Providing Asymmetric Information Advantage and Cyber Multidomain Operations Training Capabilities

J. Allen Geddes
Patrick J. Hart
Bryan A. Long Jr.
US Army DEVCOM Soldier Center
Orlando, Florida
james.a.geddes2.civ@army.mil
patrick.j.hart.civ@army.mil
bryan.a.long10.civ@army.mil

Bruce J. Gorski
Brian P. Parrish
Jared A. Arslanian
MITRE
McLean, Virginia
bgorski@mitre.org
bparrish@mitre.org
jarslanian@mitre.org

ABSTRACT

"Information is central to everything we do – it is the basis of intelligence, a fundamental element of command and control, and the foundation for communicating thoughts, opinions, and ideas." This statement by Lieutenant General Milford H. Beagle, Jr., Commanding General of the U.S. Army Combined Arms Center, highlights the significance of the information dimension in the modern operational environment, and the urgent need for U.S. forces to train to conduct information operations, to be able to effectively use and protect information, exploit information advantages, and employ cyber non-kinetic effects against peer adversaries.

To address these needs, the U.S. Army Combat Capabilities Development Command – Soldier Center has partnered with industry, academia, and government agencies to create the Information Environment for Simulation and Training (INFEST) capability. INFEST has Joint, Active Army, National Guard, and Reserve stakeholders, and is relevant to our international allies. Initial front-end analysis revealed the keys to enabling this training include representing a dynamic information environment, non-kinetic effects, and will-to-fight in Army Modeling and Simulation systems. INFEST, a working capability, has integrated synthetic populations, large language models, an internet emulator, and a cyber framework using the Army's Synthetic Training Environment simulation. INFEST will enable warfighters to train information advantage and cyber activities in a Multi-Domain Operations (MDO) environment.

The paper will start with a summary of the market research and warfighter interviews that underpin INFEST. Next is an overview of the use cases that drive the development followed by a description of the technical approach. Then it will provide examples of bi-directional cause and effect traceability between physical environment, information environment, and cyber non-kinetic effects. The paper will close with a way ahead to engage the Simulation Interoperability Standards Organization to develop an information advantage data exchange model and future INFEST efforts such as information advantage scenario generation.

ABOUT THE AUTHORS

J. Allen Geddes is a Science and Technology (S&T) Manager at the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Simulation and Training Technology Center (STTC). Mr. Geddes holds Bachelor of Science (B.S.) degrees in Management Information Systems and Software Development from the University of Central Florida and a Master of Science (M.S.) in Systems Engineering and Program Management from the Naval Postgraduate School.

Patrick J. Hart is a S&T Manager at the U.S. Army Combat Capabilities DEVCOM SC STTC. Mr. Hart holds a B.S. in Electrical Engineering from the University of Central Florida and a M.S. in Program Management from the Naval Postgraduate School.

Bryan A. Long, Jr. is a S&T Manager at the U.S. Army Combat Capabilities DEVCOM SC STTC. Mr. Long holds both a B.S. and an M.S. in Electrical Engineering from Ohio University.

Bruce Gorski is an Operations Research Analyst and Multi-Discipline Systems Engineer for the MITRE Corporation. Mr. Gorski holds a B.S. in Mechanical Engineering from the United States Military Academy, a Master of Engineering in Engineering Management from the Old Dominion University, and M.S. in Systems Engineering from Johns Hopkins University.

Brian Parrish is a Modeling and Simulation Engineer and a Multi-Discipline Systems Engineer for the MITRE Corporation. Mr. Parrish holds a B.S. in Computer Science from Missouri Western State University and a M.S. in Systems Engineering from Johns Hopkins University.

Jarod Arslanian is a Simulation and Modeling Engineer for the MITRE Corporation. Mr. Arslanian holds a B.S. in Computer Science from Missouri Western State University and a M.S. in Computer Science from Georgia Institute of Technology.

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004.

Approved for Public Release # PR2025-2605

Providing Asymmetric Information Advantage and Cyber Multidomain Operations Training Capabilities

J. Allen Geddes
Patrick J. Hart
Bryan A. Long Jr.
US Army DEVCOM Soldier Center
Orlando, Florida
james.a.geddes2.civ@army.mil
patrick.j.hart.civ@army.mil
bryan.a.long10.civ@army.mil

Bruce J. Gorski
Brian P. Parrish
Jared A. Arslanian
MITRE
McLean, Virginia
bgorski@mitre.org
bparrish@mitre.org
jarslanian@mitre.org

INTRODUCTION

Challenges and Real-World Needs

The battlefield of the future will be defined not only by physical dominance, but by the mastery of information. Military power projection in the 21st century necessitates controlling the narrative, shaping perceptions, and, when necessary, manipulating the information environment (IE) to achieve strategic objectives. This is not simply about propaganda; it is about recognizing that influence in the real world – both physical and virtual – is paramount to future military success. The increase of digital technologies and the increasing association of global networks have fundamentally altered the character of conflict, elevating the IE to a critical domain alongside land, sea, air, and space. Historically, military training has focused heavily on replicating the physical aspects of warfare. However, modern operations are inextricably linked to the open source or public information realm. Success hinges not only on what forces do, but on how those actions are perceived – by adversaries, allies, and the global public. False information tactics, and the weaponization of social media can erode public trust, incite unrest, and undermine military operations with alarming speed. Therefore, preparing warfighters for the complexities of Operations in the Information Environment (OIE) is no longer a supplementary concern, but a core requirement.

