-4 Patriot	IVO DMAIN	Theater Asset	1x MP PLT	SPF, IDF, Chemical Attack	1x MP PLT Organic Avenger System	26th MEB
5	Q-53 (Radar), FDC	IVO PL DAVE	Critical for counter fire	1x MP PLT	ENY Air, IDF, SPF, Jamming	Survivability positions, MP PLT securing	3-265 ADA 26th MEB
6	Sentinel Radar	DMAIN	Critical for air picture	1x IN PLT	ENY Air, IDF, SPF, Jamming	1x MP CO Organic Avenger PLT	3-265 ADA 26th MEB
7	DSA	FAA RAINBOW	C2, Sustainment Node	1x MP CO	SPF, IDF, Chemical Attack	1x MP CO Organic Avenger PLT	3-265 ADA 26th MEB

Figure 2. Prioritized Protection List (D+1)



#	ASSET	LOCATION	NOTES	REQUIREMENTS	THREAT	MITIGATION	UNIT TASKED
1	Bridge (Wet Gap)	IVO PL CATHY	ISO DO	1x MP CO	SPF	Survivability positions, MP CO securing	26th MEB
2	DMAIN	FAA RAINBOW	C2	1x MP CO	SPF, IDF, Chemical Attack	1x MP CO Organic Avenger & Patriot	3-265 ADA 26th MEB
3	DAM	IVO MENGCHEVIR	Critical Infrastructure	1x MP PLT	ENY Air, IDF, SPF	1x MP PLT Critical Site Security	26th MEB
4	C/3-4 Patriot	IVO DMAIN	Theater Asset	1x MP PLT	SPF, IDF, Chemical Attack	1x MP PLT Organic Avenger System	26th MEB
5	Q-53 (Radar), FDC	IVO PL DAVE	Critical for counter fire	1x MP PLT	ENY Air, IDF, SPF, Jamming	Survivability positions, MP PLT securing	3-265 ADA 26th MEB

Figure 3. Protection COP (D+5)

- ✦ Enabled more effective employment of friendly combat power to mitigate risk because the G-2 worked through the process to identify clear time horizons and enemy capabilities that could be brought to bear on friendly forces (Figure 3).
- ✦ Ensured that the division's and the major subordinate commands' information collection plans had accounted for protection requirements.

What We Learned

At the beginning of the last year's training cycle, the way that the intelligence warfighting function supported the protection cell was not entirely clear to the protection chief, G-2, or staff. As a result, we experienced some problems throughout multiple exercises. Over the course of four exercises, we learned that we needed an analytic framework with subtle distinctions to support the targeting and protection efforts.

Our initial approach to provide intelligence support to protection was to replicate our support for targeting. However, that analytic model was insufficient for the protection cell because it failed to adequately support the refinement of the division's prioritized protection list, defended asset list, and critical asset list, and it served as an inadequate model to refine risks to the mission and to the force. As a G-2 team, our understanding of intelligence support to protection evolved into a framework that focused on understanding and visualizing a basic question: What are we doing and why? We then overlaid the answer to that question with our understanding of the adversary's composition, disposition, intent, and capabilities.

> *"It is not enough for military intelligence leaders to talk about the adversary..."*

The development of an adversary HVTL and HPTL was a critical product that enabled us to refine risks to the mission and to the force, which influenced the division prioritized protection list. Without both an HVTL and an HPTL, we made the analytic leap that what the division prioritized on the prioritized protection list was often the adversary's priority. Developing both helped us to draw out the differences and create a more complete protection plan. This more mature approach to intelligence support to protection enabled the overall protection warfighting function to advance, and it set conditions for broader success across the division's deep, close, and rear operations.

Conclusion

Our experience in supporting the targeting and protection cells over the past year provides additional perspectives to intelligence leaders who are already cognizant of an analytic framework and understand the outputs of the B2C2WG. It is not enough for military intelligence leaders to talk about the adversary while allowing the rest of the staff and other warfighting functions to refine the plan. Rather, it is our responsibility to generate and employ tailored analytic models that drive the whole of staff through the planning process and into execution. How we talk and think about the enemy matters just as much as how we assess the enemy.

Endnotes

1. Department of the Army, Army Techniques Publication 3-60, *Targeting* (Washington, DC: U.S. Government Publishing Office [GPO], 7 May 2015), 1-2.

2. Department of the Army, Army Doctrine Publication 3-0, *Operations* (Washington, DC: U.S. GPO, 31 July 2019), 2-10.

MAJ Paul Ward is the operations officer, S-3, for the 719th Military Intelligence Battalion at Camp Humphreys, Republic of Korea. He previously served as the analysis and control element chief, 2nd Infantry Division. He is a 2008 graduate of the U.S. Military Academy and a graduate of the Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance. He is pursuing a master's degree from the University of Virginia. MAJ Ward has multiple combat deployments in Afghanistan and served as an intelligence officer in U.S. Army Intelligence and Security Command, U.S. Army Forces Command, and U.S. Special Operations Command formations.

207th Military Intelligence Brigade-Theater Support to African Lion 2021

by First Lieutenant Cesar Medina,
Chief Warrant Officer 5 Andrew Kelsay,
Chief Warrant Officer 2 Felix Rodriguez Faica,
Chief Warrant Officer 2 Ryan Harvey, and
Chief Warrant Officer 2 Derek Vobornik

A Royal Moroccan Air Force C-130 Hercules aircraft taxis down the runway during exercise African Lion 21 at the 3rd Royal Moroccan Air Force Base in Kenitra, Morocco, June 14, 2021. (U.S. Air Force photo by TSgt Devin Nothstine, 86th Airlift Wing/Public Affairs)

Introduction

African Lion is U.S. Africa Command's (USAFRICOM) foremost multinational joint readiness exercise in USAFRICOM's area of responsibility. The purpose of the exercise is to build the readiness of Combined Joint Task Force-Lion (CJTF-Lion), a joint multinational command with the mission to defeat a near-peer adversary in large-scale combat operations on the African continent. The U.S. Army Southern European Task Force, Africa (SETAF–AF) was responsible for manning and executing command of CJTF-Lion in Agadir, Morocco, from 7 to 18 June 2021. The 207th Military Intelligence Brigade-Theater (MIB–T), in coordination with the CJTF-Lion J-2, was responsible for bringing the intelligence enterprise to African Lion 21. From May through June 2021, the 207th MIB–T partnered with the Moroccan Royal Gendarmerie, sister services, government and nongovernment agencies, and other foreign partners to conduct full-spectrum intelligence activities to support and enable CJTF-Lion operations.

History of African Lion

The exercise was first conducted in 2002—with the participation of the U.S. Marines and Royal Moroccan Armed Forces. U.S. Africa Command increased its involvement in the exercise with the inclusion of the U.S. Army Southern European Task Force, Africa, based in Vicenza, Italy….SETAF–AF assumed lead responsibility of exercise African Lion in 2019 from the U.S. Marine Corps.[1]

A Big Exercise for a Big Continent

African Lion 2021 incorporated units and equipment from a variety of countries and services. Africa is a huge continent with a population that is expected to exceed two billion in three more decades. In this new era of "great power competition," Africa has emerged as a zone of competition for the United States, Russia, and China. In addition, violent extremist groups…have been making headway in solidifying their hold on parts of Africa.[2]

The Role of the Deployable Intelligence Support Element

The 207th MIB–T deployable intelligence support element (DISE) provided a rapidly deployable and tailorable intelligence package designed to augment SETAF–AF's early entry command post with unique single-source, all-source/fusion, and communications capabilities not otherwise available upon initial deployment anywhere within USAFRICOM's area of responsibility. In accordance with one primary goal of SETAF–AF, the DISE demonstrated unique interoperability with partner nations throughout African Lion 21. In May 2021, before the exercise began, two noncommissioned officers from the DISE served as assistant instructors, improving the intelligence fundamentals of more than 100 African Lion 21 participants from U.S. military units and foreign partner nations. The DISE also deployed most of its personnel and equipment from Vicenza, Italy, to Morocco on Royal Moroccan Air Force C-130s, yet again demonstrating interoperability with a key foreign partner.

Once established in Agadir, the DISE provided the only top secret voice, data, and video teleconferencing capability to CJTF-Lion, both for the African Lion 21 scenario and for real-world intelligence updates to the SETAF–AF G-2 and command. The DISE served as the primary fusion element for the CJTF-Lion J-2. The DISE also facilitated and enabled multidiscipline intelligence analysis and support and battle-tracked through the Distributed Common Ground System-Army (DCGS–A). The DISE maintained a digital and analog common intelligence picture using the DCGS–A Tactical Entity Database, visualized through the U.S. Army Intelligence and Security Command Cloud Initiative, also known as ICI, in the J-2 and from the 207th MIB–T analysis and control element (ACE) through reachback to Wiesbaden, Germany. Signals intelligence (SIGINT) and human intelligence (HUMINT) reporting was coordinated for releasability to partner nations through

the foreign disclosure official, while DISE analysts conducted detailed network development to illuminate hybrid threat networks and enable operational solutions or partner nation law enforcement action. The DISE also produced the graphic intelligence summary and generated analytic assessments of the current situation and current operations that were briefed to the CJTF-Lion commander twice daily.

Participation of the 337th Military Intelligence Battalion

The 337th Military Intelligence Battalion, a reserve battalion from Fort Sheridan, Illinois, that is regionally aligned to the 207th MIB–T, manned and operated its own ACE to provide reachback capabilities to African Lion 21. Personnel from the 337th also traveled from the United States to the ACE in Wiesbaden, Germany, to provide in-person analytical support for African Lion 21. The ACE tasks included analysis, indications and warning, assessments, and intelligence coordination support to the joint area of operations during this exercise via open-source intelligence (OSINT), SIGINT, and geospatial intelligence (GEOINT) platforms. The 337th successfully integrated with the 207th DISE, provided analysis of more than 200 OSINT injects to the DISE, and pushed more than 90 injects through the multifunction workstation system, which helped the DISE build the common intelligence picture. The 337th also coordinated and assisted with oversight of the GEOINT mission. The 337th's integration and participation were critical because not only did they provide CJTF-Lion active duty personnel with much needed support, but they also enabled Army Reserve Soldiers to train and build readiness to mobilize whenever needed.

HUMINT Training

HUMINT collectors from the 207th MIB–T integrated with Moroccan Royal Gendarmerie and United States Army Military Police in Tifnit, Morocco, a 45-minute drive from the CJTF-Lion headquarters. The purpose was to simulate operations in austere conditions to secure, process, screen, and interview approximately 2,000 notional displaced or captured personnel. The 207th MIB–T coordinated with the SETAF–AF Joint Theater Forensic Analysis Center to deploy individuals to train and familiarize United States and Moroccan personnel with biometric enrollment and processing of displaced and captured persons. The 207th MIB–T coordinated with the HUMINT Training–Joint Center of Excellence (HT–JCOE) to provide additional HUMINT collection and integration into the 207th MIB–T training effort.

Communications Training

The S-6 team of the 307th Forward Collection Battalion, 207th MIB–T, successfully executed a communications package for the Tifnit training event. The 307th Forward Collection Battalion team, most of which had little to no deployment experience, greatly benefited from the planning, deployment, mission execution, and redeployment process. Furthermore, every day yielded a problem related to information technology or communications that the team had to troubleshoot and solve, providing additional "boots on the ground" experience for these young Soldiers.

Recommendations for Future Training Events

The following are observations and recommendations for future African Lion exercises.

Location. Future training events should take place close to the physical location of the main effort (CJTF-Lion headquarters) rather than at a remote secondary location. The overall training benefit of this small event did not justify the coordination, logistics, and support requirements for operations in Tifnit. Life support, transportation of personnel and communications equipment, and setup and maintenance of a protected temporary classified information facility required too many man-hours for an isolated event that had limited relevance to the overall African Lion 21 effort. The 207th MIB–T S-4 successfully executed all 207th efforts from Agadir and was capable of providing the same level of excellent support to the HUMINT portion of the exercise. Additionally, the 307th S-6 team was capable of supporting a broader training audience with fewer personnel requirements if also located in Agadir. The reduction in travel and equipment transportation requirements would yield 2 to 3 days of time that would add value to the training objectives of CJTF-Lion, SETAF–AF, and the 207th.

Communications. The Transportable Tactical Command Communications system package was not needed for the Tifnit iteration. The 307th teams used these communications systems, but because of the security environment, they were required to remove all hard drives, break down the equipment, and set up everything again the following morning, which caused wear and tear on the equipment over a 15-day period. For nonsecure (Non-classified Internet Protocol Router Network) communications, a Wi-Fi hotspot would meet the requirement. For secure communications, the Global Rapid Response Information Package or a Commercial Solutions for Classified platform would meet the teams' needs (unsecured when powered down and fully secured when powered on, logged in, and with a virtual private network in use). None of these systems requires a dedicated S-6 effort, which would have allowed the S-6 to support the main effort in Agadir. A best practice would be for the individual teams to use systems organic to them and systems they would typically deploy with, providing realism to the "train as you fight" mantra.

HUMINT Training. If the HUMINT training were to take place in Agadir, or otherwise near the CJTF-Lion headquarters, the HUMINT collectors would greatly benefit if integrated into the exercise in support of CJTF-Lion. The SETAF–AF G-2X and joint partners from the Navy and Air Force manned the

J-2X forward element, and the 207th established an operational management team and analytical support element for counterintelligence and HUMINT operations. Integrating the operational management team into the HUMINT team operations, and in turn connecting the operational management team into J-2X operations, would enable the 207th MIB–T to successfully exercise its counterintelligence and HUMINT personnel at every echelon.

The HT–JCOE instructors provided excellent training to the HUMINT collectors during African Lion 21. However, future HUMINT training should be done near the rest of the 207th MIB–T support team to streamline their involvement, save money on transportation and logistics costs, and more efficiently use these valuable HT–JCOE resources to the benefit of a larger audience. Prior coordination with the African Lion planners would enable HUMINT collectors to practice collection, glean information directly tied to the scenario, and enable injects to feed the exercise in real time. This would simulate the real-world interoperability required to take place between the 207th MIB–T, CJTF-Lion CJ-2 and staff, and our foreign partners.

Conclusion

African Lion 21 met expectations as USAFRICOM's premier annual exercise. It was an excellent example of the long-term commitment the United States has to our African partners, as it strengthened shared capabilities and fortified interoperability and readiness.

Planning for African Lion 22 began in October 2021. The exercise took place again in Agadir, Morocco, as well as in Ghana, Senegal, and Tunisia, from 6 to 30 June. Militaries from multiple countries joined U.S. and host nations troops to exercise our capabilities for the common good, demonstrating that we are stronger together. The 207th MIB–T is proud of our Soldiers' accomplishments, and we look forward to participating in future African Lion exercises.

Endnotes

1. John Friberg, "Exercise African Lion 2021," SOF News, 29 June 2021, https://sof.news/exercises/african-lion-2021/.

2. Ibid.

1LT Cesar Medina is an Army Reserve military intelligence officer who previously served as the officer in charge of the analysis and control element support cell at Fort Sheridan, IL. He is currently the officer in charge of the human intelligence analysis cell at B Company, 337th Military Intelligence Battalion, Fort Snelling, MN. He holds a bachelor's degree in economics and a master's degree in public administration. 1LT Medina completed the U.S. Army Captains Career Course.

CW5 Andrew Kelsay is the 207th Military Intelligence Brigade-Theater Command Chief Warrant Officer and a counterintelligence technician. He previously served as the G-2X counterintelligence coordinating authority at U.S. Army Southern European Task Force, Africa, U.S. Army Garrison, Vicenza, Italy. He holds an associate degree in intelligence studies, a bachelor's degree in social sciences, and a master of science in education.

CW2 Felix Rodriguez Faica is an all-source intelligence technician who serves as the North Africa/geospatial planning cell team chief at the 207th Military Intelligence Brigade-Theater. He previously served as the brigade intelligence support element chief at the 1st Infantry Brigade Combat Team, 10th Mountain Division. He has completed the Digital Intelligence Systems Master Gunner Course.

CW2 Ryan Harvey is an all-source intelligence technician who serves as the deployable intelligence support element officer in charge for 207th Military Intelligence Brigade-Theater. He previously served as the senior analyst at 173rd Infantry Brigade Combat Team (Airborne). He holds a master of science in intelligence management.

CW2 Derek Vobornik is the information services technician for the 307th Military Intelligence Battalion, 207th Military Intelligence Brigade-Theater. He previously served as the information services technician for the 3rd Sustainment Brigade, 3rd Infantry Division, Fort Stewart, GA. He holds a bachelor's degree in cybersecurity from American Public University and completed the courses and certifications for CompTIA A+, CompTIA Security+, and CompTIA Advanced Security Practitioner.

MODERNIZATION: Expanding Command Deployment Discipline Programs

by Lieutenant Colonel James "Mike" Blue and Major David White

U.S. Soldiers assigned to 207th Military Intelligence Brigade, 307th Military Intelligence Battalion, are briefed prior to an M-4 carbine qualification for Lightning Focus 22, Grafenwoehr, Germany, March 8, 2022. (U.S. Army photo by CPL Austin Riel)

Introduction

The inherent tension between the Army's overdue focus on modernization and a tactical commander's need to maintain deployment discipline is particularly acute for those units charged with continuous forward-deployed operations. As the Department of the Army G-2 staff and the U.S. Army Intelligence and Security Command (INSCOM) work to integrate the intelligence warfighting functions within the Regionally Aligned Readiness and Modernization Model (ReARMM), units with continuous forward-deployed missions must address the challenge of modernizing, operating, and training while preserving the health of their force. The basis of ReARMM is a unit life cycle that applies to all units of the Total Army, conforming principally to three windows—modernization, training, and mission.[1] Charged with responding to the immediate needs of the global combatant commands and "setting the theater" in an age of prolonged strategic competition, INSCOM's military intelligence (MI) brigades-theater must be at the forefront of modernization efforts.

307th Military Intelligence Battalion

The 307th Military Intelligence Battalion (MI BN) is INSCOM's forward collection battalion aligned with U.S. Africa Command requirements. It remains a continuously employed unit focused on multidisciplined intelligence collection across the austere, complex, and diverse continent of Africa.

In February 2020, the 307th MI BN (Forward Collection) implemented a nondoctrinal operational readiness model based on the special operations forces community's Joint Operations Readiness and Training System (JORTS) in order to balance lengthy training pipelines with rotational deployment readiness and short-notice intelligence missions. The former 307th MI BN (Forward Collection) commander described the ongoing unit "experiment" in an article titled "Special Operations Forces' Structured Readiness Model Makes Conventional Military Intelligence Unit More Effective."[2] JORTS has been highly successful in providing much-needed predictability to Soldiers and their families, increasing operations capacity and effectiveness, and maturing the unit into a partner-of-choice throughout the African continent; however, an evolution of JORTS was necessary to better meet modernization imperatives and adapt to changing conditions on the ground.

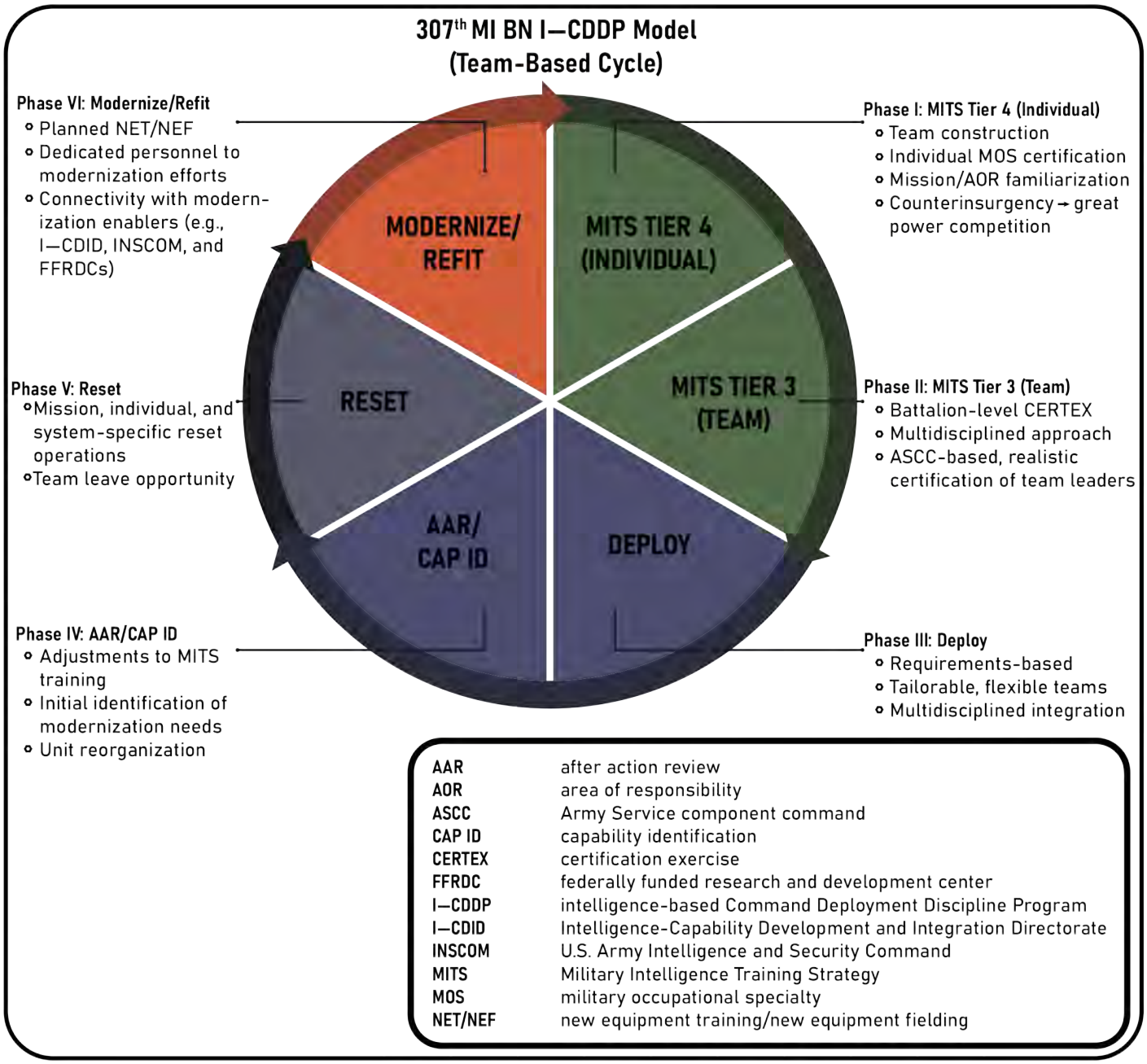
This article describes transformations that the 307th MI BN (Forward Collection) has made to its already revolutionary readiness system to better enable intelligence modernization in accordance with the ReARMM concept. The result of this effort is an intelligence-based Command Deployment Discipline Program (CDDP), known as I–CDDP, that may serve as an efficient, effective, and exportable enterprise solution.

307th MI BN's I–CDDP Model

AR 525-93, *Army Deployment and Redeployment*, the U.S. Army's policy on deployment and redeployment operations, outlines the CDDP as a mechanism for commanders at all levels intended to maintain the unit's deployment posture, evaluate and drive deployment readiness, and meet directed mission requirements.[3] Although designed for U.S. Army Forces Command units, the CDDP serves as a doctrinal foundation from which other models (such as the nondoctrinal "JORTS") can be altered to fit the needs of strategic-level, continuously employed conventional units.

The following paragraphs describe how the 307th MI BN's I–CDDP model, shown on the next page, encapsulates the Military Intelligence Training Strategy (MITS), builds on the successful elements of JORTS, and enables modernization in line with ReARMM.

Phase I (MITS Tier 4). Phase I is the company-led, company-monitored training designed to both develop individual military occupational specialty (MOS)-specific tasks and integrate sustained warrior tasks and battle drill focus. During this phase, company commanders retain the flexibility to realign talent across deployable teams. This window also gives predictable time to send Soldiers to advanced MOS training, effectively building technical capacity within the battalion. This training window integrates the Army Service component command (ASCC) mission and requirements specific to the area of responsibility to prepare these teams for deployment.



Phase II (MITS Tier 3). For this phase, the battalion-led certification exercises are conducted three times a year to maintain the rigorous standards for deploying teams. The battalion S-3 plans and resources these events, which certify all deploying teams and force multi-intelligence discipline certification. Once the battalion commander certifies signals intelligence (SIGINT), human intelligence (HUMINT), and counterintelligence (CI) teams during a certification exercise, company-level leadership cannot reorganize teams for 6 months without O5-level approval. This avoids "breaking track" and minimizes risks to the mission and the force. After certification of the teams, the company-level leadership can deploy these teams for up to 180 days without further training or certification. This will help account for the spectrum of longer traditional deployments to no-notice emerging requirements, which are routine for INSCOM's MI battalions globally.

Phase III (Deploy). During phase III, fully certified teams deploy in support of ASCC requirements but can reorganize to fill multifunctional team requirements, as needed. This maintains the flexibility required for forward collection battalion support. Clarity on advanced capability requirements from supported commands allows the unit to build a bench of technical talent through time. The model gives the flexibility to increase advanced training.

Phase IV (After Action Review/Capability Identification). The goal of the new model was to produce increased capacity and capability in support of the battalion's operational and ASCC headquarters while creating time and space for lessons learned to become the foundation for ground-up modernization. For this phase, post-mission debriefs include a formal after action review with both mission command and technical oversight leadership simultaneously. The process

identifies needed adjustments to MITS Tiers 4 and 3 training standards, advanced MOS training requirements, or equipment modernization needs to increase collection specific to the area of responsibility.

Phase V (Reset). In this phase, company command teams can "break track" and reconstruct their teams for future operational employment, professional development, and planned windows for permanent changes of station or expiration terms of service. Reset operations look diametrically different between all forward collection battalion-deploying collection teams and depend on the length of deployments and the needs of individual Soldiers. This is also a deliberate leave opportunity window for Soldiers on consistent rotation.

Phase VI (Modernize/Refit). Coming out of phase V (Reset), the redeploying team is aligned to the modernization needs identified in phase IV (After Action Review/Capability Identification). This direct alignment of personnel ensures the small forward collection battalion staff generates the right information to move modernization initiatives in the right direction. The time spent in this phase will depend on the complexity of the desired modernization goal. When warranted, teams conduct DOTMLPF-P analysis to develop white papers, ensuring higher headquarters staffs have the technical understanding to move the effort forward without distracting collectors, who are already moving back into phase 1 (MITS Tier 4). The identification of potential partnerships occurs during this phase, with INSCOM, Army Futures Command Intelligence-Capability Development and Integration Directorate, and/or federally funded research and development centers. Major system upgrades for SIGINT take months, while resetting HUMINT or CI training may only take a week for the next deployment rotation.

The Revised Model for Home-Station Operations

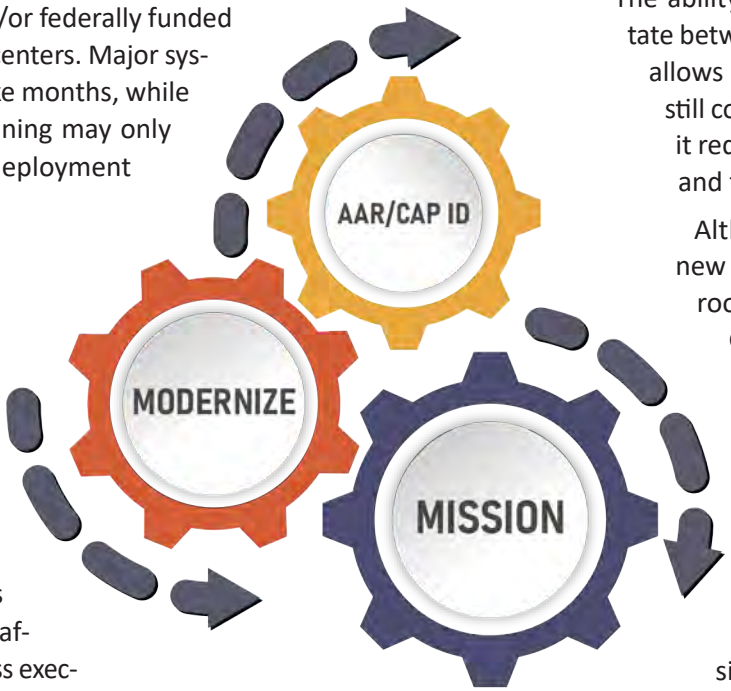
The culture in the unit must drive modernization and innovation cycles, as identified by the most recently deployed team members. This culture will find better business practices across collection disciplines after every iteration. As business executive Jim Whitehurst wrote, "If employees feel that they are listened to and appreciated—this is, when they are engaged—great things can result.[5] Advanced training for intelligence collectors requires deliberate planning and predictable mission timelines. To work effectively, the culture requires a commitment from the team members and faith in the chain of command.

Separate from deploying teams, the battalion modified the I–CDDP model to address home-station operations, which are a normal occurrence in INSCOM's forward collection battalions—as are the distractors that make it difficult to protect those vital missions on a daily basis. Traditionally, home-station intelligence Soldiers are not fenced from garrison and/or unit-level tasks. Although both MOS-specific and Soldier training must continue, the unit has shifted its view of these operationally engaged teams to enable sustained missions. Because of the nature of home-station intelligence missions, teams must execute their mission, conduct mission after action reviews, identify capability gaps, and modernize continuously. This takes a deliberate effort not to allow the daily grind of operations to distract from everything but mission execution.

For the 307th MI BN (Forward Collection), "fenced" teams include the—

- CI field office.
- CI/HUMINT operational management teams.
- Foreign Military Intelligence Collection Activities–aligned HUMINT collection teams.
- SIGINT analytics reachback.
- Niche capabilities like technical surveillance countermeasures and cyber-CI.

The ability for these teams to quickly rotate between the adapted I–CDDP phases allows consistent modernization while still completing their core mission, but it requires direct command oversight and focus.



307th MI BN I–CDDP Model (Home-Station Operations, Adapted Cycle)

Although grown from JORTS, the new all-inclusive I–CDDP model has roots in the previous Army Force Generation system. With many similarities, the I–CDDP system has fundamental differences that limit the risks associated with the legacy system. I–CDDP allows for dedicated modernization windows and flexible time windows to allow teams to be in differing phases simultaneously across the companies. This ensures training readiness for team-centric deployments while purposefully incorporating modernization designed to rapidly identify, resource, and drive needed technological improvements within

the aligned area of operations. The model, which is predicated on sustaining flexibility and improving junior leader empowerment, provides consistent readiness for deploying intelligence collection teams across the African continent and deliberate protection for home-station operations. Key tenets of the model include—

Operational Requirements. Predictable and forecasted mission requirements are vital to the success of any sustainable model. To forecast, plan, and resource home-station and advanced intelligence training, MI battalions must foundationally start with clear requirements tied to predictable time horizons. A higher headquarters' publication of clear personnel and system requirements ensures MI battalions can accurately plan and resource the MITS training and certification exercise. Certified teams fill unforecasted requirements, as the certification stands for up to 6 months.

Operational Headquarters and ASCC Understanding. The controlling headquarters of INSCOM's battalions must view a forward collection battalion's capabilities in terms of collection teams (e.g., HUMINT collection teams, SIGINT collection teams, and CI teams), or multifunctional teams, instead of looking at collectors as individuals. Conventional units must build talent iteratively through training and operational employment to fight the never-ending cycle of losing technical expertise because of personnel losses. If supported commands only demand the deployment of experienced collectors with advanced training, operational experience cannot be built to support intelligence collection in the future operational environment.

Conditions versus Time-Based. The model is not constrained by time horizons, and it is conditions-based because of the complexity and uniqueness of different intelligence-discipline collections teams. Previous models overly focused on forcing teams to execute phases in rigid timelines, resulting in missed opportunity—ultimately leading to a lack of capability expansion. The battalion-resourced certifications are used as an opportunity in which company command teams can reconstruct teams as needed to allow for employment within the next 6 months.

Mission Command. Empowerment of company command teams is the most important aspect of this new model. Company-level commanders are directly responsible for maintaining and leading collection teams through the I–CDDP phases as the administrative control headquarters. They are responsible for the management of phase changes, training management, and team construction through time. The growth in control at the company commander level in the model increases the balance of individual operational tempo and improves the predictability for small teams. While subordinate leaders manage phases of the model, the battalion enforces a disciplined approach to team leader certification and transitions of personnel between teams.

Strengthening Unit Capabilities and Individual Skills. In the modernization window, new equipment fielding and training and an equipment reset can occur in a transparent manner at echelon to ensure the latest technology integrates effectively within the unit. Advanced training for intelligence collectors requires deliberate planning, predictable missions, and validated ASCC requirements to lock in schools. The I–CDDP model increases opportunities for collectors to attend advanced MOS schooling throughout the process, while protecting the sanctity of the MITS certification process.

Conclusion

After a single iteration of each of these phases with organic HUMINT and CI teams, the 307th MI BN has seen tremendous effects in capability and capacity growth, as well as ground-up modernization efforts. The I–CDDP framework has fixed training deficits, improved the predictability our Soldiers deserve, and, as a byproduct, increased the command climate of the entire unit. With predictability and focused talent management, a new culture of commitment to mission accomplishment will continue to build. This operational-driven model, which focuses on the empowerment and development of our intelligence professionals, could likely work in any continuously employed MI unit across the enterprise.

Endnotes

1. Michael C. (Mac) McCurry, "Army Aviation Excels in Spite of Pandemic," *Army Aviation* 70, no. 4 & 5 (April/May 2021): 41, http://www.armyaviationmagazine.com/index.php/archive/not-so-current/1979-army-aviation-excels-in-spite-of-pandemic.

