

Combat Simulation to Support the Conceptual Design of Equipment for the Soldier System

Vikram Mittal¹^a, Graham Webb², Jackson Steiner², Luke Shriver² and Sierra Butcher²

¹Department of Systems Engineering, United States Military Academy, West Point, U.S.A.

²Army Cyber Institute, West Point, U.S.A.

Keywords: Combat Modelling, Cyber Capabilities, Soldier Systems.

Abstract: Simulation will play an increasingly important role in designing future equipment for soldiers. The complex operational environment necessitates that the soldier be treated as a system. A soldier system can be defined as a soldier using equipment to complete a mission. Though it is often difficult to capture the mission aspect of the system, constructive combat simulation provides a technique for testing out new equipment on a soldier early in the system design lifecycle. Though combat simulations have historically been used primarily for training purposes, they can be readily modified for analysis of new military capabilities. Additionally, these simulations can be modified to reflect the changes in physical and cognitive load associated with these new capabilities. This paper outlines a methodology for using combat simulation to perform analysis of new capabilities for the soldier system. A case study is then presented to perform a trade space analysis on different tactical-cyber capabilities given to dismounted soldiers. Using the Infantry Warrior Simulation (IWARS), the case study quantified changes in soldier survivability and lethality with the addition of new technologies.

1 INTRODUCTION

Ground combat will always play a decisive role in future conflicts. And as mission sets continue to become more complex, so must the soldier. The soldier is no longer a person with a helmet and a gun standing on a volley line, shooting at an enemy. Rather, the soldier is part of a complex system, where they use an array of cutting-edge technology to maintain a tactical advantage in a combat scenario.


As new technology gets introduced into this *soldier system*, systems level analysis is required to ensure that the technology provides the soldier with the required capabilities without producing negative consequences. This analysis requires the ability to assess the usage of the new equipment in a relevant operational environment. Combat simulation provides the ability to perform this analysis early in the conceptual phase, allowing for the determination of design requirements for new equipment. Several challenges exist with this approach, especially that these simulation packages are typically developed for training purposes and do not readily allow for the integration of new equipment.

This paper presents a methodology to use combat simulation to analyse changes to the soldier system. It then presents a case study that evaluates different tactical-cyber equipment. This analysis includes accounting for change in physical and cognitive overloading associated with these different capabilities.

2 CHALLENGES OF DESIGNING MILITARY EQUIPMENT

2.1 The Soldier System

In ancient armies, soldiers were given uniforms, protective equipment, weapons, and sustenance. As technologies advanced for one individual component, it was simply swapped out, such as the iron age resulting in the weapons changing from bronze. However, the equipment set currently carried by soldiers is significantly more advanced, creating a complex system with numerous interrelationships. As

^a <https://orcid.org/0000-0003-2485-2366>

such, the design of military equipment requires a systems-level design approach.

The systems architecture for the soldier-system, as shown in Figure 1, consists of three components: the soldier, their equipment, and the mission to be completed. This architecture leverages the Soldier System Enterprise Architecture by the Natick Soldier Research, Development, and Engineering Center (McDonnell, 2015). The equipment alone is just a set of inanimate objects; however, when coupled with a soldier, the soldier and equipment form a relationship that allows them to complete a mission. A systems analysis requires understanding the internal properties of each component and the interactions between components. These interactions create emergent effects that must be accounted for to fully characterize soldier performance.

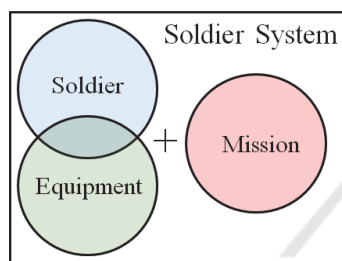


Figure 1: The soldier system defined as a soldier using their equipment to perform a mission.

2.2 System Level Analysis

Although the soldier system, as depicted in Figure 1, appears somewhat straightforward, it is difficult to actually understand all the different interactions and relationships related to the addition of a new piece of equipment. The interaction between the new piece of equipment and the user, indicated by the overlap in the Venn Diagram in Figure 1, can be understood through a standard usability assessment. However, the interaction between the soldier using the equipment to perform the mission, indicated by the plus sign in Figure 1, is difficult to analyze. This analysis becomes exceedingly difficult when the new equipment is still in the conceptual phase.