Problem to Solve and Capabilities Provided

This is where the Information Environment for Simulation Training (INFEST) capability, currently under research and development at the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Simulation and Training Technology Center (STTC), emerges as a crucial innovation. Recognizing the limitations of traditional training methods in adequately preparing personnel for the challenges in the OIE, INFEST seeks to create a dynamic and realistic simulation environment that integrates the human, informational, and physical dimensions of conflict. Achieving this will represent the chaotic, unpredictable nature of open source and public information flows and the complex interplay between real-world events and online narratives.

INFEST addresses this critical need by providing a platform capable of transcribing kinetic effects – the physical consequences of military actions – into the IE, and conversely, simulating how information operations can influence physical outcomes. Building on this, it aims to address "will-to-fight," a psychologically realistic context that allows military personnel to test their ability to navigate the ethical and strategic dilemmas inherent in information warfare. This allows for training that is not just about technical skills, but about critical thinking, judgment, and the ability to anticipate and respond to evolving information threats.

Goals and Objectives

This paper will detail the architecture and functionality of INFEST, outlining its key features and capabilities. Furthermore, we will discuss the methodology underpinning INFEST, emphasizing its proactive approach to information warfare – one that anticipates threats, builds resilience, and ensures that the narrative battlefield remains a domain of decisive advantage. Finally, we will explore the challenges and future directions of INFEST, considering its potential to revolutionize military training and enhance national security in the 21st century.

FRONT-END ANALYSIS

Analysis Summary

INFEST began with rigorous market research and front-end analysis that led to the creation of the INFEST objectives, approach, and selection of capabilities to use. The 12-month-long effort investigated training shortfalls, systems, and concepts, created digital story boards, derived user stories and requirements, and identified user needs. It also included direct engagements with warfighters, trainers, and stakeholders. This section describes the steps taken and the approach to identify needed capabilities and adapt them for military use in training.

Research into existing training simulation and warfighter engagements identified three information-related training shortfalls: lack of a dynamic IE enabling simultaneous training in the human, physical, and information dimensions; insufficient representation of will-to-fight; and the need for a low overhead IE pipeline that could rapidly support and pivot to a new region in the world. To overcome these shortfalls, the INFEST proof-of-concept defined 11 objectives, listed below and shown in Figure 1.

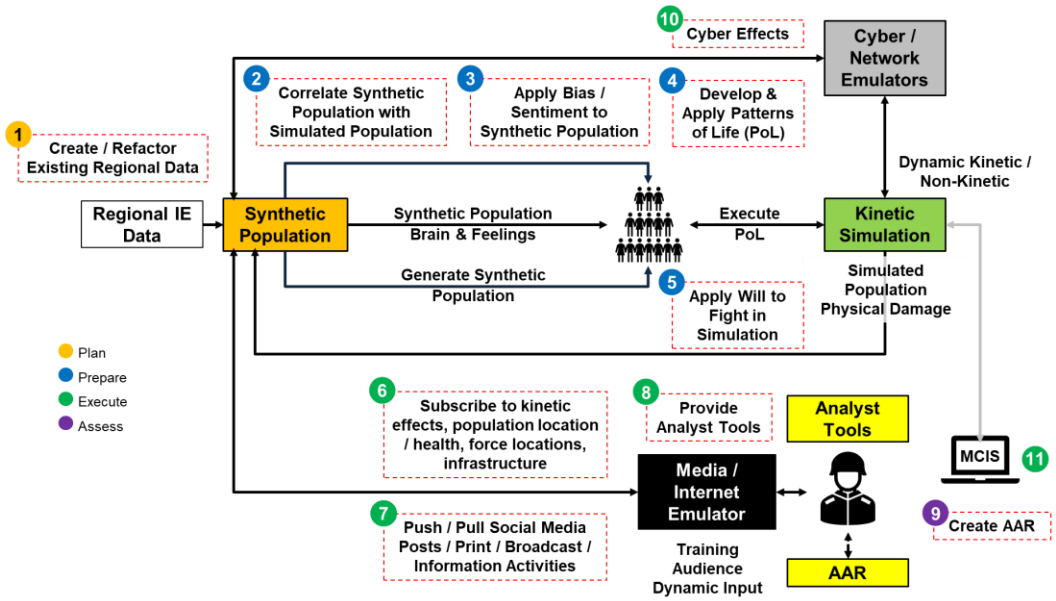

Figure 1. INFEST Objectives

- **Objective 1:** Create/refactor existing regional data.
- **Objective 2:** Correlate synthetic population with the kinetic simulation population.
- **Objective 3:** Apply bias/sentiment to the synthetic population.
- **Objective 4:** Develop and apply patterns of life.
- **Objective 5:** Apply will-to-fight in simulation.
- **Objective 6:** Subscribe to kinetic simulation effects, population location/health, force locations, infrastructure.
- **Objective 7:** Push/pull media posts/print/broadcast/information activities.
- **Objective 8:** Provide analyst tools.
- **Objective 9:** Create After Action Review (AAR).
- **Objective 10:** Provide cyber effects.
- **Objective 11:** Bi-directionally communicate with Mission Command Information Systems (MCIS).

To achieve these objectives, 56 systems were researched. The paragraphs below summarize how the INFEST core capability was selected.

