



Red Diamond Training Support Issue Summer 2021

This edition of the Red Diamond provides our readers with information about the various products and services TRADOC G2 offers to support and guide you through writing scenarios and developing exercises. We strive to ensure our users are informed about the myriad resources available to them. Reading through these articles will arm you with information about how, when, and why to use DATE to meet training objectives, ranging from classroom applications to CTCs. It will explain how and why visualizations can enhance your training, and how understanding human networks enhances training and reflects reality. There is also a description of several tools and applications readily available for users to create and enhance training. Finally, we've included an article about the forthcoming ATPs on threat tactics, which are unique in their discussion of how these actors might behave if facing the United States.

For more information, or support from TRADOC G-2, please contact Angela M. Williams, angela.m.williams298.civ@mail.mil

Contents

Gaming and Visualizations	2
TRADOC's Network Engagement Team: A Brief History and Focus on Network Data and Cognitive Maneuver Training	4
TRADOC G-2 Tools Enable Individual to Collective Training and Enhance the Operational Environment	10
Models and Simulations	14
ODIN, DATE, and the Beginnings of Scenario Development	17
Training Today's Army for Tomorrow's Threats.....	27



Gaming and Visualizations: Enhancing Understanding of the OE

by [Dave Anderson](#)

The mission of the U.S. Army Training and Doctrine Command (TRADOC) G-2 Gaming and Visualizations Division (GVD) is to customize gaming technologies to produce visualizations and virtual practical exercises and applications to support leader development, training, education, and force development—thus maximizing Soldiers' perception of the virtual operational environment. GVD is essentially a one-stop shop to accomplish this mission, with core specialties in three-dimensional modeling, game programming, and terrain development, and a professional videography team to produce the visualizations. It uses Virtual Battlespace 3 (VBS3) as the main source medium for visualization training products. GVD discovered that it could produce the visualizations faster and cheaper using VBS3 compared to live-action filming.

But why produce visualizations? The first reason is to communicate complex ideas and concepts in a more efficient and accessible way than traditional methods. For example, GVD has worked with numerous senior leaders to produce these strategic-level visualizations to introduce new concepts to the force, such as multi-domain operations, cross-domain maneuver, and cyberspace and electromagnetic activities. Next is to illustrate new or complex equipment and capabilities, with the infantry brigade combat team to 2028—developed for the Maneuver Center of Excellence—being the latest example. Another reason is to create conditions for leader development and discussion using lessons-learned visualizations like Command Observation Post Keating. Visualizations also create a clear reference point, giving coherence and immutability to the message. Finally, modern Soldiers and civilians increasingly expect this interactive and visual medium instead of more traditional products.

GVD is currently working with the Center for Initial Military Training to produce visualizations based upon Soldier Training Publication (STP) 21-2-SMCT, *Soldier's Manual of Common Tasks, Warrior Skills, Level 1*. These 62 tasks are the core elements that every Soldier is required to know and are essential to the Army's ability to win on the modern battlefield. GVD has produced 16 of these visualizations, which give instructors a new and more engaging way to present these required tasks.

For virtual trainers and applications, GVD looks at the various programs of instruction to see if there are any gaps in training. If a gap is identified, the organization then determines if a gaming solution is well suited to fill that gap. For land navigation, GVD found that the Army was not confirming the students' understanding and proper execution of the basics before testing them in a live exercise. GVD determined that the Army would be able to test students' performance of the land navigation elements in a virtual/gaming environment, correcting any issues before sending them out for a live exercise. The GVD Land Navigation trainer, built on the VBS3 platform, is its most successful game-based trainer, with over 20 custom courses available. The organization has built at least one custom terrain for every Center of Excellence, several mobilization training centers (MTCs), West Point, and a few Reserve Officer Training

Corps units. As an example of the effectiveness of this training, an MTC was having an unacceptable first-time “no-go” rate on land navigation training. GVD developed a custom course for the MTC that was integrated into the program of instruction, after which the MTC’s no-go rate approached zero percent.

One of the VBS trainer’s limitations is that it requires access to a simulation center with VBS installed. To resolve this issue, GVD developed the OEGames Land Navigation trainer. This web-based trainer is publicly available (no common access card required) and runs the user through a virtual land navigation course, reinforcing all of the core elements of basic land navigation. Finally, at the request of the TRADOC Commanding General, GVD developed a tablet-based version of the OEGames Land Navigation trainer. This trainer was built for the Fort Jackson, SC initial entry training and is available to the public on both Android and Apple mobile platforms.

GVD visualizations and virtual practical exercises are not meant to replace the Soldier’s live training exercises or core classroom instruction; rather, they use blended learning to augment these forms of training. They give Soldiers a way to further familiarize themselves with a given task using a visual representation, thus removing fear of the unknown and making the live training event that much more effective.

The following are links to GVD information and select trainers:

- YouTube: <https://www.youtube.com/user/tbocsims/featured>
- Web-based trainers: <https://oegames.tradoc.army.mil/>
- Mobile apps:
 - EquipID
 - Apple: <https://apps.apple.com/us/app/equipid/id1468947196>
 - Android: https://play.google.com/store/apps/details?id=mil.army.EquipID&hl=en_US
 - Land Navigation
 - Apple: <https://apps.apple.com/us/app/oegames-land-navigation/id1498236862?ls=1>
 - Android: https://play.google.com/store/apps/details?id=com.USARMY.LandNav_Mobile



TRADOC's Network Engagement Team: A Focus on Network Data and Cognitive Maneuver Training

By [Chris Worret](#)

“Military operations are human endeavors—a contest of wills characterized by violence and continuous adaptation among all participants. Fundamentally, all war is about changing human behavior. During operations, Army forces face thinking and adaptive enemies, differing agendas of various actors, and changing perceptions of civilians in an operational area.”¹ – *ADP 5-0 The Operations Process*

Born by a tasking from a U.S. Marine Corps major general in 2007, the U.S. Army Training and Doctrine Command (TRADOC) G-2's Network Engagement Team (NET) has grown from a temporary two-person team assigned to complete a specific task into a close-knit team of seven uniquely qualified individuals.² During that time, the NET's scope has grown from developing a methodology to understand, attack, and counter improvised explosive device (IED) networks in Iraq and Afghanistan, to partnering with the U.S. Army War College (AWC) to develop a global strategic approach for the Army and the joint force to prevail in competition with adversaries such as China and Russia. One constant throughout the NET's 14-year maturation process has been its steady focus on developing ways to better understand and influence human networks—also known as relevant actors—within the human domain.

The NET's initial Attack the Network (AtN) training program benefitted greatly from creating a distinctive military application based on the scientific field of social network analysis (SNA). This adaptation was originally developed by two professors at West Point. The two (then) Army majors travelled to Afghanistan during their 2008–2009 “Christmas vacation” and proved their new training program, “Advanced Network Analysis and Training” (ANAT), by conducting a pilot course on Bagram Airbase, Afghanistan.³ They then operationalized ANAT in Afghanistan and Iraq, and those units that embraced it were able to conduct a nuanced process of military engagements with human networks.⁴ This unique engagement process, employed with great success by the 1st Cavalry Division and others, became the basis for new Army doctrine. Army Techniques Publication (ATP) 5-0.6, *Network Engagement*, was published in June 2017 following a four-year effort by the NET, in partnership with the Maneuver Center of Excellence and a broader community of interest, under the leadership of the Army's Combined Arms Center. This ATP combines elements of AtN and ANAT, and applies them to military engagement with any human network in any operational environment at any level, from tactical to strategic. Although network engagement can be applied by any military organization at any level, the NET recognized the need to better clarify its strategic application.

The opportunity to apply network engagement (defined as “the interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an OE [operational environment]”⁵) at the strategic level came from the AWC in 2018, when

the NET began a partnership with the AWC's leading expert in human cognition. After less than two years, that partnership blossomed into a new course called "Cognitive Maneuver". The second iteration of the Cognitive Maneuver course is currently underway at the AWC. Just as the NET developed the pre-doctrinal concept of AtN into a broadly applicable doctrinal concept, network engagement, the NET is now developing the concept of cognitive maneuver, in collaboration with the AWC, into what will likely be a future doctrinal approach to countering U.S. adversaries throughout the competition continuum. Cognitive maneuver is essentially a strategic application of network engagement that is aligned with the latest concepts and thinking within DoD regarding how to achieve U.S. strategic objectives—often without resorting to armed conflict—in today's global security environment.⁶ The requirement for such a capability is clearly articulated in the 2021 Interim National Security Strategy Guidance (INSSG) and the 2018 National Defense Strategy (NDS). Cognitive maneuver is clearly aligned with the intent of the INSSG. The statement that most clearly aligns with the Cognitive maneuver course is, "we will develop capabilities to better compete and deter gray zone actions." Our adversaries will not fight us on our terms. Instead they have been attempting to erode our strategic superiority in the gray zone without resorting to armed conflict. We will raise our competitive game to meet that challenge, to protect American interests, and to advance our values."⁷ The 2018 NDS describes how the Department of Defense (DoD) and Joint Force will raise their competitive game: "To succeed in the emerging security environment, our Department and the Joint Force will have to out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors."⁸ In March of 2021 the NET revised the definition of Cognitive Maneuver and the framework of the course, based in part on recommendations from last year's AWC class, to fully align with the NDS. "Cognitive maneuver is a methodology that enables the Department of Defense and the joint force to out-think, out-maneuver, out-partner, and out-innovate revisionist powers." Not surprisingly, network engagement is an essential component of cognitive maneuver. So, the NET is now engaging in concept and doctrine development at all levels within a complex network of partnerships.