For example, suppose that the Army is considering replacing their existing body armor with a slightly heavier armor material that provides substantially more protection. However, in an urban environment, even a small increase in weight will result in the soldier moving significantly slower. In turn, the enemy soldiers can more accurately shoot the slower moving soldier, allowing them to shoot the soldier in an unarmored location, resulting in an overall decrease in survivability. This analysis would

be difficult to perform without actually developing the body armor and testing it in an operational environment. Even if the armor is developed, no commander would agree to having their soldiers carrying unproven equipment in combat.

2.3 Physical and Cognitive Loading

The largest negative emergent property from the addition of new equipment is related to physical and cognitive loading. Ideally, soldiers would be given every possible capability to aid in destroying their enemy. However, soldiers are already carrying over 100 lb of equipment consisting of weapons, armor, ammunition, food, water, and electronics (Mittal, 2019). Since soldiers are already carrying close to their maximum load, any additional equipment will displace equipment currently carried. If this displacement comes from batteries, water, or food, the maximum duration of the mission must decrease.

In addition to carrying a large amount of equipment, the soldiers must be able to operate it. The new electronics on a soldier includes radios, navigation tools, computers, minesweepers, and robots. Soldiers are expected to operate all of this equipment while “keeping their head on a swivel” and “scanning their sector.” Modern combat in urban environments, where soldiers must detect and identify enemies in a crowd, imposes a significant cognitive load on soldiers. As such, any new equipment must not significantly increase the cognitive loading on the soldier (Shanker & Richtel, 2011).

3 COMBAT MODELING

3.1 Overview of Combat Models

Combat simulation provides the capacity to test new equipment in an operational setting, albeit, both the equipment and operational setting are simulated (Washburn & Kress, 2009). The military divides combat simulation into three categories—live, virtual, and constructive. Live simulations use real soldiers with real equipment in a simulated environment, such as a training site. Virtual simulations involve real soldiers using virtual equipment in a virtual environment, similar to a video game. Constructive simulations employ virtual soldiers using virtual equipment in a virtual environment (Hodson, 2017).

Each type of simulation can play a role in developing, evaluating, and testing requirements at various stages in the system lifecycle. Live and virtual

simulations require that the system already be prototyped. As such, these simulations aid in system validation and assessing the overall system usability.

Meanwhile, constructive simulations allow for modelling a virtual soldier using virtual equipment in a simulated environment. Since the soldiers are virtual, their capabilities can be readily augmented to reflect the addition of new equipment even if the equipment has not been designed or built. Therefore, constructive simulations are inherently useful for systems still in their conceptual phase, such as those used in this analysis.

Indeed, constructive simulation is used for equipment design in a number of industries to include medical devices, automotive, and consumer products (INCOSE, 2015). Additionally, constructive simulation is used for larger defense applications. However, its usage has been fairly limited for analysis of the soldier system (Hill & Miller, 2017).

3.2 Limits of Modelling New Technologies

Though a range of constructive combat modeling programs are available, most of them are not intended for analysis; rather they are developed for training (Tolk, 2012). In particular, these software packages are used as part of larger live training events to simulate events occurring elsewhere in the battlefield. For example, a brigade will be performing a mission at the National Training Center as part of a larger overall division-level mission. The other brigades on the battlefield are simulated with the results of the simulation influencing the mission of the real unit.

Since these simulation packages are not designed for analysis, they do not readily allow for the addition of new equipment (Tolk, 2012). For example, many of these simulation packages would not readily have the capacity to model novel technologies such as an exoskeleton or adaptive camouflage patterns.

Additionally, the methodologies that underly the simulations are based on fundamental military doctrine where soldiers and units shoot, move, and communicate. The addition of new technology can substantially change these methodologies. For example, shooting algorithms rely on detecting a target, identifying that the target is an enemy, orienting towards the target, shooting the target, determining where the bullet strikes the target, and then determining the damage done from the hit. The addition of a threat recognition system would change this process because the soldier would no longer need to identify the target as an enemy; rather, the new system would automate that process for the soldier.