The analysis used the training shortfalls and the systems research to identify and select capabilities for the INFEST proof-of-concept. The first step identified the core capabilities that would provide a dynamic IE and will-to-fight. Ideally, the core capabilities would be able to create a synthetic population that dynamically interacts with a kinetic training simulation, media emulator, and the training audiences. The new Army training simulation, the Synthetic Training Environment (STE) Operational Simulation (OPSIM) that uses the MSSV protocol, is the kinetic simulation that will drive the INFEST proof-of-concept. MSSV is not an acronym; it is the communication protocol that STE OPSIM uses. The market research did not find any system that provided all these items, much less a capability that was already interoperating with STE OPSIM and MSSV. The first step was to apply screening criteria to the 16 systems to find the best candidate system to be a core capability. The screening criteria listed below reduced the pool of candidate systems from 16 to 4.

- Lacks a behavior engine.
- Creates a generic population that is not assigned to a specific town or social network.
- Used only in specific contexts, such as insurance or generic population studies, that have no military application.
- Is a spreadsheet tool that does not lend itself to integration with other capabilities.
- Lacks capabilities for data visualization.

The candidate core capability systems were then evaluated using nine weighted criteria shown below. The first four are capabilities that will help resolve training shortfalls and the last five address other important factors to consider.

- Provides sentiment/mood for the human dimension.
- Provides patterns of life.
- Demonstrates ability to interoperate with a kinetic simulation.
- Provides will-to-fight for the human dimension.
- Has an existing contract vehicle to accelerate the contracting process.
- Advantageous intellectual property rights for the government.
- Has a published application programming interface.
- Can work with external capabilities to provide an end-to-end pipeline.
- Data preparation time.

None of the candidate core systems had all four of the desired system capabilities. The choice was decided by the one candidate core system that provided a will-to-fight capability while scoring well in the other criteria. Once the core capability was identified, it was paired with other tools that offset the capability shortfalls, in this case patterns of life, content generators, and an internet emulator. When possible, systems with government purpose rights were used.

Concept research included doctrine, social-cyber maneuvers, and autonomous agents (bots) as force multipliers. A short summary of these are concepts are below.

- **Army Techniques Publication (ATP) 5-0.6 Network Engagement June 2017.** Provides doctrinal guidance on conducting network engagement activities in the operations process. Guidance changes the Commander's focus from attacking threat networks to identifying, defining, and interacting with friendly and neutral networks, while simultaneously engaging threat networks. Network engagement activities are supporting human networks, influencing human networks, and neutralizing human networks (Headquarters, Department of the Army, 2017).
- **ATP 3-57.30 Civil Network Development and Engagement February 2023.** Civil Affairs forces develop and engage civil networks to achieve situational understanding, integrate military and civilian capabilities in unified action, and leverage local resources to provide effects that support specific lines of effort, end states, and goals of the Commander (Headquarters, Department of the Army, 2023b).
- **Army Doctrine Publication (ADP) 3-13 Information November 2023.** Defines information advantage as "a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant

actor behavior" (Headquarters, Department of the Army, 2023a). The framework includes five information activities: enable, protect, inform, influence, and attack, set in the context of multidomain operations (MDO).

Actors use social-cyber maneuvers to achieve influence objectives. The market research included the social-cyber maneuvers below.

- **Dismiss, Distort, Distract, and Dismay (4Ds) Framework.** Developed in 2015 by Ben Nimmo, the director of investigations for network analysis and a former North Atlantic Treaty Organization press officer.
- **Actors, Behaviors, Content, Distribution, and Effect (ABC[D][E]) Framework.** The ABC framework, initially developed by Camille François and the Berkman Klein Center for Internet and Society, highlights three vectors of deception and online disinformation as a regulatory guide for industry responses. In 2020 Alexandre Alaphilippe expanded the ABC framework to include a D for Information Distribution (Alaphilippe, 2020), and James Pamment added E to the framework to represent the Effect of Disinformation (Pamment, 2020).
- **Disinformation Analysis and Risk Framework (DISARM).** A social cybersecurity framework created from multiple efforts. DISARM was initially based on the MITRE ATT&CK® knowledge base of adversary tactics and techniques assembled from real-world observations. In 2019 the Credibility Coalition's MisinfoSec Standards Working Group formulated Adversarial Misinformation and Influence Tactics and Techniques (AMITT). From AMITT, MITRE and Florida International University created the Structured Process for Influence Campaign Evaluation™ (SP!CE™), which generates development and decision courses of action and provides a quantifiable scoring function. AMITT and SP!CE merged to form the DISARM framework (DISARM Foundation, n.d.).
- **BEND Framework.** A social-cyber maneuver framework that includes information and network maneuvers (positive and negative) that "describe how an actor can manipulate the marketplace of beliefs, ideas, and information" (Beskow & Carley, 2019). The BEND maneuvers build on the 4Ds framework (Beskow & Carley, 2019).
- **Source, Channel, Objective, Target, Composition, Hook (SCOTCH).** SCOTCH enables researchers and policymakers to explore the underlying facets and constructs of influence, propaganda, and psychological operations (Blazek, 2021).

Bots are autonomous online accounts that interact with actors and are used as force multipliers. Bots can create or spread message content in a positive or negative manner. Bots can be a valuable tool for disseminating information and can also be the source of widespread malicious information. Bots have many forms, including representing a normal user account, amplifier bots, cyborg/trolls, coordinated bots, social influence bots, news bots, and overt bots. Bots can be a key influencer in the IE.