After the two West Point professors who developed the ANAT program handed it off to the NET in 2012, ANAT training was formally integrated into the NET's AtN training program. The formerly separate AtN and ANAT training teams combined, and they continually refined the training while also presenting it to many units, most of which were then deploying to Iraq or Afghanistan.

At the same time, the NET was working with the Maneuver Center of Excellence to refine the concept of AtN, based heavily on written accounts of units that had successfully engaged friendly, neutral, and threat human networks while deployed. Figure 1 is taken from ATP 5-06. It depicts the expansion of the AtN concept to the broader concept of network engagement. Per ATP 5-0.6, "Network engagement utilizes the three activities of supporting, influencing, and neutralizing to achieve the commander's desired end state. Commanders and staffs use network engagement activities to support and influence friendly and neutral human networks and to influence and neutralize threat human networks."⁹

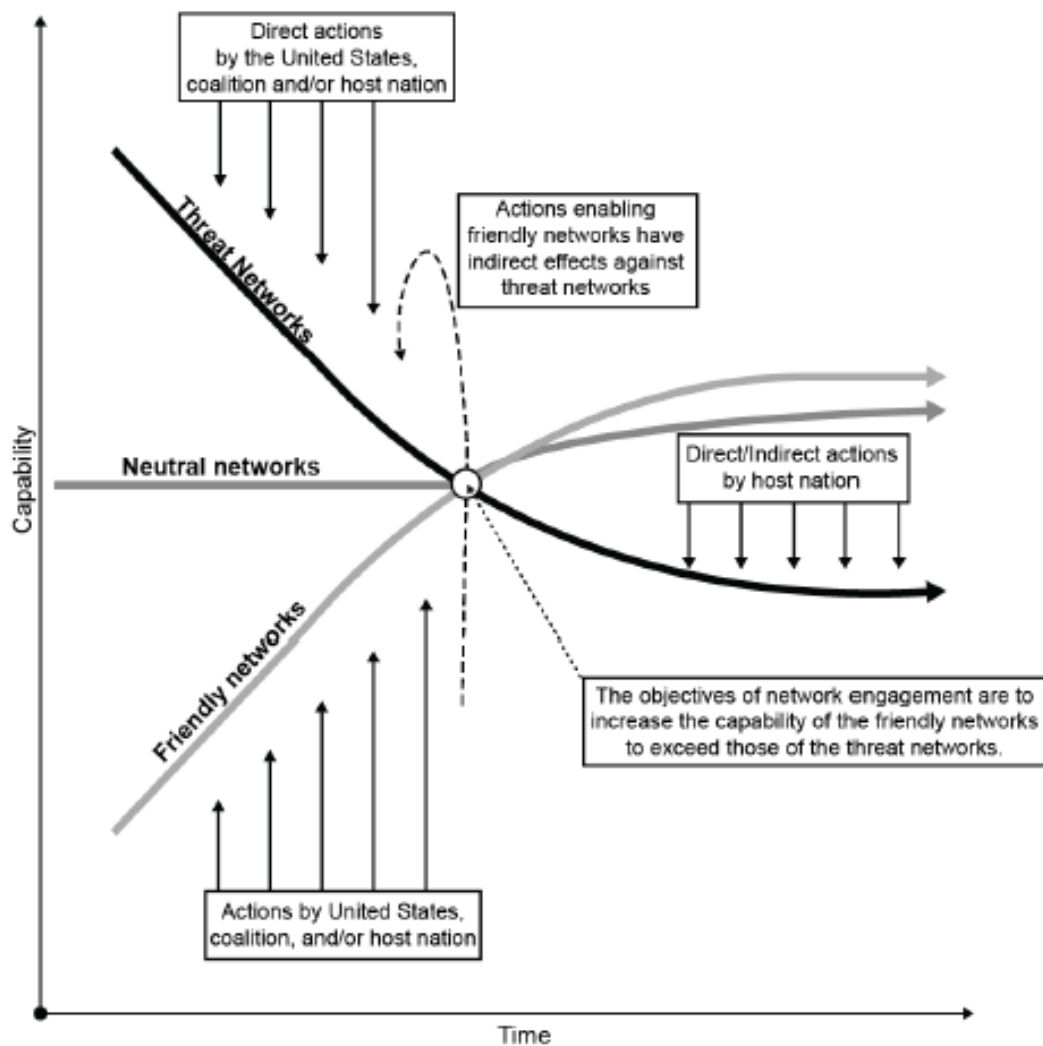


Figure 1: Network Engagement Concept¹⁰

Although ANAT training and trainers were merged with NET training and trainers, the two programs retained a degree of separate identity as two options that could be tailored based on the needs of the individual unit. ANAT training is based on the science of SNA and tends to be most effectively applied when the analyst understands applicable concepts and is open to working with mission-specific data. Performing SNA in support of specific mission objectives often leads to rapid identification of potential targets that may not have been readily apparent when using more traditional analytic methods. SNA provides understanding of how people or organizations have significance based on how they are connected to the wider network. Intelligence analysts and others who are guided only by link analysis tend to identify potential targets based on hierarchical significance and basic relationships drawn from structured data, reporting, link diagrams, or other data sources.¹¹ This type of network analysis is often largely subjective. SNA supports objective analysis because it identifies potential targets for further collection or engagement based on relational significance. Ideally, the two analytic approaches should be combined for comprehensive understanding; analysis;

course of action development; intelligence, surveillance, and reconnaissance planning; and targeting.

The NET offers pre-exercise network engagement training and on-site mentoring during exercises and events across the Army, joint, interagency, intergovernmental, and multinational communities. There are two core training programs offered by NET. The first is a standard ANAT course lasting 3-5 days, and the second is a “train-the-trainer” course lasting 7-10 days. The standard ANAT course is broken into separate blocks of instruction covering topics such as network engagement, link diagram development, networking terms and principles, structured data management, SNA methodology, practical application of SNA, and SNA software instruction (ORA, UCINET, Gephi, and R). It also includes a team-based capstone practical exercise during which students use network data to produce an informative SNA product intended to provide sound recommendations to support planning, information collection, and targeting.

Train-the-trainer instruction was designed to be a force multiplier given the NET’s relatively small size. Blocks of instruction follow the standard ANAT course but also provide an opportunity to mentor and enable students to train network engagement, ANAT, and SNA within their organization. The first week of instruction follows the same cadence as the standard ANAT course, and the second is focused on development of a standard operating procedure for network data development, application of SNA to specific missions, and network data procedure (codebook) refinement. All of these efforts enable a unit-specific standardized approach to human network data management, storage, retrieval, analysis, and visualization. This approach was primarily designed to enable more efficient and effective sharing and fusion of relational data. Through the application of network engagement and ANAT principles, teams are able to develop a better understanding of what networks are present within their respective areas of operation and the relations between people, places, processes, and activities. The NET also supports teams as they apply these principles during training, education, and leader development events.

Accurately identifying the key individuals, organizations, and other nodes within networks is challenging. By applying SNA, a team can often better identify relevant actors that potentially hold key positions, information, or serve as channels for resources—including information—throughout the network. This type of analysis can also aid a team in identifying nodes whose removal from the network would induce system-wide fragmentation. This is not intended to replace traditional link analysis but provides an objective layer to the analytical process. Through augmenting traditional link analysis with SNA, analysts are able to rapidly identify potential targets that may not be readily apparent when using more traditional methods. SNA illuminates nodes that may have significance based on how they are tied into a broader network structure, as illustrated in figure 2. Analysts guided only by link analysis are vulnerable to biases in their identification of potential targets, such as expecting hierarchical leadership where there is none and overemphasizing the importance of nodes with which they have prior familiarity. This type of analysis is largely subjective based on the analyst’s reading of the link chart or related information and intelligence reporting. SNA supports objective analysis based on a battery of quantitative measures because it identifies potential

targets for further collection or engagement based on the node's significance in the broader network.