4 METHODOLOGY

Figure 2 displays a methodology for using combat simulation to analyse different performance metrics related to future military technology. This process is applicable to all military technology; however, it is tailored to those technologies that are still in the conceptual phase that will result in substantial changes in how soldiers operate.

Similar to any type of systems analysis, the first phase is to define the problem. This phase starts by defining a set of relevant missions for a given soldier. These mission sets can be found in military doctrine. These missions are then modelled in a simulation package to provide a baseline set of performance metrics for this analysis. These simulations can achieve some level of validation through comparison to performance data from training sites.

The performance metrics from the systems-level analysis provide insight into problems that need to be solved. Typically, these metrics are survivability and lethality, with the goal that a new technology increases the ability of a soldier to kill their enemy and/or decrease their likelihood of being killed by the enemy (Washburn & Kress, 2009). Another common metric is mission success rates, which is the percentage of time that the soldiers can complete their mission.

The second step of the process is to identify a technology that will solve the problem identified in the first step by improving the relevant performance metric. The researcher then needs to understand how the new technology will be implemented into the combat scenario. They also need to determine how it will change the individual soldier's physical and cognitive loading, since any new equipment will result in changes in these parameters. Finally, it is necessary to identify how the technology will change a soldier's skills. For example, the new technology could reduce target acquisition time, make them shoot more accurately, move faster, or have an increased knowledge state about the battlefield.

The third step in the process is to perform the operational analysis. The operational analysis requires modifying the combat simulation to reflect the new technology. For example, the soldier may change their actions based on the information provided by a new piece of equipment. In another case, the soldier may simply execute their mission faster because they are carrying a lighter load.

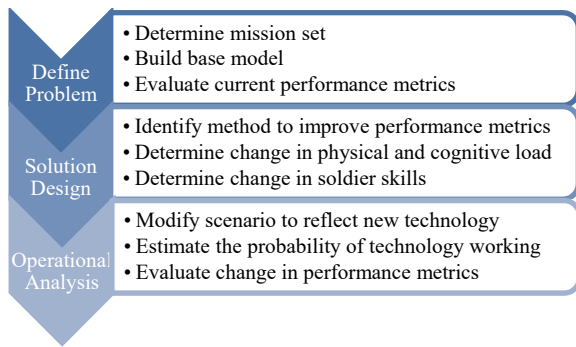


Figure 2: Methodology for performing a soldier system analysis using combat simulation.

5 CASE STUDY: TACTICAL CYBER CAPABILITIES

The methodology presented in Section 4 was specifically designed to support a study on tactical cyber capabilities for the United States Army. These capabilities are expected to play a key role in future small unit operations.

5.1 Define Problem

5.1.1 Base Scenario

Though the full span of Army mission sets is vast, this analysis is limited to those performed by small infantry units at the squad or platoon level. *FM 3-21.8: The Rifle Infantry Platoon and Squad* gives four common mission types performed by such a unit (Headquarters, Department of the Army, 2016). These mission types include:

- Raid: fast kinetic movement into an area to engage a known enemy.
- Ambush: setting a stationary trap for an enemy, then engaging when they are vulnerable.
- Combat patrol: movement through an area to find and engage enemy targets.
- Destroy bunker: engaging a fortified enemy position.

These four missions become more complex if they are performed in an urban environment. First, enemy targets are harder to detect and identify because they are blended in with civilian non-combatants. Additionally, urban combat involves multiple levels (i.e., underground sewage systems, ground level, multiple story buildings). Moreover, the buildings in urban environments provide opportunities for cover

and concealment for both forces; meanwhile, the buildings limit movement down canalized pathways.

5.1.2 Infantry Warrior Simulation

The Infantry Warrior Simulation (IWARS) is a constructive, force-on-force, combat simulation that focuses on small-unit operations. The primary IWARS simulation objects are intelligent agents that are semi-autonomous, which allows for realistic modeling of soldier and unit behaviors. The methodologies that underly IWARS are stochastic, such that the simulation must be run numerous times to get a range of output parameters to include measures of survivability and lethality (Samaloty, Schleper, Fawkes, & Muscietta, 2007).

IWARS was selected for this analysis because it models individual soldiers conducting squad to platoon size operations. Tactical cyber capabilities are focused on units at this echelon. Other more common simulation platforms aggregate individual soldiers into units, not allowing for an accurate modeling of soldiers with augmented capabilities (Page, 2016).

