Contested Homeland Environment Simulation

Keith Ladd
Applied Training Solutions, LLC
Casper, WY
kladd@appliedtrg.com

Joe Nolan
Applied Training Solutions, LLC
Orlando, FL
jnolan@appliedtrg.com

Schawn Thropp
Applied Training Solutions, LLC
Greensburg, PA
sthropp@appliedtrg.com

ABSTRACT

The U. S. Military relies on various interdependent infrastructures in the Homeland, the majority of which it does not own or operate, making its domestic operations heavily reliant on external resources. This includes dependencies on civilian infrastructure to move from installations to ports of embarkation, conduct logistical operations, and to sustain installations that are dependent on civilian infrastructure for power, communications, fuel, water, and other life support. Accordingly, today's exercises and wargames must be designed with realistic disruptions to infrastructure and key supply chains in the Homeland, and should include participation by key civilian infrastructure owners/operators and local/regional government representatives.

While current military constructive simulations are tremendous for force-on-force training and wargaming, they are not designed to simulate the dynamics of a Contested Homeland Environment, or to include our non-Department of Defense (DoD) partners. This creates a gap in military organizations' ability to realistically train Homeland Defense (HD) missions within the Homeland and with our Whole-of-Nation partners. There is a need, therefore, for a constructive simulation tool to replicate the Contested Homeland Environment by importing infrastructure from authoritative sources along with the associated metadata as map layers in order to replicate critical infrastructure systems, adversarial actions on that infrastructure, cascading effects between sectors, as well as the second order effects on the population. This simulation should also be able to stimulate a myriad Common Operational Picture tools used across the government and civilian sectors, increasing the ability to include key civilian infrastructure owners/operators and local/regional government representatives in Contested Homeland exercises and wargames.

ABOUT THE AUTHORS

Keith Ladd is a Program Manager (PM) with Applied Training Solutions, LLC (ATS). After serving for 28 years in the US Army, Keith retired as the Chief of the USNORTHCOM Domestic Operations Division, where he was responsible for providing support to Disaster Response training and operations. As a PM for ATS, he has managed numerous contracts for both military (e.g. USNORTHCOM, USSOUTHCOM, ARNORTH, IMCOM, CNIC, etc.) and civilian (e.g. PJM, E-ISAC, City of Fairfax, NMDHSEM, etc.) exercise programs focused on Disaster Response and Homeland Defense.

Jospeh Nolan is a Senior Program Manager with ATS. He served 28 years in the US Army as an infantry and FA57 Simulation Operations officer. He served as Chief of the US Army Modeling & Simulation (M&S) Office where he managed innovation investments to shape the Army's M&S Enterprise. After the Army, he served as the Director of Defense & Public Sector Business Development for Magic Leap, Inc. He is an advisory board member of the VRARA Orlando Chapter and volunteers for NTSA events such as I/ITSEC.

Schawn Thropp is the Director of Enterprise Architecture with ATS. Schawn graduated with a Bachelor of Science in Computer Science and Mathematics from the University of Pittsburgh at Johnstown along with a Master of Science in Computer Science at Johns Hopkins University. Post education, Schawn has over 30 years of research and development, software application development, and program management within the Training, Education and Learning domain. Schawn has spent the last 10 years focused on the modeling and simulation technologies.

Contested Homeland Environment Simulation

Keith Ladd
Applied Training Solutions, LLC
Casper, WY
kladd@appliedtrg.com

Joe Nolan
Applied Training Solutions, LLC
Orlando, FL
jnolan@appliedtrg.com

Schawn Thropp
Applied Training Solutions, LLC
Greensburg, PA
sthropp@appliedtrg.com

INTRODUCTION

Since its inception, our nation has enjoyed the protection afforded by geography and accordingly has practiced defense in depth. Unlike other nations, we enjoy the luxury of the majority of our military operations occurring "over there," limiting operations here in the Homeland to power projection operations to get the military "over there," logistical operations to sustain the force "over there," and leveraging unique capabilities of our military to support Civil Authorities in the Homeland. As technology has advanced, however, the world has gotten smaller and the Homeland from which we project power is no longer a sanctuary. Our adversaries now have greater access to the infrastructure that not only sustains our population's way of life, but also, is critical to our nation's ability to project power such as communications, transportation, energy, fuel and water. Our military can no longer assume that it can operate uncontested in the Homeland. As the Defense Science Board accurately states, "DoD is dependent on increasingly fragile homeland infrastructure whose interdependencies are difficult to unravel, limiting visibility into infrastructure resiliency against intentional attacks or natural disasters." (Defense Science Board, 2024).