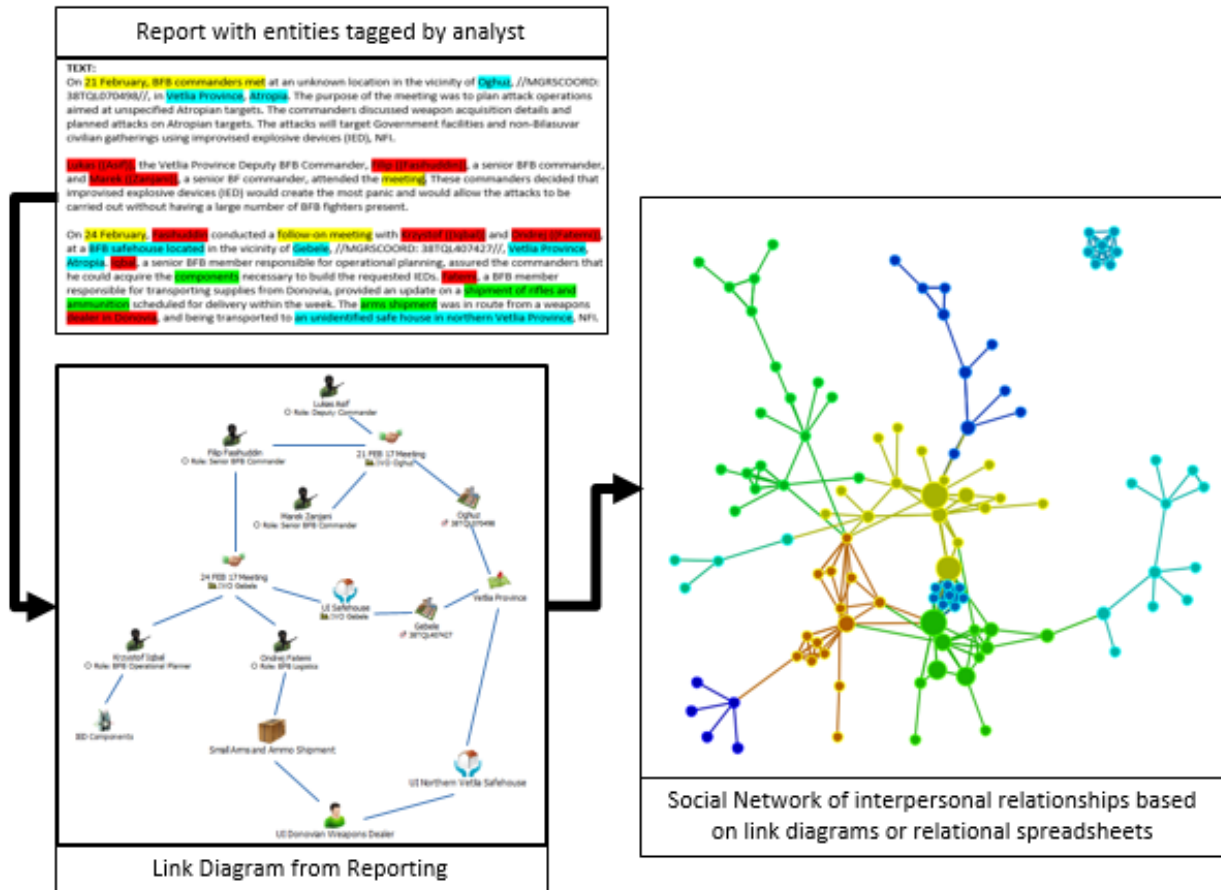


Figure 2: Process from Text Reporting to Evaluating Targets with Social Network Analysis

Despite the doctrinal expansion of AtN into the broader concept of network engagement and the integration of ANAT training within network engagement training, the NET searched in vain during 2017 for relevant examples of network analysis being applied effectively at the strategic level. The 2018 NDS and the March 2021 INSSG provide some insight as to why such an example was lacking: the United States was “emerging from a period of strategic atrophy.”¹² The NET was given an opportunity to support this emergence in 2019, when the AWC enabled the TRADOC team to develop and conduct a summer seminar titled, “Cognitive Maneuver.” Although this concept was not yet fully developed, it became clear during the July 2019 seminar that there were overlapping and common themes among the perspectives of various DoD organizations involved. The NET members involved in the seminar were able to subsequently weave together a strategic approach for cognitive maneuver. The cognitive maneuver seminar has now progressed into a course of instruction that is currently underway at the AWC, and both the concept and the strategic approach continue to be refined. What is clear, however, is that applying cognitive maneuver “as the synchronized application of physical power and informational power to influence adversaries' decision-making behaviors” will help the United States more consistently achieve strategic goals.¹³

The training offered by the NET supports the U.S. Army and joint, interagency, intergovernmental, and multinational communities by teaching and coaching students and teams from tactical through strategic levels of competition and conflict. This is consequently producing enhanced network engagement plans, operations, and strategies. Increasing an organization's ability to apply network engagement concepts enables it to more efficiently and effectively accomplish its objectives at any level. Network analysis provides important foundational skills to better understand the relevant actors within the global security environment and any of its complex components. Network engagement applied at any level increases the likelihood that the unit or organization will better understand the human domain, win the clash of wills, and achieve its objectives.

For more information, please contact Mr. Chris Worret (christopher.j.worret.ctr@mail.mil) or Mr. Matt McMillan (mathew.n.mcmillan.ctr@mail.mil).

-
- ¹ Department of the Army, *The Operations Process*, ADP 5-0 (Washington, DC: Department of the Army, 2019), 1-1.
- ² The initial tasking in 2007 that gave birth to the NET came from a stakeholder in the first of many organizations that evolved into the current Operational Environment Center (OEC). In 2007, Major General Spiese (USMC) commented at a Joint IED Defeat Organization stakeholders' meeting, "We need a methodology for Attack the Network." The AtN line of effort is widely viewed as a critical component of the higher level and more broad joint doctrinal term of network engagement.
- ³ LTC (ret.) Ian McCullough and LTC (ret.) Anthony Johnson developed TRADOC's initial ANAT course as a way to conduct social network analysis on threat networks in Afghanistan and Iraq. This course continues to be offered by the TRADOC NET.
- ⁴ The best example of this "nuanced form of human network engagement" is the 1st Cavalry Division, which clearly described the process and the results it achieved in an article in the April–June 2012 edition of *Military Intelligence*, titled "*Effective Network Targeting*". While heavily focused on the intelligence warfighting function, many of the lessons observed and captured over the past few decades have been applied across all functions, domains, staff sections, and levels of classification.
- ⁵ Joint Chiefs of Staff, *Countering Threat Networks*, JP 3-25 (Washington, DC: Joint Chiefs of Staff, 2016), x.
- ⁶ The Cognitive Maneuver seminar conducted in July 2019 assembled top DoD subject matter experts representing the Office of the Secretary of Defense, U.S. Special Operations Command, the Joint Chiefs of Staff J-2, and others who provided a range of perspectives that were subsequently woven together to form an approach for cognitive maneuver.
- ⁷ Joseph R. Biden Jr., *Interim National Security Strategy Guidance* (Washington, DC: White House, March 2021, 14).
- ⁸ James N. Mattis, *Summary of the 2018 National Defense Strategy* (Washington, DC: Government Printing Office, 2018), 5.
- ⁹ Department of the Army, *Network Engagement*, ATP 5-0.6 (Washington, DC: Department of the Army, 2017), 1-1. This expands the nested concept of AtN to the broader concept of network engagement.
- ¹⁰ Department of the Army, *Network Engagement*, ATP 5-0.6 (Washington, DC: Department of the Army, 2017), 1-3.
- ¹¹ While this course is available to U.S. Army Intelligence teams through the use of Foundry resources (GEN 305 course title) and is often applied to the intelligence warfighting function, many mission areas—from fires and effects to assessment, civil affairs, and information warfare teams—have applied these concepts with great success around the globe.
- ¹² James N. Mattis, *Summary of the 2018 National Defense Strategy* (Washington, DC: Government Printing Office, 2018), 1. While the specific phrase, "we are emerging from a period of strategic atrophy" comes from the unclassified summary of the 2018 NDS, it is well supported by the 2021 INSSG.
- ¹³ This comes from the current working definition of cognitive maneuver, which was revised by NET instructors at the AWC in March of 2021 as they prepared for the April-May 2021 Cognitive Maneuver course. Their decision was based in part on feedback from AWC staff and students who participated in the initial Cognitive Maneuver course during April–May 2020.



TRADOC G-2 Tools Enable Individual and Collective Training, Enhance the Operational Environment

by [Joel Williamson](#)

The U.S. Army Training and Doctrine Command (TRADOC) G-2 developed and maintains a set of web-based applications and tools designed to assist in the development and delivery of the operational environment (OE) to support training. All tools are government-owned and can be used at no cost. These tools help units create, develop, and deliver a more realistic OE and training environment; users can easily create exercise content from scratch or reuse previous material. This article further discusses these tools and how they can be used to enhance training. Links to all tools and applications can be found on the OE Center website at <https://oedata.army.mil>.



Figure 1: TRADOC G-2 Application Service Hub

Operational Environment Data Integration Network

The OE Data Integration Network (ODIN) digitizes and links the Training Circular (TC) 7-100 series, the three-volume Worldwide Equipment Guide (WEG), the Decisive Action Training Environments (DATEs) with associated DATE force structures, and the Virtual OPFOR Academy (VOA). It is a one-stop, authoritative resource that features an intuitive user interface as well as machine-readable outputs for the modeling and simulations community. The TC series provides composite threat-actor tactics and techniques based on best practices. The WEG supports the TC series and the equipment portrayed represents military systems, variants, and upgrades that U.S. forces may encounter. Real-world developments, capabilities, and trends are continually analyzed to ensure the WEG information remains relevant. The DATEs are constructed

using real-world conditions and composite data to provide an OE that can be modified, at echelon, to meet unit training objectives. DATE information is current, continuously updated, and feedback from the field is rapidly implemented for the best user experience. ODIN also houses the Virtual Opposing Force (OPFOR) Academy (VOA), which provides information, tools, and resources to learn, apply, and replicate OPFOR countertasks. VOA exposes users to OPFOR tasks, conditions, and standards and can be used to achieve unit training objectives within a collective training environment. ODIN does not require a common access card, and can be reached at <https://odin.tradoc.army.mil>.