An IWARS model is developed by placing blue (friendly), red (enemy), and green (civilian) forces onto a map. Each agent is assigned movement paths, behaviors, and equipment, which then allows them to perform a set of tasks that constitute their mission. The behaviors can get very complex and are often based on the actions of other agents in the scenario. The performance of the soldier and their equipment is captured through a parameterized database that can be edited to reflect new capabilities. Screenshots of IWARS is shown in Figure 3. The top image shows the top-down view of a blue unit moving into a town to clear the town of red forces. The bottom image displays the 3D image for the agents shooting at the intersection in the center of the right image.

The four missions were modeled in an urban environment using IWARS. In all four cases, a small unit of blue soldiers is conducting an operation against ten red soldiers. The raid mission has a platoon of blue forces sweeping into the town from the north to find and kill the red forces that are entrenched in the buildings. The ambush mission has a blue force establishing an L-shaped ambush at a crossroad in the center of the town. The combat patrol has a blue force being ambushed by red forces and then counter-attacking the red forces. The bunker mission has the blue forces moving into the town, get pinned down by a bunker, and then executing the battle drill to destroy the bunker.



Figure 3: Screenshots of IWARS. Top-down view of raid scenario showing blue forces moving south into a town (top). Three-dimensional view of friendly and enemy soldiers at the intersection in center of town (bottom).

5.1.3 Current Performance Metrics

The metrics of concern for this analysis are survivability and lethality. These two metrics are typically used qualitatively to describe the effect of adding new equipment into the soldier system; however, with combat modelling, these metrics can be defined quantitatively. The survivability metric is defined to be the percentage of blue forces (i.e., friendly soldiers) that survive a mission, and the lethality metric is set as the percentage of red forces (i.e., enemy soldiers) killed during a mission.

Table 1 displays the survivability and lethality metrics for the four mission sets. Each scenario was run 100 times to provide a desired relative precision of 5 percent. Table 1 indicates the following:

- **Raid:** The blue forces outnumber the red forces by a factor of 3 allowing them to overwhelm the red forces. However, the blue forces incur a high death toll because the red force is in a defensive, fortified position.
- **Ambush:** The red forces have the element of surprise, resulting in low survivability and lethality metrics for the blue forces.
- **Combat patrol:** The combat patrol has equal numbers of red and blue forces on the move, with neither side having a solid defensive posture; as such, both groups impose similar casualties.

- **Destroy bunker:** The destroy bunker mission has a fairly high blue casualty rate, though the red casualty rate is higher.

For all four scenarios, the survivability metric can be significantly increased with the overall goal of achieving a score of 100, which indicates that no soldiers were killed during the mission. The results indicate that across the scenarios, approximately half of the blue forces die in each scenario. One method of increasing the blue survivability is to increase their lethality. If the blue forces can kill the red forces faster, the red forces will impose less damage on the blue forces. The outputs from the models indicate that there is an opportunity to increase blue force lethality.

Table 1: Survivability and lethality metric scores for each of the four baseline combat scenarios.

Mission Type	Survivability		Lethality	
	Average	St. Dev	Average	St. Dev
Raid	56.6	8.0	88.3	8.0
Ambush	34.4	13.9	52.2	14.9
Combat Patrol	45.0	13.2	56.7	20.9
Destroy Bunker	44.2	11.6	76.8	14.0

5.2 Solution Design

5.2.1 Tactical Cyber Capabilities

The rapid growth of the consumer electronics market provides numerous opportunities for technologies that can increase a soldier's lethality, and hence survivability. Advances in fields such as artificial intelligence, augmented reality, cloud-computing, and micro-electronics can translate into game-changing military technology (Wilson, 2016). Meanwhile, enemy soldiers are carrying more electronics that are vulnerable to a cyber-attack (Almohammad & Speckhard, 2017). This combination of events creates the potential for a new set of *cyber weaponry* that will provide soldiers a tactical edge, potentially increasing their survivability and lethality (Porche, et al., 2018).