In his *Summary of the 2018 National Defense Strategy of the United States*, Secretary of Defense James Mattis made clear his concerns about US infrastructure in the next conflict.

> "It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated." (Mattis, 2018)

Accordingly, we need to plan, train and prepare for the disrupting and disabling of US Forces while they conduct operations in the Homeland. Indeed, exercises serve to assess and practice processes and plans, try out new doctrine, and signal our readiness to our adversaries, but to do so they must be realistic. According to the Joint Training System, you "train the way you intend to operate. Joint training must be based on relevant conditions of actual operations to the maximum extent possible and use existing operational information networks." (CJCS Guide 3501, 2015). Unfortunately, talking about realistic training is a lot easier than doing so. Simulating exercises in a contested homeland environment is a complex endeavor for a number of reasons, all of which result in the current practice of downplaying the challenges of operating in a contested homeland environment. It's too hard, so we minimize it, which has consequently left us with an immense operational blind spot. This paper seeks to analyze those challenges and offer potential features for a simulation tool that could serve to better prepare military and civilian leaders for operations in a contested homeland through realistic training, exercises and wargaming.

THE HOMELAND: A COMPLEX ENVIRONMENT

While today's operational environment for fighting our nation's fights "over there" is certainly volatile, uncertain, complex and ambiguous, our military faces an even more complex environment when operating in the Homeland. A closer look the following complexity factors will inform potential solutions for replicating a realistic training environment.

Complexity Factor 1: Whole-of-Nation Realities

The first factor impacting the complexity of the Homeland operating environment is that DoD is rarely able to act unilaterally. For starters, our military has very limited authorities in the Homeland. Our founding fathers had a wariness of standing armies that was rooted in the colonial experience, and consequently our military operations in the Homeland are in support of other agencies most of the time. On a broader level, our founding fathers were also wary of a powerful Federal government, and therefore were very specific as to its powers in the Constitution, establishing a system of federalism that codified in the 10th Amendment "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

Secondly, while incredibly well resourced for the fight "over there," our military is tremendously reliant upon other governmental agencies at the Federal, State and Local levels, as well as non-governmental organizations (NGO) and the commercial sector to conduct power projection operations to get the military "over there" and logistical operations to sustain the force "over there".

Therefore, success in Homeland operations is dependent upon the willing participation of a host of organizations that the military does not control, each with their own systems, budgets and priorities. Whereas during military operations "over there" our military can throw its immense weight around, during operations in the Homeland our military must be much more collaborative than directive. Moreover, whereas our military is relatively well-funded with large standing organizations, our partners in the Homeland have much smaller budgets and organizations, and what is important to the DoD is not always a high priority for them.

Complexity Factor 2: Interconnectedness of Infrastructure

The Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA) provides guidance to support State, Local, and industry partners in identifying critical infrastructure needed to maintain the functions Americans depend upon daily. In doing so, CISA has identified 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem made up of numerous service providers within each sector.