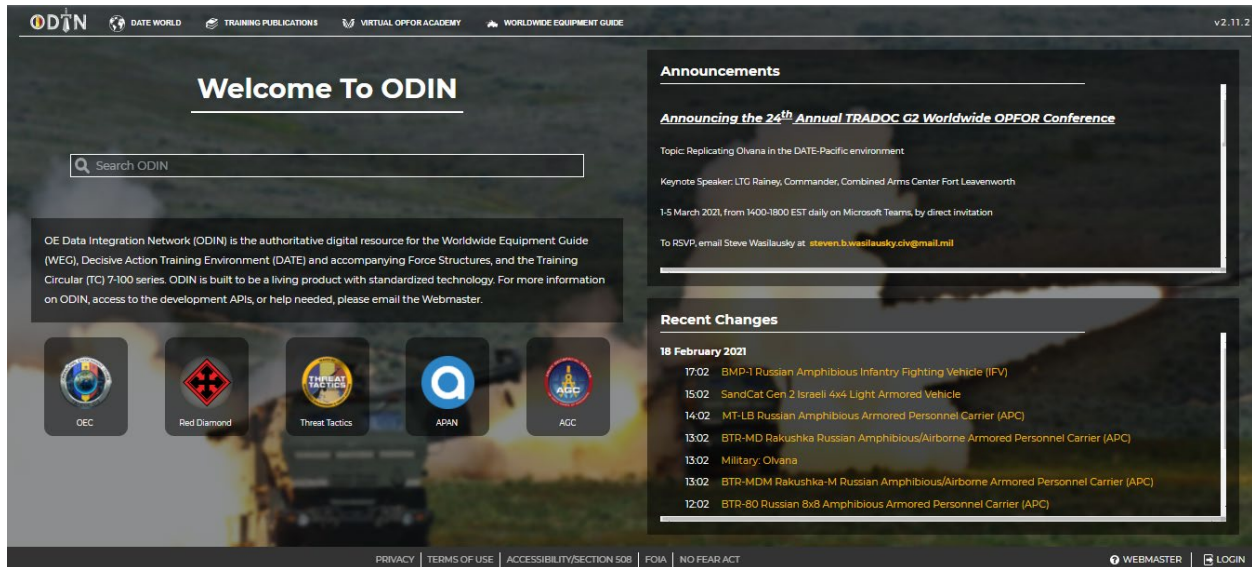


Figure 2: OE Data Integration Network (ODIN) Homepage

Information Operations Network

The Information Operations Network (ION) replicates the complexities of the information variable through an immersive environment that emulates the open internet. ION includes realistic webpages, blogs, streaming media, video, social media, and other common internet entities that units encounter in the information environment. However, unlike the internet, ION content is housed on closed intranets and accessed via the web. Content is unique to each exercise or event, allowing the training audience to search web material and social media content that matches the scenario and meets training needs.

ION facilitates individual and collective training by providing a series of connected material unique to the exercise scenario. It updates in real time and can be manipulated by the exercise control cell. There are approximately 275 different websites already available in ION. Examples created for previous exercises include:

- Country pages (Donovia, Gorgas, Ariana, Russia, Ukraine, etc.)
- News sites (Associated Press, Reuters, Drudge Report, Al Jazeera, etc.)
- CIA World Factbook
- Opensource.gov
- Popular social media sites
- Popular email sites
- Local governance sites
- Corporate pages

ION can be accessed at <https://ion.army.mil> and is accessible on NIPR, SIPR, exercise networks, or the Mission Partner Environment.

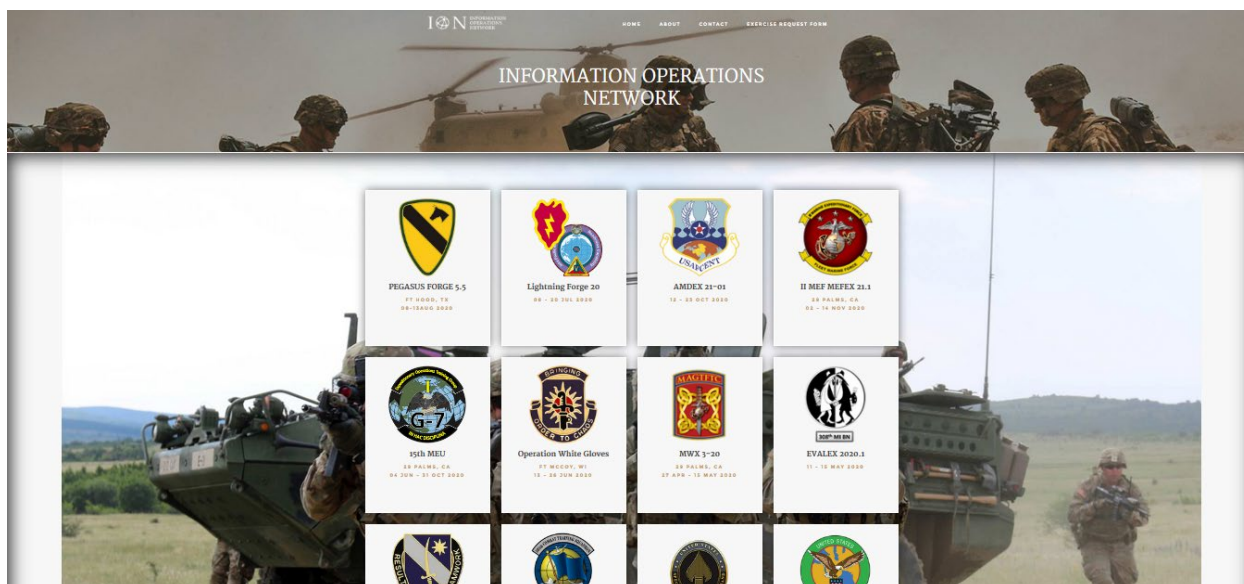


Figure 3: Information Operations Network (ION) Exercise Page

Traffic Integration Messaging System

Creating large volumes of OE baseline data to support an exercise takes a great deal of time to hand script and is cost prohibitive. This results in a low ratio of key messages to white noise that does not accurately replicate the challenge of distinguishing important information from irrelevant information while their units conduct operations. The Traffic Integration Messaging System (TIMS) allows users to ingest large volumes of real-world or notional message data and georectify, or “bend,” this data in time and space to create a more complex and rigorous training environment. Data can also be reused from a previous exercise or collected from real-world messages over a specified time period to meet training needs.

TIMS publishes message data to the Distributed Common Ground Station-Army (DCGS-A), which allows intelligence analysts to query data during training using the same command-and-control system with which they deploy. TIMS releases data according to the date and time of each message, so exercise databases are populated in real time. Exercise messages can also be added or manipulated in real time to help shape the exercise and achieve training objectives.

TIMS has many capabilities. Some of the most common features exercise planners and scenario developers implement when designing training events include:

- Quickly bending the date-time group for when messages will be published, including all dates inside the message. This allows the entire data set to be moved forward or backward in time to match actual training dates and storylines.
- Bending locational data. Users can manipulate map data by creating a single large (country-size) operations box or many smaller boxes, and move data to specific training site locations, such as villages, main supply routes, and

named areas of interest. TIMS also bends locational data—military grid reference system, latitude, and longitude—contained inside the body of a message.

- Bending key words in the data and changing names of individuals, groups, locations, and so forth.

As with ION, TIMS is available on NIPR, SIPR, exercise networks, or the Mission Partner Environment.

Exercise Support Application

The Exercise Support Application (ESA) is a repository of existing exercise support packages in varying formats and file sizes. It contains previously executed exercise content such as operations orders, graphics, concepts of the operation, and roads to war. These files can be altered and modified for reuse in a new exercise. ESA is web based, accessed with a common access card, and is a useful starting point for exercise designers and scenario developers. Exercises in ESA are organized in an easy-to-navigate file structure and can be downloaded as whole events or individual folders and documents. Once in ESA, no further authorization is needed to download materials and users can request additional support from TRADOC G-2.

To create the best training experience for warfighters or learn more about TRADOC G-2 tools and capabilities, contact the OE Center at usarmy.jble.tradoc.list.tboc-operations@mail.mil or phone 757-878-9564/9503/9696. TRADOC G-2 also hosts virtual, telephonic, and in-person tools training sessions at Fort Eustis, VA. Training includes more than just the tools listed in this article, and more information can be found on the OE Center website at <http://oe.tradoc.army.mil/OEC/>.



Models and Simulations: Enhancing OE Understanding

by [Mel Cape](#)

The U.S. Army Training and Doctrine Command (TRADOC) G-2 Models and Simulation Office (MSO) conducts delivery of models and simulations products and services to inform Soldier's understanding of an operational environment (OE) within readiness training events. It fulfills the Army Regulation 5-11 responsibility of the TRADOC Deputy Chief of Staff, G-2 to "ensure requirements of the operational environment are presented across all [modeling and simulation—M&S] communities."¹ Inherent in this mandate is the requirement to ensure that Soldiers are prepared to fight any adversary, anywhere, and in any OE. The key to ensuring successful execution of this mandate is Soldier readiness training—"enabling soldiers to shape the security environment, set the theater, and project national power."²

"We will always be ready to fight today, and we will always prepare to fight tomorrow. Our most valued assets, indeed, the nation's most valued assets, are our Soldiers and our solemn commitment must always be to never send them into harm's way untrained, poorly led, undermanned, or with less than the best equipment we can provide."
—GEN Mark A. Milley, 39th Chief of Staff of the Army

To fulfill this requirement, the MSO performs a variety of tasks that include but are not limited to the following:

- Capability development
- Concept modeling
- Requirements definition and integration
- Threat behavior use-case development and testing in support of Army M&S-enabled communities and leader development, training, and education venues:
 - Acquisition
 - Analysis
 - Experimentation
 - Intelligence
 - Test and evaluation
 - Training

Additionally, the MSO provides operational support to various combatant commands in their search for a better understanding of the OE within their areas of operation. Within these communities and venues, the MSO ensures that Army M&S methods, models, and tools are OE-compliant and capable of supporting Army warfighting events with a complex, realistic, relevant, and robust OE as required by the Army Standards for Training Proficiency.