Though cyber weaponry is typically considered a strategic level asset, many offensive cyber capabilities have trickled down to the tactical, small-unit level (Brantly & Collins, 2018). Similar to strategic cyber weaponry, tactical cyber weaponry allows dismounted soldiers to detect and exploit an enemy's communication channels. Since the full range of possible tactical-cyber-attacks is very broad, this study limits itself to looking at four types of tactical cyber-attacks. These four tactical cyber-

attacks were selected because they encompass a broad range of different capabilities. Additionally, they represent capabilities that are already fielded or under development.

The first tactical cyber-attack is a localized attack on the electric grid. Individual buildings are connected to the larger electric grid with numerous communication pathways (Congressional Research Service, 2018). These communication channels can be exploited to deny electric services to a building. This would disrupt the enemy by throwing them into a set of disarray. Additionally, if the attack is at night, the enemy would lose the ability to use lights.

Another tactical cyber-attack involves the use of radio frequency (RF) triangulation. If friendly forces know the radio frequencies associated with an enemy combatant, they can triangulate and track its position (Liu, Zhang, Su, Li, & Xu, 2013). This type of exploitation allows the soldier to observe the enemy beyond line of sight while also getting positive identification through their radio signals.

A third tactical cyber-attack is communication denial, also known as jamming. Since communication is done simply through sending radio signals through the air, the signal can be lost if the noise thresholds are increased. This can be achieved by simply pushing a large amount of radio frequency noise into the environment. This type of tactical cyber-attack does not allow the enemy to synchronize efforts.

The fourth tactical cyber-attack is communication intercepting. If the enemy forces are communicating over an unencrypted network or if the encryption key is known, friendly forces can intercept the enemy's communication, hence gaining new intelligence. This information allows friendly forces to observe enemy forces from a further range.

5.2.2 Physical and Cognitive Load

The different tactical cyber capabilities will impose a different amount of physical and cognitive loading on soldiers. To analyze the different physical loadings, it is useful to break the capabilities into two categories: active and passive (Shirey, 2000). Active implies that signals are being transmitted to disrupt the enemy's communication channels. Passive implies that the system is simply ingesting the enemy's communication channels and processing the results.

The localized grid attack and communication denial capabilities require active devices. These devices would impose a higher physical load on the soldier since the system must transmit signals, which is power intensive. A simple radio requires 10 W of power, associated to 1 lb of batteries for 10 hours of

operation. Jamming devices can require 100 W of power, requiring 1 lb of batteries for each hour of operation (Leemans & Mittal, 2018).

Passive devices would be required for RF localization and communication intercept. These devices require significantly less power since they are simply collecting radio signals. However, upon collecting the signals, the results must be analyzed which does require power. A normal computer for analyzing these results would require approximately 10 W of power, although triangulating a position would require significantly less power than decrypting and analyzing communication data (Leemans & Mittal, 2018). Though there are less heat concerns for passive devices, they often require bulky antennae that can operate at multiple wavelengths.

The cognitive load on a soldier from the devices would be based on how much human input is required for the capability. At the low end, communication denial would require minimal human input outside of turning on the device. RF localization imposes a slight cognitive loading on the soldier since they are provided with additional information, although the use of Augmented Reality can reduce this cognitive load. A localized grid attack would require significantly more human input since the soldier would be required to work around the different safeguards. Meanwhile, communication intercept would incur a large cognitive load on the soldier since they must make sense of whatever information they receive and process what is important.

5.3 Operational Analysis

5.3.1 Incorporation of Tactical Cyber

Each model was modified to reflect the addition of each of the four tactical cyber capabilities. Since IWARS does not inherently have these capabilities built in, each capability had to be incorporated through changing certain model attributes and soldier behaviors. The localized grid attack capability was incorporated by increasing the confusion and acquisition times for red agents inside the relevant structures. The RF localization capability was modeled by continuously giving the blue agents the knowledge of red force locations. IWARS provides the capability for communication denial through decreasing the probability of a successful communication transmission. The communication intercept capability was modeled by changing the blue forces mission to reflect intelligence about enemy plans.

The physical load associated with the devices can be integrated into the simulations by increasing the overall load and reducing the speed associated with soldier movement. Additionally, the cognitive load can be integrated by slowing reaction times, reducing their field of view, and including head-down time.