INFEST Digital Story Boards (DSBs), animated graphical depictions of a training task, were created and used to generate user stories and requirements. This links the user stories and requirements directly to the Combined Arms Training Strategy tasks that operational units use in training. Multiple DSBs focused on an actor or set of actors (e.g., Information Officer, Mass Communication Specialist) were created and then combined into an overarching DSB with a time sequenced event view. In addition to being useful to create user stories and requirements, the DSB also provided context to the INFEST team on what tasks needed to be trained.

INFEST user stories and requirements were derived from the DSBs, Army doctrine, and direct user engagements with warfighters, The initial set included 40 user stories and 310 requirements organized by the human, information, and physical dimensions. INFEST augmented the initial requirements set by deriving 52 IE, cyberspace, and electronic warfare threat activities from unclassified Defense Intelligence Agency military power documents and ATP vignettes about China, Russia, Ukraine, Iran, North Korea, and Israel. These user stories and requirements and cyclical warfighter engagements drive INFEST development activities. The warfighter engagements are extremely important because they focus the integration and development on the warfighters' critical user needs.

Training Audience Description

The INFEST training audience, which includes training for Information Operations (IO) practitioners (IO for IO) and training for Commanders and Staffs, Trainers and White Cells, and Tactical Commanders/Leaders, Soldiers, and the population (IO for others). The training audience includes both friendly and adversary forces and trainers. Defining the training audience was a critical step to scoping the INFEST proof-of-concept. INFEST took a broad approach to provide a tailorable capability to support different training audiences.

Commanders, Staff, and Information-Related Capabilities (IRC) practitioners perform information advantage activities in the information advantage framework (enable, protect, inform, influence and attack) and determine the effect of these activities on the population (Headquarters, Department of the Army, 2023a, pp. 2-4). This can include both friendly and adversary forces. The IRC practitioners (e.g., Public Affairs Officer, Civil Affairs Officer) train IO for IO.

Trainers and the White Cell mentor Commanders, Staffs, and Soldiers, enabling them to effectively employ information advantage activities. They also dial up or down training difficulty based on the unit's proficiency.

Friendly and adversary soldiers and Commanders operating in the tactical environment may interact with the population. They are immersed in the IE and may cause positive or negative "ripples" in the IE. They will experience the benefits and/or consequences of IO as part of tactical operations.

The population consists of the synthetic population and live players that can be role players (e.g., mayor, news agency), or represent an agency or organization (e.g., U.S. State Department). The population may interact with friendly and adversary forces. The population is also immersed in the IE and may cause positive or negative "ripples" in the IE via dynamically generated social media and other media sources (e.g., news, radio, television) content that is contextually relevant to ongoing physical and IEs.

Conceptual Approach

Figure 2 shows the INFEST conceptual approach. The activities listed below, aligned with the black-filled numbered dots in the figure, describe how INFEST will create a synthetic population and dynamic IE for a training exercise.

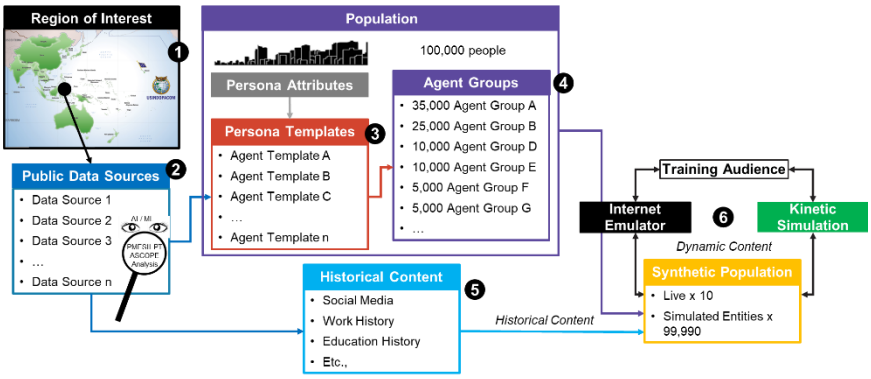

Figure 2. Conceptual Approach

Item 1 identifies a region of interest in the world. The training audience should be able to spin the globe and select any location. This step selects the region and specific location of the synthetic population to create.

Item 2 scrapes and analyzes publicly available data. Public data includes, but is not limited to, social media content, media content, internet content, dark web, census data, and other regional data sources and information. Analysis of the data provides region specific persona attributes in the human terrain.

Item 3 creates synthetic persona templates and synthetic agents. The persona attributes and data enable the creation of region-specific persona templates. The templates and data are used to create "thousands" of synthetic agents.

Item 4 assigns synthetic agents to groups to create a synthetic population. The individual agents are linked to their social (e.g., social media), work, and other networks found in the data to create groups in the synthetic population. Groups can be based on family, friends, religion, political views, etc. The synthetic population can be scaled to meet training event needs (thousands, tens of thousands, hundreds of thousands, etc.).

Item 5 uses public data to create historical context for synthetic personas. The scraped public data obtained in Item 2 is transformed using large language models to create historical content for the individual synthetic personas in the population. This will include, but is not limited to, historical social media content, work history, education history, etc. The historical content provides context to and is used to train the synthetic population cognitive model.