For example, as a valued member of the One Semi-Automated Forces (OneSAF) Co-development community since 2007, the MSO is responsible for conceptualization,

integration, and testing of OE-based capabilities and behaviors within the OneSAF software baseline. This is accomplished through participation in the annual OneSAF Requirements Integration Board and Requirements Prioritization Board where recommendations, articulated through use cases, are submitted for development by the Product Management OneSAF Software Development Team. The MSO also participates in user assessment events and requirements definition workshops, and conducts OE-based capability assessments for the myriad of methods, models, and tools that comprise the Joint Land Component Constructive Training Capability.

In addition to representing forces involved in the lethal fight, the MSO also provides resources that afford operational units an opportunity to refine their staff and leadership skills for employing the military decision-making process and course of action analysis methodologies. This is done through the use of computational modeling provided by the Athena simulation—a sociocultural analysis and training capability. This simulation is focused on the nonlethal aspects of the OE and is designed to help decision makers to anticipate social, economic, and political dynamics by evaluating a potential course of action across the full range of the operational variables—political, military, economic, social, information, infrastructure, physical environment, and time.

Athena is primarily used to support the execution of directed studies being conducted by the Joint Staff and combatant commands, as well as Army experimentation, leader development, training, and education. Athena is a scalable, laptop-based course of action development and analysis capability used to anticipate the consequences of force activities upon noncombatant groups. Athena can demonstrate the nuanced and often negative sociopolitical impacts of lethal actions, as well as the positive consequences that a whole-of-government approach may provide. Athena modeling provides a way to visualize and measure the benefits derived when plans holistically incorporate diplomatic, informational, and economic initiatives with military operations.

Finally, in addition to these legacy efforts, the MSO supports future M&S capabilities, specifically integration of OE requirements into the development efforts associated with the U.S. Army Futures Command's Synthetic Training Environment (STE) Cross Functional Team (CFT). As part of the STE CFT development community, the MSO seeks to deliver OE-based requirements and functionality, and ensure the inclusion of those emerging capabilities needed to effectively portray a complex and ever-changing OE: multi-domain operations, megacity considerations, and threat tactics, among others. As such, the MSO regularly participates in working groups, teleconferences, design reviews, and technical and user assessments, as well as in the production of the capability development documents that describe the progress of the various lines of effort associated with the STE effort. For both legacy and future efforts, representation of the OE in M&S is framed around the aforementioned operational variables as defined and discussed in U.S. Army Doctrine Publication (ADP) 3-0 and ADP 5-0, and as described in the Decisive Action Training Environment (DATE) World.

For more information, or support from TRADOC G-2 MSO, please contact Mr. Mel Cape, melvin.r.cape.civ@mail.mil.

¹ Department of the Army, *Management of Army Models and Simulations*, AR 5-11 (Washington, DC: Department of the Army, 2014), 2.

² Army Public Affairs Office, "Readiness," *STAND-TO, the Official Focus of the U.S. Army*, https://www.army.mil/standto/archive_2017-10-04/.



ODIN, DATE, and the Beginnings of Scenario Development

By [Vincent P. Matteo](#)

Introduction

One of the most famous failures in training and preparation of a world-class military force was when the Imperial Japanese Navy conducted a campaign-level wargame in May 1942 to validate the plan to destroy the U.S. Pacific Fleet at Pearl Harbor, Hawaii. The plan's primary failure in the wargame was that it required U.S. forces to react exactly as the Japanese military predicted. This premise created a false sense of security for the Japanese military, which relied on its poor knowledge of the United States. When the United States did not react to the Japanese attack as expected, Japan showed an inability to react to a changing environment throughout the rest of the Pacific War. To prevent a similar training failure against future unknown enemies, the U.S. Army uses complex realistic scenarios based on the [DATE World](#).

The DATE World provides the U.S. Army training community with a detailed description of the conditions across four regions of the globe: Africa, Caucasus, Europe, and Pacific. It presents trainers with a tool to assist in the construction of scenarios for specific training events, but does not provide the scenario. The DATE World offers discussions of OE conditions through the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) variables. The DATE World is relevant for all U.S. Army units (Active Army, Army National Guard, and Army Reserve) that participate in Army or joint training exercises.¹

DATE World provides a common training OE, accessible to U.S. Army, Joint, and International partners, created from open-source information and the U.S. Army Training Circular (TC) 7-100 series of documents regarding opposing forces (OPFOR).² DATE is produced and maintained under the oversight and approval of TRADOC G-2.

As the Army's training OE charged with creating realistic and complex challenges, *DATE World* provides the U.S. Army with the ability to train for any contingency from mission rehearsal exercises to maneuver-based warfighter exercises.³ The OE in *DATE World* provides a background for conducting simulated large-scale combat operations to practice essential tasks based on approved mission-essential task lists. This article will demonstrate the versatility of *DATE World*, the functionality of the [OE Data Integration Network](#) (ODIN), and the training value of the *DATE World* OE using DATE Pacific as an example.

The Operational Environment and Data Integration Network

ODIN is the authoritative digital resource for the Worldwide Equipment Guide (WEG), training publications, *DATE World* and force structure information, and the Virtual OPFOR Academy (VOA).⁴ The main components of ODIN consist of these sections—

- **WEG.** The WEG supports the TC 7-100 series and all OPFOR portrayals in training simulations (constructive, virtual, live, and gaming). The equipment portrayed in the WEG represents military systems, variants, and upgrades that U.S. forces may encounter now and for the foreseeable future.
- **Training Publications.** U.S. Army Training Circulars (TCs), Field Manuals (FMs), and Army Techniques Publications (ATPs) that describe opposing force operations, tactics, exercise design, and force structures reside here to assist a scenario developer in portraying a modern OPFOR.
- **DATE World.** *DATE World* provides an OE created with real-world conditions presented in a PMESII-PT construct. It comprises 20 notional countries that populate four interconnected regions—DATE Africa, DATE Caucasus, DATE Europe, and DATE Pacific. Each country in *DATE World* is a composite of the conditions from multiple real-world countries (there are no one-to-one replications).
- **Force Structure.** This part of ODIN is a searchable visual and tabular depiction of regional military hierarchy, unit equipment, and personnel. It can be used to create orders of battle for use in any exercise, meaning it is tailorable to meet the requirements of any exercise.
- **VOA.** The VOA provides users the information, tools, and resources to learn, apply, and replicate OPFOR countertasks to achieve unit training objectives within a collective training environment through videos and clear explanations of OPFOR actions.

DATE Pacific Operational Environment and Scenario Primers

In DATE Pacific, the five notional countries of Belesia, Gabal, Olvana, North Torbia, and South Torbia coexist in a state of steady competition. They are located in the vicinity of the East China Sea, South China Sea, and the Philippine Sea.⁵ The stability of the region is tenuous and may be upset through politically or economically charged events, or the accumulation of drivers of instability that may precipitate a conflict within the region. The nations within DATE Pacific are also interconnected with the states in other *DATE World* regions and can exert influence and trigger events in those regions. Conflict within the DATE Pacific region may lead to the intervention of external nations which may be honoring treaty agreements; commitments based on membership in international or intergovernmental organizations, such as the United Nations or Association of Southeast Asian Nations; or acting in their own national interest. Scenario construction begins with the development of a road to war (RTW)—a series of critical events leading to a volatile environment—that shapes the scope and focus of a

training event. The RTW and scenarios for any DATE OE will vary depending on the focused echelon of training and the training objectives of the DATE user.