2. Jesse Chace, "Special Operations Forces' Structured Readiness Model Makes Conventional Military Intelligence Unit More Effective," *Military Intelligence Professional Bulletin* 47, no. 1 (January–March 2021): 35–39.

3. Department of the Army, Army Regulation 525-93, *Army Deployment and Redeployment* (Washington, DC: U.S. Government Publishing Office, 23 October 2019), 21–22.

4. DOTMLPF–P: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

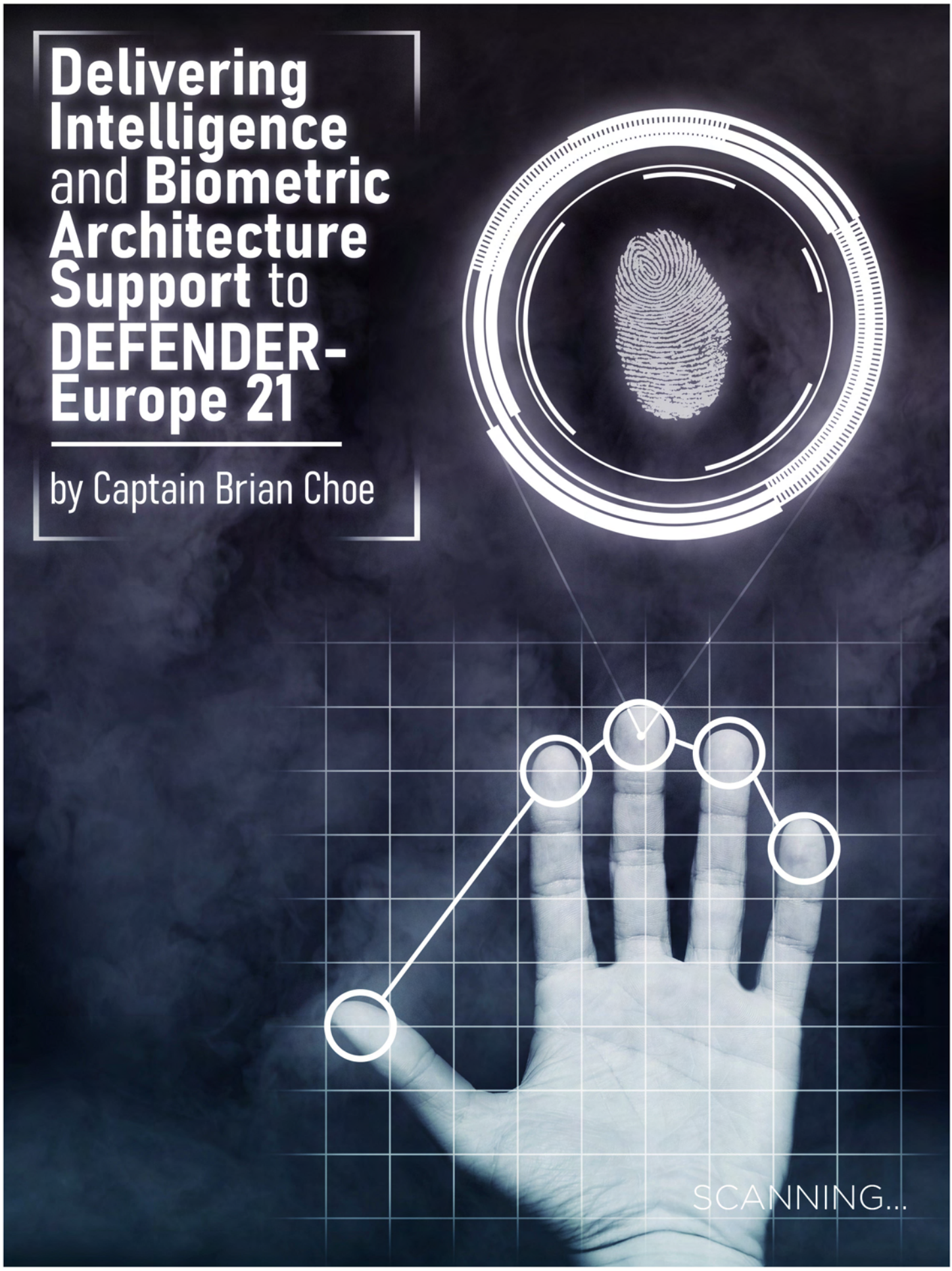
5. Jim Whitehurst, *The Open Organization: Igniting Passion and Performance* (Boston: Harvard Business Review Press, 2015), 54.

LTC James "Mike" Blue is the commander of the 307th Military Intelligence Battalion in Vicenza, Italy. He is a career military intelligence officer who has served in a variety of conventional and special operations units. He holds a master's degree in intelligence studies from American Military University and a master's degree in strategic intelligence from the National Intelligence University.

MAJ David White is the battalion operations officer (S-3) of the 307th Military Intelligence Battalion in Vicenza, Italy. He is a career military intelligence officer with collection experience at tactical, operational, and strategic levels. He also served as a joint intelligence planner for a four-star headquarters. He holds a master's degree in Middle Eastern studies and Arabic language from the American University in Cairo.

Delivering Intelligence and Biometric Architecture Support to DEFENDER-Europe 21

by Captain Brian Choe



Introduction

DEFENDER-Europe 21 was a large-scale, U.S. Army-led, multinational, joint exercise designed to build readiness and interoperability between United States, North Atlantic Treaty Organization, and partner militaries in Europe from March to June 2021. The 709th Military Police Battalion conducted security and mobility support operations and detention operations training for DEFENDER-Europe 21 in Germany, Hungary, Albania, Greece, Croatia, and Slovenia to enable friendly forces in large-scale combat operations. To support the battalion's mission, the S-2 intelligence cell conducted intelligence preparation of the battlefield for the exercise, established a concept of intelligence support, and continually refined the running estimate as part of the military decision-making process. Additionally, the 527th Military Police Company used the Defense Exploitation (DEX) training portal as an introductory familiarization platform for the submission of biometric enrollments, deoxyribonucleic acid (DNA) samples, and explosive residue.

Preparations for the exercise included an analysis of the area of operations, area of interest, and area of influence, compiled with forces available, critical planning factors, and constraints/restraints of the S-2's running estimate. The analysis identified that, in addition to support from the 18th Military Police Brigade, the S-2 cell at the tactical command post would require numerous external intelligence enablers.

Personnel Support

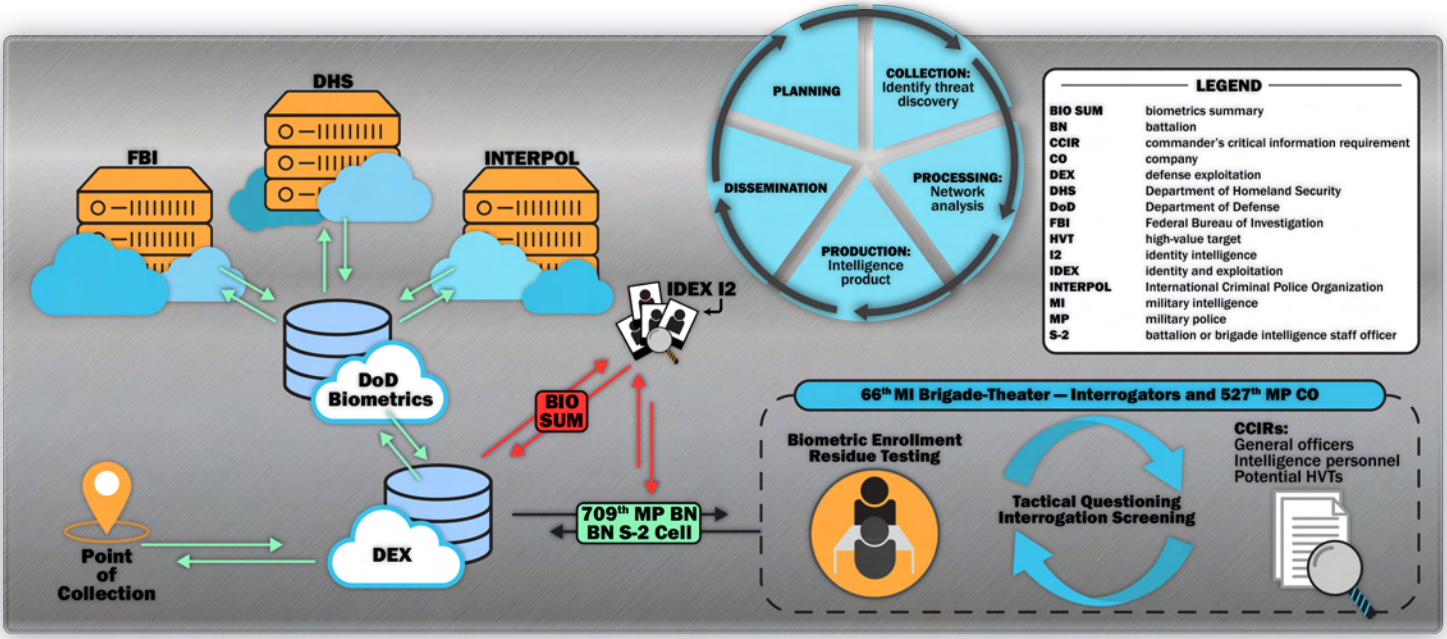
The 709th Military Police Battalion S-2 intelligence cell consisted of three internal 18th Military Police Brigade intelligence professionals:

- A battalion S-2 officer in charge/counterintelligence (CI) officer.
- An assistant S-2 officer to conduct all-source intelligence analysis directly supporting the tactical command post, battalion commander, and battalion staff.
- A human intelligence (HUMINT) collector noncommissioned officer to provide real-world foreign military intelligence collection activity debriefings.

HUMINT collectors from the 66th Military Intelligence (MI) Brigade-Theater provided vital tactical questioning training and exercise interrogation screenings. They also played an integral part in exercise/role-player development. Additionally, the MI brigade-theater deployed approximately 20 CI agents across the DEFENDER-Europe 21 area of operations, providing real-world foreign intelligence entity threat and collection activity analysis. The agents established Threat Awareness and Reporting Program channels for foreign significant activity information and mitigation efforts in support of potential insider threats.

An Air Force Albanian linguist, from Hill Air Force Base, Utah, provided external language support to the S-2 cell. This was in response to the U.S. Army Europe and Africa (USAREUR–AF) commander's initiative to use U.S. Service members with a language proficiency to meet DEFENDER-Europe 21's requirements, thereby minimizing a reliance on contractor linguists. The Air Force linguist provided technical oversight for the local national Albanian linguists hired by the Mission Essential Group for the duration of the exercise.

A contractor from the Identity and Exploitation (IDEX) Operations Branch, USAREUR–AF G-34, provided biometrics-enabled intelligence, forensic site exploitation, and identity intelligence expertise, as well as architecture support to assist with the military planning efforts of the exercise.



This illustrates the plan for integration of intelligence enablers who collectively provided tactical questioning, interrogation screenings, biometrics-enabled intelligence, forensic site exploitation, and identity intelligence for DEFENDER-Europe 21.

The battalion S-2 cell and external enablers' efforts throughout the exercise provided intelligence and biometric architecture support. Additionally, they assisted the battalion tactical command post and 527th Military Police Company by providing recommendations for biometric exploitation processes and procedures in accordance with AJP-2.5(A), *Captured Persons, Materiel, and Documents*.[1] Upon identifying gaps in the DEFENDER-Europe 21 scenario, the IDEX Operations Branch and 66th MI Brigade-Theater HUMINT collectors supported and assisted planning efforts to meet battalion- and company-level mission essential tasks and commander's training objectives.

Intelligence Analysis and Production

Before the exercise began, the battalion S-2 cell conducted intelligence analysis to generate knowledge, build the common operational picture, and assist the battalion commander and staff in their understanding of the battlefield. This included creating and disseminating intelligence through the daily battle update brief, the daily operations and intelligence brief, and periodic intelligence update briefs. The briefs included intelligence collected through intelligence information reports, open-source intelligence, and CI reports, presented through graphics, analysis, and geospatial products. The battalion S-2 cell also provided hip-pocket training to the 527th Military Police Company Soldiers about the dangers of social media activity and online cyber-hacking threats and provided a classified brief on Russia's information warfare capabilities.

The S-2 managed the integration of the Air Force Albanian linguist and HUMINT teams into the exercise, ensuring they were successful in creating and executing the training objectives. The battalion S-2 cell developed threat characteristics, friendly forces data, preliminary exercise injects, and an exercise road to war. The S-2 cell also developed and briefed a concept of support for all staff sections to ensure a shared understanding of the exercise environment. During the certification portion, the S-2 cell conducted 24-hour operations, with the S-2 officer in charge taking charge of the day shift and the assistant S-2 taking charge of the night shift.

During both shifts, the S-2 received, processed, and disseminated intelligence significant activities and exercise reporting. Collection of the information and data was in the form of biometric enrollments of U.S. role-players, SALUTE/spot reports,[2] information gathered from the 527th Military Police Company, HUMINT intelligence information reports, and open-source intelligence. The processed intelligence provided predictive analysis of enemy courses of action and threats to operations, informing and advising the commander to choose the best friendly course of action.

Planning and Scenarios

The battalion S-2 cell met with the 527th Military Police Company's command team to assist in developing the commander's training objectives derived from AJP-2.5(A) and determining their relation to the mission essential tasks implemented during DEFENDER-Europe 21.

The IDEX Operations Branch and 66th MI Brigade-Theater HUMINT collectors developed the scenario spanning 4 days, from 1 through 3 June 2021, allowing 4 June for retraining opportunities. The exercise included 14 key injects designed to exercise and evaluate mission essential tasks and commander's training objectives with the support of the Albanian 3rd Infantry Battalion–designated opposing forces (OPFOR). The 527th Military Police Company partnered with Albanian military police enablers and, with the support of the battalion tactical command post, executed the scenario. External observer coach/trainers observed and evaluated the scenario as part of exercise evaluation.

The DEFENDER-Europe 21 threat network, consisting of 3rd Infantry Battalion and 709th Military Police Battalion role players, replicated near-peer threats and malign actors. Within the scenario, the network consisted of a platoon-size element of Donovian Special Purpose Forces, Donovia, as the exercise's adversarial country threat. Role-player packets were developed, translated, and disseminated to the assigned OPFOR. The IDEX Operations Branch and 66th MI Brigade-Theater provided additional training to ensure all role players understood the expectations, biographical information, and safety considerations. Points of capture with accompanying capture circumstances and a detainee collection point were part of the scenario to exercise intelligence reporting and battle tracking.

An example exercise enemy course of action centered on a complex small arms fire attack generated by collected intelligence from exercise role players during tactical questioning interrogations.

Over the course of the exercise, eight captured persons were dropped off at the detainee collection point and one role player surrendered. Each role player was searched, administratively in-processed, screened, tested for explosive residue, processed for a DNA sample, biometrically enrolled, medically screened, and questioned. However, exercise constraints did not allow the biometric enrollment, DNA sampling, or questioning of the Albanian OPFOR.

U.S. role players functioned as "stand-ins" during biometric enrollments, DNA sampling, and questioning to meet the commander's training objectives. The Albanian OPFOR was only notionally biometrically enrolled, DNA sampled, and questioned during the exercise. Before participating in the biometric enrollments, each U.S. role player signed a Training Exercise Biometric Collection Consent form, acknowledging they had received a briefing on, and would participate in, the conduct of a privileged biometric and exploitation training exercise involving the U.S. Department of Defense. Role players understood that the activity was lawful and pursuant to the authority of the Secretary of Defense under the National Security Act of 1947, as amended. This included ensuring that within 5 days after the training exercise, authorized individuals would discard and permanently delete the collected information, including information on all training collection devices and in the exercise scenario databases.

The IDEX Operations Branch and 66th MI Brigade-Theater HUMINT collectors methodically developed and validated role-player scripts and biographical data, ensuring the exercise scenarios were properly actioned through identified key injects. The 66th MI Brigade-Theater developed several key events for role players during the exercise. These key events included attempted weapon/equipment smuggling during search procedures, escape attempts, misleading biographical information, medical complaints, and a riot attempt. The 66th MI Brigade-Theater also developed intelligence information for collection in order to tie the scenario together.

A U.S. Army role player along with an Albanian opposing forces role player notionally being biometrically enrolled, tactically questioned, and DNA sampled during the exercise.

Defense Exploitation Training Portal: Data Uploads and Reports

IDEX operations deny anonymity to malign actors, foreign intelligence entities, violent extremist organizations, and their proxies operating throughout the USAREUR–AF area of responsibility during the competition phase. The DEX training portal replicates the actual functions of the IDEX portal. The DEX portal acts as a repository and submission network for a variety of exploitable modalities: biometrics, cell phones, subscriber identity module cards, documents, media, video, weapons, drones, DNA, trace residue (including narcotics and explosives), audio files, currency, and improvised explosive device components. At the time of submission, the prospective external agency or organization receives the data for further exploitation. After exploitation, the agency or organization posts its responses to the DEX portal, which disseminates the information to the submitting unit for integration into intelligence production and operations and to assist the commander's decision making.

The 527th Military Police Company conducted three categories of tests:

- Biometric enrollments using BioSled, a device that performs multimodal biometric collection and onboard matching using a fingerprint sensor and dual iris camera.[3]
- DNA sampling with buccal swabs.
- Explosive residue testing using SEEKERe, a handheld system that uses an automated colorimetric methodology to detect trace amounts of both explosives and drugs.[4]

They then submitted the data to the DEX training portal. Through use of the IDEX Role Player Management system architecture and DEX training portal management, submitting units were able to monitor real-time responses directly related to role-player identity management. Soldiers documented in the DEX training portal each captured person processed within the 527th Military Police Company captured holding facility.

After the upload of biometric enrollments, DNA samples, and explosive residue submissions in the DEX training portal, along with the corresponding chain of custody documentation, a dossier was created for each captured person encounter.

Biometric enrollments to the DEX training portal identified historical enrollments, watch list notifications, biometric matches to the IDEX Joint European Multination Exploitation Center forensic cases, and first-time enrollments. Responses were posted on the DEX training portal, visible by the 527th Military Police Company and the 709th Military Police Battalion S-2 cell. Soldiers generated personnel encounter detail summaries and submitted them to the DEX portal, which disseminated them to DEFENDER-Europe 21 participating units. In the event of first-time biometric enrollments within the

training scenario, the S-2 made biometric-enabled watch list nominations.

DNA buccal swabs submitted to the DEX training portal generated a DNA summary report. The generated report replicated the Defense Intelligence Agency's DNA laboratory summaries. Each summary included the buccal swab; the process used to extract, quantify, concentrate, and amplify the swab; and test results and conclusions. The submissions used DEFENDER-Europe 21's internment serial number naming convention for the processing of the 527th Military Police Company's captured persons. The DNA samples were notionally ingested into the training database, and the submissions were processed. Responses were provided both to the DEX training portal and to the submitting unit to assist in intelligence production, operations, and commander's decision making.

Explosive residue testing generated real-time test summaries of role players for submission to the DEX training portal. Explosive residue submissions generated an identification match (positive hit) or a non-identifiable result (negative hit) to assist in intelligence production and operations and in commander's decision making.

Explosive residue tests for the exercise were conducted by 527th Military Police Company Soldiers using the SEEKERe, an automated colorimetric handheld device. (U.S. Army photo)

Conclusion

The 709th Military Police Battalion S-2 cell's intelligence and operations process denied adversary anonymity, assisted in identity intelligence discovery, and developed intelligence that supported operations throughout the exercise. For the first time, an exercise demonstrated the successful implementation of IDEX capabilities at the tactical level. Additionally, the 527th Military Police Company used the DEX training portal as an introductory familiarization platform for the submission of biometric enrollments, DNA samples, and explosive residue. The synergy of all intelligence professionals and linguistic enablers resulted in the successful execution of the exercise. Planning considerations must involve "thinking outside the box"—asking the questions of how one can achieve the mission and meet the commander's intent through collaborative efforts with external enablers.

Endnotes

1. North Atlantic Treaty Organization (NATO), Allied Joint Publication-2.5(A), *Captured Persons, Materiel, and Documents* (Brussels: NATO, 1 August 2007).

2. SALUTE: size, activity, location, unit identification, time, and equipment.

3. "Partner Solutions," Integrated Biometrics, 2022.

4. "SEEKERe Explosives and Narcotics Detection," DetectaChem, 2015.

CPT Brian Choe has served over 15 years in the Army. He is a counterintelligence officer/battalion S-2 for the 709th Military Police Battalion in Vilseck, Germany. Before his direct commission, he was a staff sergeant with military occupational specialties of 37F (Psychological Operations Specialist), 35F (Intelligence Analyst), and 35L (Counterintelligence Agent). He holds a bachelor of arts in psychology from Pepperdine University and a master of science in emergency services administration from California State University Long Beach. Previously, he was the counterintelligence team chief for U.S. Africa Command, Combined Joint Task Force Horn of Africa J-2X, in Mogadishu, Somalia.

***Contributor:** Mr. Matthew Haubrich is a defense contractor working as the lead forensic and biometric-enabled intelligence training and fusion integrator for U.S. Army Europe and Africa G-34, Identity and Exploitation Operations Branch. He has more than 14 years of intelligence experience and has worked for the Defense Intelligence Agency, National Ground Intelligence Center, U.S. Army Special Operations Command, and Combined Joint Task Force Horn of Africa.*

Freedom to Maneuver: Information Collection, Security, and Targeting in the Division's Consolidation Area

by Major Wesley Riddle and Captain Spencer Larson

Introduction

In 2020, the Georgia Army National Guard's 648th Maneuver Enhancement Brigade (MEB) committed to participating in warfighter exercise 21-03 as a subordinate unit to 3rd Infantry Division, tasked with security within the division's consolidation area. As a training audience, the MEB sought to exercise its mission command processes, refine and validate standard operating procedures, and train on mission essential tasks. This article describes—

- The lessons learned that made the MEB's information collection and targeting processes successful.
- The task organization that was eventually identified as the most effective given our subordinate units.
- The way the information collection plan was adapted to the limited collection capabilities internal to the MEB.
- The approach used to integrate the intelligence and fires sections to provide timely targeting and effects on enemy forces.

Additionally, this article addresses challenges we encountered in these areas and describes how we overcame or minimized them.

Achieving Staff Integration

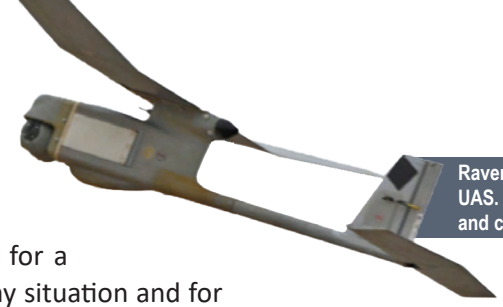
In August 2020, elements of the 648th MEB participated in a staff exercise with elements of the 3rd Infantry Division and 3rd Sustainment Brigade at Fort Stewart, Georgia. This was the first time the MEB, 3rd Infantry Division, and 3rd Sustainment Brigade had attempted to co-locate and integrate the staffs to effectively manage the division's consolidation area. The coronavirus disease 2019 (COVID-19), both its quarantine requirements and mitigation measures, had a significant impact on the MEB's ability to effectively conduct the unit's mission. In one instance, COVID-19 resulted in the quarantine of an entire signal company, severely degrading the MEB's ability to maintain situational awareness.

At the beginning of the staff exercise, the tactical operations center for the MEB was not co-located with the support area command post (SACP), and the SACP was not co-located with the tactical operations center for the 3rd Sustainment Brigade. All three headquarters were geographically separated, impeding efforts to fully integrate the respective staff sections. Initially, individual brigade and SACP commanders took the command and battle update briefs separately but did not achieve relative situational awareness of what each staff had planned. The biggest lesson learned from the staff exercise was to fully integrate the staffs of the three different elements. By the end of the exercise, intelligence section personnel from the SACP, the MEB, and the 3rd Sustainment Brigade began coordinating efforts and building an integrated planning process. This enhanced both communication and situational awareness because it eliminated three separate planning processes by different staffs.

> "The biggest lesson learned from the staff exercise was to fully integrate the staffs of the three different elements."

This lesson was carried over into subsequent command post exercises in September, October, and November, and all three staffs incrementally integrated further during each exercise. The staffs were fully integrated by command post exercise 3 in November 2020. During this 5-day exercise, the intelligence sections of each headquarters held joint briefings, shared maps and intelligence products, participated in intelligence updates, and, most importantly, were all co-located under the same tactical operations center—an enlarged SACP. While each brigade maintained its own separate command and planning tent, it was a short walk from the MEB intelligence section to the 3rd Sustainment Brigade intelligence section. The SACP intelligence section was located in between both. This setup was ideal because the SACP intelligence section maintained the intelligence picture for the SACP commander on the main floor of the combined operations and intelligence center, and both the 3rd Sustainment Brigade and the MEB intelligence sections were able to update their respective commanders as needed in separate portions of the command area.

The integration of the intelligence sections of the SACP, the 3rd Sustainment Brigade, and the MEB was a lesson learned over the course of 5 months that allowed for a better understanding of the enemy situation and for a more accurate targeting picture in the division's consolidation area. This directly enabled commanders to have a better awareness of the enemy's intent and location, allowed the MEB and 3rd Sustainment Brigade to effectively resupply the division, and allowed the division to be successful during the warfighter exercise.



Raven unmanned aircraft system (UAS). The Raven is a lightweight UAS. It is designed for rapid deployment and high mobility for military and commercial operations.

Command Post Organization and Employment Considerations[1]

Commanders organize command posts based on the mission requirements and the conditions that will provide them with the best command and control. Factors that affect the planning of command post organization and employment can be categorized as—

- Those contributing to effectiveness.
- Those contributing to survivability.

These factors often work against each other, requiring tradeoffs to balance effectiveness and survivability.

An effective command post is arranged to facilitate coordination, to exchange information, and to enable rapid decision making. However, command post survivability is vital to mission success. Depending on the threat, command posts need to remain as small as possible and retain mobility. Size makes them vulnerable to acquisitions through visual, auditory, electromagnetic, and digital signatures, which can lead to an attack.

Task Organization That Enabled Success

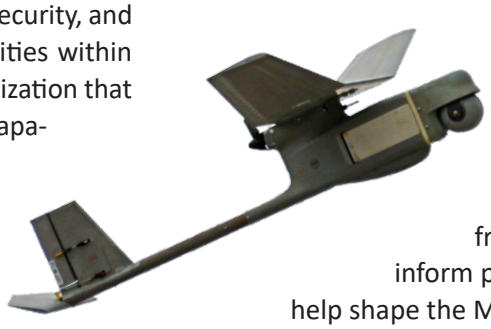
The 648th MEB's doctrinal tasks include support area operations and maneuver support operations as defined in FM 3-81, *Maneuver Enhancement Brigade*. To accomplish their mission, the MEB can be task-organized with engineer assets; chemical, biological, radiological, and nuclear assets; military police; explosive ordnance disposal assets; intelligence assets; and a tactical combat force with the MEB as the support area controlling headquarters. During warfighter exercise 21-03, the MEB was task-organized with a cavalry squadron, a light infantry battalion, additional military police assets, a fires battery of M777 howitzers, and elements of an expeditionary military intelligence battalion, all of which were critical to the success of the MEB's information collection, security, and targeting. The limited organic collection capabilities within the MEB must be reinforced through a task organization that enables the MEB to employ additional collection capabilities in the division's consolidation area. This is necessary because the division's primary collection focus, and where most of the division and national-level assets are tasked, is the deep and close areas of the fight.

Information Collection in the Division's Consolidation Area

Without being augmented by specific collection capabilities, the MEB is organically capable of limited information collection. The MEB relies primarily on collection from the Raven unmanned aircraft system (UAS) in the military police companies, the chemical threat detection from the chemical company, and the route reconnaissance capability provided by the engineer company. Outside of these limited collection capabilities, the MEB fully relies on higher or adjacent units, unless task-organized with an element that retains its organic collection capability. These can include an infantry battalion and its Shadow UAS company or a military intelligence company with its human intelligence (HUMINT), signals intelligence (SIGINT), and counterintelligence capabilities, which provide the intelligence data necessary to gain full situational awareness.

To ensure the success of the targeting process, the MEB had to maximize the use of all assets for the collection process. The military intelligence element provided passive collection, including HUMINT and SIGINT capabilities. The MEB relied on the collection from Raven UAS that are internal to subordinate units during reconnaissance patrols and security patrols. The MEB was also able to leverage collection capabilities of adjacent units. Residual collection from the Shadow UAS and Gray Eagle UAS maximized aerial surveillance of the consolidation area. Patrolling subordinate units established the common intelligence picture for the brigade. The cavalry squadron conducted reconnaissance (area, zone, and reconnaissance in force), the military police and light infantry conducted security patrols, and engineers conducted route clearance with support from explosive ordnance disposal. The operations process directed subordinate units to be proactive in their maneuver throughout the consolidation area, driving the targeting process.

Being fully integrated with the SACP intelligence section and the 3rd Sustainment Brigade intelligence section allowed the MEB to fully leverage the collection capabilities of the division and better inform the MEB commander of threats and opportunities in the division's consolidation area. It is critical for the MEB intelligence staff to be able to access reporting and intelligence feeds from division and higher assets to inform planning by the MEB staff and to help shape the MEB commander's decisions.



Targeting in the Division's Consolidation Area

The MEB refined its targeting process using the decide, detect, deliver, and assess methodology, and had two parts to the targeting process: deliberate targeting and dynamic targeting. Dynamic targeting was successful because of a preplanned process applied by the brigade fires section that outlined succinct fire clearance procedures and a developed working relationship with the Joint Air-Ground Integration Center and Division Artillery. The dynamic process of targeting maximized the use of the battalion's internal mortars, with the cavalry and infantry battalion firing 230 missions.

Deliberate targeting was less defined at the beginning, but the staff was able to refine the process. In order to implement the MEB commander's "aggressive targeting" plan, the MEB intelligence staff analyzed terrain and population areas to determine named areas of interest for collection by intelligence assets. The collection process fed directly into deliberate targeting and the MEB's targeting working group, which synchronized intelligence, fires, maneuver, and protection warfighting functions. The targeting working group also dictated requirements to coordinate with higher headquarters and adjacent units following division targeting within the air tasking order cycle. The significant challenge to deliberate targeting within the consolidation area is predictive analysis. The division's consolidation area continually expands as the division close fight extends across the battlefield. Analysis and intelligence collection have two priorities to support targeting: identification of bypassed and left behind threat forces and dynamic threats to security. The MEB's success in deliberate targeting was the synchronization of the warfighting functions to drive subordinate units to be proactive in security, going out and finding threats within the area of operations. The synchronization during the targeting working group turned named areas of interest into target areas of interest, which allowed fires to pre-plan targets for quicker delivery and assessment.

While the MEB targeting process is still developing, warfighter exercise 21-03 provided significant insight and gains into how the staff integrates and synchronizes efforts to maximize security within the division's consolidation area and support area. Targeting within the area of responsibility allows the MEB to conduct support area operations, a mission essential task. Proactivity in the support area is key to enforcing protection and deterring the enemy. A MEB does not have the organic assets needed to accomplish the mission; task organization is crucial to its success. The staff provides assessments and recommendations, allowing the MEB to be a multifunctional headquarters in support of division operations.

Conclusion

The MEB's experience during warfighter exercise 21-03, including the staff exercise and three command post exercises leading to the main exercise, emphasized the need for additional collection capabilities through task organization. These capabilities enable the MEB to maintain situational awareness throughout the division's consolidation area. They also provide the means for more deliberate and informed planning during the military decision-making process that identifies potential named areas of interest (both in the division's consolidation area and projecting forward as the fight moves) that become target areas of interest. Additionally, these capabilities enable the development of an effective fires coordination process and flexible staff in the fires and intelligence sections who can dynamically target and synchronize across warfighting functions to empower the MEB's mission.

Endnote

1. Department of the Army, Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington DC: U.S. Government Publishing Office, 16 May 2022), 7-8–7-11.

MAJ Wesley Riddle is the brigade intelligence officer for the 648th Maneuver Enhancement Brigade in the Georgia Army National Guard. He holds a master of strategic intelligence from the National Intelligence University and is a designated Strategic Intelligence Officer. He previously served as an instructor at the College of Strategic Intelligence with the National Intelligence University and as the battalion operations officer of the 221st Expeditionary Military Intelligence Battalion. He has one deployment to Afghanistan in support of Operation Enduring Freedom.

CPT Spencer Larson is a military intelligence officer in the Georgia Army National Guard. He is the brigade assistant S-2 for the 648th Maneuver Enhancement Brigade. He holds a master of science in intelligence management with areas of focus in counterintelligence and counterterrorism. He previously served in the 3rd Infantry Division Main Command Post Operational Detachment as the company commander and operations officer, deploying to Afghanistan in support of Operation Freedom's Sentinel and Resolute Support.

INTELLIGENCE INTEROPERABILITY, ADVISING, & ARTEMIS

by Sergeant First Class Joshua R. Brown

Introduction

Security force assistance brigades (SFABs) operate worldwide across the three levels of warfare: tactical, operational, and strategic. Since October 2021, the 2nd SFAB's Maneuver Company Advisor Team 2120 has been employed in Senegal, building upon a Department of State-funded peacekeeping operations training. This effort is preparing Senegalese trainers for future United Nations (UN) missions across the western and central African regions. Maneuver Company Advisor Team 2120 advisors have planned and are executing tactical and operational-level foundational training, but that is a fraction of what a company-level advising team can do. In this case, the training recipients are the Senegalese Army tactical training centers' cadre tasked with preparing contingents of the Senegalese Army to support various UN missions. Using the *United Nations Infantry Battalion Manual (UNIBAM)* as a common framework, advisors and partners recognize the overlap and differences in doctrine and tactics, techniques, and procedures (TTP) across the tasks a UN infantry battalion must execute while in support of peacekeeping operations.