Item 6 creates dynamic content. Interaction between the training audience, kinetic simulation, internet emulator, and the synthetic population drives the creation of dynamic content with cause and effect traceability for the IE. For example, kinetic effects, such as collateral damage to a national monument from military operations, can result in viral social media outrage that reduces information sharing with friendly forces. Another example is when social media non-kinetic effects in the IE impact activities in the kinetic simulation. For example, analysis of social media content reveals a distributor of improvised explosive devices and the distribution facility location, which results in a physical attack on the facility and capture of the distributor.

INFEST USE CASES

INFEST Use Case Framework

Use cases were a critical component needed to drive INFEST capability development and integration. To ensure use cases were appropriate and suitable, the INFEST team collaborated with warfighters to obtain their most important user needs. From this interaction, the INFEST team developed a broad INFEST use case framework. The framework was then augmented with a tailored implementation that provided context with a description, a set of sequence flows, and anticipated effects that would be achieved. After developing the use case framework, the INFEST team followed up with warfighters to obtain feedback and adjusted the framework. The framework included use cases for utility outage, information operations, provide services, environmental, death/injury of a non-combatant, communications interruptions, information-related capabilities, will-to-fight, combatants, interrupt patterns of life, destroyed/damaged infrastructure, non-combatants, and medical.

Figure 3 shows the INFEST use cases. A list of methods is included with each use case that could be expected to cause the use case. For example, patterns of life (e.g., going to work, school, etc.) can be interrupted by migration of internally displaced people (IDP), military operations, protests, and other items.

- Information Operations
- **Interrupt Pattern of Life**
- Medical
- Information Related Capabilities
- Non-Combatants
- Combatants
- Will-to-Fight
- Death / Injury of Non-Combatants
- Destroyed / Damaged Infrastructure
- Provide Services
- Environmental
- Utility Outage
- Communications Interruption

Figure 3. INFEST Use Case Framework

Recurring Abstract User Stories

Analysis of the INFEST use case framework identified eight abstract user stories, shown below, that occurred multiple times in the different use cases.

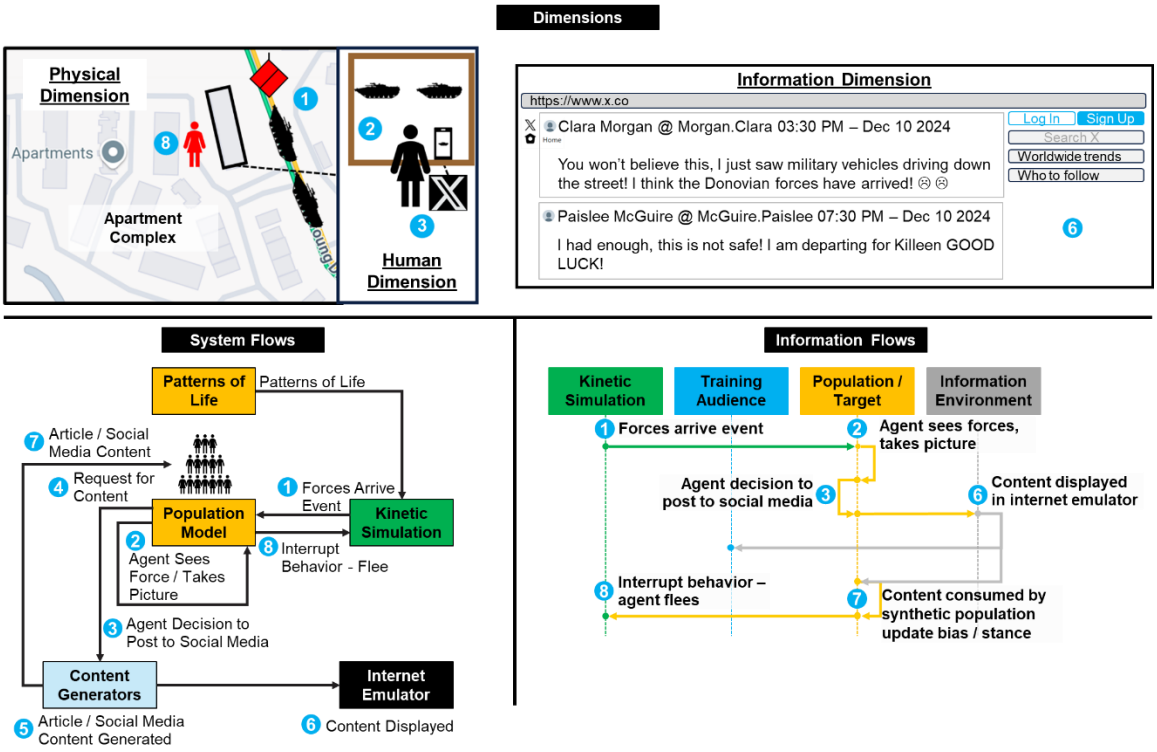

Figure 4. Interrupt Patterns of Life Internally Displaced Person Use Case

- **Pattern of Life.** A synthetic population agent executes patterns of life.
- **View.** A synthetic population agent views (is aware of) events in the kinetic simulation.
- **View – IE.** A synthetic population agent views (consumes) information in the IE.
- **React.** A synthetic population agent reacts to a simulation event.

- **React – IE.** A synthetic population agent reacts to information in the IE.
- **Sentiment.** A synthetic population agent uses kinetic simulation event information to alter sentiment.
- **Sentiment – IE.** A synthetic population agent uses information in the IE to alter sentiment.
- **Post Social Media/News Article.** A synthetic population agent uses kinetic simulation event information to create a social media post or article.