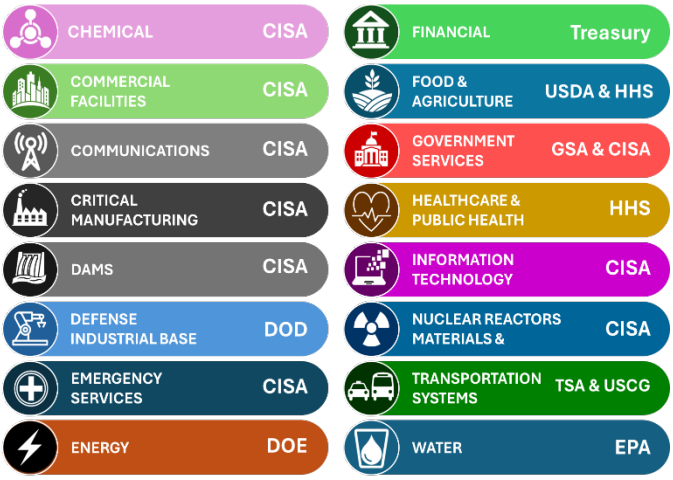

Figure 1: 16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

While the DoD has established a Defense Critical Infrastructure Program (DCIP) (DoD Directive 3020.40, 2005) that is beyond the scope of this paper, the Defense Science Board has identified "four sectors critical for force deployment and operations from the homeland: **energy** (both electric and fuel), **communications**, **transportation**, and **water**. Each is critical to DoD operations in and of themselves but are also highly interdependent." (Defense Science Board, 2024)

In its 2024 report on Threats to Critical Infrastructure, RAND addresses the concept of Cascading Hazards, stating "There are many interdependencies...among sector assets that often result in outsize impacts and effects,...damage to various sectors often creates ripple effects across other sectors and industries that rely on similar foundational scaffolding. For example, damage to the energy sector can hinder internet connections (in the communications sector) or the movement of people and goods (in the transportation sector)." (RAND, 2024) Creating an exercise environment that replicates effects on one sector is challenging; replicating cascading effects across multiple sectors is exponentially more difficult given the sheer volume of assets, interdependencies, and effects that might occur in response to various types of attacks.

Complexity Factor 3: Population Resiliency

Our military enjoys immense respect from and strong ties with American society. Military bases and the families they house are an integral part of the communities which surround them. While there are economic benefits to routine mutual cooperation, the strength of these relationships is often best demonstrated during crises when there is a shared experience of coming together during difficult times. During contested homeland operations, however, these ties are likely to be strained. Emergency managers typically use a planning factor of 72 hours for restoration of services after a disaster in order to prevent widespread looting and civil unrest. A large-scale attack on critical infrastructure will rapidly affect the population's availability of food and water, power for living, fuel for vehicles, and the ability to communicate with friends and family, all while the military is focused on mobilizing and deploying forces overseas in response to the attack and may not have the resources to dedicate to disaster response efforts.

An adversary's attack on critical infrastructure would most likely be accompanied by information operations against our population to gain advantage through the manipulation and control of information. Whether using scores of human threat actors or conducting operations via automated bots, adversaries would inevitably spread disinformation (false and deliberately created to mislead, harm or manipulate) and/or malinformation (based on fact, but intentionally used out of context to mislead, harm or manipulate) to exacerbate the physical disaster and possibly turn portions of the population against the military, impacting its ability to conduct operations in the Homeland.

EMERGING THREATS

In their 2024 Homeland Threat Assessment, DHS articulates several trends in threats to the Homeland. These include trends like the convergence of the cyber and physical domains, stating that:

> "Malicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber attacks—against targets, including pipelines, railways, and other US critical infrastructure. Adversarial governments, most notably the PRC, are developing other AI technologies that could undermine US cyber defenses, including generative AI programs that support malicious activity such as malware attacks." (DHS, 2024)

Another of the more interesting emerging trends is the proliferation of commercial drones. A report from MarketsAndMarkets projects the commercial drone market to see significant growth over the next 5 years due to low cost and easy operation (MarketsAndMarkets, 2024).

One of the unintended consequences of this growth is the increase in malicious actors' ability to successfully defeat critical infrastructure physical security systems like walls, barriers and checkpoints.