The Interoperability Nexus

The overlap and differences in TTP are opportunities to build upon a shared understanding of a common military exchange. This type of opportunity is what the team refers to as an *interoperability nexus*, also called an IN. INs are areas where any team geographically at the tactical edge (physical or digital) can strengthen the relationship, enhance the lethality of the combined force, and mature the theater by establishing a mutual understanding of "how." Enhancing INs minimizes differences in execution, enabling combined formations to do the tasks of planning, executing, and communicating (horizontally and vertically) with greater functionality.

A Maneuver Company Advisor Team advisor demonstrates the Aerial Reconnaissance Tactical Edge Mapping and Imagery System airframe to partner forces. (Photo by SFC Michael Ortiz)

A Senegalese Army lieutenant and a Maneuver Company Advisor Team advisor review a sand table in support of the United Nations Multidimensional Integrated Stabilization Mission in the Mali contingent combined arms live fire exercise. (Photo by SSG Dylan Garner)

INs exist across all levels of the interoperability framework (operational, systems, technical, and procedural) and all warfighting functions. Three primary lines of effort provide an opportunity to generate greater interoperability. The team must—

- ✦ Identify INs and areas where there are differences.
- ✦ Ensure that there is an observed training requirement at the tactical and operational levels.
- ✦ Demonstrate a willingness to take an innovative approach when confronted with a task. Sometimes a partner cannot procure a particular capability because of limited financial resources. However, some creative thinking and innovative design with commercially procured items used as training aids can reduce the gap and bridge the partner's material limitations.

These three lines of effort enable advisors and partners to set conditions for both elements' success. Every IN is an opportunity for partners and advisors to mature an immature theater, regardless of which paradigm, placement, or access an advising team is targeting to develop.

UN doctrine, specifically the *United Nations Infantry Battalion Manual (UNIBAM)* and the *United Nations Military Peacekeeping-Intelligence Handbook (MPKI HB)*, is the common foundation that brought Maneuver Company Advisor Team 2120 advisors together with Senegalese Army counterparts. These two documents describe the common standards for UN elements. They ensure interoperability across planning, operating, and communicating.

United Nations Infantry Battalion Manual (UNIBAM)

"The purpose of...[this manual] is twofold. It provides Troop Contributing Countries (TCCs) with guidance on how to train [and] equip units deploying to UN Peacekeeping Missions, and it provides battalion commanders and staff, company commanders, platoon commanders and sub-unit leaders in UN Peacekeeping with a reference to effectively plan and conduct operations and tasks in support of a UN mandate. This manual does not replace national doctrine. Rather, it is designed to highlight UN operational standards, which should be overlaid on existing doctrine, thereby assisting a conventional Infantry Battalion (Inf Bn) operating in its national role to prepare for UN operations as 'blue helmets.' "[1]

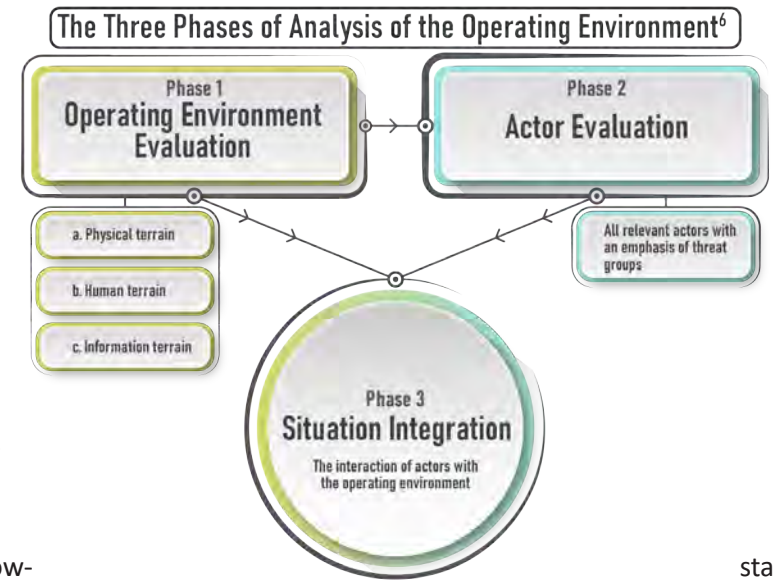
United Nations Military Peacekeeping-Intelligence Handbook (MPKI HB)

"The aim of this handbook is to support personnel deployed in MPKI roles in UN peacekeeping operations...Key to understanding peacekeeping-intelligence is its distinction with information...The primary difference between the two is that information is factual reporting about events that have happened, while peacekeeping-intelligence is an assessment—derived from the analysis of the reporting.[2]

A critical IN that Maneuver Company Advisor Team 2120 sought to improve is within the first step of the UN military decision-making process, which addresses analysis of the operating environment.[3] This includes small unmanned aircraft systems (sUAS) operations and information acquisition, a key focus area for Maneuver Company Advisor Team 2120. Expanding this IN involves deepening the UN peacekeeping contingent's familiarity with incorporating these skills into the planning phase. The aim is to demonstrate the required skillset to develop an operational to tactical intelligence enterprise and then to include the full breadth of the contingent's organic sensors and architecture into mission planning. This will result in enhanced situational understanding and lower risk during mission execution, two areas that the current contingent commander and our assessment had identified as a gap. It will also lead to improving our partners' ability to mitigate anticipated future risk to the force and mission.

Integrating Innovation—Training Fundamentals

Before the 2nd SFAB's inaugural deployment to Afghanistan in 2019, the National Geospatial-Intelligence Agency's Warfighter Support Office partnered with the brigade S-2 to train, equip, and field the Aerial Reconnaissance Tactical Edge Mapping and Imagery System (ARTEMIS). Throughout that deployment, the Train, Advise, Assist Command-East G-2 employed ARTEMIS with resounding success. Successes in Afghanistan triggered a similar approach between the National Geospatial-Intelligence Agency and the 2nd SFAB force package (FP) 22-1. To that end, FP 22-1 fielded and employs ARTEMIS in Ghana and Senegal.



ARTEMIS is a low-risk, low-cost mapping platform that places the entire tasking, collection, processing, exploitation, and dissemination (TC–PED) cycle in the hands of the consuming element. Supplying outputs comparable to theater mapping assets (for example, Light Detection and Ranging, known as LIDAR, and Buckeye) at scale, ARTEMIS operationalizes the TC–PED timeline for the tactical consumer. Effectively, a platoon element could reconnoiter a route or objective at 0800, process the data by 1200, integrate it into their common visualization (for example, Tactical Awareness Kit or Google Earth) by 1300, incorporate it into their mission analysis, and still have 7 to 9 hours to rehearse before executing a night mission.

Maneuver Company Advisor Team 2120 developed two TTP exchanges between the United States military and the Senegalese military during the deployment. The first exchange focused on understanding sUAS operations, with an emphasis on shifting the use of sUAS from the execution phase to the planning phase, identified from an assessment and a gap based on prior partner training. To this end, the discussion consisted of breaking down the TC–PED cycle and understanding organic information acquisition assets in terms of sensor, processor, output, and transport (SPOT). The second exchange built on the concepts covered during the first exchange and deepened information acquisition fundamentals, applying these fundamentals to a broader array of assets within a constructive exercise environment. Attendees analyzed the operating environment and then evaluated the "known" actors. Upon working through step one (operating environment evaluation) and step two (actor evaluation) of the analysis of the operating environment in the *United Nations Military Peacekeeping-Intelligence Handbook (MPKI HB)*, attendees developed an information acquisition plan.[4] This included identifying requirements, assessing assets, tasking assets against the requirements, assessing the collection, and using insights gained to more fully integrate the situation, which is step three (situation integration) of the analysis of the operating environment.[5]

Coordinated Efforts—Transformational Benefits

The value captured for SFABs lies in using ARTEMIS not merely as an organic information acquisition asset but also as a tool to assist with training processes. The key takeaway is not "how to operate this particular sUAS," but rather to understand that information acquisition is a series of techniques designed to achieve specific goals. Regardless of the sensor, we use these techniques and processes at the tactical and operational echelons (and higher echelons, at scale). Deepening this IN is the result of reps and sets, applying the techniques to specific tasks (reconnaissance versus surveillance), different sensors (Soldier as a sensor, publicly available information, and human intelligence), and different conditions and constraints. ARTEMIS is merely the chisel used to widen this specific IN. ARTEMIS is a resource that the advisor can use, coupled with podium instruction, to demonstrate, hands-on, the entirety of SPOT and TC–PED within a compressed timeline. Additionally, using a tool such as ARTEMIS adds the ability to build upon

the transformational relationship between the United States and Senegal, creating a common bond of trust and enhancing our military partnership. This approach allows both elements to gain without an anticipated reciprocal return. It will pave the way for continued placement and access as we share nested objectives against the worldwide threat of terrorism.

Setting Conditions for Continued Success—Assess

The concept of INs transcends warfighting functions. Coupling agile acquisition efforts with grassroots innovation, any advisor on a team can identify a nexus and develop a novel solution to enhance it, as solutions range across DOTMLPF–P.[7] Sometimes the answer is hardware. Sometimes a standard process or the solution can manifest in a conversation during a shared meal. Regardless, in the case of ARTEMIS and FP 22-1, the solution cart preceded the nexus horse. FP 22-1 arrived in theater with a capability and at once set about fully using it. Assessments and insights gleaned through FP 22-1's experience can help identify future INs for future force package teams. Applying these lessons learned ensures continued success and relevancy. Taken as a whole, these lessons learned contribute to the very essence of maturing the theater in tandem with a partner and a country team who are already identifying new and exciting requirements, with future SFAB force packages as the delivering party and the United States as the preferred partner.

Endnotes

1. United Nations Department of Peace Operations, *United Nations Infantry Battalion Manual (UNIBAM)* (New York: United Nations, 2020), viii.

2. United Nations Department of Peace Operations, *United Nations Military Peacekeeping-Intelligence Handbook (MPKI HB)* (New York: United Nations, 2019), introduction.

3. Ibid., 105.

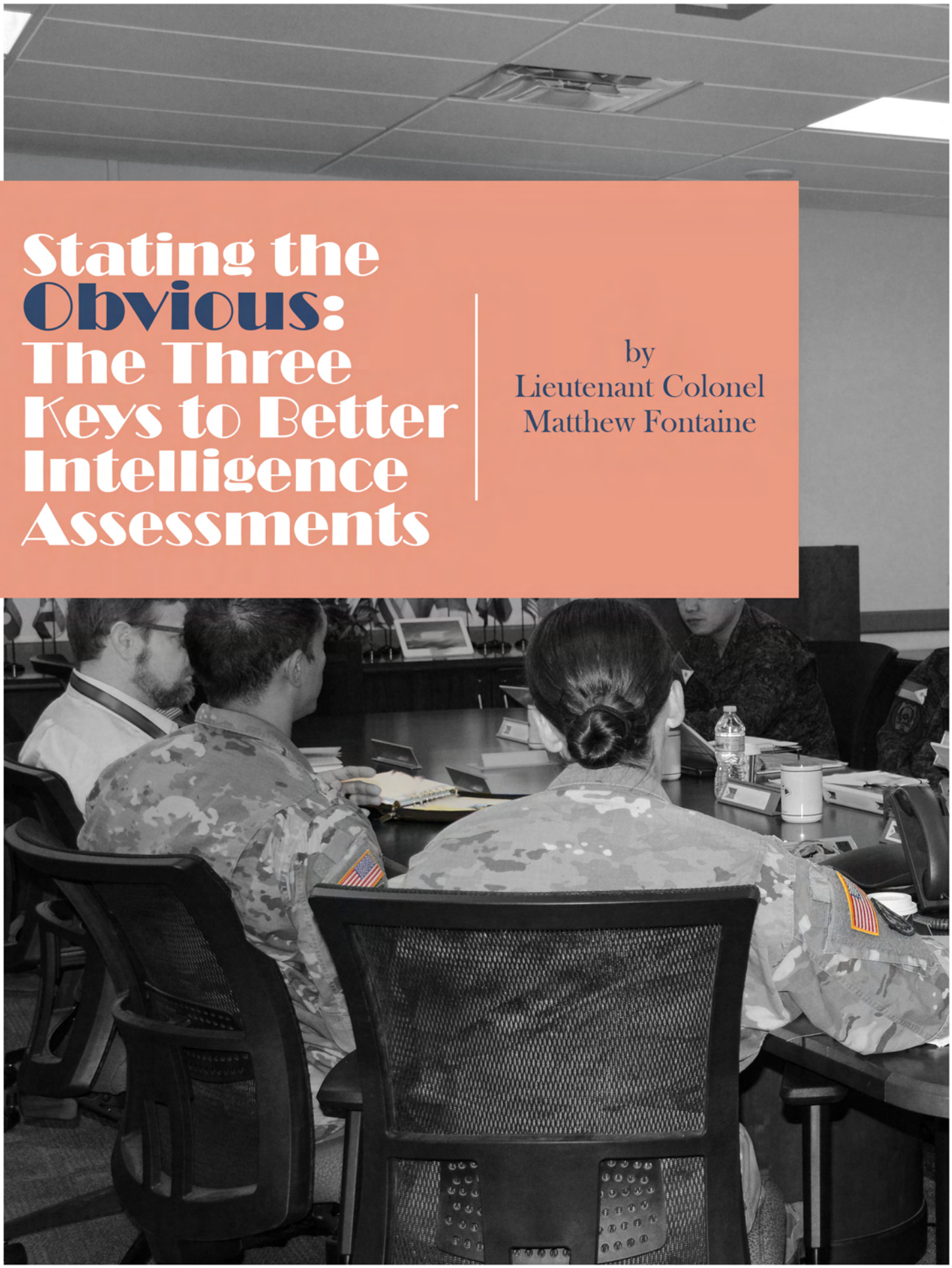
4. Ibid., 75.

5. Ibid.

6. Ibid., adapted from original.

7. DOTMLPF–P: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

SFC Joshua Brown serves as the intelligence advisor on Maneuver Company Advisor Team 2120, currently in Thiès, Senegal. He has served at every echelon at 2nd Security Force Assistance Brigade, most recently as the senior signals intelligence sergeant and technical integrator in the brigade S-2. His military education includes the Basic Operator Training Course, the Digital Network Exploitation Advanced Course, the Advanced Individual Terrorism Awareness Course, the Security Force Assistance Advisor Course, and the Digital Intelligence Systems Master Gunner Course. He served as a flight trainer at Alpha Company, 3rd Military Intelligence Battalion (Aerial Exploitation), and as the Task Force Observe, Detect, Identify, and Neutralize (ODIN) liaison to the General Command of Police Special Units. He also served as the Headquarters and Headquarters Company platoon sergeant and operations noncommissioned officer at the 743rd Military Intelligence Battalion. SFC Brown's campaign support includes Operation Freedom's Sentinel. He is currently on assignment to the 207th Military Intelligence Brigade-Theater.



Stating the Obvious: The Three Keys to Better Intelligence Assessments

by
Lieutenant Colonel
Matthew Fontaine

Introduction

There is no shortage of stories, books, or articles on military intelligence failures. In recent history, the two most famous examples are the September 11 terrorist attacks and the inability of the United States to find weapons of mass destruction in Iraq, even though intelligence assessments indicated the likely existence of those weapons and provided justification for the 2003 invasion of Iraq.[1] Even more recently, the media was abuzz (some would argue unfairly) with the "intelligence failure" in Afghanistan after the Taliban's swift takeover in August 2021.[2] I recall my own failed assessment during a rotation at the Joint Readiness Training Center as a lighthearted example. I confidently announced to the brigade commander, while an observer coach/trainer's video camera rolled (*ouch*), that the enemy's main attack was along the northern avenue of approach, just shortly before the bulk of their forces came crashing through our southern positions.

Assessments are essential to successful outcomes. Based on my observations and the experience I gained from assessing assessments while assigned to a Department of Defense agency, I now understand the *greatest secret* to a well-developed assessment—one most likely to support a *winning decision* because of its discussion-generating potential.[3] According to decision-making process experts J. Edward Russo and Paul J. H. Schoemaker, a winning decision is about "getting it right the first time."[4] While I will not argue for or against the effectiveness of United States intelligence in Iraq and Afghanistan, or the Joint Readiness Training Center for that matter, I believe that analyzing an assessment's building blocks will lead to more useful outcomes. Specifically, I believe that the best assessments—

- ✦ Make an argument.
- ✦ Make a prediction.
- ✦ Use estimative language.

Yes, it is that simple. My definition might seem trite; it might seem obvious. Yet, in my experience, too few intelligence assessments contain these three basic keys. While quality intelligence is the result of many factors, if your assessment fails to make a clear argument, make a prediction, or use estimative language to express the likelihood of an event or the level of confidence attributed to a judgment, your organization is bound to run into difficulties.[5] Intelligence professionals make assessments all the time. We assess the impacts of the weather, craft threat courses of action (COAs), and take a stance on what a strategic competitor may or may not do in an area of interest. Intelligence assessments are our products, what we go to work to do.

This article will discuss each of the three keys in detail and your part in assessment development. I will start by revisiting the definitions of terms according to doctrine and professional literature. Then I will demonstrate how the three keys are grounded in those ideas. It is my hope you will agree with all-American athlete and professional coach Dan John, who says, "the greatest secret…in every field of life is always something obvious" and recommends that we master the obvious first before addressing the smaller details.[6]

The Intelligence Assessment in Doctrine and Professional Literature

Doctrine defines *intelligence estimate* as "the appraisal…of available intelligence relating to a specific situation or condition with a view of determining the courses of action open to the enemy or adversary and the order of probability of their adoption."[7] Simple enough. Doctrine and common usage use the word *assessment* interchangeably with *estimate* and *appraisal*.[8] For this article, I will do the same.

In professional literature, I will use Sherman Kent, a towering figure in the history of the Central Intelligence Agency, as my expert. Sherman Kent wrote, "estimating is what you do when you do not know" in his essay on estimative intelligence, first published in 1968.[9] He imagined the perfect estimate as a complete pyramid (Figure 1, on the next page).[10] Near-certain facts relevant to the examined situation represent solid blocks of stonework that form the pyramid's base.[11] The ideal apex of the pyramid is the precise answer we are looking for—"that if we know this with certainty we will have what we are after."[12]

Working from the base, the analyst builds the pyramid's foundation by stacking new material through the art and science of analysis.[13] The analyst constructs the pyramid's actual peak for a real-world estimate when the analyst can no longer support new, genuine deductions—"we reason our way up the pyramid toward the top."[14] Sherman Kent calls this peak a "*useful approximation*"—"a mix of fact and judgment," which he says is the "next best thing to 'knowing' " (Figure 2, on the next page).[15]

Sherman Kent's pyramid analogy also incorporates confidence levels. The facts stack vertically to create the general slope of the pyramid. The shape of the peak represents the

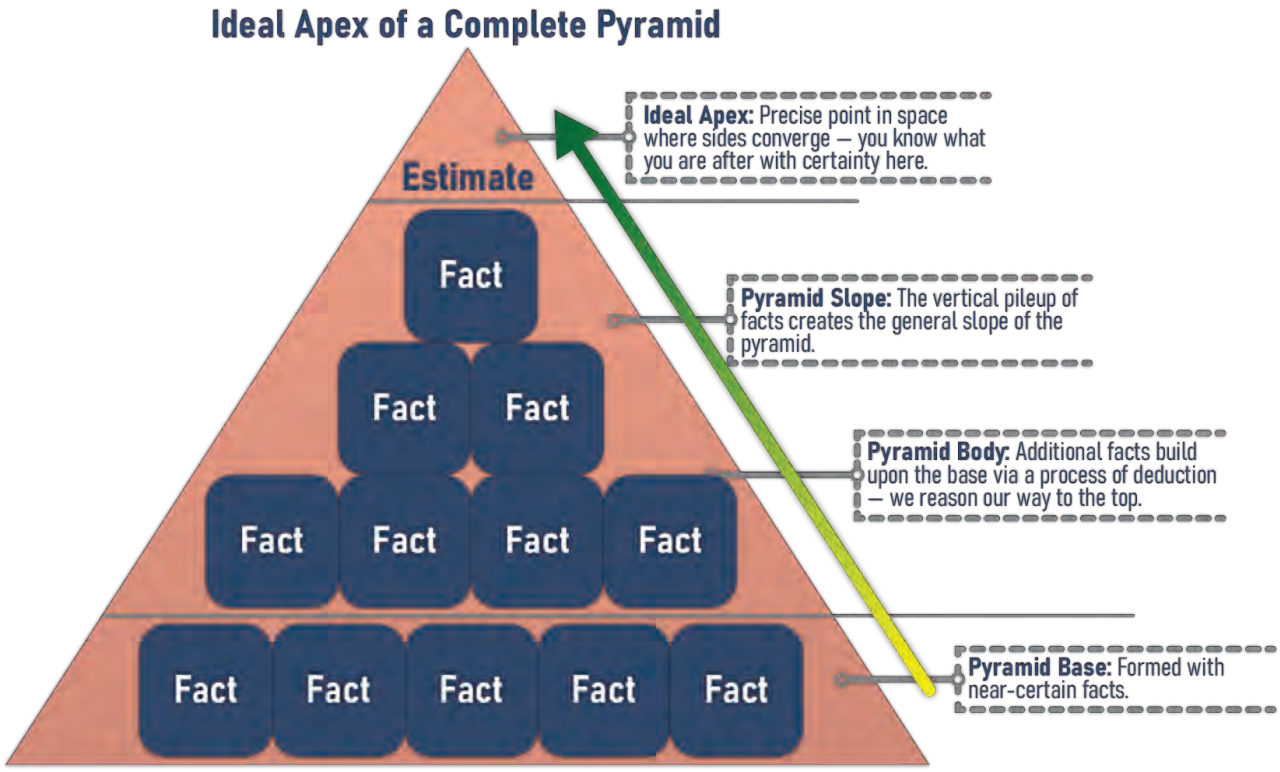


Figure 1. Sherman Kent's Pyramid of a Perfect Estimate[16]

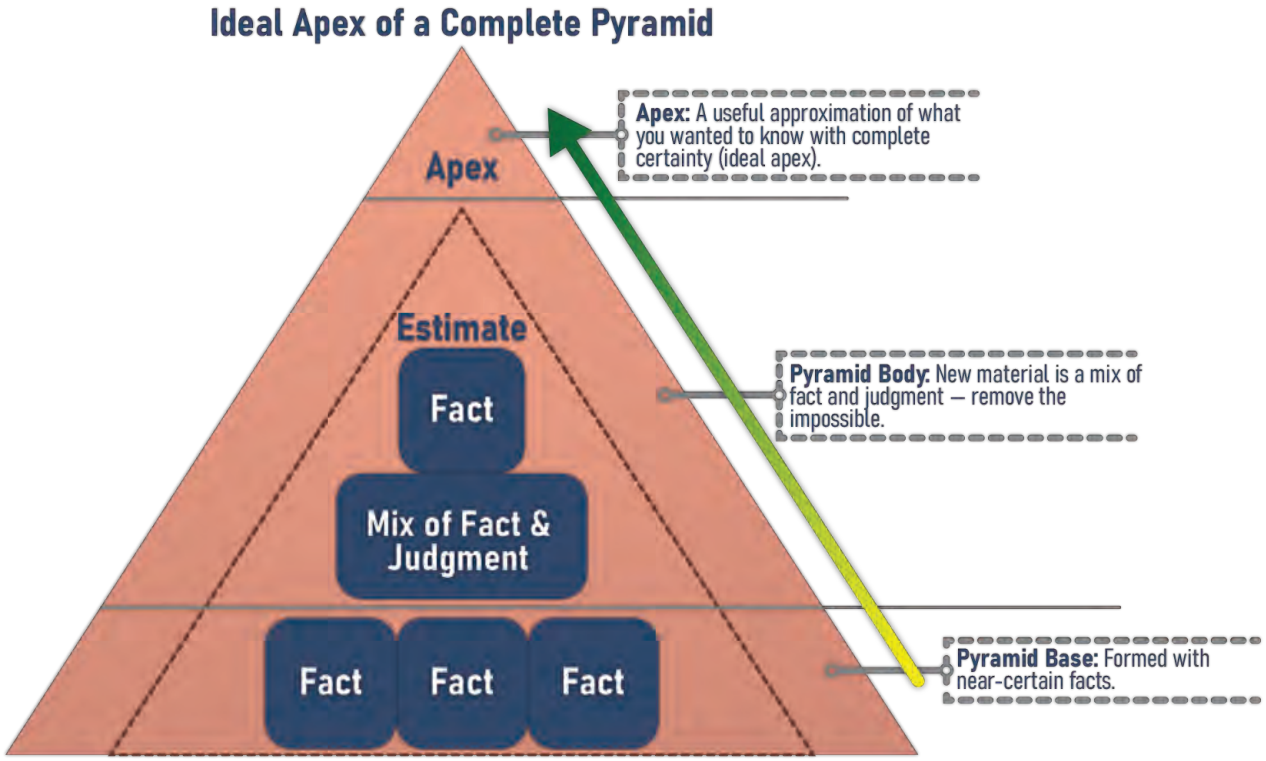


Figure 2. Sherman Kent's Pyramid of a Real-World Estimate[17]

analyst's degree of certainty to be conveyed to their audience in the finished product. A sharp rise demonstrates high confidence in an individual assessment, while increasing truncation of the pyramid (bluntness) corresponds to a lower confidence level and, therefore, a wider range of possibilities (Figure 3). The least useful assessments do not move beyond the base's facts and can hardly even be considered intelligence.[18]

As you can see, the three keys are in both doctrine and professional literature. When we make an argument and a prediction, doctrine asks us to predict a future adversary's COA based on the current situation. Similarly, Sherman Kent urges us to deduce a useful approximation of what we wish to know—one block (fact, judgment, or assumption) at a time. The judgment expressed in our COAs and useful approximations serves as our main analytic arguments. For estimative language, doctrine asks us to express future adversary actions in order of likeliness (probability). In comparison, Sherman Kent speaks of incorporating degrees of confidence in our estimates. Now that I have established their links to doctrine and professional knowledge, I will elaborate on each of the three keys and the danger of omitting them from our assessments.

The Three Keys and Their Associated Assessment Outcomes If Omitted

The best assessments contain clear arguments. A clear argument follows the basic paragraph structure:

- ✦ It opens with a central idea that takes a specific position.
- ✦ It supports the central idea in the ensuing body of the paragraph with several points.
- ✦ It ends with a conclusion while recapping the central idea.[19]

Obvious, yes, but too often, many assessments either fail to support a central idea with its pertinent facts and key assumptions or, worse, have no main idea at all. When this occurs, the principal is presented with raw data bereft of connections.[21] Using the pyramid analogy, we present a teetering obelisk (an unsupported central idea) (Figure 4, on the next page) or a shallow foundation (information only) (Figure 5, on the next page). In contrast, the best assessments—like the best arguments—leave no uncertainty regarding your primary contention and its supporting rationale.[22]

The most useful assessments also make predictions. The utility of intelligence is it anticipates future occurrences and informs the decision maker by revealing the variances in possible COAs.[23] Using Sherman Kent's analogy once more, we imagine a nonpredictive assessment as a pyramid with a severely truncated top (many COAs), so broad and featureless that the audience cannot discern anything that would indicate the occurrence of one possibility over the other. In this instance, the analyst fails to move beyond the basic facts and produces an assessment more akin to "news" as opposed to intelligence.[24] The analyst becomes a broadcaster.

Finally, analysts must use estimative language to convey confidence levels, expressions of likelihood, and ranges in their key analytic judgments.[25] Using the terms *low*, *moderate*, and *high* is a simple way to express a confidence level in a judgment.[26] The analyst's confidence level rests on the number of key assumptions, source credibility and diversity, and strength of argumentation.[27] As with an argumentative paragraph, an analyst must be able to justify their confidence level in a judgment using these three factors. Expressions of likelihood refer to the probability of a situation occurring

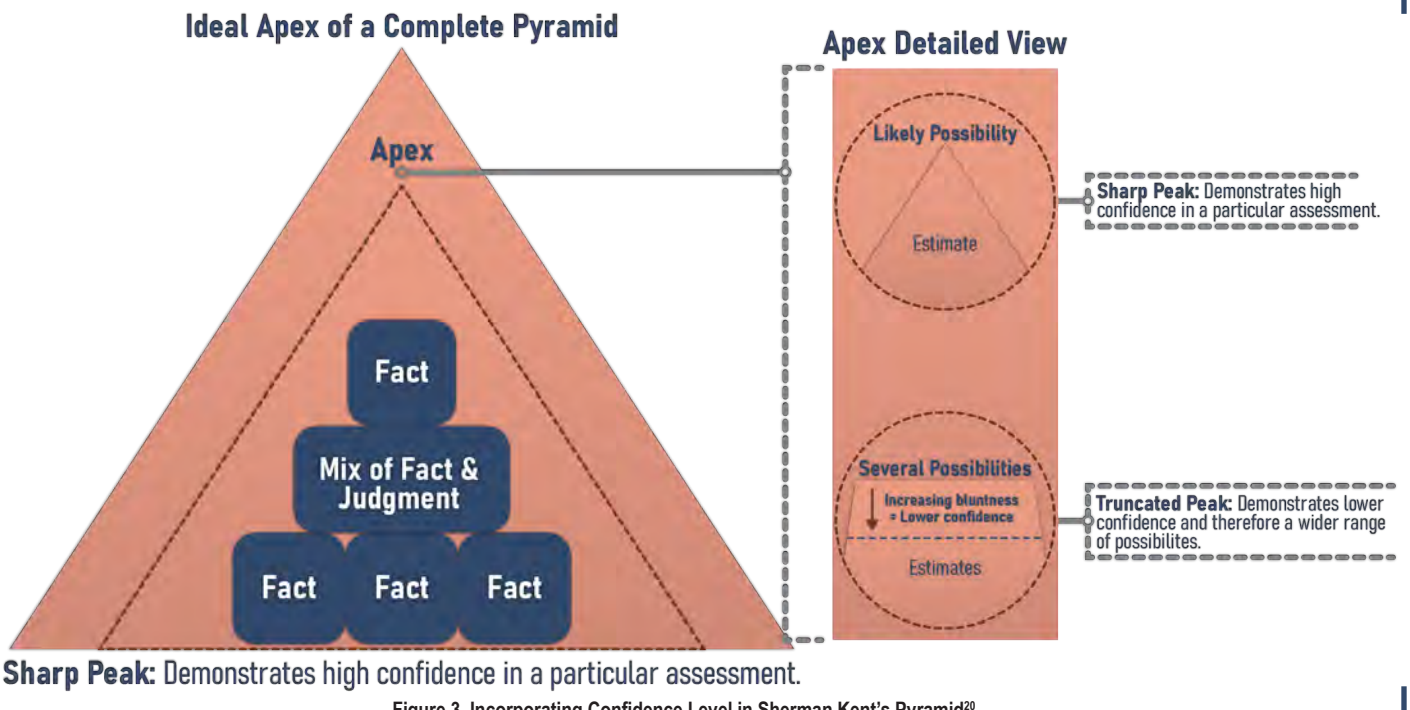
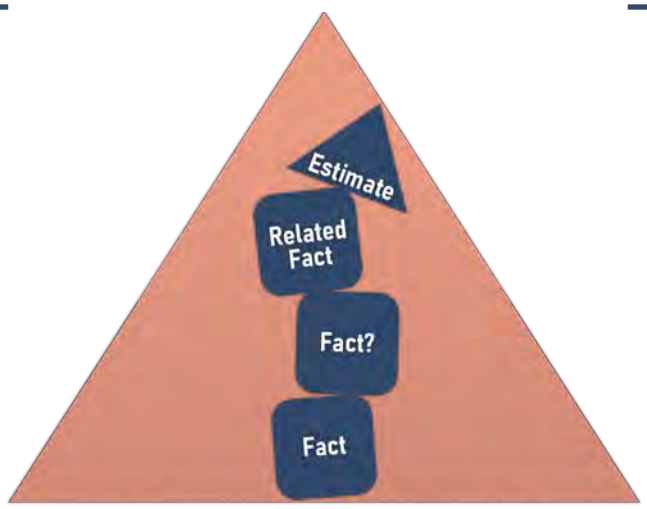
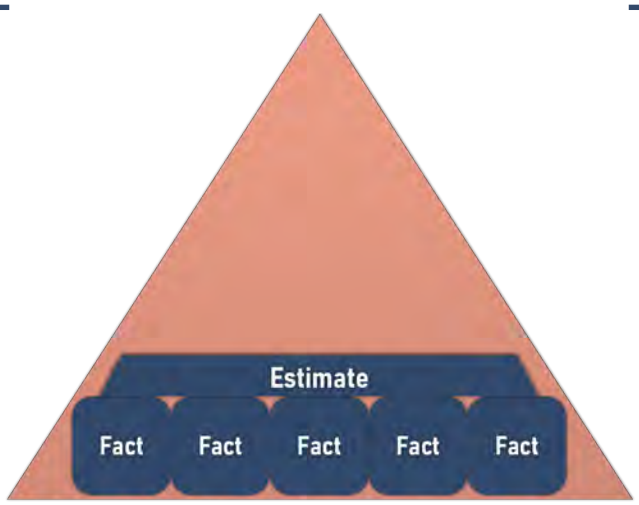


Figure 3. Incorporating Confidence Level in Sherman Kent's Pyramid[20]



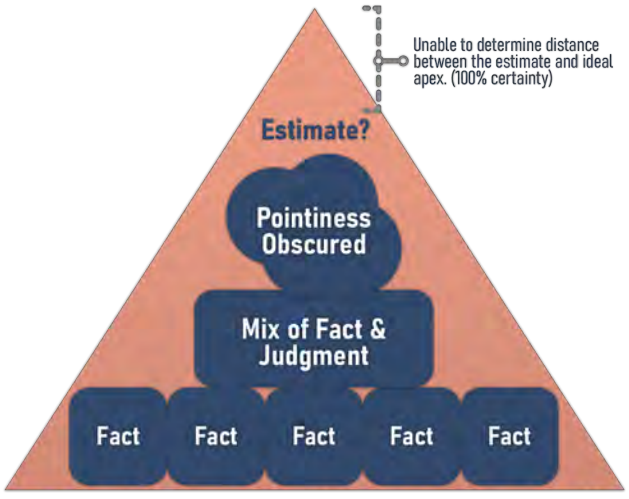
Unsupported Argument: Main idea presented with raw data bereft of connections.