INFEST Interrupt Patterns of Life Internally Displaced Persons Use Case

Tailoring sets the use case in the context of a training scenario. In this example, the use case is described as thousands of IDP that are forced to flee their homes due to an invading force and are moving to the west into a nearby city to a government-operated IDP camp. Events (physical/ informational) are then injected into the simulation to obtain the desired effects for the training event. The events can be preplanned in the simulation, occur dynamically as an outcome of operations in the simulation, or be dynamically caused by the population model as a synthetic population behavior or physical event. Both physical and information events can trigger the system flows between the capabilities and information flows. Figure 4 (see next page) shows the interaction of the physical, human, and information dimensions; system flows between the capabilities; and information flows between the dimensions. The numbered dots in the figure align to the eight events listed below and correlate to activities in the dimensions, system flows, and information flows. Not in this example, but ongoing, are patterns of life (e.g., go to work).

Item 1, which triggers this thread, is caused by a system flow from the kinetic simulation. The kinetic simulation publishes the "forces arrive" physical event message that the population model subscribes to. An information flow is sent to synthetic population agents that are in the vicinity of the forces. This results in some of the synthetic population agents in the human dimension being aware of ("seeing") the forces arrive.

Item 2 is an effect of seeing the forces arrive. Based on the attributes of the synthetic agents that see the forces arrive, some synthetic population agents decide to take a picture of the arriving forces. This is an internal action of the population model (system flow) that results in an internal message to specific synthetic population agents to take a picture (information flow), as shown in the human dimension. This is enabled by the population model subscribing to the kinetic simulation unit position updates.

Item 3 is also an effect of seeing the forces arrive. Again, based on the attributes of the synthetic agents that see the forces arrive, some synthetic population agents decide to post a social media message about the forces arriving. This is an internal action of the population model (system flow) that results in an internal message to identified synthetic population agents to post a social media message, as shown in the human dimension.

Item 4 is an effect of the synthetic agents in the population model deciding to post to social media. The population model publishes a "request for content" (system flow) that includes the synthetic agent identification (who), a topic (what), their stance (slant), and the posting media type (e.g., social media X/Twitter account). This results in an information flow to the content generators that subscribe to the request for content.

Item 5 is an effect of the request for content. This is an internal action of the content generators (system flow). The content generators use the information in the request for content to generate content. This can be a long form (article) or short form (social media post). In this example an X post is created.

Item 6 is a system flow from the content generator to the internet emulator, the publication of the generated content that is then displayed on the internet emulator. This results in an information flow to the live training audience who can read the X post in using the internet emulator and when appropriate scrape the data for analysis.

Item 7 is a system flow from the content generators to the population model. The population model subscribes to the published X content. This results in an information flow to the appropriate agents in the synthetic population as data so it can be consumed and impact the individual synthetic agents' bias and stance.

Item 8 is an effect of the updated agents' bias, stance, and persona attributes. When thresholds are attained, the population model publishes an "interrupt behavior" message for identified agents to flee for safety (system flow). This includes the agent identification (who), the behavior (e.g., flee), and the location to flee to. The kinetic simulation subscribes to the "interrupt behavior" and begins movement of the identified agents to the location they are fleeing to. Agents can flee on foot or use transportation methods available to them in the kinetic simulation (e.g., car). This is viewable by the training audience (human dimension) as individual agents moving in the simulation.

PUTTING IT ALL TOGETHER

Technical Approach

Figure 5 shows the INFEST technical approach, which is a Modular Open Systems Approach (MOSA). The approach enables functional capabilities and simulations to be exchanged and/or added by conforming to or modifying the data model in the INFEST STE MSSV extension.

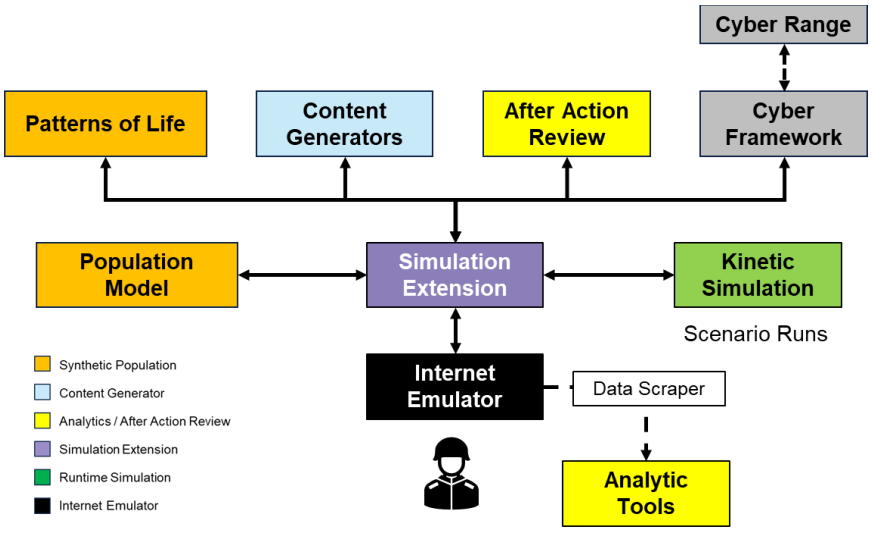

Figure 5. Technical Approach

Functional capabilities are in color-coded boxes where:

- Orange boxes are synthetic population capabilities, the population model and patterns of life generator.
- The blue box is the content generators; short (e.g., social media posts) and long form (e.g., news articles, leaflets).
- The black box is the internet emulator; the live audience can read media content and scrape data for analysis.
- Yellow boxes are analytic tools and After Action Review capabilities.
- The grey boxes are cyberspace capabilities. This includes a cyber framework that can connect to external cyber effects and cyber ranges (e.g., the Persistent Cyber Training Environment).
- The green box is the kinetic simulation - STE MSSV/OPSIM. OPSIM is where the scenario runs are simulated.
- The purple box is the INFEST STE MSSV extension (e.g., middleware). This is the data model that enables the functional capabilities to communicate and exchange data with each other.