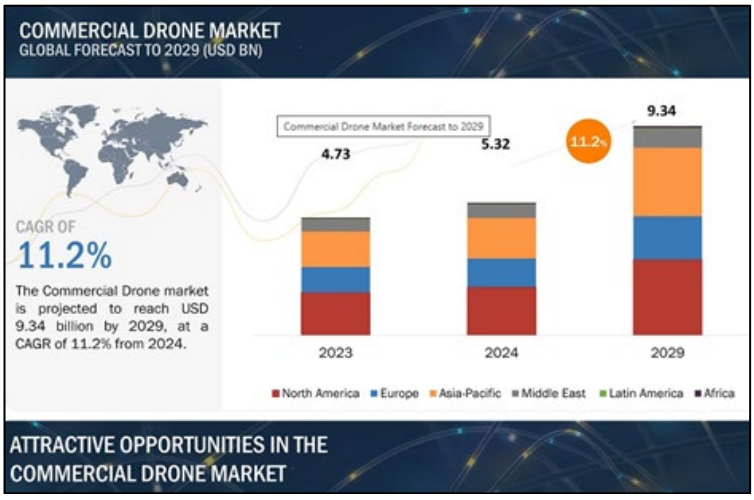

Figure 2: 16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

Another trend that DHS identifies is the increase in foreign misinformation, disinformation, and malinformation, predicting that:

> "Nation-state adversaries likely will continue to spread mis-, dis-, and malinformation aimed at undermining trust in government institutions, our social cohesion, and democratic processes. The proliferation and accessibility of emergent cyber and AI tools probably will help these actors bolster their malign information campaigns by enabling the creation of low-cost, synthetic text-, image-, and audio-based content with higher quality. Russia, China, and Iran continue to develop the most sophisticated malign influence campaigns online." (DHS, 2024)

EMERGING DOCTRINE

In light of these emerging threats, DoD has begun to develop new doctrine for operations in a contested homeland. For instance, the U.S. Army has added an appendix to its Operations Manual (FM 3-0) entitled "Contested Deployments" (Appendix C), in which state "Key planning and training considerations are-

- The local, state, and federal authorities able to mitigate deployment disruptions.
- Coordination and relationship building with local, state, and federal civilian law enforcement agencies to ensure effective movement control from fort to port.
- Understanding about critical infrastructure vulnerable to sabotage and unsuited for the movement of heavy equipment along surface lines of communication, both road and rail.
- Planning to use alternate railheads and marshalling yards and multiple lines of communication to reach ports of embarkation.
- Developing alternate surface transportation options to deliver unit equipment to a seaport of embarkation when rail service is degraded or disrupted.
- Establishment of fuel, maintenance, and rest locations along lines of communications.
- Implementation of a communication plan that informs the public while maintaining operations security.
- Establishing specific cyber defenses for systems and associated data used to support movement." (FM3-0, 2022)

The Contested Deployments appendix also does a great job of summarizing both Homeland Defense (HD) and Defense Support of Civil Authorities (DSCA) operations, demonstrating how the two might overlap in Contested Homeland scenarios.

In concert with US Army doctrine, US Army North has recently developed the concept of Multi-Domain Resiliency Zones (MDRZ), which "create modular, layered, defense-in-depth for key defense critical infrastructure, a strategic priority for homeland defense and force projection capabilities. Placed at critical installations, a network of MDRZs would create pockets of resilience across the United States to recover quickly after an attack in any domain. While it would be infeasible to defend everything at all times, layering protection with resiliency would ensure continuity of operations and minimize the impacts of adversarial interference." (US Army North, 2024)

Additionally, USNORTHCOM has begun to develop a concept of Civil Support to Defense Authorities (CSDA), recognizing that in times of national mobilization to a near-peer threat, our military would likely need support from civil authorities at the Federal, State and Local levels. This comes at a time when the current administration is changing the focus of FEMA's role in disaster response to empowering State and Local preparedness (Trump, 2025). One possible outcome is to re-establish FEMA's mission during national mobilization. As Quinton Lucie states in "How FEMA Could Lose America's Next Great War,"

> "….the United States has not had a comprehensive strategy to protect its civilian population and defense industrial base, or to mobilize and sustain the nation during time of war for almost 25 years. Without an investment in these activities by FEMA and the DHS, America risks losing its next war with one or more major nation states….Unfortunately, efforts so far may not have reflected the fact that it is the morale and purpose of the American people that will be the crucial factor to prosecuting any future great war. It is the American public, and their supporting political system and critical infrastructure that could quite possibly be the focus of our enemy's attacks if it decides to bypass the American military juggernaut and go directly after the citizens it serves to protect. The Federal Government and the Congress must recognize that fighting a great war will extend to the homeland

and take more than just meeting the increased manpower, industrial, technological and logistical needs of the military." (Lucie, 2019).