Figure 4. Pyramid Missing the Three Keys to Better Assessments-The Teetering Obelisk[28]



No Argument or Prediction: No argument or prediction presented, just the facts — akin to reporting the news.

Figure 5. Pyramid Missing the Three Keys to Better Assessments-The Broadcaster[29]



No Estimative Language: No certainty or confidence expressed in in the judgment — audience left to determine validity.

Figure 6. Pyramid Missing the Three Keys to Better Assessments-Your Guess is as Good as Mine[30]

and include terms such as *almost no chance*, *roughly even chance*, or *almost certain*.[31] Additionally, an analyst's estimative language should incorporate ranges to provide a more accurate sense of uncertainty in assessment.[32] A range is the area between a specific judgment's upper and lower limits at a particular confidence level or expression of likelihood.[33]

Confidence levels, expressions of likelihood, and range estimates work together to complete a quality assessment. Please make use of them! However, analysts must be careful not to mix confidence and likelihood terms in the same sentence. Statements such as "we assess with low confidence (confidence term) that country Y will likely (likelihood term)…" can create confusion for your audience.[34] Instead, use the full suite of estimative language throughout your assessment. For example, "we assess with high confidence (confidence level) the main enemy attack will comprise 1 to 4 (range) tank companies and low confidence the main enemy attack will comprise 3 to 4 (range) tank companies. The enemy attack will almost certainly (likelihood) commence in the next 24 to 48 (range) hours due to…."

Unfortunately, even these simple estimative language terms or ranges are often missing in our assessments or are not always presented in the same way if included. According to doctrine, it is the very "estimative nature of intelligence [that] distinguishes it from the mass of other information available to the commander."[35] If that is true, much analytic output is not intelligence at all.

If we use the pyramid analogy once more, the audience has no idea of the pyramid's height (pointiness) in comparison to the ideal apex. If we cannot express the certainty or range of our assessments, we can hardly expect our principals to have what they need to make the right decisions. A non-estimating analyst tells the principal that their "guess is as good as mine" even though the analyst had the advantage of reviewing the judgment's supporting facts and assumptions in detail (Figure 6).

The Three Keys to Improve Decision Making via Discussion

Well-structured, predictive, and estimative assessments improve decision making by generating productive discussion within the organization. A clear statement such as "we assess with low confidence the enemy will attack along avenue of approach one with 2 to 3 tank companies" or "we assess with high confidence the fielding of weapon X by country Y will lead to regional conflict in 6 to 12 months" will no doubt raise important questions from the principal or staff. These questions might include—

- Why this confidence level or that range?
- Why these assumptions?

- What alternate hypothesis are we not considering here?
- What can be done to improve our position?

Feedback and follow-on actions (new analysis or collection) provide the information necessary to narrow the range of an assessment with an even greater level of confidence.[36] This iterative process results in an increasingly defined set of COAs by stripping away the impossible.[37]

Your Role in the Assessment Production Process

So, what role do YOU play in the assessment production process? If you are an analyst, incorporate the three keys into your main assessments (obviously). For everyone else, I see two priorities:

First—Increase Opportunities for Discussion. If you are an analyst, your role is to serve as an informal sounding board and critic of your fellow analysts' work. Supervisors enact a formal team and section review process to further increase the number of discussion iterations before briefing the assessment to the principal and staff. Formal review processes should use checklists—a tactic almost "ridiculous in its simplicity" to avoid disaster.[38] Fortunately, ATP 2-33.4, *Intelligence Analysis*, provides a wealth of analysis evaluation tools to incorporate into your checklists (for example, step 7, Evaluate analysis, in Table 9-1, Analytic design to tactical intelligence analysis crosswalk, shows a list of doctrinal concepts and references to apply in your review process).[39] However, as argued here, although analysts need to deal with the smaller details and advanced techniques in ATP 2-33.4, they must first master the obvious three keys.

Step 7, Evaluate Analysis
Doctrinal Concepts and References[40]

ATP 2-33.4:

- Answer the '*so what*' from the commander's perspective, par. 1-21.
- Determine relevancy before producing assessments, par. 1-27.
- Appendix B, *Cognitive Considerations for Intelligence Analysts*. (This appendix describes thinking abilities, critical and creative thinking, and avoiding analytical pitfalls.)
- Appendix C, *Analytic Standards and Analysis Validation*. (This appendix discusses the analytic standards that govern intelligence analysis.)

Second—Check Our Analytic Ego at the Door. The purpose of intelligence is to support the right decision, not to provide the right answer. Although careful analysis can reduce uncertainty, Sherman Kent's ideal apex is not likely to be reached for anything other than the simplest questions or just before an event occurs. Therefore, no analyst, team, or supervisor should ever feel wedded to an assessment. Additionally, no person has so much expertise on a topic that they would not benefit from the insight obtained from a diverse group. Woe to the intelligence section that sends an unchallenged, non-estimative best guess to a principal so as not to upset someone's ego. Artistic freedom is a thing; analytic freedom is not. Encourage analytic humility.

Putting It All Together—An Example Assessment with the Three Keys

I will now combine all three keys into the following simple assessment to demonstrate their use in a large-scale combat situation:

We assess with high confidence **(confidence level)** the 311BTG reinforced by 2–4 tank companies **(range)** attacks to seize objectives (OBJs) BULL and LION along avenue of approach (AA)1 in order to enable the seizure of the BIG BEND DAM **(prediction)**. **[ARGUMENT MAIN IDEA]** The attack will almost certainly **(likelihood)** commence in the next 24–48 hours **(range)** due to weather conditions favoring the offense **(prediction)**. **[SUPPORTING FACT]** Forward reconnaissance elements and single-source intelligence reports indicate the movement east of no less than two plus tank companies and possible, supporting artillery to 311BTG staging areas and battle positions 15 kilometers west of OBJ BULL along AA1. **[SUPPORTING FACT]** Coalition forces to our south report minimal enemy activity along AA2. **[SUPPORTING FACT]** Additionally, enemy reconnaissance elements were just observed in the vicinity of BIG BEND DAM. **[SUPPORTING FACT]** We assume the seizure of the BIG BEND DAM will provide political justification for the enemy offensive. **[ASSUMPTION]** These well-corroborated reports strongly affirm that the reinforced 311BTG is committed to the imminent seizure of BIG BEND DAM along AA1, but they do not preclude the possibility of a surprise attack along AA2. **[CONCLUSION]**.[41]

This clear assessment provides the friendly commander with the right intelligence at the right time. Remove any of the three keys and the strength of the argument drops considerably. Based on the assessment and the follow-on discussion, we would expect the commander to be capable of providing the necessary guidance to confirm and then effectively counter the enemy COA. In other words, we expect a winning decision.

The Great Secret

At this point, you likely realize the great secret to a well-developed assessment is no more than a common-sense statement of the obvious (Figure 7, on the next page). That is okay because you are in good company. BG Oscar Koch, who served as the G-2 for GEN George Patton in World War II, remarked that an important quality of an intelligence officer is "an abundance of honest-to-goodness, matter-of-fact, feet-on-the-ground common sense!"[42]

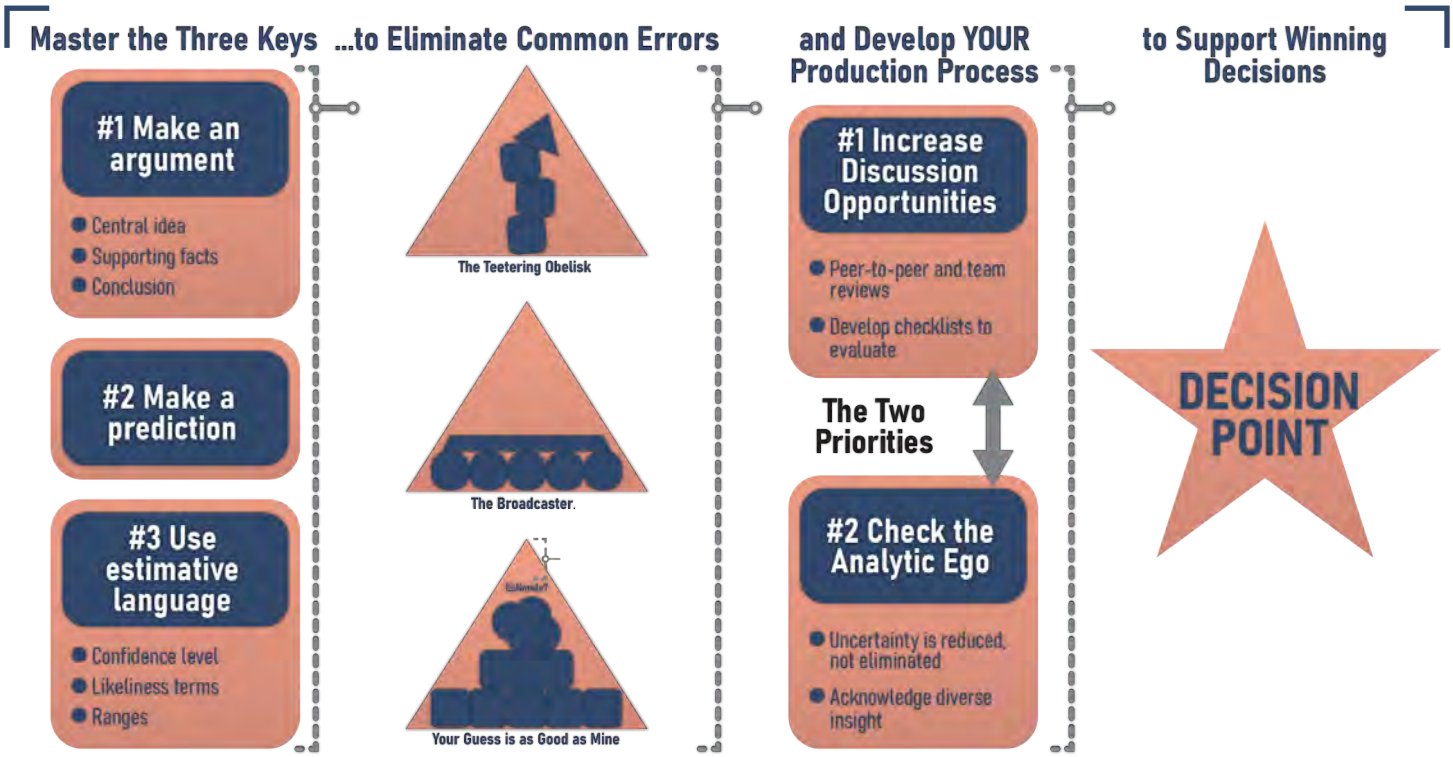


Figure 7. The Great Secret to a Well-Developed Assessment[43]

Conclusion

If your main assessment always makes a clear argument, makes a prediction, and uses estimative language, then continue to strive for superior analytic rigor using the advanced details and techniques in ATP 2-33.4. If your assessments are hit or miss in these areas, focus on mastering the three keys and the two assessment production priorities to generate the discussion needed to support better decision making ***now***. In the future, maybe you will be asked a question like "What makes you so sure they are going north?" before it is too late.

Endnotes

1. Michael A. Turner, *Why Secret Intelligence Fails* (Washington, DC: Potomac Books, 2006), x–xi.

2. Natasha Turak, Abigail Ng, and Amanda Macias, " 'Intelligence failure of the highest order'—How Afghanistan fell to the Taliban so quickly," CNBC, 18 August 2021, https://www.cnbc.com/2021/08/16/how-afghanistan-fell-to-the-taliban-so-quickly.html. The authors attribute the quotation to Bill Roggio, a senior fellow at the Foundation for Defense of Democracies.

3. Dan John, *Attempts: Essays on Fitness, Health, Longevity and Easy Strength* (Aptos, CA: On Target Publications, 2020), 21–29. I quote Dan John's term *greatest secret*. J. Edward Russo and Paul J. H. Schoemaker, *Winning Decisions: Getting it Right the First Time* (New York: Currency Doubleday, 2002), xii. I quote Russo and Schoemaker's term *winning decision*.

4. Russo and Schoemaker, *Winning Decisions*, xii.

5. John, *Attempts*, 21–29. Obviously, Dan John does not comment on intelligence production, but I adapted his argument that we should first "embrace the obvious" in our endeavors or risk failure. Department of the Army, Army Techniques Publication (ATP) 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. Government Publishing Office, 10 January 2020), C-2.

6. John, *Attempts*, 26.

7. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 22 May 2022), iii-7.

8. For example, the *DOD Dictionary of Military and Associated Terms* defines *commander's estimate* as an "initial assessment" and defines *battle damage assessment* as an "estimate of damage." JP 2-0, *Joint Intelligence*, defines *intelligence estimate* as an "appraisal." Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington DC: The Joint Staff, May 2022), 24, 41; and Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, GL-16.

9. Sherman Kent, *Sherman Kent and the Board of National Estimates: Collected Essays*, ed. Donald P. Steury (Washington, DC: History Staff, Center for the Study of Intelligence, Central Intelligence Agency, 1994), 35.

10. Ibid., 36.

11. Ibid.

12. Ibid., 37.

13. Kent, *Collected Essays*, 36–38.

14. Ibid.

15. Ibid. (emphasis added)

16. Graphic by author, using information from Kent, *Collected Essays*, 35–39.

17. Ibid.

18. Kent, *Collected Essays*, 35–39.

19. *Merriam-Webster*, s.v. "argument (*n.*)," accessed 24 January 2022, https://www.merriam-webster.com/dictionary/argument; and Jolyon Dodgson, "Argumentative Paragraph Writing," Excellent-Proofreading-and-Writing.com, accessed 24 January 2022, https://www.excellent-proofreading-and-writing.com/argumentative-paragraph.html. This description is adapted from *Merriam-Webster* and Excellent-Proofeading-and-Writing.com.

20. Graphic by author, using information from Kent, *Collected Essays*, 35–39.

21. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, I-2.

22. Dodgson, "Argumentative Paragraph Writing."

23. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, I-2.

24. Kent, *Collected Essays*, 38.

25. Russo and Schoemaker, *Winning Decisions*, 107–108. I use the authors' concept of ranges (and their benefits). I focus on the obvious, but Russo and Schoemaker's work offers a wealth of tools to improve decision making.

26. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, C-2.

27. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, A-3.

28. Graphic by author, using information from Kent, *Collected Essays*, 35–39.

29. Ibid.

30. Ibid.

31. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, C-1–C-2.

32. Russo and Schoemaker, *Winning Decisions*, 107–108.

33. *Merriam-Webster*, s.v. "range (*n.*)," accessed 24 January 2022, https://www.meriam-webster.com/dictionary/range; and Russo and Schoemaker, *Winning Decisions*, 107–108.

34. Office of the Director of National Intelligence, *Intelligence Community Directive 203: Analytic Standards* (Washington, DC, 2 January 2015), 3.

35. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, I-1.

36. Russo and Schoemaker, *Winning Decisions*, 107–108.

37. Kent, *Collected Essays*, 36.

38. Atul Gawande, *The Checklist Manifesto: How to Get Things Right* (New York: Picador, 2011), 13.

39. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, 9-8.

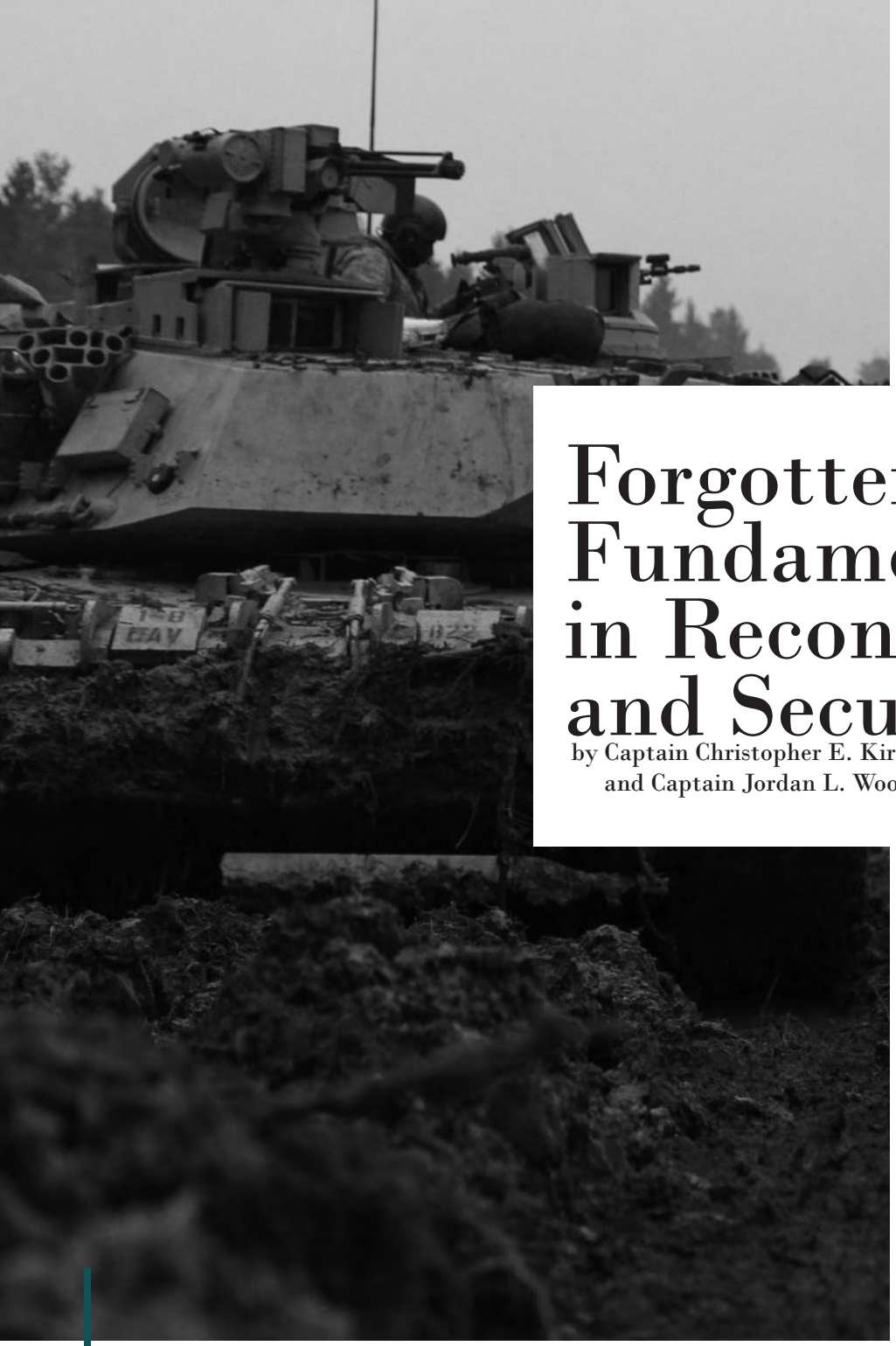
40. Ibid.

41. Example adapted from Department of the Army, ATP 2-33.4, *Intelligence Analysis*, 8-1–8-3; and Matthew Fontaine, "Enemy Course of Action Development," *Military Intelligence Professional Bulletin* 45, no. 4 (October–December 2019): 23–27.

42. Oscar W. Koch and Robert G. Hays, *G-2: Intelligence for Patton* (Atglen, PA: Schiffer Military History, 1999), 124.

43. Compilation by author, using various sources cited in the article.

LTC Matthew Fontaine is the G-2 for the U.S. Army Joint Modernization Command. He has deployed twice to Iraq and twice to Afghanistan, serving as an executive officer, platoon leader, battalion S-2, military intelligence company commander, and analysis and control element chief. He holds two master of military art and science degrees, one in general studies and the other in operational art and science, from the U.S. Army Command and General Staff College.



Forgotten Fundamentals in Reconnaissance and Security

by Captain Christopher E. Kiriscioglu
and Captain Jordan L. Woodburn

Tanks from 1st Battalion, 8th Cavalry Regiment, conduct security operations during exercise Combined Resolve XIII at the Joint Multinational Readiness Center, February 2, 2020. (Photo by Army National Guard SGT Fiona Berndt)

Introduction

Executing mission tasks that are built from mere running estimates, fighting for information to inform higher headquarters, and shaping an operational environment with few "knowns," cavalry squadrons routinely lean on the reconnaissance and security fundamentals while operating in austere environments. Through their ability to fight for information and answer intelligence requirements, cavalry organizations enable freedom of maneuver and decision making for commanders at echelon. However, observations from training centers indicate that numerous cavalry formations are falling short in their ability to shape the fight, retain combat power, and set conditions for the brigade's main effort. When we neglect the fundamentals of reconnaissance and security, the squadron becomes an inhibiting liability rather than a dominating enabler. From multiple rotations at the Joint Multinational Readiness Center, the message is clear—cavalry organizations are forgetting the fundamentals.

U.S. Army Soldiers assigned to 1st Squadron, 91st Cavalry Regiment, conduct dismounted troop reconnaissance training **for a platoon external evaluation at Hohenfels, Germany, on January 26, 2021. (U.S. Army photo by SGT Julian Padua)**

Adjacent Unit Coordination

- ✦ Orient on the protected force (fundamental of security).[1]

Communication issues will always be at the heart of every unit's after action review but most will focus on communication *up*, to the higher headquarters, or communication *down*, to subordinate units. Few, however, will focus on *lateral* communication issues inherent in coordination with adjacent units. This is paramount for a cavalry organization because of the nature of reconnaissance handovers during forward passage of lines and rearward passage of lines. The reconnaissance handover consists of a battle handover, or a transition of area of operations responsibility, as well as an intelligence handover, a transition of targets and collected information requirements. Squadrons must be able to facilitate the transition of intelligence, targets, and terrain knowledge to the protected force during reconnaissance handovers in order to set conditions for the follow-on force to accomplish its mission.

The largest obstacle inhibiting effective reconnaissance handovers is the failure to plan and rehearse with adjacent units. During planning, units fail to exchange mutually supporting operations graphics or mission intent before execution. This inevitably leads to miscommunication, lost engagement opportunities, and preventable combat loss. To mitigate degraded adjacent unit coordination, squadrons must include representatives of all units involved in reconnaissance handovers at the combined arms rehearsal.

In the defense, the reconnaissance handover must be rehearsed at the respective squadron or battalion combined arms rehearsals, even to troop level, if possible. All observers and leaders in the cavalry (down to the platoon leader level) should know what platoon or element is behind them, along with their future task and purpose. Cavalry troops must have mutually supporting graphic control measures, at a minimum. It is important to use target reference points along key avenues of approach to rapidly pass a target and facilitate its subsequent destruction. Simply reporting to brigade is not enough to enable a timely target acquisition or transition. Special considerations must also be established to account for the surface danger zones of defending and screening units. The probability of fratricide directly correlates to the level of dissemination and coordination of direct fire control measures between adjacent units. Squadrons must take ownership of coordinating shared understanding along their unit boundaries, especially during displacement operations.

In the offense, successful cavalry squadrons not only seek to answer priority intelligence requirements (PIRs) for the brigade, but they also identify how their scheme of maneuver ties into the overall concept of operations. For example, if the cavalry squadron is conducting a zone reconnaissance leading up to an objective, discussions between the squadron and the follow-on assaulting battalion should occur, focused on what the battalion commander will need to know in order to enable their attack. Battalion PIRs, route trafficability, obstacles, enemy composition and disposition, suitable avenues of approach, and any other specified information are all likely information requirements that the cavalry squadron needs to provide. These reports should flow not only to the brigade but also to the customer battalion immediately to the cavalry squadron's rear. This is the true definition of enabling timely decision making.

Displacing the Squadron

- ✦ Retain freedom of maneuver (fundamental of reconnaissance).[2]
- ✦ Provide reaction time and maneuver space (fundamental of security).[3]

British soldiers of the Queen Royal Hussars prepare for tactical maneuvering during Saber Junction 17 at the Hohenfels Training Area, Germany, May 6, 2017. (U.S. Army photo by SPC Michael Bradley)

With special consideration to the defense, cavalry squadrons rarely define what it means to reach their displacement criteria. When the trigger is met to displace, troops and squadrons have rarely prepared to displace in contact or under pressure. Ideally, displacement must consist of preplanned (and rehearsed) subsequent battle positions that are supported by indirect fires to enable the cavalry squadron to transition while maintaining combat power. Units must also be deliberate, not hesitant, in initiating their displacement. It exists for a reason and ultimately allows the cavalry to properly transition while maintaining the ability to continue to fight for the brigade. Triggers to initiate displacement must be clear and easily understood to the lowest level. Hesitation at the transition will lead to unnecessary combat losses.

Part of maintaining freedom of maneuver also relies on the squadron's ability to deny freedom of maneuver to the enemy. Since aggressive direct fire engagements are likely to compromise observation posts and increase unwanted decisive engagement, obstacles become the squadron's primary means of disrupting enemy force maneuver. Effective obstacle emplacement continues to be the most neglected component for cavalry organizations conducting a security mission task, almost to the point of nonexistence. Although the squadron's obstacles will not be as robust as obstacles that are along the support brigade's main defensive belt, they still need to be as deliberate. Emplacing obstacles directly correlates to providing increased reaction time and maneuver space for the protected force, especially during a guard.

Enduring Operations in Reconnaissance and Security

- ✦ Retain freedom of maneuver (fundamental of reconnaissance).[4]
- ✦ Provide early and accurate warning (fundamental of security).[5]

While not the perfect solution for enabling security operations, the use of engagement area development in the screen undeniably enables success for the cavalry squadron. By using all the steps in the process (including the commonly neglected rehearsal, which should include adjacent units, a verification of the reconnaissance handover plan, and the displacement plan), the cavalry can ensure it is prepared to answer intelligence requirements, fight for reconnaissance if necessary, and retain combat power. Any dead space should be mitigated using dismounted observation posts in depth, which platoon leaders and troop commanders should employ after careful analysis of the sector sketch.

Furthermore, establishing a narrative of how to interact with the enemy, codified as engagement criteria within commander's reconnaissance or security guidance, will allow the squadron to impose deliberate lethality and to preserve combat power. Too often, squadron staffs relegate engagement criteria into the rudimentary box checks, "engage enemy infantry fighting vehicles, but not tanks," rather than guiding the echeloned engagement of weapon systems in order to balance lethality with economy of force. (For phase II, use 155 mm to destroy enemy observation posts undetected, 120 mm mortar fire to disrupt or displace enemy-mounted reconnaissance, vehicle-mounted antitank systems to initiate direct fire contact with section-sized or below BRDMs, .50 caliber for squad-sized dismounts, etc.). In order to retain combat power, the cavalry squadron must tailor its engagement criteria appropriately to avoid becoming decisively engaged. Engagement criteria must be definitive and eliminate the guesswork for the scout on the ground. Otherwise, reconnaissance units will become unnecessarily compromised and unable to continue information collection efforts because of observation posts meeting disengagement or troop displacement criteria.

Feeding the Brigade's Information Collection Plan

- ✦ Ensure continuous reconnaissance (fundamental of reconnaissance).[6]
- ✦ Orient on reconnaissance objectives (fundamental of reconnaissance).[7]
- ✦ Report all information rapidly and accurately (fundamental of reconnaissance).[8]
- ✦ Perform continuous reconnaissance (fundamental of security).[9]

Cavalry formations continue to struggle with leveraging reconnaissance and security operations to enhance the brigade's information collection plan. Whether it is from collecting on irrelevant PIRs that do not enable the brigade commander to make an advantageous decision, or failing to answer PIRs within the latest time information is of value (LTIOV), reconnaissance organizations routinely neglect their critical role in information collection.

In order to influence the collection plan, squadron staff must integrate with their higher headquarters during intelligence preparation of the battlefield or risk degrading the full development of a focused reconnaissance objective and supporting PIR. Nesting with brigade during the earliest steps of the military decision-making process will enable the squadron staff to synchronize across all warfighting functions with its higher headquarters and ensure that the ground reconnaissance elements understand their role in answering PIRs. Inversely, failure to synchronize with higher headquarters will contribute to a domino effect of ambiguous reconnaissance objects, confusing information requirements, and wasted effort from troop collection assets that feed into an unfocused brigade collection plan. It is not just information that the squadron must collect; it is also the development of that information through analysis, as well as feedback to the brigade, that will lead to answering PIRs.

Cavalry organizations transition information into intelligence in order to drive brigade operations. Information itself is worthless unless it contributes to intelligence, and intelligence is useless unless it contributes to an assessment. With supporting intelligence, assessments are what allow the brigade S-2, and ultimately the brigade commander, to visualize the operational environment and make advantageous decisions within it. If we can make assessments lower in echelon, those assessments will portray, in a more timely and more accurate manner, the true events of enemy forces on the battlefield. Furthermore, troop commanders who are empowered to make decisions will decrease the amount of time it takes to answer a PIR within LTIOV and in turn allow the brigade commander to exert control over the enemy's decision-making cycle. In order to provide assessments, commanders at echelon must be able to comprehend and differentiate between the multitudes of possible enemy courses of action, which only occurs when the squadron staff is fully nested and integrated with brigade planning cycles.

All-Weather, Day or Night

Cavalry squadrons provide the most reliable set of eyes and ears for their higher headquarters to employ. Charged to dominate the operational environment, they must ensure shared understanding of both enemy and terrain and do so by adhering to a set of universal fundamentals. Fundamentals that, if ignored, prevent ground reconnaissance elements from achieving the reconnaissance objective and, subsequently, the brigade from realizing its decisive operation. Cavalry formations must be prepared to provide early warning and detection, generate assessments from collected information requirements, and destroy select enemy targets in order to enable reaction time and maneuver space for the protected force. Cavalry squadrons cannot accomplish this task if they are compromised, destroyed, or fixed by enemy reconnaissance. To live up to the status of being all-weather, day or night, squadrons must embrace *all* the fundamentals of reconnaissance and security.

Endnotes

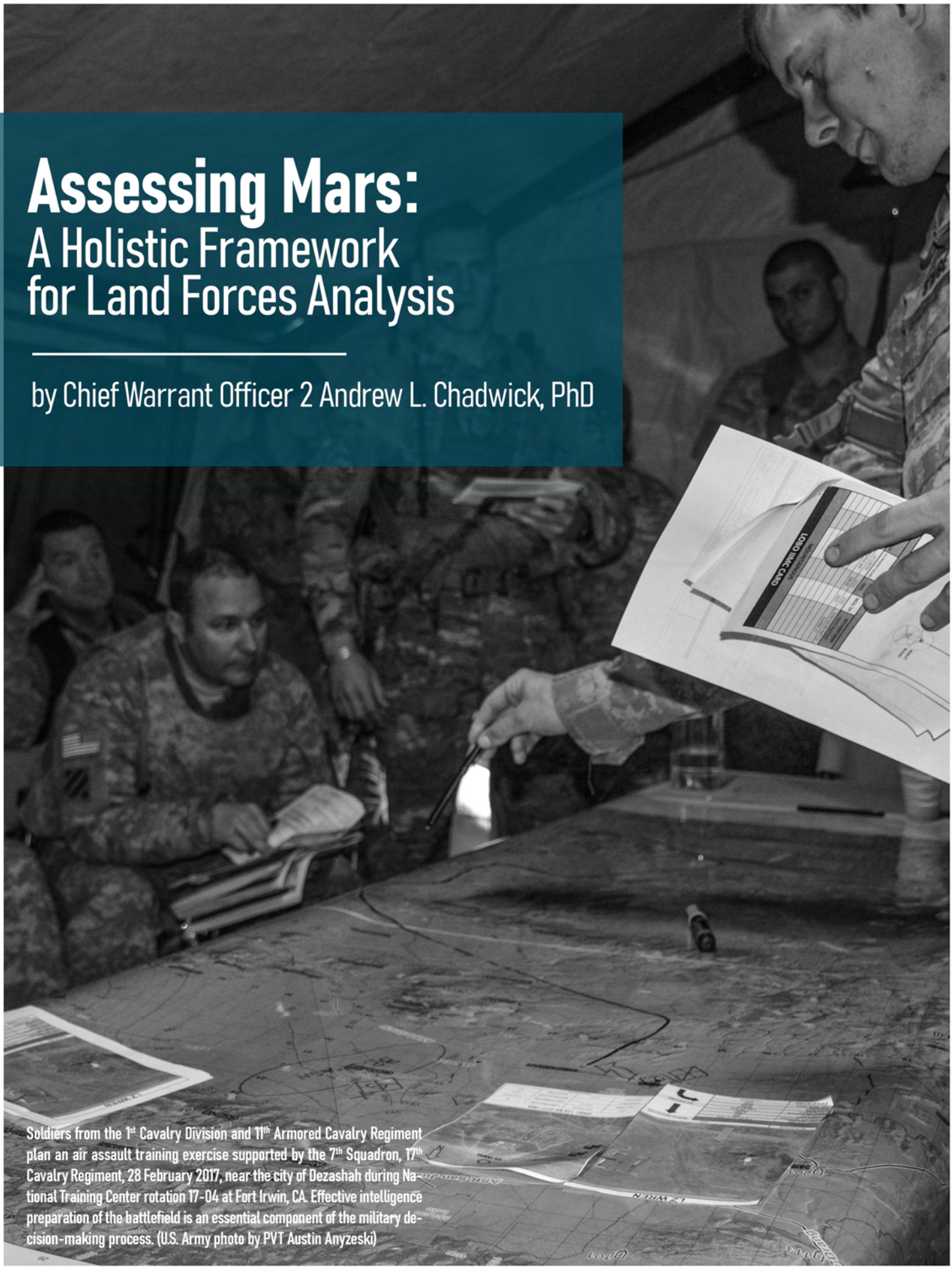
1. Department of the Army, Field Manual 3-98, *Reconnaissance and Security Operations* (Washington, DC: U.S. Government Publishing Office, 1 July 2015), 6-2.
2. Ibid., 5-1.
3. Ibid., 6-2.
4. Ibid., 5-1.
5. Ibid., 6-2.
6. Ibid., 5-1.
7. Ibid.
8. Ibid.
9. Ibid., 6-2.