Bi-directional Cause and Effect

Below are four bi-directional cause and effect examples that INFEST addresses:

Training Audience Kinetic Effect Thread. The cause in this thread is a training audience physical event (kinetic operation; maneuver, fires, etc.). The agents (friendly or adversary forces, civilians, bots, etc.) in the synthetic population are aware of the kinetic operation through direct observation or by consuming media content. The result is an effect where the agents act in the IE. This can be a force side information advantage activity, individual agents' social media posts, news interviews and articles, radio and television broadcasts, or bot operations that impact other synthetic agents and the training audience.

Training Audience Information Effect Thread. The cause in this thread is a training audience information activity that reaches the synthetic population and/or the targeted segment of the population. The result is an effect where the agents in the synthetic population take some action in the IE. This can be a force side information advantage activity, individual synthetic agents' social media posts, news interviews and articles, radio and television broadcasts, or bot operations that can impact other synthetic agents and the training audience.

Synthetic Population Kinetic Effect Thread. The cause in this thread is synthetic population behavior that results in physical events. The physical events include fleeing, protesting, executing patterns of life, and simulated forces maneuvers or artillery fires. The population model's cognitive model publishes a message that the simulation subscribes to resulting in physical actions occurring in the simulation. The training audience can see the event in the simulation viewer and the synthetic population will be aware of the event after the simulation publishes the event message. The result is an effect where the training audience and/or the Opposing Forces (OPFOR) conduct military operations such as employing military police forces to assist people fleeing or to control a protest. The training audience and the OPFOR can also conduct information advantage activities to influence the events; for example, posting messages and articles, and broadcasting instructions for people fleeing and consequences for violent protests.

Synthetic Population Information Effect Thread. The cause in this thread is a synthetic population information activity that reaches other synthetic population agents and the training audience. The training audience can view the information activities using the internet emulator and can perform analysis of the scraped data. The effect is when the training audience responds with physical events in the simulation and/or act in the IE.

Feedback and User Needs

The INFEST team strives to steer INFEST development to maintain warfighter relevancy. Direct engagement with warfighters elicits their training challenges, user needs, and requirements for training information advantage activities in an MDO environment. Distribution of feedback forms and the question and answer period at the end of each quarterly demonstration provides feedback on existing capabilities and provides ideas for new capabilities.

Employment Considerations

A goal for INFEST is to support a warfighter, command post exercise, or home station training event in 2027. This will enable the INFEST team to obtain warfighter feedback in the context of a training event, like a Soldier Touch Point and would provide value by eliminating white cards that current training simulations use to stimulate the training and minimize the need for role players. Three ways to support training events include:

Stand Alone. This is the easiest, lowest amount of effort, and lowest-risk method to support a training event; however, it provides the least training value. INFEST will not interact with the simulation used for the training event. INFEST will use the current synthetic population, scenario, terrain, and use cases to support the training event.

Aligned. This is a moderate amount of effort and a low-risk method to support a training event that provides more training value. INFEST will not interact with the simulation used for the training event. However, the INFEST synthetic population, scenario, and use cases will be developed to match what is used in the training event (aligned). Because of classification issues and terrain availability, INFEST will use the best available terrain, which may not match the training event. The INFEST events will unfold as if they were integrated into the training event.

Integrated into Event. This is a large amount of effort and highest-risk method to support a training event that provides the most training value. INFEST is employed on the same network as the training event and is exchanging data with the simulation used in the training event. This would require that INFEST has appropriate Security Implementation Guides (STIGs) and an Authority to Operate (ATO) on the network; both present challenges to INFEST. INFEST is investigating STIGs to accelerate achieving an ATO when INFEST transitions to a program.

CONCLUSIONS AND WAY AHEAD

Summary

As the modern battlespace extends into the cognitive and informational realms, military preparedness must evolve. INFEST emerges not just as a training innovation, but as a strategic imperative – addressing a critical shortfall in how warfighters are prepared for OIE. By fusing psychological realism with information flow dynamics, INFEST offers a simulation environment where perception, influence, and truth are as consequential as kinetic actions.

The urgency is underscored by China's military doctrine, which prioritizes cognitive dominance as a key objective: "Seizing mind dominance in the cognitive domain and subduing the enemy without fighting is the highest realm of warfare" (U.S. Department of Defense, 2024, p. 37). This is a broader strategy centered on achieving information superiority and shaping global narratives in their favor; enabled by "intelligentized warfare" that integrates artificial intelligence, psychological operations, and cyber capabilities (U.S. Department of Defense, 2024, p. 93).