PROBLEM

By now it should be very apparent that today's military needs to prepare for operations in a Contested Homeland. As the Defense Science Board highlights, "Overarching the entire Department's approach, exercises should be designed and executed with realistic disruptions to the homeland and other key supply chain(s). In almost every case, key civilian infrastructure owners/operators and local/regional government representatives should be included as advisors, if not players." (Defense Science Board, 2024). The problem, however, is that we do not have the right simulation capabilities to do so. While current military constructive simulations are tremendous for force-on-force training and wargaming, they are not designed to replicate the dynamics of a Contested Homeland Environment. This creates a gap in military organizations not being able to realistically train for operations within a Contested Homeland by incorporating the latest threats, emerging doctrine, our Whole-of-Nation partners and critical infrastructure, which increases our vulnerability to adversarial actions.

RECOMMENDED SOLUTION

DoD needs a synthetic training, exercise, wargaming environment that replicates the complexities of conducting operations in a Contested Homeland Environment to include actual infrastructure critical to HD operations, interrelationships of sectors and cascading effects, and the information environment and its effect on US population. Given our military's dependence on other Federal, State and Local organizations, NGO, and commercial organizations in the Homeland, this simulation needs to ensure integration with non-DoD players. Given the effects of a Contested Homeland on military operations "over there", this simulation should also be integrated with other military simulations in order to create a single operational environment for Globally Integrated Exercises (GIE). To successfully accomplish these, we recommend this simulation have at a minimum the following eleven features.

Feature 1: Constructive Simulation

Constructive simulations normally include real people providing inputs to the simulation but not involved in determining the outcomes and normally include two or more sides with each side making independent decisions based on its perception of the conditions in the environment. Constructive simulations bring versatility, cost savings and fidelity to exercises by using computer models to represent individuals and systems, allowing for complex interactions and scenarios like those in a Contested Homeland Environment.

A Contested Homeland simulation should be scalable, able to support exercises ranging from the local to the national level. It should also have a realistic map environment with GIS data support in which the scenarios play out, providing participants with the real-world physics of time and space for their operations. This single exercise environment would provide a consistent "ground truth" across all of the participating organizations.

Feature 2: Low Overhead

Most military simulations require high-end, costly hardware to conduct an exercise over a network that is only accessible through a finite set of locations across the U.S. To include our Federal, State, Local, NGO and commercial partners in Contested Homeland exercises, a Contested Homeland simulation would need to be run on more common hardware to fit their limited budgets. Likewise, most military simulations require a large footprint to develop and execute an exercise. Training simulation cell (SIMCELL) workstation operators/role players on the system can take up to three 8-hour days, and running the SIMCELL for an exercise could take 16-20 personnel for a 24 hour/day exercise. Our Federal, State, Local, NGO and commercial partners do not have the personnel, time or money to support this level of exercise support requirement.

Feature 3: Entity-Based

In order to provide the necessary level of realism, a Contested Homeland simulation would focus on simulating the behaviors individual entities within the operational environment, tracking their attributes and interactions as they progress through the simulation. These entities would represent individuals and equipment within both military and non-military organizations, with the ability to aggregate entities within an organization in order to reduce exercise overhead (see Feature 2 above) and be scalable for local to national level exercises.

On one hand, since a Contested Homeland simulation would need to integrate with other military simulation systems, it would need to use Military Standard (MIL-STD-2525) templates for military entities, and comply with Distributed Interactive Simulation (DIS) and High Level Architecture (HLA) required for interoperability between military simulations. On the other hand, since one of the main purposes of a Contested Homeland simulation would be to integrate with non-military organizations, it would also need to use other templates for non-military entities. For example, it could use data from the FEMA Resource Typing Library Tool (RTLT) which provides an online catalogue of national resource typing definitions, including payload volume, fuel capacity, mission capability parameters, and other data for realistic entity portrayal within the simulation. This flexibility and range of entities would be essential in order to accurately portray emerging technologies such as commercial drones discussed above under Emerging Threats.