CPT Christopher Kiriscioglu is a cavalry and reconnaissance observer coach/trainer with the Grizzly Team at the Joint Multinational Readiness Center in Hohenfels, Germany. His past duty assignments include squadron intelligence officer, 1st Squadron, 71st Cavalry Regiment, 10th Mountain Division; assistant brigade intelligence officer, 10th Division Artillery, 10th Mountain Division; battalion intelligence officer, 1st Battalion, 10th Attack Reconnaissance Battalion, 10th Combat Aviation Brigade, 10th Mountain Division; fire support officer, 3rd Battalion, 69th Armor Regiment, 1st Armored Brigade Combat Team, 3rd Infantry Division; and fire direction officer, 1st Battalion, 41st Field Artillery Regiment, 1st Armored Brigade Combat Team, 3rd Infantry Division. His military schooling includes the Military Intelligence Captain's Career Course, Cavalry Leader's Course, Joint Fires Observer Course, and Geospatial-Intelligence Officers Course. He holds a bachelor of music in cello performance from the University of Michigan.

CPT Jordan Woodburn is a cavalry and reconnaissance observer coach/trainer with the Grizzly Team at the Joint Multinational Readiness Center in Hohenfels, Germany. His past duty assignments include commander, Company B, 3rd Combined Arms Battalion, 67th Armor Regiment, 2nd Armor Brigade Combat Team, 3rd Infantry Division, Fort Stewart, GA; commander, Company D, 1st Combined Arms Battalion, 64th Armor Regiment, 1st Armor Brigade Combat Team, 3rd Infantry Division, Fort Stewart, GA; long-range surveillance detachment leader, Company C, 3rd Battalion, 38th Cavalry Regiment, 201st Military Intelligence Brigade, Fort Lewis, WA; and cavalry platoon leader, Company B, 3rd Battalion, 38th Cavalry Regiment, 201st Military Intelligence Brigade, Fort Lewis, WA. His military schooling includes Maneuver Captain's Career Course, Cavalry Leader's Course, Army Reconnaissance Course, Ranger School, Airborne School, Air Assault School, and Pathfinder course. He holds a bachelor of science in political science from The Citadel, Charleston, SC.

Assessing Mars:
A Holistic Framework for Land Forces Analysis

by Chief Warrant Officer 2 Andrew L. Chadwick, PhD



Soldiers from the 1st Cavalry Division and 11th Armored Cavalry Regiment plan an air assault training exercise supported by the 7th Squadron, 17th Cavalry Regiment, 28 February 2017, near the city of Dezashah during National Training Center rotation 17-04 at Fort Irwin, CA. Effective intelligence preparation of the battlefield is an essential component of the military decision-making process. (U.S. Army photo by PVT Austin Anyzeski)

Editor's Note: This article was originally published in the May–June 2022 issue of Military Review, the Professional Journal of the U.S. Army, Combined Arms Center, Fort Leavenworth, Kansas. The author revised portions of the article, and MIPB is now reprinting it through coordination with Military Review.

Introduction

U.S. Army practices for assessing the capabilities of adversarial land forces need a major update. Namely, such practices place an insufficient emphasis on the critical human dimensions of a land force, such as leadership or morale. As the United States experience in Afghanistan shows, the human dimensions can play a decisive role in determining the outcomes of battles and even wars. Additionally, Army intelligence practices tend to examine adversarial forces in isolation from friendly or allied units, which reduces opportunities to identify qualitative or quantitative imbalances. To address these shortfalls, this article describes how analysts can use methods that military historians and strategic intelligence organizations employ to create more holistic assessments of an adversarial land force. Such assessments, moreover, can enrich the intelligence preparation of the battlefield (IPB) process to inform plans and operations.

What Is a Framework?

The primary value of a framework is that it lays out the key variables—something that changes in response to internal or external stimuli—of a particular system, event, or phenomenon under examination. This, in turn, helps guide the research and analysis of a topic by ensuring analysts properly account for each constituent part of a subject and the relationships between those parts. For example, an analysis of land forces must consider some basic variables, including equipment, personnel, planning processes, and doctrine. It must also account for how those variables interact by showing, for instance, how an army's doctrine helps determine what equipment it acquires, how it trains, and more.

Ultimately, the value of an analytic framework is that it provides a sense of clarity and common language.[1] That is, it clarifies what is important and why. For organizations like the U.S. Army, it helps everyone speak the same language in how they approach the research, analysis, and presentation of their findings and assessments. This helps mitigate the tendency of some analysts to make judgments on the capabilities of a particular adversary on intuition alone or on incomplete analysis.

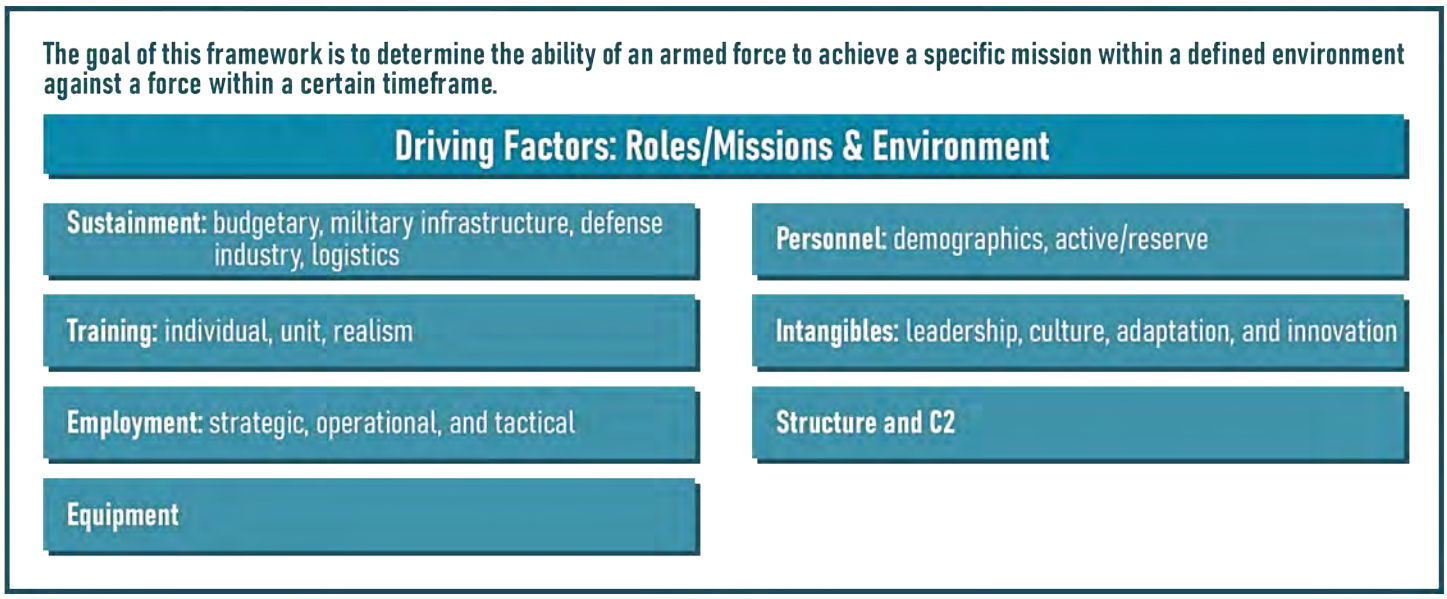
Despite their value, frameworks, as one historian rightly cautioned, are simplifications of reality and, therefore, "inexact and incomplete."[2] In other words, having the framework does not guarantee an accurate interpretation of a topic and it most certainly does not guarantee accurate predictions of how those topics will evolve over time or respond under certain circumstances. This is especially true of land forces analysis—and military analysis in general—in which analysts are operating with incomplete and at times contradictory evidence. Also, the wars and operations in which those land forces fight are inherently unpredictable. As Carl von Clausewitz observed in his analysis of war: "No other human activity is so continuously or universally bound up with chance."[3] Chance—or unpredictability—reflects the fact that war is a social and political phenomenon determined largely by the actions, judgments, and misjudgments of people who, by nature, are unpredictable, especially as a collective and when under stressful conditions like war.[4]

The Limits of U.S. Army Intelligence Doctrine

Even though Clausewitz is widely taught in U.S. military educational institutes, U.S. Army intelligence doctrine overlooks the human factors of war. The Army's current set of analytic tools, as detailed in ATP 2-01.3, *Intelligence Preparation of the Battlefield*, and ATP 2-33.4, *Intelligence Analysis*, largely examines material and conceptual factors, such as enemy equipment, doctrine, and order of battle.[5] For those variables, this doctrine does provide detailed guidance and useful tools, such as order of battle charts and threat templates that illustrate the means and methods an opposing force likely will employ in combat.[6]

Buried within the example templates in ATP 2-01.3 are important assessments regarding human factors, such as "force x lacks the will for prolonged engagements."[7] However, ATP 2-01.3 and ATP 2-33.4 provide incomplete guidance for how to make judgments regarding the human and material conditions that would cause a force to lack the will for prolonged engagements. Rather, they essentially assume analysts know how to obtain that information or that their higher echelons will provide it to them. Such assumptions are highly tenuous, given the varied skills, experience, motivation levels, enterprise endurance, and connectivity of formations across the Army. In other words, doctrine must be more specific on how to acquire and employ that information using examples and more direct guidance.

Finally, ATP 2-01.3 and ATP 2-33.4 do not clearly break down their constituent variables, like composition and disposition, into their individual parts. Instead, they largely leave that information up to analysts to discover on their own, assuming they have the time and ability to do so. Fortunately, another framework is available within the Department of Defense that can help fill some of these gaps.



Defense Intelligence Agency Military Capabilities Framework[8]

Alternative Frameworks

The Defense Intelligence Agency (DIA) uses a more comprehensive set of variables in its military capabilities framework than the U.S. Army. As shown in the figure above, DIA's framework breaks down the capabilities of a military into nine key variables, two of which—roles/missions and environment—are considered driver variables.[9] Such variables are considered more important because they play a greater role in shaping the character of others. An army's mission, for instance, and the terrain it fights on will play an important role in shaping its structure, training, and equipment. Unlike the U.S. Army, DIA breaks down some of its variables further by showing how personnel matters also must account for Soldier demographics and whether they are active Soldiers (full time) or reservists (part time).

DIA's framework, however, is still incomplete and does not focus on land forces, given its purpose to help inform military capabilities analysis in general. Its use of driver variables is important in that it shows how variables relate, but it gives the impression those variables (roles/missions and environment) are the only ones that shape the character of others. Additionally, the relationship also appears to be one way, not accounting for how factors like personnel and budgets can play extremely important roles in shaping an army's roles and missions.

The field of military history offers a more robust framework for land forces capabilities analysis. For example, in their multivolume study on military effectiveness, historians Allan Millett and Williamson Murray present a framework to assess and compare the effectiveness of multiple armies during the major wars of the 20th century. They do so by looking at armies at all levels of command. To measure effectiveness, the volumes provide a list of general attributes, as shown in Table 1, on the next page, which account for human and material factors.[10] The authors also acknowledge those attributes reflect a host of different constraints, whether natural like geography, or political or cultural in nature, such as a society's willingness to serve in the military.[11] Ultimately, understanding these attributes and constraints will enable researchers to conduct more in-depth comparative studies of a particular armed force against its adversaries under certain historical circumstances.[12]

The problem for military intelligence professionals, however, is that this framework focuses on informing the fields of strategic studies and military history. Thus, it provides no guidance on how to employ its methods within existing U.S. Army staff processes.

In short, these frameworks all have their own strengths and shortcomings, but unfortunately, the U.S. Army framework is the most incomplete, especially regarding human factors and matters above the tactical level. The proposed framework that follows aims to address these shortfalls.

A Holistic Land Forces Framework

The following framework for land forces analysis is built on three core propositions. First, it must fit into the U.S. Army's existing analytical tasks and processes to ensure it speaks the same language as the Army professionals employing it. Second, it must be multivariable and account for the human factors that existing doctrine mostly overlooks. Third, it must be comparative to identify relative strengths and weaknesses between friendly and adversarial forces. Ultimately, this framework should produce two key outputs:

- A land forces category statement
- A land forces capabilities statement.

If incorporated in the Army's first analytical task, generate intelligence knowledge, these outputs can provide critical context for IPB step 3 (evaluate the threat) by helping define the characteristics of an opposing force and determining the ways that force operates.

Table 1. Millett and Murray's Military Effectiveness Framework[13]

Political	Strategic	Operational	Tactical
Obtaining resources for the war effort/military, which includes— 1. Reliable access to financial support. 2. Sufficient military-industrial base. 3. Sufficient quantity and quality of manpower. 4. Control over the conversion of resources into military capabilities. 5. Political elite attitudes regarding the military. 6. Officership as a distinct profession.	Employment of armed forces to achieve national goals, which includes— 1. Planning, analysis, and selection of objectives and linking those objectives to campaign or contingency plans. 2. Ability to communicate plans and assessments to national leaders to seek logical goals. 3. Consistency of force size and structure with strategic goals and courses of action. 4. Alignment of strategic objectives with logistical, technological, and industrial bases. 5. Integration of objectives with those of allies or ability to convince allies to align their objectives. 6. Plans that place the strengths of a military organization against the critical weaknesses of an adversary.	Analysis, selection, and development of institutional concepts or doctrines for employing forces to achieve objectives in a theater of war, which include— 1. Ethos to deal with operational problems in a realistic ways. 2. Ability to combine capabilities to cover weaknesses and take full advantage of strengths. 3. Ability to adapt psychologically and physically and to move rapidly in unanticipated directions. 4. Consistency between concepts and operational concepts and available technologies. 5. Ability to support concepts with required intelligence, supply, communications, medical, and transportation systems. 6. Consistency of operational concepts to strategic objectives. 7. Degree to which doctrine and organizations place their strengths against an adversary's weaknesses.	Techniques to fight engagements to meet operational objectives, which include— 1. Tactical approaches consistent with strategic objectives. 2. Concepts consistent with operational capabilities. 3. Emphasis on all arms integration. 4. Emphasis on surprise and rapid exploitation of opportunities. 5. Consistency with morale, cohesion, and relations between noncommissioned officers, officers, and enlisted personnel. 6. Alignment of training to tactical systems. 7. Alignment of training to support capabilities. 8. Extent to which tactical systems place strengths against an adversary's weaknesses.

Land Forces Category Statement. Table 2, on the next page, provides an overview of the key variables for determining the nature of a particular land force.[14] Namely, what are the force's purpose, structure, and ways of war? Answering those questions enables analysts to produce a baseline assessment of the nature of a particular land force and its general strengths and weaknesses. This statement, in turn, can frame more detailed discussions regarding an adversary's capabilities by warfighting functions (fires, maneuver, protection, etc.).[15]

Land Forces Capabilities Statement. Once the nature of a land force is established, deeper analysis can occur regarding its ability to achieve a specific purpose. To do so, analysts can use Table 3 and Table 4, on page 7, which list broad attributes that can help determine the effectiveness of a land force at the strategic, operational, and tactical levels of command. Table 3 lists general attributes of an effective land force, regardless of its intended purpose.[16] Table 4 focuses on conventional operations against a state adversary (attributes for effective counterterrorism/counterinsurgency operations are outside of the scope of this article).[17]

There are two ways to use these frameworks. First, analysts can simply use them to guide their assessments regarding whether the land force under examination can perform a particular mission. Second, analysts can make a quantitative assessment based on these attributes. Now, such an assessment can be problematic because wars and the land forces that fight in them are highly dynamic and generally defy quantitative analysis. That said, using the frameworks to produce quantifiable assessments can help enable the staff to compare an adversarial force with friendly or allied forces.

To make such quantitative assessments, analysts should use a combination of several sources—intelligence reporting, finished intelligence from organizations like the National Ground Intelligence Center and DIA, academic studies, and press reports—to complete the following steps:

- Finalize attributes, using or modifying the ones in Tables 1 through 4 or adding others based on the situation.
- Add a single point for each attribute that a land force meets in the general category (if the attribute is not applicable, then do not add a point). Make sure to organize the final count by strategic, operational, and tactical categories, meaning the top score for strategy would be a 19, while a top operational score would be a 19 and a tactical score would top out at 15.
- Repeat the same process for the conventional land forces framework.
- Add the scores for the general and conventional frameworks to produce total scores for the strategic, operational, and tactical attributes (staffs could also weigh some attributes higher than others, depending on the situations).
- Redo the entire assessment process for the opposing force. (Note: Intelligence personnel should consult with other staff sections, especially when comparing adversarial forces to friendly forces.)
- Use the score to compare capabilities with opposing forces/allies, as depicted with a historical example in Table 5, on page 8.[18]

Table 2. Land Forces Category Statement[19]

Variables		Examples	General Strength	General Weakness
Primary Focus	Internal defense	Present-day Iraqi Security Forces	May be more prepared for conducting counterterrorism/counterinsurgency operations	Are less prepared for conventional military operations against states
	Conventional defensive operations	Present-day Japanese Armed Forces	May be more prepared to defend against an attack from a state adversary	Are less prepared for offensive operations against a state or counterinsurgency/counterterrorism scenario
	Conventional offensive operations	Present-day U.S. Army	May be more prepared for offensive operations against a state	Are less prepared for defensive operations against a state or counterinsurgency/counterterrorism scenarios
Active Structure	Short-service conscript (mandatory service for 1 to 4 years)	Israel Defense Forces	Are likely capable of generating a large army relative to its population	Generally, are less well trained than a longer-service volunteer
	Long-service conscript (mandatory serve for more than 4 years)	19th Century Russian and British Armies	May be able to field a large and highly experienced army	Long-service conscript may lead to the growth of a large and expensive army
	Volunteer (service is voluntary and may extend beyond the typical 1 to 4 years of a conscript)	Present-day U.S. Army	Are likely able to develop higher skills and more experience than conscripts	Are generally smaller than a conscript army; soldiers are more expensive to recruit and retain
	Cadre (an army with a small professional cadre that prepares to oversee an expanded wartime army composed of volunteers/conscripts)	United States Army and German Army during the interwar years (1920s and 30s)	Maintain highly skilled cadre of leaders; reduce financial costs of peacetime army	Are unlikely to be ready for an unexpected conflict (need time to recruit and train new soldiers)
	Dual structure (an army composed of a mixture of volunteers and conscripts)	Present-day Russian Armed Forces	Can create elite units within an army for offensive operations while the conscript units focus on easier tasks	Creates a dual structure in which some units are less ready for combat than others
Reserve Structure	Individual replacements/augmentees (reservists do not serve in complete deployable units, rather they are used to fill gaps in the ranks of active units)	Present-day U.K. Army Regular Reserve (separate from Army Reserve)	Allow reservists to fall under command of full-time personnel	Have no reserve units to replace exhausted/degraded active units
	Units (reserve units deploy as full units)	U.S. Army National Guard	Have a trained reserve capable of replacing exhausted/degraded active units	Quality of reserve units are likely not on par with active-duty units, especially in armies that train reservists infrequently
	Militia/territorial defense (a reserve that does not deploy outside of its national borders and performs purely defensive functions)	Territorial defense forces of the present-day Baltic states	Relieve active-duty units of burden of routine tasks such as border security	Reserve is unlikely to be deployable for missions abroad; quality is likely much lower than active-duty formations
	Hybrid (a reserve that consists of individual replacements and full, deployable units)	Present-day U.S. Army Reserve	Have flexible reserve structure to fill immediate personnel needs in active army while providing reserve units to backfill/replace active-duty ones	Reduces number of reserve units available to replace/augment active ones, given large percentage of reservists serving as individual replacements or augmentees
Strategic Way of War	Attritional (seeks to defeat enemy by slowly degrading its ability and will to fight over time)	French Army in the interwar years (1920s and 30s)	Can deter adversaries by raising the prospects of a long and potentially costly war	Likely will struggle to conduct offensive operations and maneuver outside of prepared defenses
	Maneuver – short war (seeks to defeat enemy through rapid offensive operations aimed at quickly destroying their will or ability to fight)	Present-day U.S. Army	Reduce likelihood of long, costly wars	Force may be ill-suited for withstanding heavy attrition or for waging a defensive war
	Indirect (seeks to avoid direct conflict and relies on proxies or standoff capabilities, like UAVs and rockets, to degrade enemy's ability or will to fight)	Present-day Iranian military	Can reduce exposure to attack by relying on proxies or standoff attack capabilities	Are likely to struggle in a force-on-force ground conflict

Table 2. Land Forces Category Statement (*continued*)

Variables		Examples	General Strength	General Weakness
Tactical Way of War	Multidomain (integration of air, maritime, cyber-electromagnetic warfare, and space capabilities)	Present-day United States Army and Russian Army	Can converge an entire array of attack and defense capabilities to degrade opposing forces	Units may struggle to execute this high-skilled, high-tech form of war (especially if they are composed of short-service conscripts or undertrained reservists)
	Combined Arms (integration of armor, artillery, infantry, and combat engineering)	Present-day Israel Defense Forces	Can maximize the full combat potential of land force	Units may struggle to execute this high-skilled, high-tech form of war (especially if they are composed of short-service conscripts or untrained or undertrained reservists)
	Single Arm (formations composed primarily of a single arm)	Israel Defense Forces pre-1970s	May simplify planning, operations, and logistics	Are likely at a disadvantage against a combined arms force; tanks (if present) will be more vulnerable to enemy infantry and antitank weapons; infantry may lack sufficient mobility and firepower to combat enemy tanks
C2 Arrangement	Centralized to Strategic-Level Commanders	Egyptian Army 1967, 1973	Help ensure unity of effort	Reduce chances to rapidly exploit opportunities; vulnerable to decapitation strikes
	Centralized to Operational-Level Commanders and Above	Cold War Soviet Army		
	Flexible Mission Command Type Arrangement	Present-day U.S. Army	Help enable more flexible operations to respond to threats and opportunities	Can reduce unity of effort
Tactical Formations	Corps and above	Present-day U.S. Army		
	Division and below	Present-day U.S. Army		
	Brigade and below	Present-day Estonian Defense Forces		

Example Category Statement: The U.S. Army, which is an all-volunteer force backed by a fully deployable army reserve of units and individual replacements, focuses primarily on offensive operations against state adversaries. Its primary way of war is to end conflicts quickly through offensive maneuvers by brigade to army-sized units employing a flexible command arrangement overseeing combined arms and multidomain capabilities. A key strength of the U.S. Army is its high-tech and high-skilled formations. A key weakness is its limited preparedness for counterinsurgency/counterterrorism operations and the high costs of its personnel and equipment, which reduces its ability to recover quickly from high battlefield attrition.

- ✦ Incorporate findings into IPB step 3 to help determine threat characteristics, build threat models, and identify high-value targets. Then, transition to an examination of the adversary's likely courses of action as part of IPB step 4.

Use by Echelon

The land force framework presented in this article is most suitable for employment by a theater army or corps. Intelligence staffs at the division level and below likely lack the time or resources to conduct an in-depth study of an adversarial land force, especially during combat operations. Thus, these higher-level staffs can use the framework to paint a broad picture of the land forces under examination, providing context for divisions, brigades, and battalions to develop more nuanced, tactically focused products.

The framework also has value in a competition environment by helping intelligence sections to develop in-depth studies of the land forces within a particular area. Such studies can help inform contingency planning and training plans to build partner capacity to compensate for any quantitative or qualitative imbalances with adversarial forces.

Table 3. General Land Forces Framework[20]

Strategic/National	Operational	Tactical
1.1 Strategic plans place strengths against an adversary's weaknesses	2.1 Military has experience conducting the types of operations it is undertaking	3.1 Tactics are consistent with operational plans
1.2 Military leaders willing and able to communicate honestly and effectively with national leaders	2.2 Operational plans are consistent with strategic plans/priorities	3.2 Have defined tactical doctrine that is understood throughout the force and taught in school/training systems
1.3 State and society believe the mission at hand is critical to their security and is willing to devote time and resources to achieve the mission	2.3 Has a professional military education and training program for all ranks to build and enhance technical and leadership skills	3.3 Corps, division, and brigade-level units have combined arms capabilities
1.4 State has a history/national ethos that inspires/motivates soldiers	2.4 Has an organizational culture that values honest feedback and has mechanism for addressing such feedback	3.4 Corps, division, and brigade-level units have—or have access to—tactical electromagnetic warfare and cyber capabilities
1.5 Society respects and values military service	2.5 Conducts dynamic training with an opposing force	3.5 Tactical units can request and receive air support from fixed-wing, rotary, and unmanned aircraft
1.6 Military is loyal to the state and is fully responsive to the orders of its national leaders	2.6 Trains in type of terrain they will operate in (urban, mountain, desert, etc.)	3.6 Tactical units have joint terminal attack coordinators to speed process of providing close air support to land forces
1.7 Military is willing and able to recruit high-skilled and educated personnel	2.7 Trains above the battalion level	3.7 Corps, division, and brigade-level units have tactical signals intelligence, geospatial intelligence, and mapping capabilities for enhancing situational awareness and targeting
1.8 Able to generate sufficient numbers of soldiers to meet mission requirements	2.8 Reserve units conduct individual and collective training in peacetime (at least 14 to 30 days a year)	3.8 Tactical-level units have—or have access to—unmanned aircraft for intelligence, surveillance, and reconnaissance
1.9 Has defined and practiced plans for mobilizing/integrating reserve units/individual replacements	2.9 Has a culture that demands full accountability and maintenance of equipment	3.9 Able to field ad hoc task forces at the company to division level
1.10 Land forces have access to strategic-level intelligence sensors that look deep into enemy's support areas for targeting, battle damage assessments (BDAs), and warning of troop/equipment movements	2.10 Has a multidomain capability that can integrate land forces with air, cyber-electromagnetic warfare, space, and maritime capabilities	3.10 Has a short-range air defense capability in tactical units for dealing with unmanned aerial vehicle, rotary, and fixed-wing aircraft threats.
1.11 Has a professional officer corps built around a defined education/training program and a promotion system based on merit	2.11 Employs a planning process that is used/understood throughout the force	3.11 Has a tactical engineering capability for identifying, breaching, removing obstacles and for creating obstacles
1.12 Has a professional noncommissioned officer corps; officers trust and empower noncommissioned officers	2.12 Has a flexible planning process that can adapt rapidly to changing circumstances	3.12 Has ability to provide timely re-supply to tactical units engaged in combat
1.13 Land forces are somewhat or fully interoperable with main allies	2.13 Empowers mid- and junior-level leaders to take the initiative	3.13 Has an airborne and air assault (helicopter) infantry capability
1.14 Military does not segregate units by ethnicity/language	2.14 Has an integrated air defense network for defending land forces from air and missile threats	3.14 Has a culture and supporting programs for building and maintaining physical and mental fitness
1.15 Units composed of soldiers who speak the same language	2.15 Has an information operations capability capable of producing timely and effective messages that resonate with targeted populations	3.15 Tactical command, fires, and intelligence systems are able to communicate to provide a common operational picture and to inform targeting
1.16 Military has effective processes to identify and punish individuals for crimes, corruption, and other undisciplined behavior	2.16 Has operational-level intelligence capabilities for identifying and tracking targets outside of tactical engagement areas/battle zones	
1.17 Not dependent on foreign suppliers for mission essential military equipment	2.17 Has unified command to ensure unity of effort	
1.18 Is fighting on a single front/theater of operations (not confronted by attacks on multiple fronts)	2.18 Has an organizational culture that is willing and able to experiment and innovate	
1.19 Key economic and population centers are protected from enemy attacks	2.19 Has a quantitative advantage in forces over adversary	

Table 4. Conventional Land Forces Framework[21]

Strategic/National	Operational	Tactical
1.1 State has the willingness and ability to withstand heavy combat losses	2.1 Has a long-range precision strike capability to destroy high-value targets in enemy support areas	3.1 Fires integrated with intelligence sensors to enable rapid identification, destruction, and assessment of targets
1.2 If conducting expeditionary operations, has international transportation and logistics networks to project and sustain sufficient numbers of combat forces to achieve desired tasks	2.2 Has a doctrine for engaging and defeating opposing forces in depth	3.2 Fires systems have the same range or outrange the fires systems of opposing forces
1.3 If operating on the defensive, has the territorial depth to absorb attack and recover	2.3 Has specialized units and doctrine for defending support areas from opposing special operations and insurgent/militant forces	3.3 Main battle tanks have the same range or outrange the systems of opposing forces
1.4 If operating on the offensive, has the element of surprise to catch defenders not fully prepared for attack	2.4 Strategic and operational-level intelligence organizations networked to tactical units to enhance situational awareness	3.4 Has mechanized and/or motorized infantry capability
		3.5 Infantry has antitank capabilities capable of defeating opposing main battle tanks
		3.6 Has tactical human intelligence capability for conventional military operations (enemy prisoner of war debriefings)

Conclusion

This framework, if incorporated into the generate intelligence knowledge task, can provide critical context for IPB step 3 (evaluate the threat), likely helping an intelligence staff to form more holistic judgments on the nature, capabilities, and relative strengths and weaknesses of an adversarial land force. Like all frameworks, however, the one presented in this article is incomplete and cannot fully account for all the dimensions of a land force in every situation. However, it can get the conversation started on how to conduct a holistic assessment of an adversarial force, which can enable more informed plans and decisions.

Table 5. Israel versus Egypt, 1973[22]

Level of War	Total Score of Israel	Total Score of Egypt	Advantage
Strategic	13	16	Egypt
Operational	14	10	Israel
Tactical	10	10	Neutral

Summary: During the 1973 Yom Kippur War, Egypt had the strategic and tactical advantage over Israel because its attack across the Suez caught the Israelis by surprise and forced them to fight outnumbered on multiple fronts (Syrians attacked simultaneously in the Golan Heights). Egypt also neutralized Israel's main tactical advantages—its armored corps and air force—through the use of new anti-tank guided missiles and mobile surface-to-air systems (SAMs). Egypt also crafted its war plan around its main strength: its ability to fight defense battles using well-rehearsed tactics. However, Israel was able to reverse the tide of the war when the Egyptians sacrificed these advantages and advanced beyond their protective SAM umbrella along the Suez Canal into the open deserts of the Sinai. This enabled Israel to take advantage of its superior tank gunnery and flexible operational and tactical culture to outgun and outmaneuver Egypt and bring the war to a close and prevent a deeper attack into Israeli territory. Despite the Israeli tactical and operational successes, Egypt still accomplished its primary strategic objective: compel Israel to re-engage in diplomatic negotiations and return the Sinai to Egyptian control.

Endnotes

1. John A. Lynn, *Battle: A History of Combat and Culture* (New York: Basic Books, 2004), 359.

2. Ibid.

3. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 2008), 75, 101.

4. Ibid., 101, 136.

5. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. Government Publishing Office [GPO], 1 March 2019), 5-4, Change 1 was issued on 6 January 2021; and Department of the Army, ATP 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. GPO, 10 January 2020).

6. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 5-10.

7. Ibid.

8. Figure adapted from Defense Intelligence Agency (DIA), *Tradecraft Note 02-15: Assessing Military Capability* (Washington, DC: Office of the Research Director, DIA, 3 December 2015).

9. DIA, *Tradecraft Note 02-15*.

10. Allan R. Millett and Williamson Murray, *Military Effectiveness: Volume 1, The First World War* (New York: Cambridge University Press, 2010), 4–26.

11. Ibid., 3.

12. Ibid., 4–26.

13. Table by author; adapted from Millet and Murray, *Military Effectiveness*, 3.

14. Assessment derived from Abraham Rabinovich, *The Yom Kippur War: The Epic Encounter That Transformed the Middle East* (New York: Schocken, 2007); Central Intelligence Agency (CIA), *The World Factbook*, CIA website, accessed 19 February 2022, https://www.cia.gov/the-world-factbook/; "Who We Are: The Army Reserve," UK Army website, accessed 19 February 2022, https://www.army.mod.uk/who-we-are/the-army-reserve/; Eugenia C. Kiesling, *Arming Against Hitler: France and the Limits of Military Planning* (Lawrence, KS: University Press of Kansas, 1996); and John Gooch, *Armies in Europe* (London: Routledge, 1980).

15. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 5-18.