INFEST meets this challenge by doing more than just simulating outcomes; it transforms the training paradigm. By eliminating the use of white cards, INFEST ensures that information effects are generated using simulation dynamics,

not manual adjudication. This preserves immersion and promotes authentic decision making. Furthermore, the reduction of role players and the reduced time required to generate input content significantly increase training efficiency, allowing for more frequent and scalable exercises without compromising fidelity.

In a world where disinformation spreads faster than bullets and perception can decide the victor, INFEST provides the U.S. military with a decisive edge. It fosters judgment, adaptability, and ethical clarity necessary to fight and win in the information domain. As the Department of Defense faces the pacing challenge posed by China's expanding military capabilities (U.S. Department of Defense, 2024, p. VI), tools like INFEST are essential.

INFEST's MOSA is a flexible approach that is not tied to a particular capability. Being tailorable, INFEST will meet the needs of multiple different training audiences. INFEST's information and cyber non-kinetic effects will provide warfighters and trainers with an adaptable MDO capability that enables training in the physical, information, and human dimensions simultaneously, resolving existing training shortfalls. Integration of INFEST capabilities with the Army's STE MSSV protocol will also provide value to the wargaming, experimentation, and analytic communities.

Cause-and-effect traceability between kinetic events and non-kinetic information and cyber events enables training. INFEST includes complexities that real-world operations encounter, such as congestion and IDP movement, military deception, electronic warfare, cyber and information advantage non-kinetic effects, and patterns of life, that increase training realism. INFEST will reduce the need for white cards that supplement limitations with current simulations.

INFEST is working toward a low overhead capability. It automates synthetic population social media account creation and content generation. The use of synthetic population influencer/spokesperson agents can supplement or replace the need for live role players. INFEST also includes capability that will reduce the time needed to produce input content.

A practical application of INFEST is to run the scenario for months during the pre-competition phase. This will provide multiple benefits, including shaping world and regional opinion, influencing will-to-fight, and setting the IE conditions at the start of the competition phase when the forces deploy for operations creating realism for the training audience.

Future Plans

INFEST plans include Application Programming Interface (API) development; creation of an information advantage interoperability standard; and the development of INFEST scenario generation, White Cell Dashboard, and AAR capabilities. These areas are addressed below.

API Development. INFEST currently uses both API and manual file exchanges. To minimize/eliminate manual file exchanges INFEST is exploring point-to-point virtual private network connections and using containers in both the Training Resource Management Center and CyWar-T laboratory environments.

Information Advantage Standard. The INFEST team will engage the Simulation Interoperability Standards Organization to propose a study group that could lead to a product development group to create an Information Advantage (IA) Data Exchange Model (DEM). The INFEST STE MSSV extension data model would help accelerate the creation of an IA DEM. An IA DEM would assist the community in creating interoperable capabilities.

Scenario Generation Capability. INFEST is developing a scenario generation wireframe that when transformed into working software will enable the training audience and trainers to upload, modify, or create an information advantage plan for their training event. Primarily used to establish the plan in the simulation during the plan/prepare phases, it will also provide a capability for a White Cell to approve assets controlled by the unit's higher headquarters and to implement changes during simulation runtime. This can help dial up or down the training difficulty to better align to the unit's training proficiency.

White Cell Dashboard Capability. INFEST is developing a White Cell Dashboard wireframe that when transitioned into working software will provide the White Cell with multiple metrics to gauge how the training unit is progressing. For example, the dashboard will include the ground truth of the synthetic population's bias and sentiment. This will enable the White Cell to gauge the effectiveness of the training unit's information advantage activities and provide feedback to coach and mentor the training unit to help it achieve a higher level of training readiness.

After Action Review Capability. A training event is not complete without an AAR to help the training audience learn what was done well, what could be done differently, and what needs improvement. INFEST plans to develop an AAR wireframe. When transformed into working software, this capability will augment current AAR capabilities by bringing in the cyber and information advantage non-kinetic effects into the discussion.

REFERENCES

Alaphilippe, A. (2020, April 27). *Adding a 'D' to the ABC disinformation framework.* Retrieved February 29, 2024, from Brookings: https://www.brookings.edu/articles/adding-a-d-to-the-abc-disinformation-framework/

Beskow, D. M., & Carley, K. M. (2019, March-April). Social cybersecurity: An emerging national security requirement. *Military Review*, pp. 123-125.

Blazek, S. (2021, May 24). *SCOTCH: A framework for rapidly assessing influence operations.* Retrieved February 29, 2024, from Atlantic Council: https://www.atlanticcouncil.org/blogs/geotech-cues/scotch-a-framework-for-rapidly-assessing-influence-operations/

DISARM Foundation. (n.d.). *A brief history of DISARM*. Retrieved February 29, 2024, from DISARM Foundation: https://www.disarm.foundation/brief-history-of-disarm

Headquarters, Department of the Army. (2017). *ATP 5-0.6 network engagement.* Washington, D.C.: U.S. Army.

Headquarters, Department of the Army. (2023a). *ADP 3-13 information.* Washington, D.C.: U.S. Army.

Headquarters, Department of the Army. (2023b). *ATP 3-57.30 civil network development and engagement.* Washington, D.C.: U.S. Army.

Pamment, J. (2020, September 24). *The EU's role in fighting disinformation: Crafting a disinformation framework.* Retrieved February 29, 2024, from Carnegie Endowment for International Peace: https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720

U.S. Department of Defense. (2024). *Military and Security Developments Involving the People's Republic of China 2024 Annual Report to Congress.* Washington, D.C.: U.S. Department of Defense.