Entities within a Contested Homeland simulation would also represent the real-world infrastructure involved in a Contested Homeland scenario, which would be imported along with all associated metadata from authoritative data sources like the Homeland Infrastructure Foundation-Level Data (HIFLD) which would then be turned into data objects for use as entities within the system.

Feature 4: Effects-Driven

In order to provide the necessary level of realism, a Contested Homeland simulation would input data from authoritative models to create effects that would have impacts on entities within the simulation. For instance, if the scenario called for hurricane, exercise planners could use National Oceanic and Atmospheric Administration (NOAA) Sea Lake and Overland Surges (SLOSH) models to create flooding conditions which would impede entity movement. Likewise, if the scenario called for a nuclear detonation, exercise planners could use Defense Threat Reduction Agency (DTRA) plume models to depict radiation effects which would cause entity sickness/death. This use of authoritative data is crucial not only to accurately depict effects, but also, serves to practice integration with partners "left of boom".

Due to the complexities of replicating cascading effects across multiple infrastructure sectors, it would be imperative to import modeling from organizations like the DHS's National Counterterrorism Innovation, Technology, and Education Center (NCITE), a Center of Excellence of more than 40 university and industry partners led by the University of Nebraska, which is developing a tool to assess the impact of disruption of one sector on multiple different sectors.

Feature 5: Dynamic Changes

Most military simulations require a time-consuming process of building the simulation database and have a data cut-off date for making changes leading up to an exercise. Likewise, should there be a need to add additional organizations or changes to the operational environment during an exercise, these simulations require a pause in the exercise to implement the changes. While the military might have the luxury of time and money required by these time-consuming processes, our civilian partners do not have the resources for building simulation databases or the time for their personnel to sit around during exercises waiting for the changes to be implemented. A Contested Homeland simulation, therefore, must feature a less time-consuming process of building simulation databases, and allow for dynamic changes to entities, organizational structure, and effects within the simulation environment without pausing the exercise.

Feature 6: MSEL-Based

Because of the need to include Whole-of-Nation partners in Contested Homeland exercises, a Master Scenario Events List (MSEL) needs to be developed to act as a script for the simulation and drive participants to accomplish their exercise objectives. These objectives are often-times very different, but the MSEL serves to synchronize participants through a series of chronological injects, which can look like the following:

#	Start Date	Subject	Inject
4	2025-05-30 06:00:00 AM	National GuardArmory Surveillance	National Guard units report that drones are hovering around their units' armories. Nearly all of t
9	2025-05-30 06:00:00 AM	FEMA Region IMAT Request	FEMA Reg V IMAT is requested by the SEOC.
10	2025-05-30 06:00:00 AM	GovernorDisaster Dec	Governor Smith issues a Disaster Declaration for the counties of Oscoda, Alcona, and Iosco Cou
11	2025-05-30 06:00:00 AM	Iosco CoDamage Assessment	The Mio Dam release has completely devastated the towns of Oscoda and Au Sable with a wall o
12	2025-05-30 06:00:00 AM	Iosco Co Mortuary Affairs Request	The Iosco County EM has requested mortuary affairs assistance to handle the hundreds of decea
13	2025-05-30 06:00:00 AM	Iosco Co Shelter Tentage Request	The Iosco County EM has established a 2,000-person shelter at the hangars at the Oscoda-Wurts
14	2025-05-30 06:00:00 AM	Iosco Co Water Purification Request	The Iosco County EM has requested water purification assistance to provide potable water to the
17	2025-05-30 06:00:00 AM	Mio DamBreach	A group of coordinated nefarious actors executed a cyber-physical attack on the Mio Dam, locate
18	2025-05-30 06:00:00 AM	Mio Dam RoadDamage Assessment	The Mio Dam release has completely destroyed the following routes crossing the Au Sable River:
20	2025-05-30 06:00:00 AM	Oscoda CoDamage Assessment	The Mio Dam release has completely devastated the town of Mio with a wall of water over 10 feet
21	2025-05-30 06:00:00 AM	Oscoda Co ShelterTentage Request	The Oscoda County EM has established a 1,000-person shelter at the Mio Ausable Schools, locat
22	2025-05-30 06:00:00 AM	Oscoda Co WaterPurification Request	The Oscoda County EM has requested water purification assistance to provide potable water to t
23	2025-05-30 06:00:00 AM	PresidentialDisaster Dec	POTUS issues a Disaster Declaration for the counties of Oscoda, Alcona, and Iosco County due t
25	2025-05-30 12:00:00 PM	Iosco Co DebrisCleanup Request	The Iosco County EM has requested assistance with debris cleanup in Iosco County as a result o
26	2025-05-30 12:00:00 PM	Oscoda Co DebrisCleanup Request	The Oscoda County EM has requested assistance with debris cleanup in Oscoda County as a res