16. Millett and Murray, *Military Effectiveness*, 4–26.

17. Ibid.

18. Assessment derived from Rabinovich, *The Yom Kippur War*.

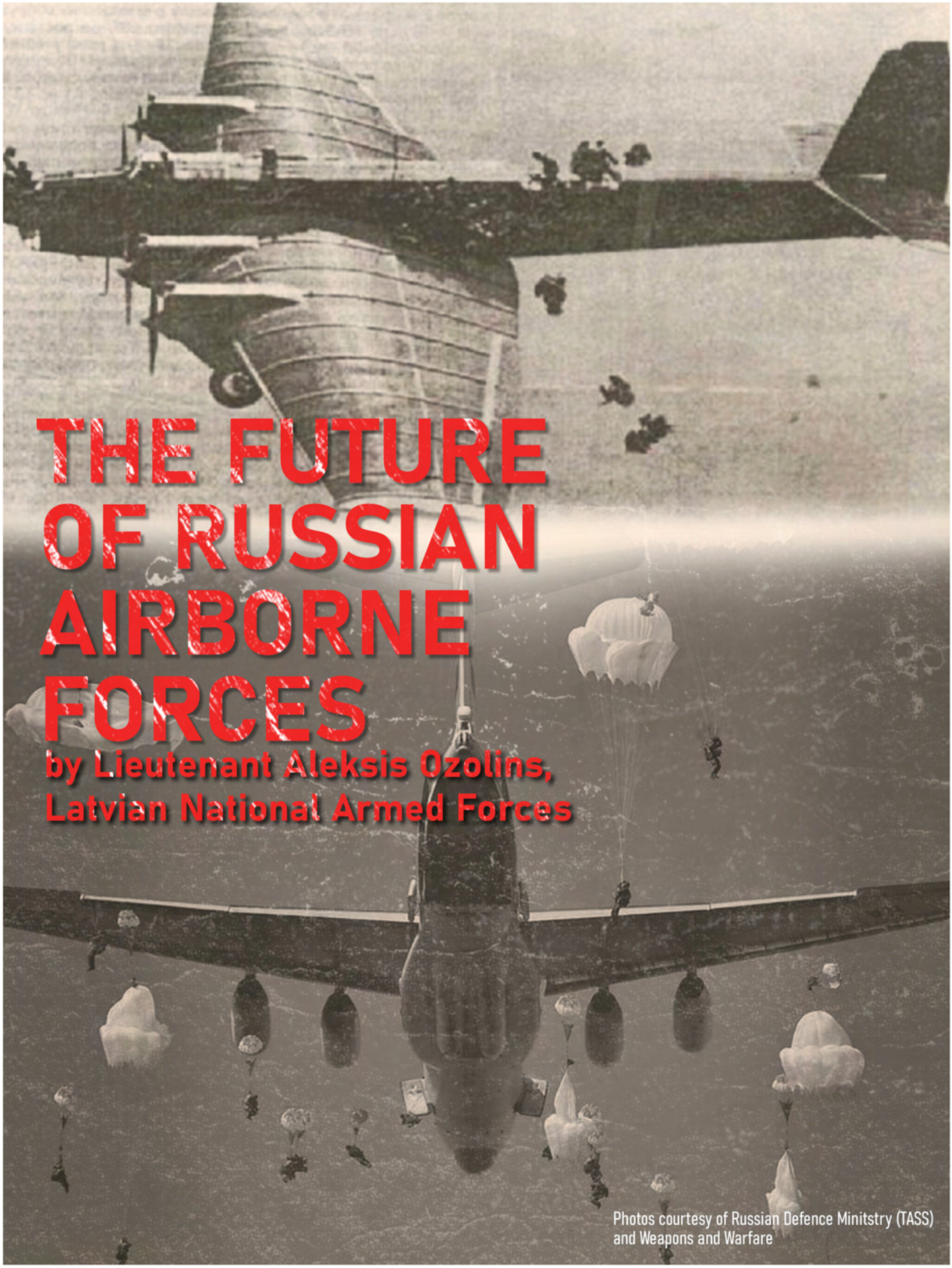
19. Table by author.

20. Ibid.

21. Ibid.

22. Ibid.

CW2 Andrew Chadwick, PhD, Army National Guard, is an all-source intelligence technician with the 29th Infantry Division, Maryland Army National Guard. As a civilian, he serves as an intelligence analyst with the Department of Defense. He holds a doctorate in history from the University of Maryland, College Park, and a master of arts in international security from the University of Denver.



THE FUTURE OF RUSSIAN AIRBORNE FORCES

by Lieutenant Aleksis Ozolins,
Latvian National Armed Forces

Photos courtesy of Russian Defence Minitstry (TASS) and Weapons and Warfare

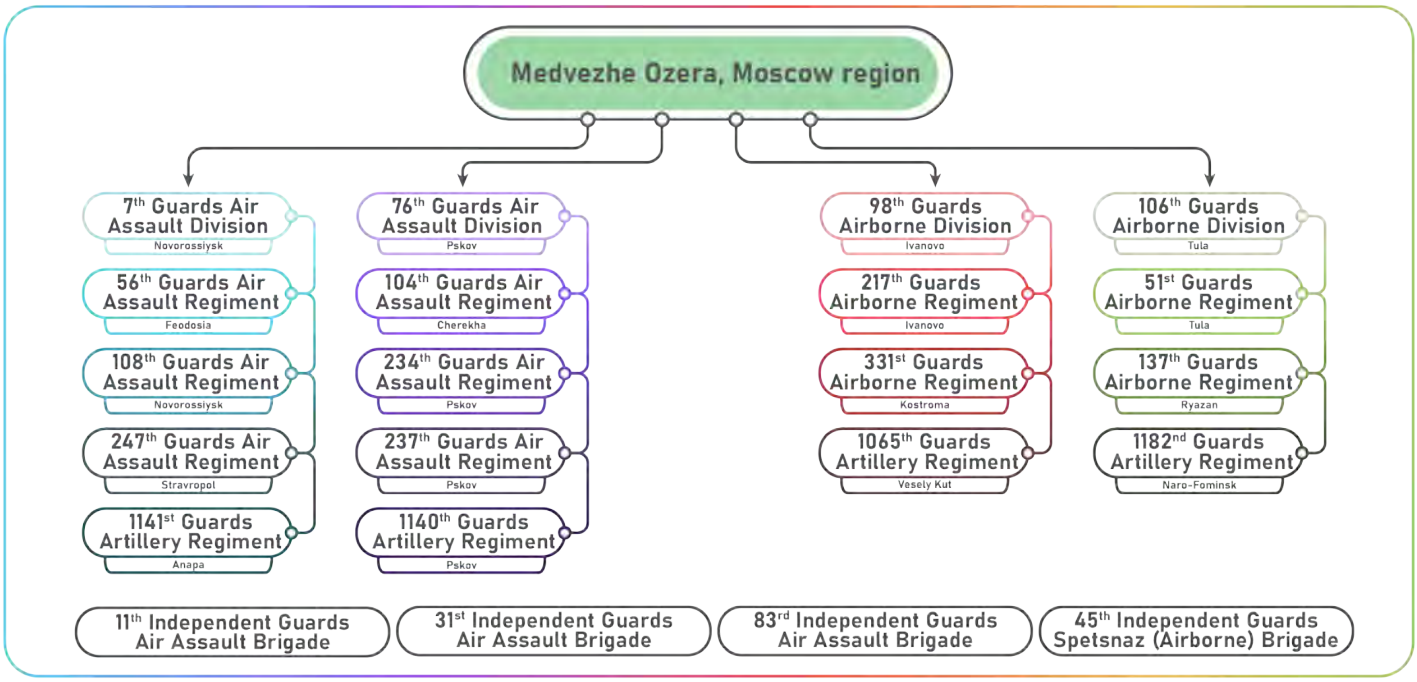


Figure 1. Russian Airborne Forces Retool for an Expanded Role[1]

Introduction

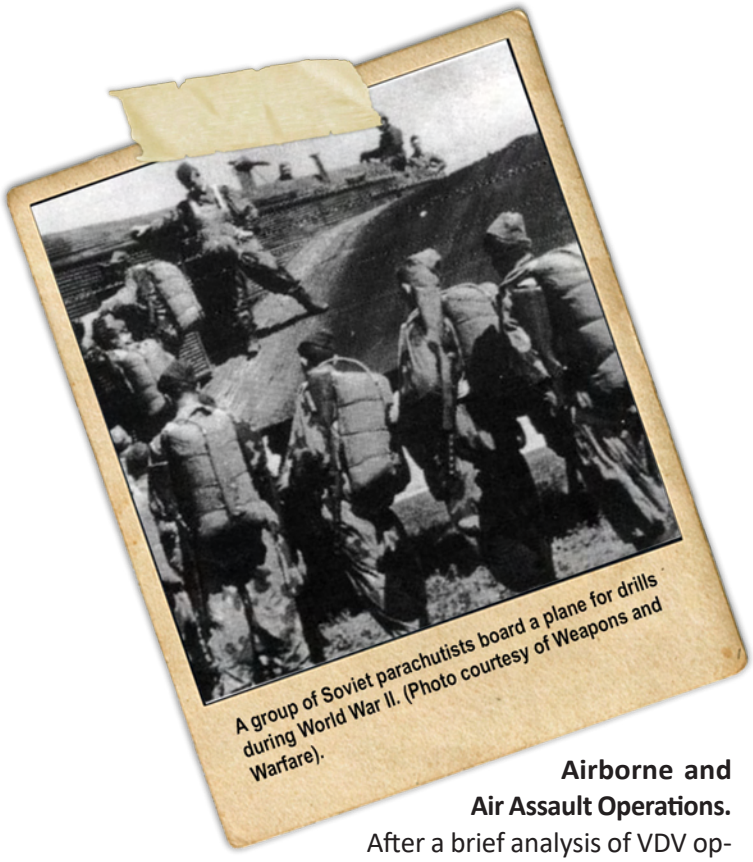
The Russian Airborne Forces, known as the Russian VDV (from the Russian *vozdushno-desantnye voyska*), have a long history and a significant role in the Russian military signature and its ethos. The Russian VDV consists mostly of professional service contract soldiers, making it an elite unit. During the Cold War and after the collapse of the Soviet Union, this force was a strategic threat, capable of airdrop operations far behind enemy lines with a variety of assets. These included infantry fighting vehicles, mortar-howitzers, air defense artillery, and command and control vehicles. After the Russian-Georgian war in 2008, when Russia launched its military transformation and modernization program, the Russian VDV began to receive various wheeled platforms. Many of them are still in use, and some were deployed during interventions in Syria, Kazakhstan, and Ukraine. This change in equipment corresponds to a change of tasks for the Russian VDV. For example, accepting the role of a rapid reaction force, being able to deploy at short notice, and having the capability to travel on wheels for long distances. By knowing what equipment the Russian VDV will use in the near future, the intelligence community can assess the future order of battle for the VDV's battalion tactical groups and its support units.

Role of the Russian Airborne Forces

The Russian VDV originated in the 1930s. This force fought in World War II and deployed to stop insurrections in Hungary (1956) and in Czechoslovakia (1968). The Russian VDV also participated in the Afghanistan campaign (1979 to 1989), both Chechen wars (1994 to 1996 and 1999 to 2000), the war with Georgia (2008), the invasion of Ukraine (2014), and the war with Ukraine (2022 to present). The Russian VDV's participation in these conflicts highlights the significant role of this force. Additionally, the exceptionally high percentage of contract soldiers (80 to 100 percent) makes it considerably more professional and elite than other units in the Russian Armed Forces.[2]

Currently, the Russian VDV consist of two air assault divisions, two airborne divisions, three independent air assault brigades, and one independent Spetsnaz (from the Russian *spetsialnogo naznacheniya*, or special purpose/forces) brigade (Figure 1), making it the largest airborne force in the world. Throughout its 90-year history, the Russian VDV has changed, shifted, and influenced many times.[3]

Historically, parachute divisions were intended to be strategic forces under the command of the general staff, while air assault units were operational forces that supported military district commands. However, during its history, the VDV has also conducted operations as light infantry because of the VDV's superior skills, greater proportion of professional soldiers, and willingness to complete the mission.[4] Also the VDV, equipped with its specialized BMD light armored vehicles, conducted ground forces tasks. For this reason, from 2009 to 2010, the minister of defense and his chief of general staff tried to abolish the VDV as a separate combat arm and to transfer all its existing assets to the army. However, this change never happened because some members of the high command and political leadership wanted to keep the VDV intact. Nonetheless, it created the challenge of identifying a role for the VDV that would justify its separate command structure and distinctive range of equipment.[5]



A group of Soviet parachutists board a plane for drills during World War II. (Photo courtesy of Weapons and Warfare).

Airborne and Air Assault Operations. After a brief analysis of VDV operations in the last 20 years, the intelligence community can distinguish four main roles of the VDV forces:

- Strategic airborne operations in the enemy rear with or without mechanized platforms.
- Operational air assault operations to support the seizure of key terrain.
- Mechanized force to support the main effort axis.
- Rapid reaction force in support of peacekeeping operations, stability operations, and rapid military campaigns around the world.

Operations in Ukraine from late February to early March 2022 confirmed the customary practice of seizing airfields using—

- Air assault of up to a battalion size element to secure a landing zone.
- Parachuted airdrop of a battalion tactical group with armored vehicles.
- Landing of support weapon systems like the T-72B3 main battle tanks, SA-13 air defense artillery systems, and D-30 howitzers.

In most cases, operations were halted after the air assault because the air assault units could not secure the landing zone and destroy Ukrainian air defense artillery assets, thereby denying the arrival of the battalion tactical groups.

Rapid Reaction Force. In early 2019, the Russian Ministry of Defense revealed its intent to revise the role of Russian VDV, changing it from a conventional airborne force to an expeditionary operations force for global hotspots. The force would keep its current types of equipment, including the latest innovations in the order of battle, such as wheeled armored vehicles, main battle tanks, and artillery. At the same time, it would keep a capacity for rapid deployment. The VDV's role would be somewhere between a force of heavy mechanized units, which has great firepower but takes a long time to deploy, and a Spetsnaz force, which is quick to deploy but lacks firepower.[6]

New Equipment for the Russian VDV Forces

In 2016, the Russian Armed Forces reiterated a commitment to shape the VDV as a rapid reaction force. This commitment included new guidelines for rearmament policies, stating that VDV forces should receive the following improvements by 2025:

- BMD-2 upgraded to BMD-2M as a primary infantry fighting vehicle.
- BMD-2 replaced by BMD-4M as a primary infantry fighting vehicle.
- BTR-MD replaced by BTR-MDM multirole armored vehicle.
- 2S9 (Nona) replaced by 2S42 Lotos 120mm self-propelled gun.[7]

Since 2014, Russian VDV forces have received, and are schedule to receive, many wheeled platforms, including—

- 4x4 IVECO Rys (Lynx) as a scout/reconnaissance vehicle.[8]
- 4x4 GAZ-2975-Tigr as a scout/reconnaissance and Spetsnaz vehicle.[9]
- 4x4 K-4386 Typhoon-VDV, a Mine-Resistant Ambush Protected (MRAP) vehicle that has a seven-man dismount and a 30mm autocannon.[10]

Russian Airborne Troops spearhead the Collective Security Treaty Organization's intervention in Kazakhstan (Photo courtesy of the Centre for Economics and Foreign Policy Studies [EDAM])

- 8x8 2S43 "Malva" 152mm self-propelled wheeled artillery system that will serve in the Russian VDV artillery brigade. Accepting wheeled artillery systems into the Russian Armed Forces is a change of approach since the 1980s. Russia expects more military involvement in conflicts in the Middle East and Africa. Terrain in these theaters is more favorable for wheeled platforms and allows the exploitation of its benefits, such as mobility, reliability, maintenance time, and costs.[11]
- 4x4 2S41 "Drok" 82mm mortar, based on the K-4386 Typhoon platform.[12]

Use of Wheeled Platforms—Current Experience

During the past 9 months, the Russian VDV has taken part in two major events that included full or near-full VDV battalion tactical group emplacement—opposing the insurrection in Kazakhstan and the invasion of Ukraine.

Insurrection in Kazakhstan. Responding to Kazakhstan's call for the Collective Security Treaty Organization's support against the insurrection,[13] Russia allegedly deployed approximately 2,500 troops to assist in conducting security operations in key areas in Kazakhstan. Russian officials reported that the Russian Armed Forces deployed the 45th Separate Air Assault Spetsnaz Brigade, elements of the 98th Airborne Division and 31st Separate Air Assault Brigade, and elements of the 76th Air Assault Division.[14] Observing the Russian Armed Forces' composition and the relatively short period of time during which the forces reached Kazakhstan, it can be assessed that this deployment confirmed the VDV's role as a rapid reaction force.

Open-source photo and video evidence from the deployment revealed a high presence of these wheeled platforms. The 31st Separate Air Assault Brigade likely consisted of one mechanized BMD-2 based company, two mechanized BTR-82A based companies, and one motorized K-4386 Typhoon based company, as well as a sustainment company.[15] The 45th Separate Air Assault Spetsnaz Brigade was presumably represented by a company-size element consisting of GAZ-2975-Tigr and BTR-82A vehicles and a sustainment element. An undetermined size of BMD-2 based subunits represented the 98th Airborne Division contingent.

Invasion in Ukraine. On 24 February 2022, the Russian Armed Forces once again invaded Ukraine. Initially, unclassified sources did not provide reliable information about the exact positions of Russian military units. Nevertheless, footage of combat across all axes of the Russian Armed Forces' advance provided a similar pattern about the use of wheeled platforms. Spetsnaz and reconnaissance units have widely used the GAZ-2975-Tigr and KamAZ-63968 vehicles, mostly in urban areas. Generally, VDV units have been performing with BMD-2 and BMD-4 vehicles, reinforced by T-72B3 tanks; however, some units within those formations are using BTR-82A platforms. A few K-4386 Typhoon vehicles were used, typically within naval infantry and Spetsnaz forces, confirming previous reports of a priority to supply these vehicles. Notably, the VDV forces were set to conduct the encirclement of the city of Kiev; however, the operation to seize Antonov airport near Hostomel first did not progress as planned.[16]

Possible Future Order of Battle

Current developments in Russian VDV forces lead to an assessment that, in the midterm, VDV divisions will keep tracked vehicles, replacing the BMP-2 with the BMP-2M and the BMP-4M. Also, in order to unify the motor pool and ease logistical and repair procedures, different support vehicles will be replaced with the ones on the BMP-4 chassis (Figure 2).

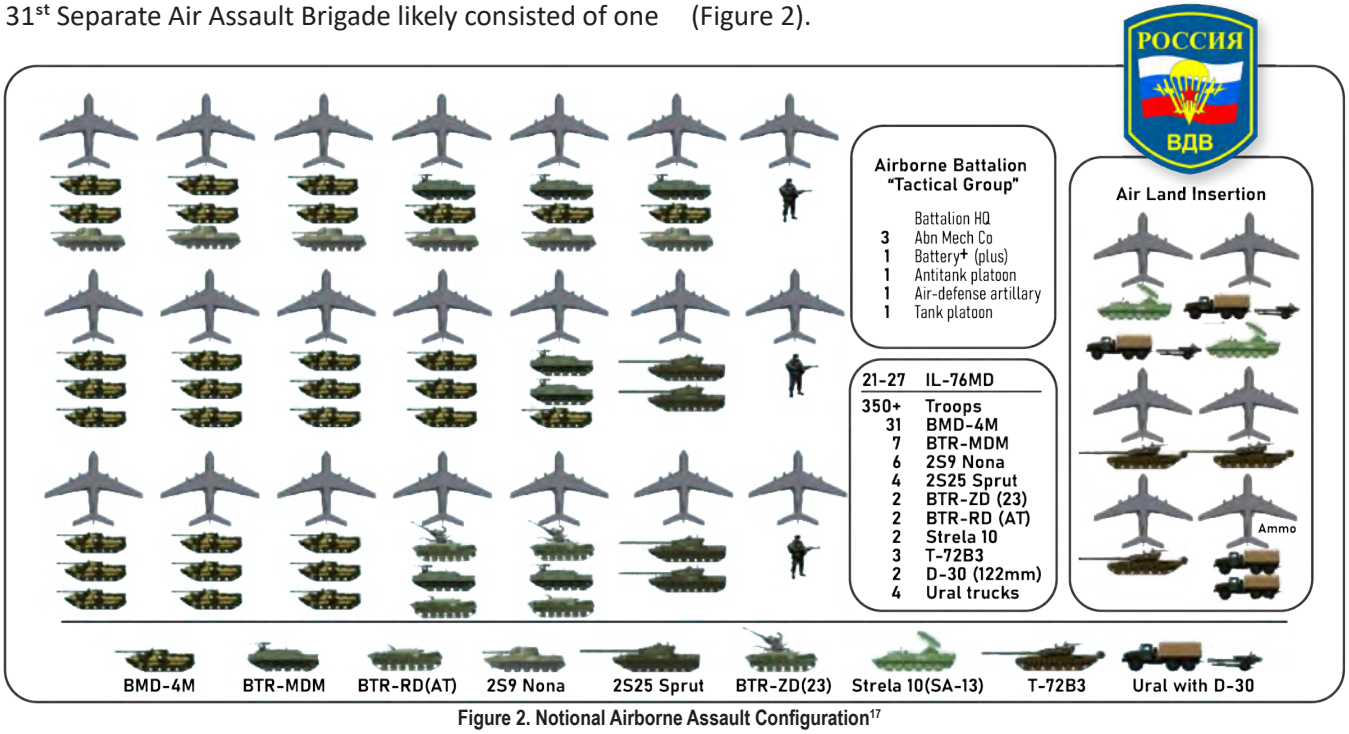


Figure 2. Notional Airborne Assault Configuration[17]

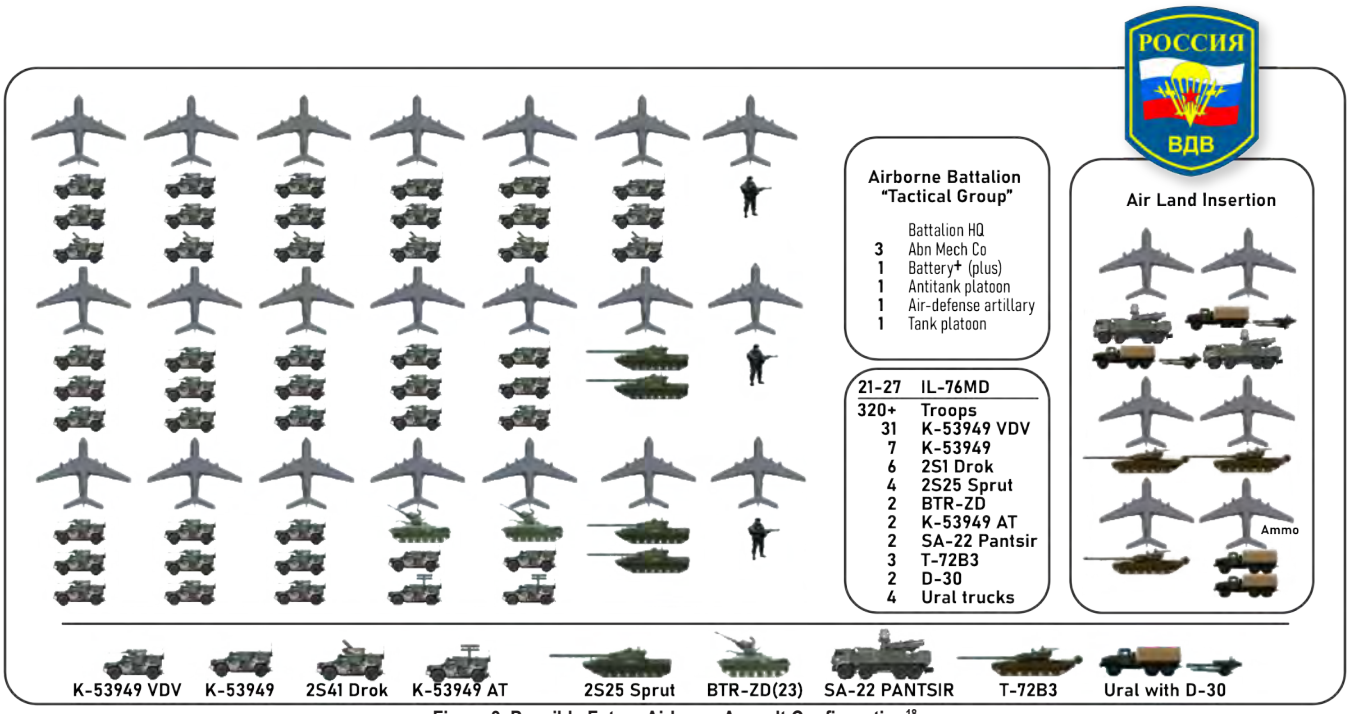


Figure 3. Possible Future Airborne Assault Configuration[18]

The Russian VDV's separate brigades, for instance the 11th, 31st, and 83rd Independent Guards Air Assault Brigades, have received more wheeled platforms in the last 5 years. The intelligence community assesses that these units are testing various possible unit configurations. Taking into consideration recent Russian Ministry of Defense contracts for the procurement of more K-53949s and recent various modifications of this vehicle, it is likely these platforms could create a core for the future VDV independent brigades (Figure 3). The Russian Armed Forces' logistical lessons in the Ukraine campaign indicate it is possible that future VDV forces will simplify their vehicle platforms in order to simplify the corresponding maintenance and repair. Also, it is most likely that the future VDV will significantly increase its sustainment element in order to prevent common fuel and food shortages.

The first 4 weeks of war in Ukraine confirmed the importance of road infrastructure, indicating that modern warfare is highly dependent on controlling urban areas and having ready access to the road and rail infrastructure. The change from tracked vehicles to wheeled vehicles in the order of battle would also generate an economy of force because the K-53949 platforms consist of two crew members, a personnel reduction of approximately 10 percent. Because of the aging BTR-ZD technology, it is also highly likely that the Russian military industry will use mounted air defense systems (K-53949 platform-based).

Conclusion

The Russian Armed Forces are constantly and rapidly changing; however, having a significant number of Soviet-era armored vehicle stocks will delay the forces' modernization. Considering the impact of economic sanctions, it is unlikely Russia will succeed in continuing most of its projects (for example, the Armata Universal Combat Platform and the Typhoon MRAP projects) with the expected speed and volume of output. It is highly likely that Russia will replace its significant losses from the war in Ukraine with refurbished and modernized older-generation vehicles because it is the cheaper solution. Nevertheless, highly mobile forces will be necessary to support friendly regimes threatened by insurrection, to boost economic recovery, and to strengthen economic ties with friendly governments in the Middle East and Africa. This will be the role for the wheeled rapid reaction force—independent air assault brigades.

Endnotes

1. Adapted from Mark Galeotti, "Russian airborne forces retool for expanded role," Janes, October 25, 2021, https://www.janes.com/defence-news/news-detail/russian-airborne-forces-retool-for-expanded-role.

2. Jörgen Elfving, *An Assessment of the Russian Airborne Troops and Their Role on Tomorrow's Battlefield* (Washington, DC: The Jamestown Foundation, April 2021).

3. Rob O'Gorman, "Nobody, but us! Recent developments in Russia's airborne forces (VDV)," Open Briefing, 23 March 2016, https://www.openbriefing.org/publications/intelligence-briefings/nobody-but-us-recent-developments-in-russias-airborne-forces-vdv/.

. Michael Kofman, "Rethinking the Structure and Role of Russia's Airborne Forces," Russian Military Analysis, February 2, 2019, https://russianmilitary-analysis.wordpress.com/2019/01/30/rethinking-the-structure-and-role-of-russias-airborne-forces/.

5. Galeotti, "Russian airborne forces retool."

6. Karl Soper, "Russian Airborne Troops could become airmobile expeditionary force," Janes, January 21, 2019.

7. Nikolai Novichkov, "Russia to focus on re-equipping airborne forces," Defense Weekly, 5 May 2016.

8. Galeotti, "Russian airborne forces retool."

9. Elfving, *Assessment of the Russian Airborne Troops*.

10. ВДВ получили новейшие броневики "Тайфун-ВДВ" ["Airborne Forces received the latest Typhoon-VDV armored vehicles"], ria.novosti.ru, April 4, 2021, https://ria.ru/20210804/tayfun-vdv-1744261952.html.

11. Антон Лавров, А. Ч. Грядка для "мальвы": гаубицы-кабриолеты направят в сухопутные войска [Anton Lavrov, "A bed for 'Mallow': convertible howitzers will be sent to the ground forces,"], June 14, 2021, https://iz.ru/1178521/anton-lavrov-anna-cherepanova/griadka-dlia-malvy-gaubitcy-kabriolety-napraviat-v-sukhoputnye-voiska.

12. Mark Cazalet, "Army 2019: Russia displays 4S21 Drok 82 mm self-propelled mortar," Janes, June 28, 2019, https://www.janes.com/defence-news/news-detail/army-2019-russia-displays-4s21-drok-82-mm-self-propelled-mortar.

13. The Collective Security Treaty Organization (CSTO) is a Russia-led military alliance of seven former Soviet states that was created in 2002. The CSTO's purpose is to ensure the collective defense of any member that faces external aggression. Karena Avedissian, "Fact Sheet: What is the Collective Security Treaty Organization?" EVN Report, October 6, 2019, https://evnreport.com/understanding-the-region/fact-sheet-what-is-the-collective-security-treaty-organization/.

14. Sean Spoonts, "We Think We Know Why Russia Really Sent Troops To Kazakhstan," SOFREP, January 9, 2022, https://sofrep.com/news/we-think-we-know-why-russia-really-sent-troops-to-kazakhstan/.

15. "Deployment of 31st GAABde," TVZvezda, January 8, 2022, https://tvzvezda.ru/news/2022161419-4wCvb.html.

16. Stijn Mitzer and Jakub Janovsky, "Attack On Europe: Documenting Equipment Losses During The 2022 Russian Invasion Of Ukraine," Oryx, February 24, 2022, https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html; and Stavros Atlamazoglou, "Russia's failures in Ukraine have dented the 'elite' status of its paratrooper force," Business Insider, April 3, 2022, https://www.businessinsider.com/russian-failures-in-ukraine-dent-airborne-paratroopers-elite-status-2022-4.

17. Adapted from original by Rob Lee (@RALee85), "*Notional Airborne Assault Configuration*," Twitter, 17 February 2019, 12:49 p.m., https://twitter.com/RALee85/status/1097221595750416384.

18. Adapted from original created by author.

LT Aleksis Ozolins is an intelligence officer of the Latvian National Armed Forces Land Forces Mechanized Infantry Brigade. He authored this article while in the Emerging Leader Program as an international military student in the Military Intelligence Captains Career Course at the U.S. Army Intelligence Center of Excellence.

CONDUCTING NONSTANDARD AERIAL SUPPORT & COLLECTION

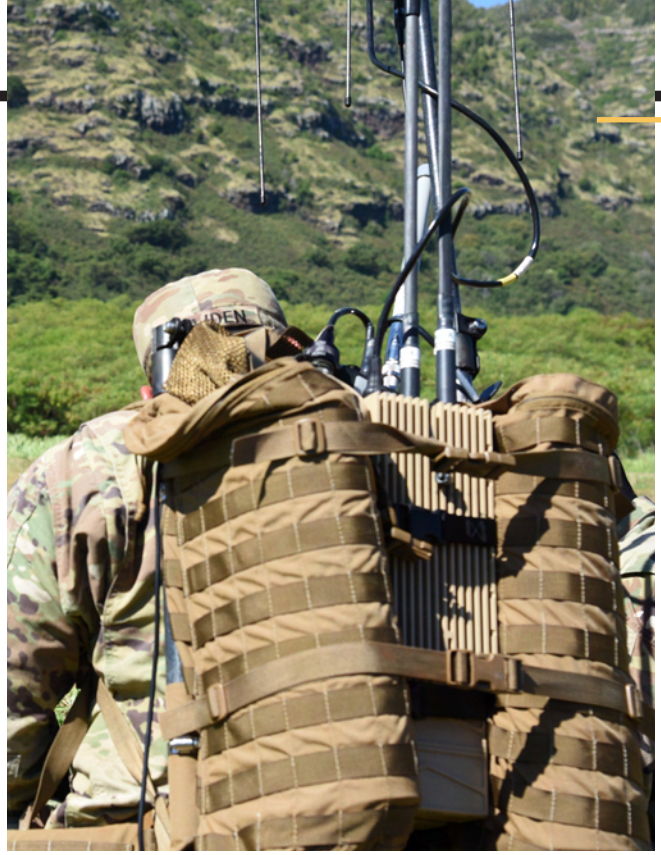
by First Lieutenant Cassandra Mundekis

Introduction

The Full On-the-Move (OTM) and At-the-Halt (ATH) Manpack Collection and Geolocation Solution (HPack) and the Versatile Radio Observation and Direction (VROD) are organic electromagnetic warfare (EW) and signals intelligence (SIGINT) direction finding (DF) systems operated across the battlefield. These two systems use the electromagnetic signature from the enemy to provide early detection and warning. In July 2021, 25th Infantry Division Soldiers from 2nd Infantry Brigade Combat Team and 3rd Infantry Brigade Combat Team evaluated the effectiveness of these organic EW and SIGINT assets when operated from an aerial platform. The purpose of this training was to validate the division's concepts for integrating EW and SIGINT on the battlefield, to create new training plans for EW and SIGINT operators, and to explore new capabilities for 25th Infantry Division to employ in a spectrum-contested environment.

Background

Low-level voice intercept (LLVI) and DF teams use information networks and triangulation to fix enemy targets on the battlefield. The EW and SIGINT teams operate together in constant communication to provide ground force commanders with accurate and timely information, both OTM and ATH. The HPack and VROD are the organic assets available at the brigade level to acquire advanced collection throughout the electromagnetic spectrum. Current tactics, techniques, and procedures (TTP) employ these assets through the ground force, using dismounted movement on foot or from a mounted vehicle. Given the steep terrain and dense vegetation of environments within the Indo-Pacific area of responsibility, utilization of these assets from an aerial platform would add to the division's capability to find, fix, and engage targets in rough terrain, archipelagos, and jungle environments.