DATE Pacific

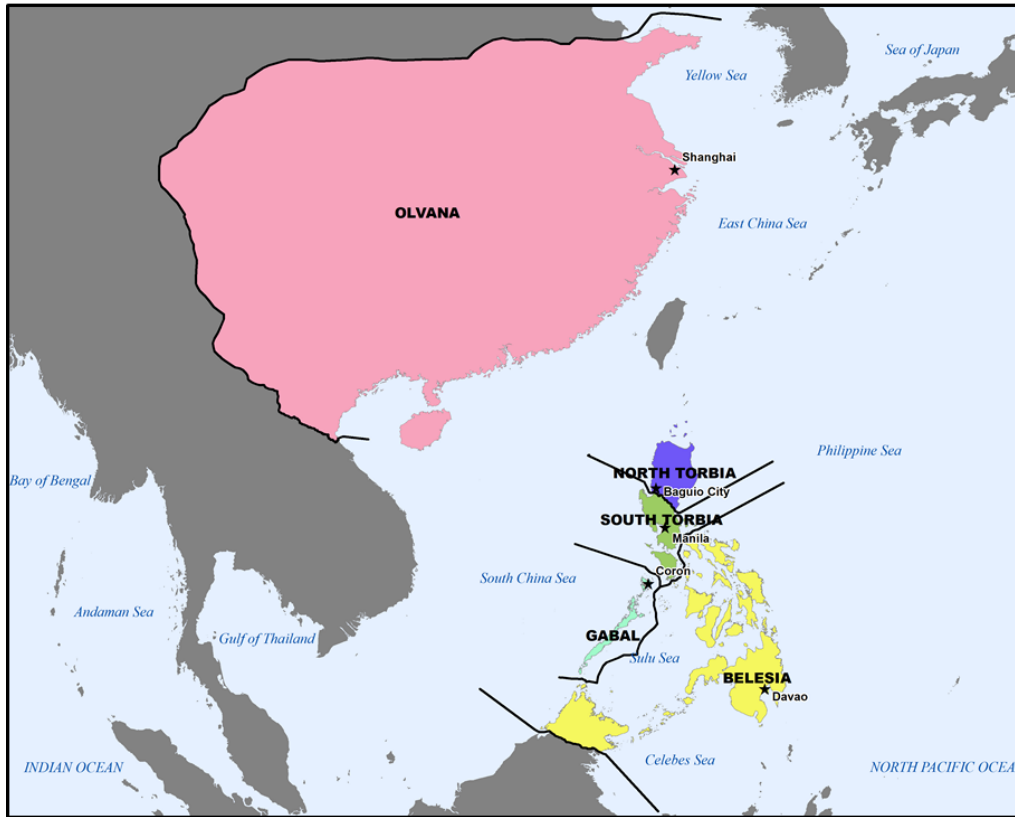


Figure 1: The DATE Pacific Region

Using the DATE Pacific Environment

With the inclusion of nonstandard scenario components and vignettes integrated into an exercise, the DATE Pacific OE is uniquely positioned to facilitate training multi-domain operations with echeloned formations that conduct intelligence, maneuver, and strike activities across all five domains (air, land, maritime, space, and cyberspace) as well as the information environment and the electromagnetic spectrum.⁶ The DATE Pacific topography is well suited for enabling distributed ground operations, as well as naval, amphibious, and littoral operations. Additionally, the DATE force structure tool provides the flexibility to tailor threat formations and capabilities to satisfy training unit requirements.

In the DATE Pacific OE, any of the five countries can be used as a friendly, enemy, or neutral actor. The most likely antagonists in the region are North Torbia and OLVANA, based on their national strategic goals, political policies, and regional aspirations. These two countries have been developed with the military capabilities, economic conditions,

and willingness to conduct information warfare (INFOWAR) that most closely align with potential adversaries in the real-world Pacific region.

North Torbia's self-imposed isolationism and its military first policies, paired with economic sanctions levied by the international community, leads to it having a particularly sensitive and reactive geopolitical posture. Olvana is the region's most influential actor, with hegemonic aspirations, a steadily growing economy, and modern military capability all combining to position it as a major regional and global power.

Next, this article will explore specific hooks in the DATE Pacific content that scenario developers can use to build a scenario with Olvana as the enemy. Scenario designers use a simple RTW formula: **Desire + Capability + Instability = Conflict/RTW**. The following brief descriptions outline how a complex challenge can be designed.⁷ Note that this is just one example of many possibilities.

DESIRE: Olvana's Approach to Competition

Political. Olvana intends to exert control over what it perceives as its sphere of influence, and impose its will in other areas of the world to further its economic and political goals. While its national borders have been set for over half a century, Olvana contends that its dominion extends into territory claimed by other regional actors. It supports North Torbia as a proxy to offset other actors within the region, and uses economic and military intimidation to influence other regional actors. Olvana's political relationship with Belesia and Gabal is complex and, at times, tense, in part because of territorial disputes and Olvana's competitive advantage in regional markets.

Military. Driven by national interest, Olvana maintains the largest military in the DATE Pacific region. The Olvana People's Army (OPA) is composed of a land force, a naval force (Olvana People's Navy, or OPN), and an air force (Olvana People's Air Force, or OPAF). Olvana maintains and strengthens its hegemony by actively deploying advisors to various countries and by regional sales of military weapons to its allies.

Information and Information Warfare. Olvana’s INFOWAR capability is highly developed and leads the world in a number of critical areas. Olvana utilizes the full range of INFOWAR operations to present a credible peer-level threat to the United States and its regional partners. Olvana’s INFOWAR is directed toward information detection sources, information channels, and information-processing and decision-making systems. Olvana aims to gain information superiority against adversaries and disrupt their information control capabilities, while maintaining and protecting its own information systems and capabilities. To achieve these aims, Olvana actively looks to establish information dominance during competition, enabling it to shape the information environment should a crisis or conflict emerge.

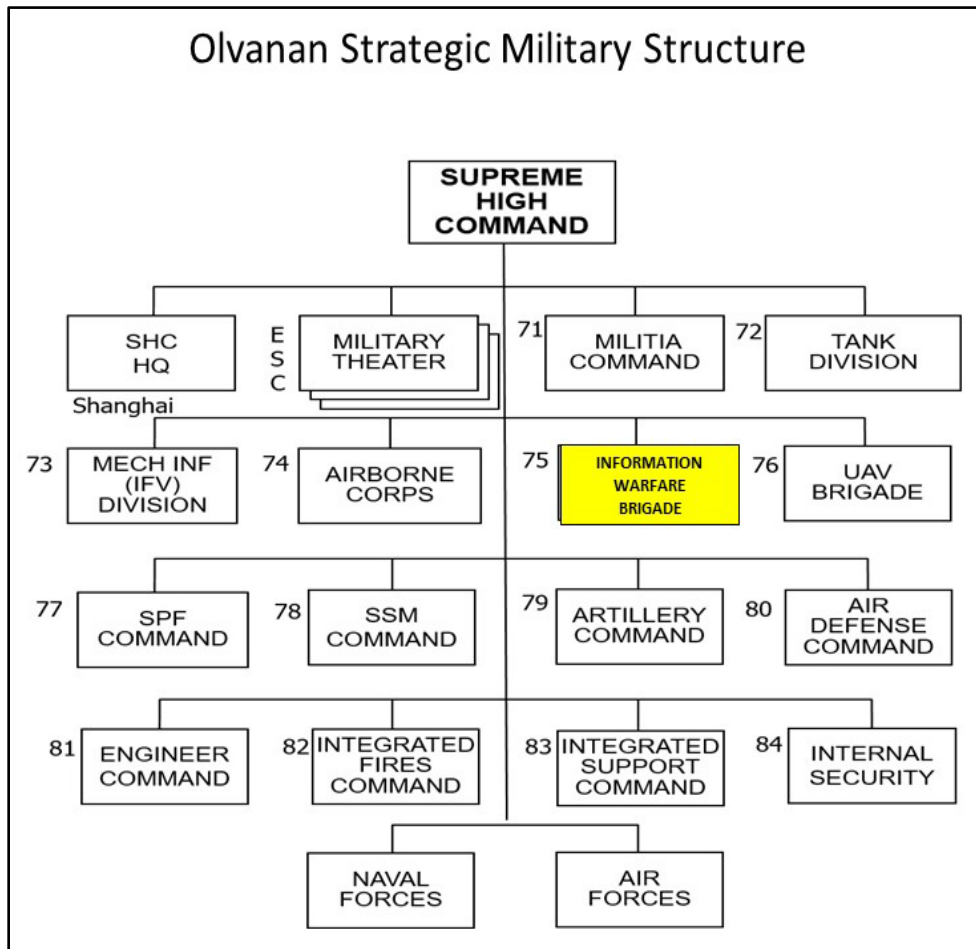


Figure 2: The OPA 75 INFOWAR Brigade within its Chain of Command

CAPABILITY: Information Warfare and Space

In its drive for regional hegemony, Olvana is in a state of constant competition with both regional and global actors, exploiting regional conditions to the extent possible while remaining below the threshold of armed conflict. Olvana achieves this through the integration of diplomatic and economic actions, unconventional warfare, INFOWAR

(social media, false narratives, and cyber attacks), the actual or threatened employment of conventional forces, and covert support to likeminded geopolitical proxy entities.⁸

Olvana's INFOWAR capability is highly developed. To achieve information dominance, Olvana adheres to the following fundamental principles when conducting INFOWAR:⁹

- **Be offense-oriented.** Seek information dominance through the disruption of adversarial information systems while preserving friendly systems' capabilities.
- **Conduct Early and Aggressively.** Maximize INFOWAR effects through the element of surprise.
- **Mass and Synchronize across All Domains and Time.** Blur the line between peacetime and wartime.

Olvana's Information Warfare Capabilities

Electronic Warfare. Olvana has the most advanced and robust electronic warfare (EW) capability across all echelons and services in the Western Pacific. Olvana's ability to synchronize EW effects maximizes convergence across the air, land, maritime, and cyberspace domains.¹⁰

Computer Attack. Olvana's cyberspace warfare capability is among the world's best. It integrates offensive and defensive cyberspace operations to support larger objectives. Olvana's offensive cyberspace capabilities include distributed denial of services and hacking, and its defensive capabilities consist of surveillance and counter-intrusion. Olvana can conduct computer attacks against domestic or international targets. Successful operations are based on deniability and outcome. Additionally, it is possible that Olvana is also training personnel from North Torbia in cyberspace warfare operations.¹¹

Information Attack. Olvana's information attack capability ranks among the best in the world. Olvana is expert at integrating information attack with other INFOWAR elements.¹²

Deception. Olvana's deception operations are world class. At the strategic level, its deception operations consist of false actions conducted by diplomatic officials, fake military targets, and propaganda. At the tactical and operational levels, Olvana can employ high-fidelity decoys that, when deployed, deceive or confuse adversary collection assets.¹³

Physical Destruction. Olvana recognizes the importance of physically destroying enemy INFOWAR capabilities. Olvanan doctrine stresses the eventual destruction of enemy INFOWAR assets after their neutralization. Among these assets is a growing antisatellite capability. This effort includes a robust sensor-to-shooter kill chain using a variety of ground-based radar and visual sensors to cue ground-launched missiles. It is

likely that antisatellite efforts would attempt to neutralize adversary space-based surveillance and communications efforts early in any potential conflict.¹⁴