Figure 3: Example Contested Homeland Exercise Master Scenario Event List (MSEL) Injects

Given the simulation's realistic map environment with GIS data support required by the complexities of Contested Homeland effects, the simulation would need to have the capability for an inject from the MSEL to automatically initiate effects in order to synchronize them in time and space. Moreover, the MSEL functionality would need to have the ability to support a wide means of delivering injects, ranging from the use of common communications systems (e.g. email, SMS text, etc.) to directly stimulating data fields within mission command tools (e.g. MAVEN) and civilian Common Operating Picture (COP) tools (e.g. WebEOC).

Additionally, as exercise designers build events, they use time-proven and standardized processes to generate products like MSELs. Unfortunately, military and civilian emergency management agencies use different processes, so the Contested Homeland simulation must be able to incorporate both the military's Joint Training System (JTS) and the Homeland Security Exercise and Evaluation Process (HSEEP) as partners work together to build integrated exercises.

Feature 7: Population-Centered Information Environment

Given the critical role of the U.S. population in a Contested Homeland scenario, the simulation must emulate how the public consumes and responds to information—across both traditional and social media channels—capturing the influence of mis-, dis-, and malinformation. To reflect real-world dynamics, the simulation should incorporate population effect models that track and visualize shifts in public sentiment, behavior, and civil stability over time. The simulation's realistic map environment must portray public sentiment at varying levels of granularity, allowing civil unrest to emerge and evolve based on scenario events. Equally important, it must enable the training audience to take deliberate actions—such as public messaging or policy changes—and measure their effectiveness in reducing unrest and restoring order.

Feature 8: Mission Command System/Common Operating Picture Tool Agnostic

While there is tremendous value in using a constructive simulation to drive Contested Homeland exercises, that value is exponentially increased when the simulation output stimulates the training audience's real-world decision-making tools that display relevant information in order to provide a shared situational awareness for better coordination, decision-making, and response. For military participants, those tools are their Mission Command Systems. For non-military participants, those tools are their COP tools. The irony is that while the word "common" is in "Common Operating Picture", each organization has their own COP, so there is not a single common operating picture that all partners use. Given the need to integrate Whole-of-Nation partners in Contested Homeland exercises, the constructive

simulation must be able to simultaneously stimulate a myriad different COP tools, providing each participant with a shared perspective of the Contested Homeland environment displayed on their own COP tools. To do so the simulation should output to file formats and protocols commonly used by geo-spatial COP visualization tools, so that the training audiences see the same information regardless of which tool they are using.

Feature 9: Flexible in Time

Given the varying requirements of government, NGO and commercial partners, a Contested Homeland simulation must have the flexibility to adjust time. For some exercises, the simulation would run in real-time. During other exercises, exercise controllers might need to pause the simulation to seize upon a learning moment. Other exercise scenarios might play out over weeks in the simulation, but participating organizations might not have the time to play for that long so the simulation would need to be accelerated. For instance, FEMA's Incident Command System (ICS) uses operational periods, typically 12 to 24 hours long, during which a set of tactical actions are executed as outlined in the Incident Action Plan (IAP). At the end of each operational period, planners assess the changing environment and adjust the response plan accordingly. Once the adjusted plan is replicated in the simulation, the simulation could be accelerated to the end of the next operational period, significantly decreasing the amount of time required to play out a lengthy scenario.

Another benefit of being able to accelerate the scenario within the simulation is that organizations could repeat scenarios for comparison of outcomes, helping to test different strategies and Tactics, Techniques and Procedures TTP) for operating within a Contested Homeland.