Electronic warfare specialists assigned to 2nd Infantry Brigade Combat Team, 25th Infantry Division, conduct radio checks before fielding the Versatile Radio Observation and Direction (VROD). (U.S. Army photo)

Data and Findings

The collection team conducted the training with the 25th Infantry Division Combat Aviation Brigade on 27 July 2021. They operated from a UH-60 Blackhawk helicopter flying in an aircraft traffic pattern around Wheeler Army Airfield, Hawaii. Rabbits (the targets) operating Baofeng radios posed as opposing forces during the training, providing constant radio signals and LLVI for the operators. During the approximately 48-minute flight, operators recorded 28 lines of bearing from the signals provided by the rabbits, 5 of which were accurate within 100 meters of the targets. The system proved moderately successful in giving a general direction of the targeted emitter's location. During the next training event, operator skills, training on the aerial platform, and a signals environment with less electromagnetic or radio frequency interference will be necessary to produce a refined answer about the accuracy the system can provide while mounted on the aerial platform.

Capabilities and Limitations

Designed for ground collection, the HPack and VROD displayed specific challenges and limitations when performing collection from an aerial asset. Normally carried in a medium ruck with the DF antenna protruding from the top, the HPack and VROD need to be secured by the five-point AmSafe restraint system in the seat closest to the doors of the UH-60. When conducting collection from the aerial platform, a minimum of two operators and the system itself require seats on the manifest, which reduces the number of personnel the aircraft can carry. However, the HPack is secured in such a way that Soldiers can easily emplace the HPack system within minutes of arriving at the aircraft. This allows operators to use the system for air assault missions or collection during movement to or from an objective without creating a time burden on the unit.

The SIGINT collection asset outperformed the VROD when used from the UH-60. The VROD's Global Positioning System (GPS) software updates the location of the system every 5 seconds, while the HPack GPS can provide almost real-time GPS data. The speed of the aircraft created a lag in GPS that inhibited the VROD from gaining a GPS lock on any of the targets. The HPack locked in and gained fixes on the targets from a considerable distance.

The altitude of the helicopter increased the line-of-sight capability of the HPack system. The system performed best when the platform was perpendicular to the target. Although many relatively accurate line-of-bearing readings were produced, the collection environment proved difficult for the operators, and some readings were erroneous because of wind, roll, and pitching of the aircraft.

Beyond DF, the LLVI capability was present but severely degraded because of the loud conditions of the aircraft. Further testing using different signal strengths, headphones, and settings of the system is necessary to examine the LLVI capabilities from an aerial platform.

Intelligence Collection

Collection from an aerial asset will increase on-the-ground situational awareness and will directly increase mission success rate. Whether this system is used in direct support of air assault operations or for collection on priority intelligence requirements, the capability to gain a wider area of collection provides a better early warning capability for ground force commanders looking to clear through or occupy an area.

Further training from this platform leading to TTP for operation during flight would greatly increase the DF capability of this system on the aerial platform. Using a team in both a lead and a trail helicopter with HPacks oriented in opposite directions would provide the best coverage of the area of interest. The first test-run placed both systems in the same helicopter with both doors open, creating a wind tunnel in the platform. These conditions affected the operators' ability to use the system and efficiently communicate the results. The second test-run used one collection team with one of the UH-60 doors open. Minimizing the wind tunnel in the helicopter created a better collection environment for the operators.

SIGINT personnel can use the HPack from the aircraft alone or in conjunction with the ground-based, vehicle-mounted program of record-B system and other available collection assets. Each collection method provides its own advantages and disadvantages; however, a combination of collection methods would increase the overall ability to provide commanders with accurate and timely information.

Way Forward

Using the HPack from an aerial platform provides a short-term answer for aerial collection throughout the electromagnetic spectrum. Acquiring an unmanned aerial vehicle with the capability of DF (such as the EW pods) would increase precision and accuracy as an aerial collection asset. While less accurate, the HPack is more versatile in mounted or dismounted collection and can provide similar results as an asset for an organic brigade combat team's military intelligence company. Performing collection on this aerial platform immensely increases the competency of the operators and provides division-level capabilities and intelligence to maneuver commanders at echelon.

1LT Cassandra Mundekis serves in Delta Company, 29th Brigade Engineer Battalion, 3rd Brigade Combat Team, 25th Infantry Division, as the signals intelligence platoon leader. She previously served in 3rd Battalion, 7th Field Artillery Regiment, as the assistant S-2. She holds a bachelor of science in English from the United States Military Academy at West Point.

A Cyber Electronic Warfare Officer assigned to the 37th Infantry Brigade Combat Team, monitors Versatile Radio Observation and Direction (VROD) equipment during a training mission, similar to the mission discussed in this article, at Camp Grayling, MI, August 14, 2022. (U.S. Army photo)

On the Outside, Looking In: Three Simple, Accessible Tools to Enhance Your Assessments

by Lieutenant Colonel Matthew Fontaine

Introduction

Predicting the future is not easy. Most people, including expert forecasters, are downright lousy at it.[1] Many people cannot admit to, or are blind to, the "systematic flaws in their judgment" that undermine their predictive powers.[2] Intelligence professionals are no different. The world is also becoming more complex at an accelerated pace.[3] Despite these challenges, principals rely on analysts to provide "timely, accurate, relevant, and predictive intelligence" to support decision making in what can be life-or-death situations.[4] It is a tremendous responsibility.

My aim is to provide three simple, accessible tools to increase the richness and predictive accuracy of your assessments. This article is primarily for intelligence professionals, but any staff member or commander will find value in it. Staff should employ the tools in design, in planning, and during the reverse intelligence preparation of the battlefield process. Commanders will find the tools personally valuable when visualizing and will gain improved analytic products simply by encouraging their intelligence sections to use these tools.[5]

This article will not turn you into an advanced analyst or a "superforecaster."[6] That would be a tall order given the experience level of the typical analyst and the high personnel turnover rates common to any unit. I also understand that doctrinal prescriptions for improving analytic rigor appear daunting to busy intelligence personnel. Fortunately, the three tools are easy to use and improve your predictions by increasing the richness of your threat models and courses of action (COAs). They are—

- Theory.
- The "outside view."[7]
- Historical examples.

These tools work because they shift an analyst's initial focus from the details of the examined case to the broader patterns influencing the situation (Figure 1). Great analysts are gung ho; however, analytic enthusiasm ungoverned by theory, uninformed by the outside view, and ignorant of history leads to incomplete (or worse) analytical products. This article demonstrates how each of the three tools improves finished intelligence. It also offers two simple methods for incorporating the tools into your analytical production process. Use the tools together and in the presented sequence for the best results. By the end of this article, I think you will agree that it pays to be on the outside, looking in, when using the analytic process.

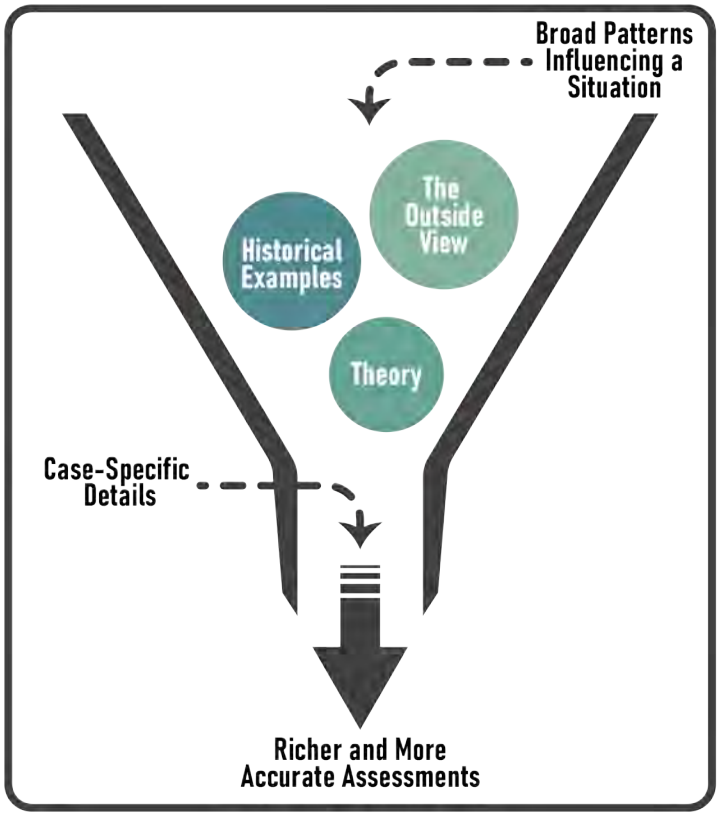


Figure 1. Three Simple, Accessible Tools to Enhance Your Assessments[8]

The Threat Model Defined

Before we go further with the three tools, what is a *threat model*? ATP 2-01.3, *Intelligence Preparation of the Battlefield*, defines a threat model as an "analytic tool" that an analyst uses to "accurately portray how threat forces normally execute operations and how they have reacted to similar situations in the past."[9] Analysts leverage threat models to predict enemy COAs and to illuminate potential friendly counteractions.[10]

Simply put, a threat model predicts the decision that a rational actor will take in a particular situation.[11] It stands to reason that the greater the analyst's understanding of the threat's characteristics, the better the threat model will be. Doctrine indeed urges analysts to "use all available sources to update and refine threat models."[12] Step 3 of the intelligence preparation of the battlefield process identifies *11* threat characteristic research categories. Moreover, ATP 2-33.4, *Intelligence Analysis*, lists dozens of additional unique analytic considerations across the strategic roles to ensure no stone is left unturned.[13]

That's a lot of information to analyze. How are analysts supposed to approach this complex task and make sense of what they uncover? That's where the first tool—theory—comes in.

The Value of Theory

A *theory* is a set of "ideas intended to explain something, especially one based on general principles independent of the thing to be explained."[14] Theorists believe a discoverable and underlying order to social activities exists.[15] Authors and political theorists James N. Rosenau and Mary Durfee describe the underlying order using the activity's "*central tendencies*."[16] The term *tendencies* is a deliberate choice. Theoretical constructs on human happenings are probabilistic, and no ironclad law exists that can predict human behavior with 100 percent accuracy.[17] Instead, theory outlines something's "inclination toward a particular characteristic or type of behavior."[18]

Analysts need theoretical frameworks to make sense of complex operational environments.[19] In my experience, when analysts need to provide an assessment on a given topic, many of them jump into the mass of classified intelligence reports without first adopting a theory to guide their thinking and a research plan. As a result, the analyst develops ineffective search queries that pull too many or too few reports because they are unsure of what to examine, or they enter a sort of "analysis paralysis"—unable to draw conclusions from what looks like a hopelessly complicated situation.[20]

Analysts engaged in haphazard research or plagued by analysis paralysis often produce assessments without a strong central argument—assessments that are more like report summaries than intelligence. Noncontextualized observations do not provide the insight to support an organization's decision-making process effectively. Without theory, an analyst is "destined for endless confusion, for seeing everything as relevant and thus being unable to tease meaning out of the welter of events, situations, trends, and circumstances" of a particular affair.[21] In contrast, analytic output governed by theory is more likely to provide the "insight into future conditions or situations"[22] that principals need to gain an advantage in an operational environment.

The "Of-What-Is-This-An-Instance" Question

So, how do analysts leverage theory in intelligence production? At every opportunity, analysts must get into the habit of asking what Rosenau and Durfee call the "of-what-is-this-an-instance" question.[23] The of-what-is-this-an-instance question effectively shifts the analyst's mindset from viewing everything as a unique event to something linked to a broader pattern.[24]

The analyst begins by asking "Of what is this an instance?" to contextualize the examined phenomena within a greater category of social activity (Figure 2).[25] The analyst then casts a wide net to find theoretical construct(s) related to the examined situation's reference category. Once found, the analyst extracts the central tendencies (premises) of a given situation according to the theoretical framework.[26] These tendencies act as a "sorting mechanism" to determine the most and least valuable sources of information to examine.[27] With theory as a guide, the analyst can now tackle the mass and complexity of the available information to overcome analysis paralysis. The goal of the process is to transform "raw observations into refined hypotheses and meaningful understandings" (think, predictive COAs tied to a detailed collection plan).[28]

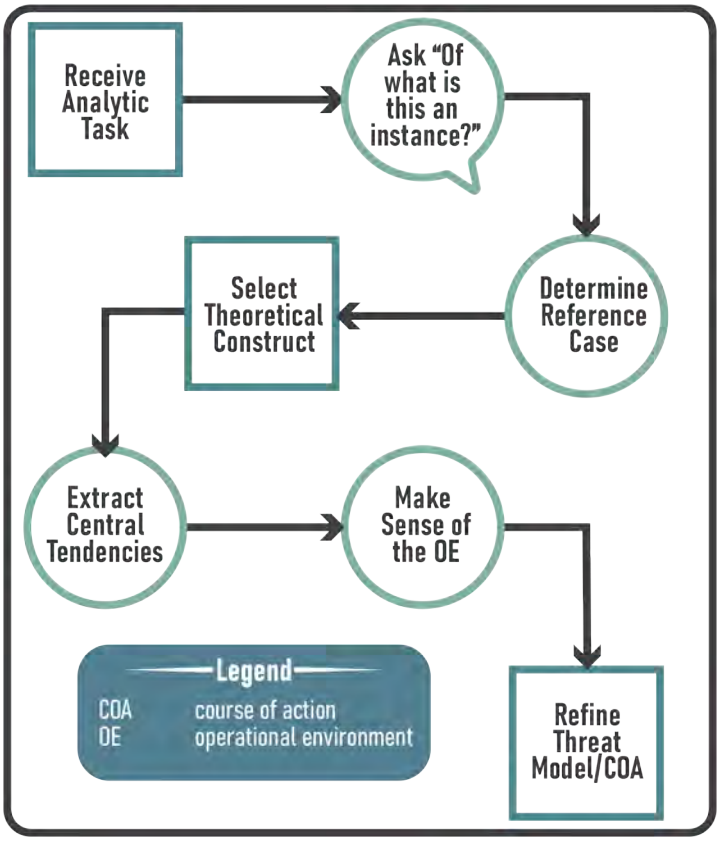


Figure 2. Theory as a Tool Process[29]

Let me illustrate the of-what-is-this-an-instance question process. Imagine an analyst needs to develop threat COAs for the initial ground phase of an anticipated invasion of Country A by Country B. The analyst asks what the **threat** is an instance of, and the analyst defines Country B as a peer threat. The analyst then asks what kind of **activity** Country B may use in the invasion. The analyst determines this to be an instance of a deliberate offensive operation in **multiple domains**. Next, the analyst references peer threat, offensive tactics, and multidomain theory to extract the central tendencies of these frameworks. The analyst incorporates the central tendencies into the Country B threat model. The threat model serves as the base for COA development.

The Threat Force Paradigm

When theorizing, my primary recommendation is simple: use the analytic frameworks already in doctrine or in classified repositories (country studies) to build your threat model. Doctrine is, after all, a kind of *prescriptive* theory because it advocates "fundamental principles that guide the employment" of "*rational*" forces.[30] Threat, activity, and multidomain theory form what I call the threat force paradigm (Figure 3). The threat force paradigm is the U.S. Army's model of how a threat rationally behaves in the modern operational environment. Analysts who leverage the threat force paradigm build richer and more accurate threat models than someone who goes it alone without the aid of an explanatory framework. Unfortunately, many analysts do just that!

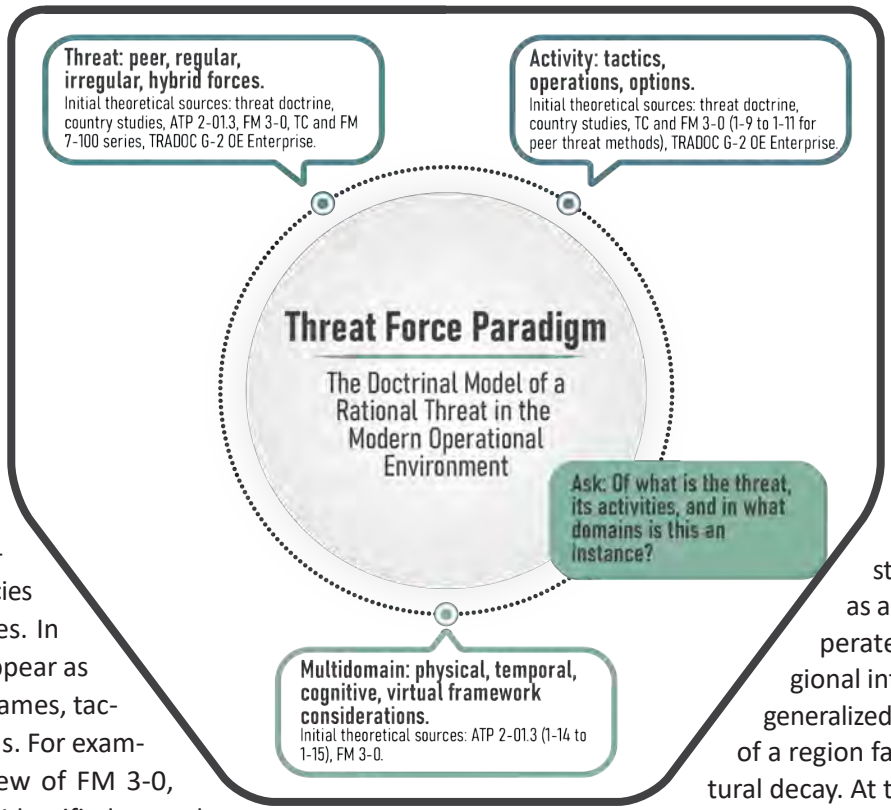


Figure 3. The Threat Force Paradigm[31]

It is up to the intelligence section to extract the central tendencies from theoretical sources. In doctrine, tendencies appear as analytic frameworks, frames, tactics, or lists of assertions. For example, the analyst's review of FM 3-0, *Operations*, could have identified several central tendencies of peer threats such as—

- **Tendency One.** "Peer threats prefer to achieve their goals without directly engaging U.S. forces in combat" but "possess roughly equal combat power" in a given region in comparison to the United States.[32]
- **Tendency Two.** Peer threats may leverage their benefit of cultural kinship in a specific region to gain a "relative advantage" over the United States.[33]
- **Tendency Three.** Peer threats "often employ information warfare in combination with conventional and irregular military capabilities to achieve their goals."[34]

Armed with these tendencies, the analyst gains insight into Country B's current behavior and possible actions. Tendency One supports the possibility of a Country B invasion. Still, it causes the analyst to consider other COAs the threat may take to achieve its ends without directly engaging U.S. forces. Tendency Two compels the analyst to consider the human terrain to determine areas more likely to be supportive or resistant to Country B's aggression. Tendency Three alerts the analyst that no peer threat COA is complete without discussing information warfare and irregular forces. All this insight from just a few tendencies!

A Climb up the Ladder of Abstraction

The threat force paradigm is a great framework, but the analyst does not have to stop there. The analyst can continue to ask "Of what is this an instance?" to develop more and more incorporating simplifications. Each explanation offers fresh insights and raises new questions to guide future research or collection.[35] Rosenau and Durfee visualize this theorizing process as "moving up a ladder of abstraction"[36] (Figure 4, on the next page).

To demonstrate further theorizing, the analyst views the invasion of Country A as a grab for critical resources. At the next rung of the abstraction ladder, it is seen as a corrupt oligarchy's desperate attempt to retain regional influence. Higher still, it is generalized as the political outcome of a region facing economic and cultural decay. At the top, it is the act of a state in the final stages of utter ruin.[37] As before, the analyst leverages theory relevant to each rung to refine the threat model and COAs.

It gets trickier, but not impossible, to find relevant theories as you move up the ladder. Unclassified and classified government repositories remain an excellent source, and some offer

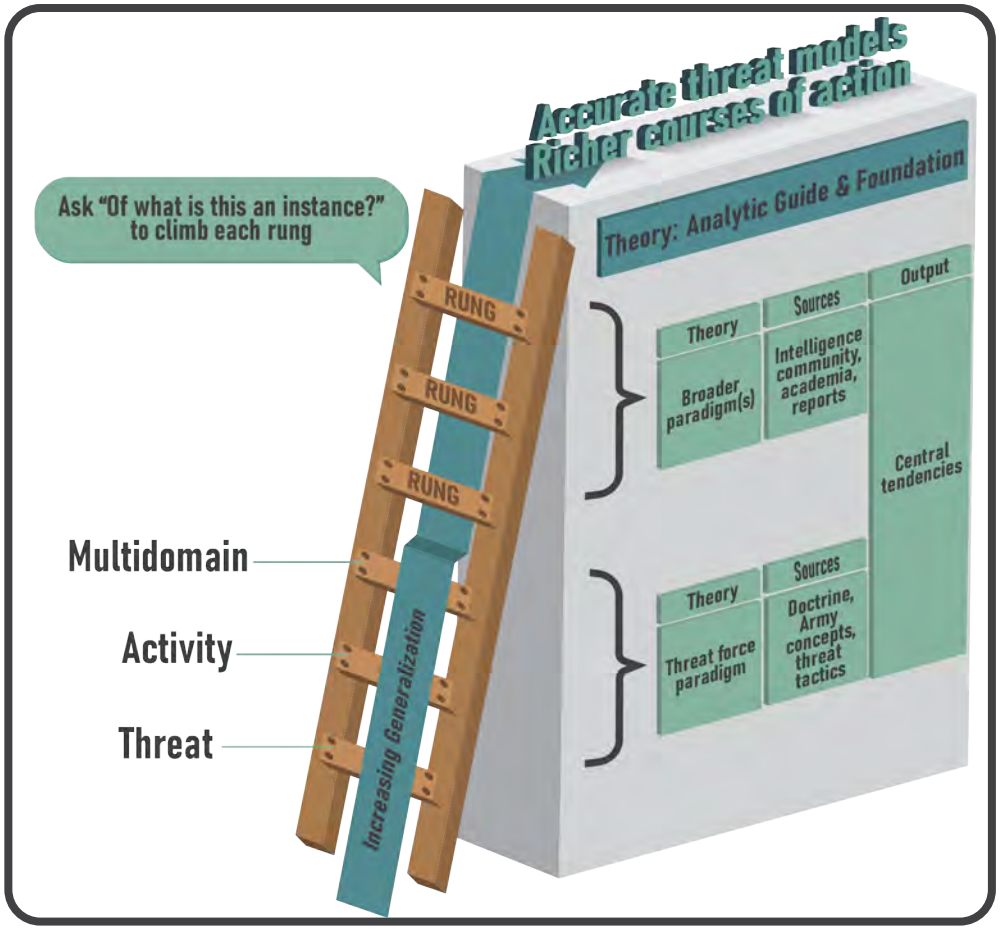


Figure 4. The Ladder of Abstraction[38]

specific models for how a threat or political leader is likely to behave in a given situation.[39] Your higher headquarters is another resource. Outside military channels, news, academic articles, and books are an outstanding theory source.

To illustrate, global political theories provide an excellent explanatory and predictive framework to enhance the Country B threat model. Doctrine suggests regular threats apply the *realpolitik* approach in their political thinking.[40] Let us start there. A quick unclassified search on realpolitik reveals its central tendencies:

- **Tendency One.** "Politics based on practical objectives rather than on ideals."[41]
- **Tendency Two.** "In diplomacy it is often associated with relentless, though realistic, pursuit of the national interest."[42]

The analyst leverages the realpolitik framework to gain insight beyond the threat force paradigm into Country B's possible behavior. For example, the analyst may increase the assessed likeliness of invasion because Country B will pursue its objectives without regard for international norms. Interestingly, the realpolitik lens may also cause the analyst to consider COAs where Country B pursues only limited objectives (perhaps the partial seizure of Country A's territory). This thinking is linked to Tendency Two because, though "relentless," Country B must be "realistic" with its objectives. The analyst may then examine reports or recommend collection to determine the feasibility of Country B's long-term occupation of Country A.

Theory's value is it predicts how a rational adversary is likely to act in a typical situation. The of-what-is-this-an-instance question is your ticket to leveraging theory in your analysis. It guides the research and collection plan and prompts the consideration of newer, richer COAs. However, how is a value assigned to a prediction, and how typical is typical in probabilistic or likeliness terms? Next, I will discuss the outside view and the way it simplifies establishing a forecast's base value.

Outside View

Authors Daniel Kahneman and Amos Tversky have identified "two profoundly different approaches to forecasting" that they dubbed the "inside view" and "outside view."[43] The inside view is the approach many of us take when predicting—we emphasize "our specific circumstances" and hunt "for evidence in our own experiences."[44] This approach often leads to inaccurate forecasts. We overweight the importance of information available to us and do not fully appreciate how the gaps in our knowledge or unanticipated future events could cause our forecast to be wrong.[45] The outside view takes a different approach. It is "the prediction you make about a case if you know nothing except the category to which it belongs."[46] The analyst determines the broader category for the examined case using the of-what-is-this-an-instance question. The analyst researches this "reference case" to develop an "anchor" value to base all future predictions.[47] The analyst then applies the "case-specific information" to adjust the baseline prediction appropriately and continuously.[48]

Suppose an analyst must predict how long a conflict will last in Country C—a state on the brink of civil war. The analyst asks the of-what-is-this-an-instance question to determine a suitable reference case. The analyst determines that the average length of modern intrastate conflict is the reference category. An unclassified search reveals that "since 1945, civil wars tend to last an average of about seven to 12 years."[49] The 7-to-12-year range is the anchor. The analyst is then free to research case-specific information—for example, Country C is increasingly unable to curb terrorist activity inside its borders—to adjust the estimate range and the assessed expression of likelihood. Easy.

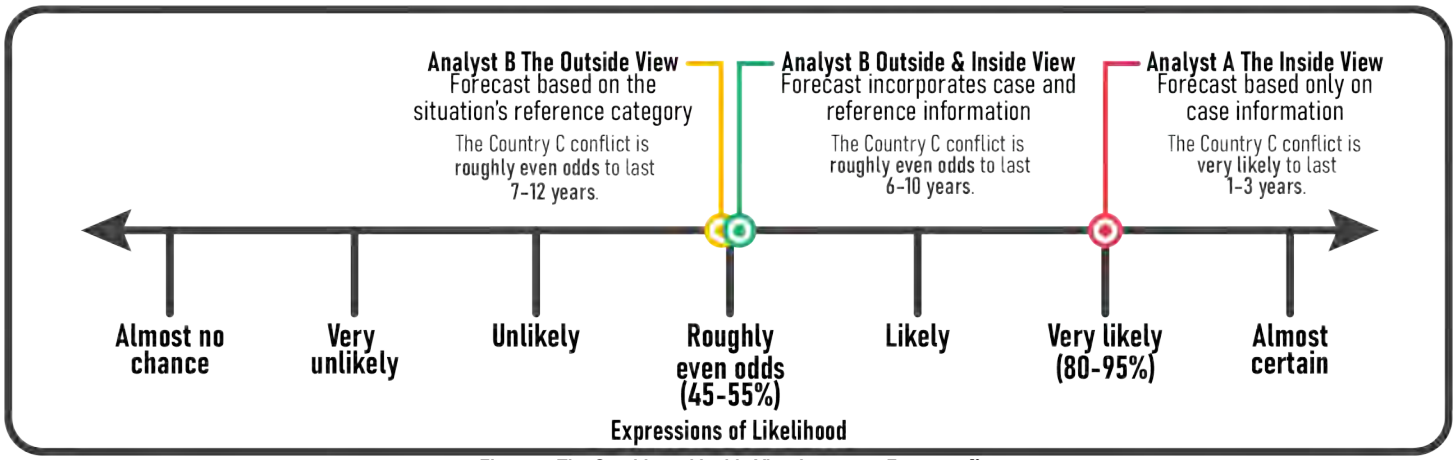


Figure 5. The Outside and Inside View Impact on Forecasts[50]

Outside view "ballpark" assessments work because the real-world examples they take into account incorporate all the messy "contingencies" (more on this later) and friction that we either cannot predict or are prone to overlook.[51] In contrast, inside view assessments can be almost laughably (or tragically) at odds with historical precedent.[52] Analysts develop these historically incongruent forecasts because, like many people, they too tend to overweight accessible information and discount inaccessible or unexamined information in their judgments. The outside view mitigates these common biases. It makes sense to adjust a ballpark figure with inside view information, and it will also make sense to your commander.[53]

Consider the Country C example once more to see how the inside view and outside view affect a forecast (Figure 5). With no outside view information, Analyst A forecasts the conflict is very likely (80 to 95 percent in probabilistic terms) to last 1 to 3 years for whatever inside view reasons or biases. This is an assured (and common) forecast given the astounding complexity and unpredictability inherent to war. In contrast, Analyst B uses the outside view to develop an initial ballpark forecast of a 7-to-12-year conflict for roughly even odds (45 to 55 percent). Analyst B narrows the range to 6 to 10 years at roughly even odds given Country C's inability to curb terrorist activity. Analyst B continuously refines the estimate as new information is received. What estimate would you use if faced with an important decision related to this situation?

Maybe you still need convincing. Kahneman's work and the demonstrated success of the Good Judgment Project's "superforecastors" strongly suggest an analyst should take an outside view. Good Judgment's cofounder is Philip Tetlock, coauthor of *Superforecasting: The Art and Science of Prediction*.[54] An extensive Intelligence Advanced Research Projects Activity competition found that superforecastors were "30% more accurate than intelligence analysts with access to classified information."[55] The outside view is a simple, readily available tool the superforecastors employ when they first approach a situation.[56] We should follow their lead.

The outside view anchors our theoretical frameworks in reality. You may be feeling confident that theory and the outside view are all you need to produce better models. That is *partially* true. The problem is theory is inherently probabilistic—uncertainty can never be completely ousted from human activity. So, we now turn to history to appreciate the role that central tendencies and uncertainty play in real-world situations.

Take a Historical Perspective

Historical information is an important factor in the commander's understanding of an adversary and the often unpredictable dynamics of war.[57] Mark Twain is reputed to have said, "History doesn't repeat itself, but it often rhymes."[58] Knowing this intuitively, many analysts strive to incorporate history's lessons within their judgments, some with good effect. Unfortunately, not every analyst understands how to apply historical insight to their assessments. I will describe the best use of history to develop richer and more predictive COAs (Figure 6, on the next page), but before I do, I will outline the pitfalls to avoid when using historical examples.

Military theorist Carl von Clausewitz observed historical examples were "seldom used to such good effect."[59] Why? First, people tend to draw evidence or theoretical assertions from a historical event even though they lack a deep understanding of the situation. This can be because only limited information is available, or the analyst never put in the effort to deeply understand the historical example. Second, people often cherry-pick from many historical examples to provide supposedly non-subjective proof for a judgment. The analyst may do this because of biases or a desire to keep a pet theory or opinion. (Biases could result from the analyst being blind to counterexamples or ascribing greater weight to supporting examples.) Third, analysts may examine cases made inapt because of extreme geographic or technological dissimilarities.[60] All three pitfalls are severe and can lead to poor assessments.