Protection and Security Measures. Olvana's protection and security measures continue to evolve. Sustained investment in training for all personnel that use information systems is intended to ensure that personnel adhere to published directives.¹⁵

Perception Management. Olvana's perception management is a robust and integral part of its INFOWAR program. The objective is to portray the government as a powerful and peace-loving member of the international community. Olvana uses different initiatives in the diplomatic, economic, and information realms to project itself as a non-threatening regional power. While publicly portraying a positive image to the international community, other Olvanan elements covertly expand Olvanan influence abroad, especially within emerging and smaller nations.¹⁶

Olvana's Use of Space

Regional Satellite Telecommunications. Olvana possesses a wide range of satellite capabilities. Most are suited for dual use by the OPA, OPN, OPAF, and civilian users. Olvana operates seven commercial telecommunications satellites and four military communications satellites utilizing Ku- and C-band transponders in a geostationary orbit. If necessary, the commercial satellites may be used to support military operations.¹⁷

Regional Navigation Satellites. Olvana operates 16 navigation satellite systems using E-band transponders. The combined systems create a network of navigation services and provide coverage of the Asia-Pacific region. The services are free to civilians and licensed to the Olvanan government and military.¹⁸

Regional Drivers of INSTABILITY

Drivers of instability enhance the OE without providing prescriptive elements. The drivers exist to show areas of tension and historical use of capabilities that could be introduced into the training event without disrupting the accomplishment of mission-essential tasks. The drivers could be used as a capability to plan against or to mitigate undesired effects thereof.¹⁹ There are several primary regional drivers of instability associated with Olvana.

International Order. Olvana's actions indicate its strategic intent is to change the status quo in the South China Sea. Olvana's position seems to be one of entitlement, citing its territorial claims and economic status as a reason to have a much greater say in how the international order should operate in the South China Sea.

Olvana's Line of Maritime Sovereignty. Olvana's claims of maritime territory extend approximately 500 km from its shores into the South China Sea. These unilateral claims

are disputed by other regional actors, but appear to be the basis for Olvana to claim large swaths of territory for security and economic reasons. Olvana's claims are based on historical legacy and are generally not accepted by others within the regional and global communities. Olvana exercises its authority in disputed maritime territories by taking actions to ensure its own freedom of navigation throughout the South China Sea. However, Olvana does not extend such freedom to its regional competitors, creating the potential for military escalation as regional actors' warships operate in close proximity to each other.

Artificial Islands and Territorial Status. Olvana has sought to bolster its maritime claims by converting small outcroppings of sand and rock in the South China Sea's international waters into habitable installations, thus extending its land-based territorial claims. This includes building military infrastructure on previously uninhabited islands, including runways and air defense systems. These military outposts, often built in disputed territories, are ostensibly changing the facts on the ground regarding territorial claims.

Creating a Road to War

Using training objectives and command-directed tasks, an RTW is developed to highlight the logical progression to conflict, providing depth to scenarios. It also identifies OPFOR attributes and capabilities for scenario designers to build a peer or near-peer OPFOR. The following is an example of a potential RTW that a scenario developer could construct to highlight OPFOR INFOWAR capabilities for a training unit to defeat. This example RTW is for a fictitious exercise scheduled for the fall of 2021:

- **February 2020.** Olvana sells North Torbia modernized intelligence, surveillance, reconnaissance and EW equipment.
- **June 2020.** Olvana and North Torbia conduct a combined amphibious training exercise on the shores of North Torbia.
- **August 2020.** Olvana increases patrolling in the South China Sea, exercising control over waterways and commercial trade.
- **August 2020.** The Olvanan fleet flies an unmanned aircraft within 1 km of a South Torbian missile frigate in the South China Sea.
- **September 2020.** Olvana conducts an EW exercise in the South China Sea during a South Torbian naval training event, in which Olvana uses electronic jamming aircraft, unmanned aircraft, and EW systems capable of suppressing command and control communications.
- **October 2020.** Olvana incites a protest in South Torbia against the presence of a U.S. Navy surface warfare group in international waters outside of a South Torbian port.
- **February 2021.** Olvanan-trained North Torbians temporarily disrupt port operations in South Torbia through a cyberspace denial of service attack, halting the flow of commercial goods for 24 hours.
- **April 2021.** South Torbia catches Olvana inciting a protest to disrupt South Torbian Army land maneuvers.

- **May 2021.** Belesia shoots down a North Torbian unmanned aircraft over one of its naval bases.
- **July 2021.** Olvana disrupts Global Positioning System (GPS) and navigational aids to lure a South Torbian frigate into disputed waters.

Next Steps

At the theater level, DATE Pacific has provided a comprehensive OE, easily accessed on the ODIN platform. It is the responsibility of scenario designers to use the foundational conditions described on ODIN to design a scenario and add detail or make adjustments to the OE where needed to achieve training objectives. Using the force structures provided on ODIN, they develop an order of battle for OPFOR and a plan for the OPFOR to execute. The designers also develop blue theater or land component commander-level products to provide to a higher headquarters.

The DATE OE provides the foundational/encyclopedic information needed to inform planning and the context for the required assumptions to complete the military decision-making and order production process. Exercise planners and scenario writers may also use DATE to develop area-specific, cross-domain challenges for a training unit to negotiate. Carrying forward the concept of Olvanan INFOWAR, an information operations expert may develop a *DATE World*-informed training vignette to counter Olvanan perception management operations and integrate friendly military information support to operations. A public affairs expert could challenge the training unit's public affairs section to counter Olvanan perception management and develop command messaging.

The potential scenarios that can be developed using the authoritative content on ODIN are endless. TRADOC G2 analysts are available to assist if needed.

¹ US Army Training and Doctrine Command, "Date World," *ODIN*, accessed May 14, 2020
<https://odin.tradoc.army.mil/DATEWORLD>.

² Department of the Army, *TRADOC Standard Scenarios for Capabilities Development*, TR 71-4 (Rescinded) (Washington, DC: Department of the Army, 2014).

³ Department of the Army, *Operations*, ADP 3-0 (Washington, DC: Department of the Army, 2019), 3-1.

⁴ US Army Training and Doctrine Command, "WEG," *ODIN*, accessed May 14, 2020
<https://odin.tradoc.army.mil/WEG/>.

⁵ US Army Training and Doctrine Command, "Pacific," *ODIN*, accessed May 14, 2020
<https://odin.tradoc.army.mil/DATE/Pacific/>.

⁶ Department of the Army, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Washington, DC: Department of the Army, 2018), x.

⁷ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020
<https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.

⁸ Department of the Army, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Washington, DC: Department of the Army, 2018), iii-vi.

⁹ Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), <https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/>.

¹⁰ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020
<https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.

-
- ¹¹ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹² US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹³ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁴ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁵ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁶ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁷ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁸ US Army Training and Doctrine Command, "Olvana," *ODIN*, accessed May 14, 2020 <https://odin.tradoc.army.mil/DATE/Pacific/Olvana>.
- ¹⁹ Michael A. Marra, *Troubled Waters – 10 Flashpoints in the South China Sea: Friction Points that May Lead to War* (Carlisle, PA: U.S. Army War College, 2018), 1-29.

References

- Costello, John and Joe McReynolds. *China's Strategic Support Force: A Force for a New Era*, edited by Phillip C. Saunders. *Center for the Study of Chinese Military Affairs Institute for National Strategic Studies China Strategic Perspectives*, No. 13. Washington, DC: National Defense University Press, 2018.
- Defense Intelligence Agency. *China Military Power Modernizing a Force to Fight and Win*. Washington, DC: Defense Intelligence Agency, 2019. www.dia.mil/Military-Power-Publications.
- Department of the Army. *The Army Universal Task List*, ADRP 1-03. Washington, DC: Department of the Army, 2015.
- Department of the Army. *Irregular Opposing Forces*, TC 7-100.3. Washington, DC: Department of the Army, 2014.
- Department of the Army. *Opposing Force Tactics*, TC 7-100.2. Washington, DC: Department of the Army, 2011.
- Department of the Army. *TRADOC Standard Scenarios for Capabilities Development*, TR 71-4 (Rescinded). Washington, DC: Department of the Army, 2014.
- Department of the Army. *The U.S. Army Functional Concept for Intelligence 2020 – 2040*, TRADOC Pamphlet 525-1. Washington, DC: Department of the Army, 2017.
- Department of the Army. *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1. Washington, DC: Department of the Army, 2018.
- Department of the Army. *Exercise Design*, TC 7-101. Washington, DC: Department of the Army, 2010.
- Marra, Michael A. "Troubled Waters – 10 Flashpoints in the South China Sea: Friction Points that May Lead to War." Carlisle, PA: U.S. Army War College, 2018.
- Saunders, Phillip C., Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow, eds. *Chairman Xi Remakes the PLA, Assessing Chinese Military Reforms*. Washington, DC: National Defense National Defense University Press, 2019.
- Thomas, Timothy L. "Nation-State Cyber Strategies: Examples from China and Russia." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, D.C.: National Defense University Press, 2009. <https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/>.



Training Today's Army for Tomorrow's Threats

By [Jennifer Dunn](#)

The U.S. Army has spent the past four years grappling with its role in confronting adversaries in joint multi-domain operations (MDO). In the future the U.S. military will be confronted with a battlespace where it will be contested by adversaries across all domains, no longer assured freedom of action in the air, space, maritime, and cyber domains. The Training and Doctrine Command (TRADOC) is helping the Army prepare for this environment through its training, education, and development of both today's and tomorrow's force.