Feature 10: Flexible in Security

While the integration of Whole-of-Nation partners is critical for success within a Contested Homeland, not all of the partners have the same access to varying levels of classified information or the networks to access that information. In some instances, in order to exercise with local authorities, the Contested Homeland simulation would need to be Web-based, accessible from a commercial network. In other instances, in order to exercise with certain Federal partners, the simulation would need to have an Authority To Operate (ATO) on classified and unclassified networks.

To support broad participation, the simulation must have security built in from all levels. This requires robust cybersecurity measures, including role-based access controls, data segregation, and end-to-end encryption, to protect sensitive data and ensure compliance with government security standard

Feature 11: Flexible in Location

Most military simulations require the training audience to either be in a single location or be in a handful of locations on military installations. This is problematic, as our Whole-of-Nation partners have challenges accessing military installations and the Simulation Centers within them, and in more cases than not are dispersed geographically from those installations. Additionally, they have neither the time nor the funding to travel lengthy distances for extended amounts of time to participate in these exercises. To include our Federal, State, Local, NGO and commercial partners in Contested Homeland exercises, there would need to be the ability to establish Contested Homeland exercise SIMCELLs in multiple locations operating concurrently within the same exercise. This would enable higher levels of local and functional expertise within SIMCELLs, as well as reduce partner travel time and expenses allowing for greater participation.

CONCLUSION

Our adversaries understand the strategic importance of our military's ability to project combat power to their region, sustain combat power in their region, and support the response to disasters in our Homeland. By disrupting that capability, our adversaries are able to impose their will by reducing our time and options. Therefore, we should count on having to conduct operations within a Contested Homeland. Our ability to do so today is hampered by an inability to accurately reflect the complex dynamics of that environment within our training, exercises and wargaming. The urgency of the situation demands that we not shy away from the challenges of replicating a Contested Homeland

Environment. Having a Contested Homeland Environment Simulation that is constructive, entity-based, effects-driven, MSEL-based, population-centric, COP-agnostic, and offers flexibility of dynamic changes, time, security and location will serve to address the complexities presented by the Whole-of-Nation realities, interconnectedness of infrastructure, and population aspects inherent to a Contested Homeland Environment, and better prepare military and civilian leaders for operations within that environment.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the help of Mr Brent Ruhlen and Mr Jon Ford. Their unsurpassed excellence and inspirational leadership ensure successful Modeling & Simulation support to USNORTHCOM, US Army North, and numerous other organizations at the National, State and Local levels, serving to increase the preparedness of our great Nation. The authors also wish to acknowledge the invaluable collaboration with the consummate professionals on staff at USNORTHCOM/J7 and ARNORTH/G7 who tirelessly work to ensure the Homeland is ready for the next challenge.

REFERENCES

CJCS Guide 3501(2015). *The Joint Training System: A Guide for Senior Leaders*. A-3.

Defense Science Board (2024). *Department of Defense Dependencies on Critical Infrastructure.* Executive Summary [1-3], Recommendations [8].

Department of Homeland Security (2024). *Homeland Threat Assessment 2024*, 6,18.

James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: Department of Defense, January 2018), 3.

Lucie, Quinton. *"How FEMA Could Lose America's Next Great War."* Homeland Security Affairs 15, Article 1 (May 2019), 20-21.

MarketsAndMarkets (2025). *Commercial Drone Market* https://www.marketsandmarkets.com/Market-Reports/commercial-drone-market-66171414.html#:~:text=Based%20on%20End%20Use%2C%20the,the%20growth%20of%20this%20segment

RAND (2024). *Threats to Critical Infrastructure,* 22.

Trump, Donald (2025). "*Achieving Efficiency Through State and Local Preparedness"* https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/

U.S. Army (2022). *FM 3-0 Operations.* Appendix C. C-4

U.S. Army North (2024). *Framing the future of homeland defense: Multi-Domain Resiliency Zones* https://www.arnorth.army.mil/Media/News/Article/3922295/framing-the-future-of-homeland-defense-multi-domain-resiliency-zones/#:~:text=The%20Multi-Domain%20Resiliency%20Zone,Air%20Base%20Wing%20Public%20Affairs