Fortunately, the best use of history results in richer COAs and takes these pitfalls into account. The first step is to

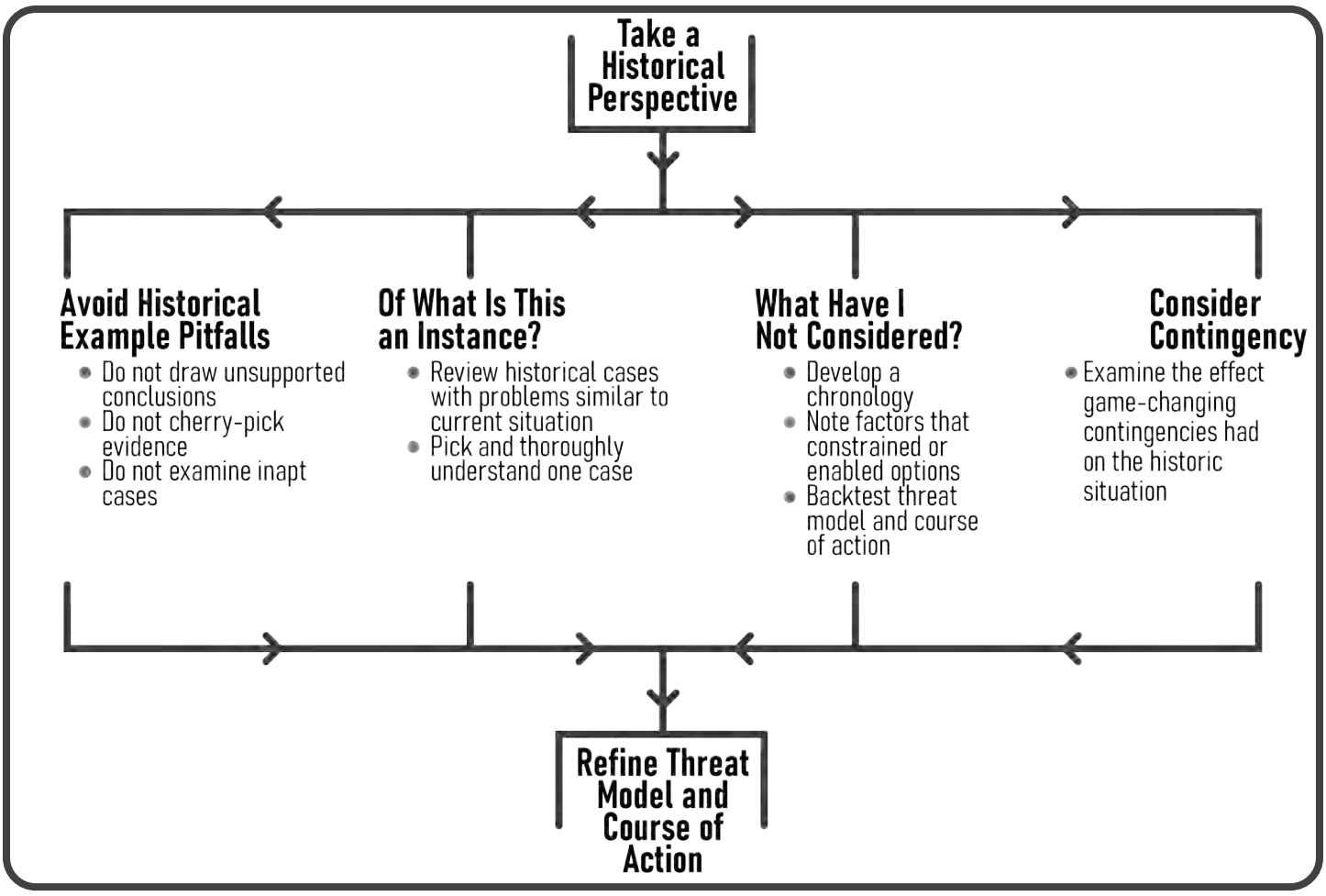


Figure 6. The Historical Perspective[61]

compare the situation to *one* similar and "*thoroughly*" understood single case.[62] As with theorizing, the analyst asks the of-what-is-this-an-instance question to determine a relevant historical category. This should be easy because the analyst has already generalized the situation with the theory and outside view tools. The analyst and section then make a judgment call to select one historical case to study. It is best to choose an example with a problem similar to the one the current adversary is attempting to solve.[63]

Next, the analyst compares the historical case to the current situation by asking "What have I not considered?" throughout the process.[64] The analyst reviews unclassified and classified sources to develop a chronology of the historical example that, according to authors Richard Neustadt and Ernest May, "plot[s] key trends while also entering key events, especially big changes."[65] The analyst carefully notes the factors that constrained or enabled the options available to the examined decision maker and the way these factors influenced their pursued goals.[66] The gleaned insights "*suggest*" how the modern-day decision maker might be similarly enabled or limited.[67] Additionally, the analyst uses the case to backtest their draft model to see how well (or poorly) it would explain the historical outcome. The objective of the historical comparison and test is to reveal unconsidered details, constraints, options, or central tendencies to refine the modern-day models and assessed probabilities. Most importantly, this process reveals the profound impact of "contingency."[68]

Enter Contingency

Humans at war are unpredictable. Clausewitz believed "no other human activity is so continuously or universally bound up with chance" as war, partly due to factors such as "courage, boldness, or even foolhardiness,"[69] so much it would seem for any model that assumes rational actors or claims "absolute" prescriptions.[70] Do not worry; theory remains invaluable so long as we remember it deals in tendencies, not absolutes.[71] With that in mind, we study historical contingency to appreciate the role of uncertainty in human affairs.

Author and historian John Lewis Gaddis defines *contingencies* as "phenomena that do not form patterns."[72] This aspect makes contingencies difficult or impossible to predict ahead of time.[73] In Neustadt and May's language, contingencies might be behind the "big changes" in a situation's chronology. Contingencies can occur because "of the actions individuals take for reasons known only to themselves"[74] or perhaps unknown even to the actor. These acts can be irrational and outright contrary to the behavior predicted by theory, or they can be the novel combination of previously separate, predictable tendencies can lead to unforeseeable

and volatile results.[75] Contingency's common factor is "we generally learn about them only after they've happened."[76] Especially frustrating for an analyst, contingencies are usually explicable only "*after*" they have occurred.[77] (An example of this is the September 11 attacks).

Contingencies make a mess of things and can completely change the central tendencies of a given situation. Analysts must account for this in their assessed COAs and collection plans. An analyst appreciates how a contingency may affect the current operational environment by thoroughly examining how unanticipated game-changing events altered a similar situation in the past. This analysis reveals indicators to watch for, or scenarios to be wary of, in the current operational environment (history rhymes). The aim is not to predict a specific event that is by definition unpredictable but to develop collection plans that continuously monitor the operational environment for subtle or radical changes from the predicted behaviors. When change occurs, analysts immediately update their threat models and COAs accordingly.

Imagine once more Country B's anticipated invasion. The analyst examines Country B's incursion into Country D to gain historical insight into the current situation. The analyst develops a detailed timeline of the invasion and uses the information to refine the current situation's event template. The analyst then examines Country B's information operations (a previously underappreciated aspect in the analyst's Country B threat model) in the invasion's lead-up to add new details to the present COA. Finally, the analyst notes the outsized consequences following the destruction of a border checkpoint in Country D at the start of the conflict. Unknown to Country B, a Country D soldier live-streamed the attack. The video generated an intense will to resist in Country D and dramatic worldwide condemnation (contingency). The analyst develops new social media collection requirements with this insight for the present-day situation.

One thoroughly understood historical example will go far in developing richer, more predictive COAs because history demonstrates how a theoretical model played out in the real world.[78] Keep in mind, historical studies include multiple domains (cyberspace, for example) and should be drawn from recent history if possible.[79]

Incorporating the Three Tools

An intelligence section can easily integrate the three tools into the analytic production process using two methods:

- **Brainstorming sessions**—The section incorporates brainstorming sessions in the section's standard operating procedure to collectively determine applicable theoretical construct(s), the outside view reference category, and the most relevant historical case.
- **Professional reading program**—The intelligence section leverages its professional reading program to set the conditions for the effective use of the tools. The program should include wide-ranging military case studies and theoretical examinations specific to the unit's threat or geographic area of interest.[80] This ensures the intelligence section has a catalog of relevant theory and ready historical examples at the start of any new situation requiring a major analytic assessment.

Conclusion

Theory (or the threat force paradigm), the outside view, and historical examples are your simple, accessible tools to improve the comprehensiveness and accuracy of your assessments. Analysts use the three tools to overcome analysis paralysis, make sense of complex situations, and mitigate the common biases that undermine analytic output.

Each tool is interrelated and works on the same principle. We should first discern the broader patterns influencing a particular situation (outside view) before diving into its specific details (inside view). Theorists average many historical cases to develop a theory's central tendencies (anchors). Theory is, therefore, like the outside view of a particular human activity. Likewise, forecasters (especially the *super* ones) average the impact of historical trends and contingencies of many related situations to arrive at a reasoned ballpark figure for a given theoretical prediction. History anchors theory in the real world and provides a vivid (inside view-level detail) warning about contingency's unpredictable impact. Analysts use all three tools to craft richer threat models and COAs. These assessments represent our theory of how an adversary will behave in a particular situation.

So, go ahead and give these ideas a try! If you do, you will not only become a better analyst but also a better *theorist*.

Endnotes

1. David Epstein, "The Peculiar Blindness of Experts," *The Atlantic*, June 2019, https://www.theatlantic.com/magazine/archive/2019/06/how-to-predict-the-future/588040/.

2. Ibid.

3. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018).

4. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 6 July 2018), 1-1.

5. I gained an appreciation for the tools as a student at the Advanced Military Studies Program (AMSP) from 2016 to 2017. The program's curriculum contained several of the authors and works cited in this article, demonstrating the tools' broad applicability beyond the intelligence warfighting function. I credit AMSP for the general insights in this article and, in particular, Dr. G. Stephen Lauer, who was an associate professor of military history at AMSP. Dr. Lauer underscored the value of James N. Rosenau and Mary Durfee's "of-what-is-this-an-instance" question. It stuck. Of course, any errors are mine.

6. Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Broadway Books, 2015), 3.

7. Daniel Kahneman, "Daniel Kahneman: Beware the 'inside view,' " *McKinsey Quarterly*, November 1, 2011, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/daniel-kahneman-beware-the-inside-view.

8. Graphic by author, using information from Kahneman, "Beware the 'inside view.' "

9. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. GPO, 1 March 2019), 5-9. Change 1 was issued on 6 January 2021.

10. Ibid., 5-3, 5-5.

11. Ibid.

12. Ibid., 5-9.

13. Department of the Army, ATP 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. GPO, 10 January 2020).

14. Lexico, s.v. "theory," accessed 8 July 2022, https://www.lexico.com/en/definition/theory.

15. James N. Rosenau and Mary Durfee, *Thinking Theory Thoroughly: Coherent Approaches to an Incoherent World* (Boulder, CO: Westview Press, 1999), 229.

16. Ibid., 6, 229.

17. Ibid.

18. Lexico, s.v. "tendency," accessed 8 July 2022, https://www.lexico.com/en/definition/tendency.

19. Rosenau and Durfee, *Thinking Theory Thoroughly*, 1–2.

20. Ibid., 2. In their book, *Thinking Theory Thoroughly*, Rosenau and Durfee use the term *intellectual paralysis*.

21. Ibid., 7.

22. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 26 May 2022), I-2.

23. Rosenau and Durfee, *Thinking Theory Thoroughly*, 5.

24. Ibid., 230–231.

25. Ibid., 3.

26. Ibid., 4–7.

27. Ibid., 2. Theory is a "sorting mechanism"; therefore, the theory that the analyst selects can profoundly influence their interpretation of an examined subject. I recommend Rosenau and Durfee's work, *Thinking Theory Thoroughly*, for greater detail, as well as Epstein's "The Peculiar Blindness of Experts" for a primer on the value of incorporating many viewpoints when forecasting. Combining the three tools (as opposed to one or two) automatically brings multiple views into a forecast.

28. Ibid., 5.

29. Graphic by author, using information from Rosenau and Durfee, *Thinking Theory Thoroughly*, 1–7, 229.

30. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, May 2022), 114; and IGI Global, s.v. "What is Prescriptive Theories," accessed 16 March 2022 (emphasis added), https://www.igi-global.com/dictionary/rational-decision-making-dual-processes/23280. The word *rational* is from IGI Global.

31. Graphic by author, using information from Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 1-14–1-15, 5-1–5-3; Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), 1-9–1-11. Change 1 was issued on 6 December 2017; and Rosenau and Durfee, *Thinking Theory Thoroughly*, 1–7.

32. Department of the Army, FM 3-0, *Operations*, 1-9.

33. Ibid.

34. Ibid.

35. Rosenau and Durfee, *Thinking Theory Thoroughly*, 2–4.

36. Ibid., 2.

37. Rosenau and Durfee, *Thinking Theory Thoroughly*, 3–4. Example adapted from Rosenau and Durfee, *Thinking Theory Thoroughly*.

38. Graphic by author, using information from Rosenau and Durfee, *Thinking Theory Thoroughly*, 1–7.

39. Examples of unclassified government repositories are the Defense Intelligence Agency's Military Power Publications, https://www.dia.mil/Military-Power-Publications/, and the U.S. Army Training and Doctrine Command G-2's Operational Environment Enterprise, https://oe.tradoc.army.mil/.

40. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 5-2.

41. *Encyclopedia Britannica Online*, s.v. "realpolitik," accessed 18 March 2022, https://www.britannica.com/topic/realpolitik.

42. Ibid.

43. Kahneman, "Beware the 'inside view.' "

44. Ibid.

45. Ibid.

46. Ibid.

47. Ibid.

48. Ibid.

49. Max Fisher, "Political science says Syria's civil war will probably last at least another decade," *Washington Post*, October 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/10/23/political-science-says-syrias-civil-war-will-probably-last-at-least-another-decade/. Max Fisher cites James Fearon's 2002 study for average civil war length. Max Fisher's entire article is an excellent real-world example demonstrating the value of outside view thinking (not a term he uses). It also reflects the application of central tendencies to support his prescient 2013 forecast—Syria's civil war was likely to last a long time.

50. Graphic by author, using information from Kahneman, "Beware the 'inside view' "; and Department of the Army, ATP 2-33.4, *Intelligence Analysis*, C-2.

51. Kahneman, "Beware the 'inside view.' " *Ballpark* is Kahneman's term; and John Lewis Gaddis, *The Landscape of History: How Historians Map the Past* (New York: Oxford University Press, 2002), 30. The term *Contingencies* is from Gaddis.

52. Epstein, "Peculiar Blindness of Experts."

53. Kahneman, "Beware the 'inside view' "; and Tom Koller and Dan Lovallo, "How to take the 'outside view,' " McKinsey & Company, March 5, 2019, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-to-take-the-outside-view.

54. "Superforecasting will change the way you think about the future," Good Judgment, accessed 29 March 2022, https://goodjudgment.com/about/.

55. Ibid.

56. Tetlock and Gardner, *Superforecasting*, 117–124. I recommend a complete reading of this work. I believe the outside view to be one most powerful and easily applicable concepts to military affairs described in the book.

57. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 5-4.

58. Quote Investigator, "History Does Not Repeat Itself, But It Rhymes," *Quote Investigator*, accessed 18 March 2022, https://quoteinvestigator.com/2014/01/12/history-rhymes/.

59. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 170.

60. Ibid.; and Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision-Makers* (New York: The Free Press, 1986), 237–238.

61. Graphic by author, using information from Rosenau and Durfee, *Thinking Theory Thoroughly*, 1–7; Clausewitz, *On War*, 85–86, 170–174; Neustadt and May, *Thinking in Time*, 235–238; and John Lewis Gaddis, *Landscape of History*, 30–31.

62. Clausewitz, *On War*, 173 (emphasis added).

63. Neustadt and May, *Thinking in Time*, 237–238.

64. Ibid., 235–236. The question in quotations is a simplification and adaption of Neustadt and May's "journalist questions," not a direct quote.

65. Ibid., 235.

66. Ibid., 235–237. This is a simplification. I recommend a thorough reading of Neustadt and May's *Thinking in Time* to gain the full utility of their model.

67. Ibid., 236 (emphasis added).

68. Gaddis, *Landscape of History*, 30.

69. Clausewitz, *On War*, 85–86.

70. Ibid., 86.

71. Rosenau and Durfee, *Thinking Theory Thoroughly*, 229.

72. Gaddis, *Landscape of History*, 30.

73. Ibid.

74. Ibid., 31.

75. Ibid. Gaddis attributes this insight to Scott D. Sagan.

76. Ibid.

77. Ibid., 66. Gaddis attributes this insight to Jay Gould.

78. Clausewitz, *On War*, 172–173 (emphasis added).

79. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, D-1; and Clausewitz, *On War*, 173–174.

80. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield*, 5-8.

LTC Matthew Fontaine is the G-2 for the U.S. Army Joint Modernization Command. He has deployed twice to Iraq and twice to Afghanistan, serving as an executive officer, platoon leader, battalion S-2, military intelligence company commander, and analysis and control element chief. He holds two master of military art and science degrees, one in general studies and the other in operational art and science, from the U.S. Army Command and General Staff College.

HUAWEI: EXPANDING CHINA'S TECHNOLOGY WEB

by Chief Warrant Officer 4 Charles Davis

Image courtesy of Flickr

Introduction

In 2019, the *Journal of Political Risk* asserted Huawei was the most valuable telecommunications company worldwide. The company's net worth was estimated at US$38 billion, controlling 10 percent of the global smartphone market with a compound annual revenue growth of 26 percent.[1] Huawei's 2021 annual report indicated that it provided telecommunications connectivity to more than 70 countries and regions.[2] Additionally, the company reported significant gains in artificial intelligence development and integration, boasting a top 30 listing as a Super Artificial Intelligence Leader.[3]

In September 2021, both Huawei's high-resolution millimeter wave radar and its artificial intelligence algorithm-based cloud warning technology won the Global New Energy Vehicle Cutting-edge and Innovative Technologies Award from the World New Energy Vehicle Congress.[4] Soon, Huawei expects to achieve automation, self-healing, self-optimization, and autonomy for its Autonomous Driving Networks. These milestones will incorporate four features: advanced intelligent sensing, digital mapping, self-learning, and adaptive decision making.[5] Given such significant global success, why would the United States be concerned with Huawei leading the development of 5th generation mobile network (5G) capabilities in America? The answer is clear: Global industries and government infrastructure are increasingly relying on mobile networks. 5G network integration could pose significant domestic, strategic, and national security risks. Which means the United States needs a clear understanding of the relationships between nation states and corporations that develop those technologies.

Private Company or Arm of the State?

Huawei was founded in Shenzhen, Guangdong, China, in 1987 by Ren Zhengfei, a former People's Liberation Army officer. The company is officially owned by 80,000 of its 180,000 employees. However, Zhengfei maintains veto power over the majority in all organizational decisions. Uncertainty over Zhengfei's relationship with the Chinese government and lack of corporate transparency has resulted in the United States banning Huawei from bidding on United States government contracts. The ban also imposes severe restrictions on federal employees' use of Huawei's products.

The Chinese government may feel motivated to guide and support Huawei's business dealings and contracts because of traditional Chinese Communist Party (CCP) behavior. The People's Republic of China would leverage the Belt and Road Initiative to integrate and strengthen its relationship with Huawei. In his 2019 remarks on National Security and Foreign Policy Implications, Dr. Christopher Ford, then Assistant Secretary of State for International Security and Non-proliferation, stated:

Though they may have formally private ownership and operate in the national and in the international marketplace, global Chinese firms–including Huawei–are in key ways not genuinely private companies and do not make decisions entirely for economic and commercial reasons. Whether de facto or de jure, such giants can in some important respects or for some purposes act as arms of the state–or, more precisely, the Chinese Communist Party, to which the Chinese state apparatus is itself subordinate.[6]

Members of Congress and several key partners from intelligence organizations echoed Dr. Ford's observations and concerns.

U.S. Congress Investigates Huawei

Huawei's first red flag appeared in 2007. The Congressional Research Service report, *Huawei and U.S. Law*, indicated Huawei partnered with American private investment firm Bain Capital LP to acquire an ownership interest in 3Com Corporation, an American digital electronics firm. The deal raised national security concerns because 3Com provided cybersecurity systems to the U.S. military.[7] By 2008, Bain Capital decided the partnership was too risky and dropped its bid for 3Com. After failed partnering attempts with Sprint

Corporation in 2010 and 3Leaf Systems in 2011, Ken (Houkun) Hu, the technologies chairman for Huawei USA, wrote an open letter to the U.S. Government.[8] In an effort to find some way to compete in the U.S. market, Hu denied security concerns and offered a formal investigation to alleviate any reservations.

The U.S. Congress established a committee and ordered a review to determine the relevancy and degree of threat associated with allowing Huawei to participate in government contracts. The committee documented numerous concerns with Huawei's level of cooperation and veracity during the investigation. Additionally, former Huawei employees provided internal documents asserting Huawei provides special network services to an elite cyber-warfare unit within the People's Liberation Army and still others provided information on continued incidents of alleged visa violations.[9] Interviews further suggested that the alleged visa violations primarily involved employees brought to the United States as engineers, who were not serving in that capacity.

The Congressional report further states that "throughout the investigation, Huawei consistently denied having any links to the Chinese government and maintains that it is a private, employee-owned company."[10] However, current and former employees of Huawei USA confirm it is "managed almost completely by the Huawei parent company in China,"[11] which is counter to Huawei's claim that its United States operations are largely independent of the parent company. However, Huawei's leadership did concede the CCP maintains a party committee within the company but did not provide an explanation of the functions those representatives perform.

Ultimately, the congressional committee determined:

Huawei operates in what Beijing explicitly refers to as one of seven 'strategic sectors.' Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP (Chinese Communist Party) ensures that 'national champions' dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.[12]

The committee submitted its report in 2012.

Australia's Concerns About Huawei

Earlier in 2012, elements of the Australian Signals Directorate contacted United States partners indicating they had detected a sophisticated intrusion within Australia's telecommunications systems. The Australian Signals Directorate was confident the incident was initiated during a software update from Huawei, which included malicious code. Numerous former national security officials confirmed receiving briefings about the breach from Australian and United States agencies from 2012 to 2019.[13] "Digital forensics on those systems revealed only fragments of the malicious code's existence, and investigators reconstructed the attack using a variety of sensitive sources, including human informants and secretly intercepted conversations, the former officials said."[14]

Details about the breach of Australia's telecommunications system suggest the malicious code worked much like a traditional wiretap. The code reprogramed infected equipment to record all communications and route those recordings back to China. A self-erasing program activated after several days of data capture, resulting in much of the code being deleted.[15] Coincidentally, the Australian Signals Directorate's investigation determined involvement by Huawei's system maintenance engineers in espionage.[16] This information seems to support the visa violation allegations presented in the U.S. Congressional investigation.

By 2017 Australia's then Prime Minister, Malcolm Turnbull, was faced with tough decisions about 5G integration across the Australian continent. Given the events of 2012 he directed the Australian Signals Directorate to "red team" courses of action should China leverage its relationship with Huawei. The team determined, "if that government has sway over a 5G vendor in the country it wants to strike…'you can get there quicker from flash to bang with zero cost of entry.' It could be done with a simple instruction to the company operating in the target nation's 5G system."[17] The consequences of a hypothetical, yet foreseeable, attack of this sort would not just be about intercepting information. An attack could disrupt sewage pump stations, clean water supply systems, public transportation dispatching, electric vehicle operation, and interfere with networks supporting critical economic functions. Ultimately, the red team identified more than 300 risks and had significant difficulty in trying to reverse engineer the company's design to identify potentially malign code.

The United States and Australia are not alone in their concerns over the risks associated with reliance on Huawei's 5G infrastructure. In Jan-Peter Kleinhans's policy recommendations for Europe's 5G development, he stated that "the IT security of mobile networks must be addressed on four different levels–standards, implementation, configuration, operations."[18] Kleinhans also described these networks as "highly modular and complex networks that blur the line between vendor and operator,"[19] expressing the difficulties in defining and clarifying the lines of responsibility. RAND analyst Timothy Heath assessed that "as an equipment vendor, it is technically possible for Huawei to conduct espionage through the network, or even for it to disrupt communications with disastrous consequences. As more devices are connected to the internet, including autonomous vehicles and electrical grids, this threat becomes all the more real."[20] This gray zone provides China significant operating space and plausible deniability for companies like Huawei.

Industry leading security experts also took a hard look at Huawei's potential vulnerabilities. Finite State and ReFirm Labs, acquired by Microsoft in 2021, did their own analysis using new automated searches of firmware files. Terry Dunlap, Refirm Labs' co-founder, indicated that in about 30 minutes his program could obtain a "complete profile on passwords that may have been accidentally left in, cryptographic keys that may or may not be warranted [and], … insecure coding practices that could be exploited."[21] In less than 2 days' time, Finite State was able to review more than 500 Huawei enterprise networking products from business systems. On average each device had 102 vulnerabilities, at least a quarter of them severe enough to let a hacker easily gain full access.[22]

Not Everyone Wants to Limit Huawei's Access

Not everyone is on board with restricting Huawei's access and limiting the company from competing and providing their advanced solutions. The Swedish Institute of International Affairs is not convinced a ban of Huawei will reduce any threats of espionage from China. "We do not follow the mainstream argument put forward by critics of a ban that the use of Huawei technology is essential to avoid losing ground in the development and roll-out of 5G."[23] The Swedish Institute of International Affairs is especially concerned over the potential political repercussions associated with negative action against the company. This is not surprising because President Xi Jinping is wholly invested in Huawei securing its place as the leader in the global internet, going so far as to suggest to former President Trump that a ban would be harmful to bilateral relations.[24] Implications for the European Union are precarious at best. Poland and the Czech Republic are firmly in line with the United Kingdom, Australia, and the United States in what has become a 60 State coalition, while Germany, France, Italy, and Portugal are leaning toward some degree of inclusion for Huawei.

For its own part, Huawei continues to counter any negative image presented by the United States and its partners. In 2019, Huawei commissioned Oxford Economics to conduct a study of the implications and impacts of preventing a key 5G supplier from building infrastructure. The study, released in December 2019 finds, "restricting a key supplier of 5G infrastructure from helping to build a country's network would increase that country's 5G investment costs by between 8% to 29% over the next decade."[25] It further asserts that restricting competition and participation would delay 5G access to millions and would slow technological innovation and growth. It is not surprising the study favors allowing all competitors equal access to countries developing 5G capabilities and is in line with information management and narrative framing common to the CCP. The U.S. Government does not share this assessment.

U.S Restrictions Through the National Defense Authorization Act

It is doubtful these findings will sway any of the 60 countries already committed to protecting their domestic infrastructure from China's threat. Over the past 4 years the United States has continuously elevated restrictions through the National Defense Authorization Act (NDAA). The 2018 NDAA prohibits the Department of Defense (DoD) from procuring certain telecommunications equipment or services from Huawei and others as part of DoD's missions related to nuclear deterrence and homeland defense.

The 2019 NDAA included a more comprehensive set of restrictions for Huawei, which encompassed the Executive Branch. Executive agencies are no longer allowed to procure systems that contain Huawei's equipment or services, nor are they allowed to contract with companies using Huawei equipment or services.[26]

The 2020 NDAA restricts the Secretary of Commerce's ability to remove Huawei from the Entities List, requiring four conditions to change its status:

- Resolution by Huawei of the charges that were the basis for its addition to the Entity List.
- Resolution by Huawei of any other charges that it violated U.S. sanctions.
- Implementation of regulations that sufficiently restrict exporting to, and importing from, the United States items that would pose a national security threat to U.S. telecommunications systems.
- Mitigation by Commerce, to the maximum extent possible, of other threats to U.S. national security posed by Huawei.[27]

U.S. Department of Commerce Entities List

The Entity List is a tool utilized by the Department of Commerce's Bureau of Industry and Security to restrict the export, re-export, and transfer (in-country) of items subject to the Export Administration Regulations to persons (individuals, organizations, or companies) reasonably believed to be involved, or to pose a significant risk of becoming involved, in activities contrary to the national security or foreign policy interests of the United States. Additional license requirements apply to exports, re-exports, and transfers (in-country) of items subject to the Export Administration Regulations to listed entities, and the availability of most license exceptions is limited.[28]

The U.S. Senate is proposing cooperative agreements with partner nations and reporting requirements to monitor Huawei's capabilities and intentions in Senate bill S.1260, *United States Innovation and Competition Act of 2021*.[29] Additionally, Executive Order 14032, *Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China*, prohibits U.S. investments in Chinese companies that undermine the security or democratic values of the United States and its allies, effective June 3, 2021.[30]

Huawei's Technology in the United States

Despite recent prohibitions, Huawei technology remains in the U.S. infrastructure. Many rural wireless carriers use the technology in their networks, predominantly because of the low price afforded to these groups. Restricted budgets continue to create opportunities for exploitation. In 2018, 25 percent of the Rural Wireless Association members reported current deployment of equipment from Huawei, or its sister company ZTE, in their networks.[31] Huawei equipment in these rural areas posed a potential threat to several military installations, as Bloomberg Law noted in November 2019.[32]

Federal Communications Commission and Congressional concerns regarding the Huawei presence in rural carriers resurfaced upon the release of a Cable News Network (CNN) special report in July 2022. The CNN investigative piece asserts that the Federal Bureau of Investigations identified, "Chinese-made Huawei equipment atop cell towers near military bases in the rural Midwest."[33] The investigation determined the components could capture or disrupt restricted DoD communications. Of particular concern is U.S. Strategic Command, which oversees the country's nuclear weapons and could potentially be affected by the technology's vulnerabilities.[34] Additionally, the CNN report stated that "around 2014, Viaero [the largest regional provider in the area] started mounting high-definition surveillance cameras on its towers to live-stream weather and traffic, a public service it shared with local news organizations. ... But they were also inadvertently capturing the movements of US military equipment and personnel, giving Beijing—or anyone for that matter—the ability to track the pattern of activity between a series of closely guarded military facilities."[35]

Options to a Persistent Threat

The United States counterintelligence community identifies China as the world's most active and persistent perpetrators of economic espionage.[36] Former National Counterintelligence Executive, Mr. Robert Bryan, testified, Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data. China prizes comprehensive and effective cyberspace and human-related espionage; incorporated with sophisticated technology, it retains the capability to introduce malicious hardware into both Chinese manufactured components and vendor serviced systems. These results can be catastrophic to private industry and state government, leaving both inoperable, ineffective, and unaware of the threat until it is too late.

To provide a secure and competitive option to Huawei, DoD is continuing industry partnerships. In October 2020, US$600 million dollars in research funding was earmarked for 5G experimentation. This development represents the largest full scale 5G dual use testing in the world. "Projects will include piloting 5G-enabled augmented/virtual reality for mission planning and training, testing 5G-enabled Smart Warehouses, and evaluating 5G technologies to enhance distributed command and control".[37] Test sites span across all Service components including Naval Base San Diego, California; Marine Corps Logistics Base Albany, Georgia; Nellis Air Force Base, Nevada; Hill Air Force Base, Utah; and Joint Base Lewis-McChord, Washington.

Most recently, an August 2, 2022, press release indicates DoD is directing innovative efforts toward Open6G with open radio access networks (Open RAN).[38] Northeastern University's Kostas Research Institute will manage the project. Initiatives such as these ensure the United States is matching strides with pacing threats while protecting American infrastructure, financial institutions, and technology.

Endnotes

1.Douglas Black, "Huawei and China: Not Just Business as Usual," *Journal of Political Risk* 8, no. 1 (January 2019), https://www.jpolrisk.com/category/diplomacy/page/8/.

2. Huawei Investment & Holding Co, Ltd., *2021 Annual Report*, 7, https://www.huawei.com/en/annual-report/2021.

3. Ibid., 68.

4. Ibid., 68.

5. Ibid., 70.

6. Dr. Christopher Ashley Ford, "Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," (remarks, Multilateral Action On Sensitive Technologies [MAST] Conference, Loy Henderson Auditorium, Department of State, Washington DC, September 11, 2019), https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html.

7. Library of Congress, Congressional Research Service, *Huawei and U.S. Law*, Stephen P. Mulligan and Chris D. Linebaugh, CRS Report R46693 (Washington, DC: Office of Congressional Information and Publishing, February 23, 2021), https://crsreports.congress.gov/product/pdf/R/R46693.

8. Ken Hu, "Huawei Open Letter," https://www.wsj.com/public/resources/documents/Huawei20110205.pdf.

9. Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong., 2nd sess., October 8, 2012, 25, 35, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

10. Ken Hu, "Huawei Open Letter."

11.Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues*, 13.

12. John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.

13. Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," *Bloomberg*, December 16, 2021, https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack.

14. Ibid.

15. Ibid.

16. Anees, "Huawei products-Australia and the United States grasped from 2012," Quepan, n.d., https://quepan.net/post/huawei-products-australia-and-the-united-states-grasped-from-2012.

17. Peter Hartcher, "Huawei? No way! Why Australia banned the world's biggest telecoms firm," *The Sydney Morning Herald*, May 21, 2021, https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html.

18. Jan-Peter Keinhans, *Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge* (Berlin, Germany: Stiftung Neue Verantwortung, 2019), https://www.stiftung-nv.de/de/publikation/whom-trust-5g-world-policy-recommendations-europes-5g-challenge.

19. Ibid.

20. Kate O'Flaherty, "Huawei Security Scandal: Everything You Need to Know," *Forbes*, February 26, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=7d3239d773a5.

21. Sydney J. Freedberg Jr., "Hacker Heaven: Huawei's Hidden Back Doors Found," *Breaking Defense*, July 5, 2019, https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/.

22. Ibid.

23. Tim Rühlig and Maja Björk, *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe* (Stockholm, Sweden: The Swedish Institute of International Affairs, 2020), https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-paper-no.-1-2020.pdf.

24. Peter Hartcher, "Huawei? No way!"

25 Oxford Economics, *The Economic Impact of Restricting Competition in 5G Network Equipment: An Economic Impact Study*, December 2019, https://www.oxfordeconomics.com/resource/economic-impact-of-restricting-competition-in-5g-network-equipment/.

26. Library of Congress, Congressional Research Service, *Huawei and U.S. Law.*

27. *National Defense Authorization Act for Fiscal Year 2020*, Public Law 116-92, Sec. 1260I (a) (1), (2), (3), (4), https://www.govinfo.gov/content/pkg/PLAW-116publ92/html/PLAW-116publ92.html.

28. Department of Commerce, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement," *Office of Public Affairs*, July 9, 2021, https://www.commerce.gov/news/press-releases/2021/07/commerce-department-adds-34-entities-entity-list-target-enablers-chinas.

29. Senate, *United Stated Innovation and Competition Act of 2021*, S 1260, 117th Cong., 1st sess., introduced in Senate on April 20, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1260/text.

30. "Executive Order 14032 of June 3, 2021, Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China," *Code of Federal Regulations*, title 3 (2021): 30145-30149, https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples.

31. Mike Dano, "Huawei equipment currently deployed by 25% of U.S. rural wireless carriers, RWA Says," Fierce Wireless, December 11, 2018, https://www.fiercewireless.com/wireless/huawei-equipment-currently-deployed-by-25-u-s-rural-wireless-carriers-rwa-says.

32. *Bloomberg Law*, "FCC Wants to Know if Huawei Gear Is near U.S. military Bases," November 5, 2019, https://news.bloomberglaw.com/tech-and-telecom-law/fcc-wants-to-know-if-huawei-gear-is-near-u-s-military-bases.

33. Kate Bo Lillis, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications," *CNN*, Politics, July 25, 2022, https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

34. Ibid.

35. Ibid.

36. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, DC, October 2011), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

37. Department of Defense, "DOD Announces $600 Million for 5G Experimentation and Testing at Five Installations," October 8, 2020, https://www.defense.gov/News/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati/.

38. Department of Defense, "Three New Projects for DOD's Innovate Beyond 5g Program," August 2, 2022, https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/.

CW4 Charles Davis serves on the faculty of the Warrant Officer Career College. He currently instructs International Strategic Studies at all levels of Warrant Officer Education. CW4 Davis is a graduate of the U.S. Army War College Strategic Broadening Program and holds a master's degree with honors in intelligence studies from American Military University. CW4 Davis is also a recipient of the Military Intelligence Corps Knowlton Award.