The TRADOC G-2, as the Army's proponent for developing and approving the operational environment (OE) for training and opposing force (OPFOR) doctrine, is chartered with continuous analysis of peer, near-peer, and other potential threats. This analysis ensures Army training, now and into the future, is relevant and representative of the kinds of actions our adversaries will take to challenge us in MDO. The fruits of TRADOC G-2's continuous analysis are two series of doctrinal publications. The first, Training Circular (TC) 7-100 series, includes manuals designed to provide the U.S. Army training community a challenging, realistic adversary for training events. The second, Army Techniques Publication (ATP) 7-100 series, includes four manuals designed to provide the Army with official unclassified assessments of real-world adversaries' tactics, applicable for both training environments and real-world threat analysis.



TRAINING & DOCTRINE COMMAND, G-2

OPPOSING FORCES SOURCE COMPARISON

WHICH SOURCE SHOULD INFORM OPFOR TACTICS FOR AN EXERCISE?

<p>TRAINING CIRCULAR (TC)</p>  <p>The TC series presents the Army with an assessment on how a <u>composite model threat actor</u> would execute tactics and techniques if the US were the enemy.</p>		<p>ARMY TECHNIQUES PUBLICATION (ATP)</p>  <p>The ATP series presents the Army with an assessment of how <u>specific threat actors</u> would execute tactics and techniques if the US were the enemy.</p>
<p>Derived from merging practices from threats around the globe, creating a composite adversary</p>	<p>SOURCE WHERE THE INFORMATION COMES FROM</p>	<p>Derived from unclassified open-source Intelligence on specific actors, replicating an explicit adversary</p>
<p>Use when directed to be representative of best practices of any combination of threat actors or when the use of a specific threat is not needed</p>	<p>UTILITY WHEN EACH SHOULD BE USED</p>	<p>Use when directed to add techniques and procedures from a specific threat actor and requiring the incorporation of the whole training package for effect</p>
<p>Composite model that represents best practices of real-world threats to create the toughest conditions</p>	<p>DESIGN THE DIFFERENCE BETWEEN THE MODELS</p>	<p>Distinct model that represents best practices of specific actors to create tailored and particular conditions</p>
<p>Designed to challenge task proficiency, requiring increased rigor and agility to succeed against an <i>optimized</i> adversary</p>	<p>TRAINING SELECTION INFORMED BY TRAINING TASKS</p>	<p>Designed to challenge adversary focused readiness, requiring threat familiarity and precision to succeed against the actions of an identified adversary</p>
<p>Best suited for decisive action exercises in order to yield maximum task proficiency</p>	<p>IMPLEMENTATION USING THE RIGHT TOOL FOR THE JOB</p>	<p>Best suited for regionally focused or mission-readiness exercises in order to develop specific capabilities</p>

Additional resources:
 - OE Data Integration Network, <https://odin.tradoc.army.mil/>
 - AR 350-2, Operational Environment and Opposing Force Program
 - TC 7-101 Exercise Design

Ms. Penny Mellies
 penny.j.mellies.civ@mail.mil
 OE Integration Directorate
 TRADOC G-2

Figure 3: OPFOR Source Comparison

TC 7-100 Series: Threat Best Practices for OPFOR Doctrine

The TC 7-100 series comprises six publications, produced to inform U.S. Army training exercises by facilitating exercise design and Army learning (TCs 7-101 and 7-102), and providing instructions on how the Army OPFOR should operate in a training environment where the 'enemy' is the U.S. Army (TCs 7-100, 7-100.2, 7-100.3 and 7-100.4). The latter books are the Army's official doctrinal support material for threat representation in training events. These manuals, in particular TC 7-100.2 *Opposing Force Tactics* and TC 7-100.3 *Irregular Opposing Forces*, herein referred to as OPFOR Doctrine, provide Army OPFOR practitioners with details on how a composite model threat actor would execute tactics and techniques if the United States were the enemy.

OPFOR Doctrine, while not directly labeled or tied to any specific threat actor, is informed by threat analysis. These books were created through an intensive review of the tactics of state and non-state actors from around the globe for the sole purpose of identifying the *best practices* of those actors' tactics. It is important to understand this concept: The OPFOR Doctrine composite model is *not* a threat model made up by intelligence specialists in the TRADOC G2, but rather a model that is representative of the world's best tactical practices; an exemplar of the most dangerous adversary the United States could face in a tactical fight.

TRADOC G-2 created this composite model for two reasons: (1) To capture the types of actions executed by actors around the world that represent best tactical practices and (2) to provide the U.S. Army an opposing force capable of challenging every task a U.S. Army Brigade (BDE) is expected to conduct. Finding one single actor in the real-world that has the equipment and organization and executes tactics in a way that can adequately challenge the task proficiency of a BDE has historically not been possible. For this reason, training events that are focused on task proficiency should reference the OPFOR Doctrine manuals because the composite model, as an *optimized adversary*, best yields maximum task proficiency.

ATP 7-100 Series: Threat Tactics Doctrine

While the Army needs an OPFOR doctrine that is representative of the most challenging adversary it could expect to encounter in order to yield an exceptionally proficient force, there is a need to also have unclassified assessments of how specific threat actors would execute tactics and techniques. These assessments would provide the Army with an understanding of the nuanced differences between actor application of tactics and techniques, in particular the application of those tactics and techniques in a conflict with the U.S. Army.

TRADOC G-2 is currently undertaking an initiative to produce Threat Tactics Doctrine in order to deliver this information to the Army. This doctrine, found in the ATP 7-100 Series, will provide the Army with official unclassified assessments of projected tactics from four countries. The publications that make up this series are ATP 7-100.1 Russian

Tactics, ATP 7-100.2 North Korean Tactics, ATP 7-100.3 Chinese Tactics, and ATP 7-100.4 Iranian Tactics.

These four tactical assessments all contain roughly the same kind of information: introductions to the actors' national strategies, descriptions of how they perceive their place on the international (and/or regional) stage, overviews of their entire military force, details on their ground forces' organizations, and in-depth reviews of the tactical actions their ground forces are likely to employ in conflict with the United States. While some of the material can be found in other U.S. government publications, these manuals are unique in the level of detail dedicated to exploring *how* these actors would likely approach specific types of tactical actions if confronted with U.S. Army formations enabled by joint MDO capabilities as an enemy.

Due to the actor-specific focus of these ATPs, they are not as suited to be broadly used in Decisive Action training events that need to challenge task proficiency as is the TC series of OPFOR Doctrine. Rather, these manuals serve as source material of specific actor tactics and techniques that can be used to challenge U.S. Army adversary-focused readiness. They are best suited for use in mission rehearsal exercises or other training events where success of U.S. forces is dependent upon familiarity with a specific threat. The ATP series of Threat Doctrine is designed to provide that familiarity with a specific threat's tactics and techniques, the sum of which may not challenge all U.S. tasks.

The ATP series also serves another function for the U.S. Army. As the Army's official unclassified doctrinal source of the tactics of countries like North Korea, China, Russia, and Iran, this material serves as a foundational baseline assessment for each actor. These assessments are based on the most up-to-date information available and have been vetted by subject matter experts within the Department of Defense and Intelligence Community ensuring their veracity and applicability to the Army training and intelligence audiences. Additionally, the material in the ATPs serves as a starting point for the concept and capabilities development community. The ATPs, in conjunction with TRADOC G-2's Battlefield Development Plans, have informed TRADOC and Army Futures Command's simulations and tests that will drive changes to the Army's future force as it prepares for joint MDO.¹

What's Next?

Unlike the already published TC series, the ATP series is currently in production with the first due to be published, distribution unlimited, in the summer of 2021. This first published ATP will be ATP 7-100.3 *Chinese Tactics*. As of the writing of this article, ATP 7-100.2 *North Korean Tactics* is in its final approval stage and is expected to be released by this fall. All ATPs will be digitally published by the Army Publishing Directorate (APD) available for mass consumption, accessible through APD's website.

¹The TRADOC G-2 Battlefield Development plans are classified analytic assessments of Russian and Chinese systems warfare. These were deliberately produced to support TRADOC concept and capabilities development in light of joint MDO.

The next ATP delivered to the force will be ATP 7-100.1 *Russian Tactics* followed by ATP 7-100.4 *Iranian Tactics*; both books are being drafted and should be available in early 2022. After drafts are complete, both the Iran and Russia publications will be staffed during the world-wide staffing phase of the Combined Arms Doctrine Directorate's publishing process; those interested in participating in the review of these manuals should get in touch with the element of their command that distributes Army doctrine staffing.

Many of the manuals in the TC series of doctrine are nearing their ten-year anniversary and, over the past several years, in particular throughout the duration of the production of the ATPs, TRADOC G-2 has been collecting material to inform updates to the books in this series of manuals. Right now, an update is underway for TC 7-101 *Exercise Design Guide*, and an update to FM 7-100.1 *Opposing Force Operations* is in the planning stages (this is the only OPFOR doctrinal publication that is an FM instead of a TC). TRADOC G-2 will continue to consider and plan updates to the OPFOR doctrine to ensure the Army's OPFOR training materials still provide the most robust and dangerous enemy the Army could face in a tactical fight.

In order for the Army to remain ahead of its adversaries, training against a robust, realistic threat for task proficiency is essential. It is also essential for the Army, especially the elements that are regionally aligned, to thoroughly understand the adversary they are most likely to encounter in future conflicts. Collectively, the TC and ATP series of doctrine provide the Army the most up-to-date realistic unclassified threat material needed to enable success in future conflicts against any enemy.