5.3.2 Scenario Results

Each of the four scenarios were rerun with the incorporation of each of the four different tactical cyber capabilities. Table 2 displays the survivability score for each run, and Table 3 displays the change in lethality score. The items in bold indicate a substantial improvement from the baseline.

The results indicate that there was only a marginal increase in the lethality metric in most of the mission sets. For the most part, the simulations represent doctrinal missions consisting of battle drills that are intended to make the blue forces fairly effective at killing the red forces. As such, the new capabilities logically only provide marginal benefit in regard to the number of red soldiers killed. However, further analysis found that the blue forces were able to kill the red forces earlier in the scenario.

As such, each of the new capabilities provided a significant increase in survivability in at least one of the mission sets. The RF localization capability increases blue survivability for the raid and combat patrol, by allowing the blue forces to avoid traps and “fatal funnels” set by the red forces. Other capabilities, such as communication denial provided an increase in survivability by putting the red forces into disarray and hindering their ability to coordinate an attack. The communication intercept and localized grid attacks also provide an increase in survivability; however, these increases are limited.

Table 2: Survivability metric for each of the 4 combat scenarios for the four different tactical cyber capabilities (italicized number is the +/- 95% confidence interval).

Mission Type	Base	Grid Attack	RF Local.	Comm Denial	Comm Int.
Raid	56.6	55.5	82.6	67.9	72.9
	<i>±1.6</i>	<i>±2.1</i>	<i>±1.0</i>	<i>±0.6</i>	<i>±0.8</i>
Ambush	34.4	30.7	56.1	38.7	48.7
	<i>±2.7</i>	<i>±2.7</i>	<i>±3.1</i>	<i>±2.8</i>	<i>±3.0</i>
Combat	45.0	42.0	73.4	67.2	71.2
Patrol	<i>±2.6</i>	<i>±2.6</i>	<i>±2.6</i>	<i>±2.5</i>	<i>±2.6</i>
Destroy	44.2	46.0	45.4	55.4	49.2
Bunker	<i>±2.3</i>	<i>±1.9</i>	<i>±2.2</i>	<i>±1.7</i>	<i>±2.2</i>

Table 3: Lethality metric for each of the 4 combat scenarios for the four different tactical cyber capabilities (italicized number is the +/- 95% confidence interval).

Mission Type	Base	Grid Attack	RF Local.	Comm Denial	Comm Int.
Raid	88.3	82.8	97.3	88.8	88.7
	<i>±1.6</i>	<i>±1.7</i>	<i>±1.6</i>	<i>±1.6</i>	<i>±1.6</i>
Ambush	52.2	57.8	53.1	56.2	57.8
	<i>±2.9</i>	<i>±2.7</i>	<i>±3.1</i>	<i>±2.8</i>	<i>±3.0</i>
Combat	56.7	56.9	58.0	57.0	56.1
Patrol	<i>±4.1</i>	<i>±4.4</i>	<i>±4.3</i>	<i>±3.8</i>	<i>±4.3</i>
Destroy	76.8	78.7	77.8	81.3	77.4
Bunker	<i>±2.7</i>	<i>±2.0</i>	<i>±2.5</i>	<i>±2.2</i>	<i>±2.3</i>

5.3.3 Validation of Results

Since the technology for the different cyber capabilities are not available, the models cannot be validated through real-world comparison. The base scenarios, however, were compared to performance reports for small-unit exercises in a similar training site; the model results aligned well with these reports.

The different models were also validated by consulting with infantry and signal officers who served as subject matter experts that could evaluate the scenarios and determine if the model results align with their expectations. The infantry officers agreed that based on their best judgement, they would expect comparable changes in red and blue force casualties to what the simulation found.

5.4 Case Study Conclusions

The four scenarios of interest—the raid, ambush, combat patrol, and destroy a bunker—currently incur a high casualty rate for the infantry squad. However, the combat models indicate that the inclusion of new tactical cyber capabilities will allow the unit to take less casualties over the mission.

The grid attack capability provided a statistically insignificant increase in survivability across the mission sets. Though the enemies were less organized, the increase in cognitive loading on the soldiers offset this benefit. The RF localization capability offered the largest increase in survivability in three of the four mission sets. The benefit for RF localization is that the system required the least change in physical and cognitive loading. The communication denial system and communication intercept systems both provided benefits in certain mission sets. However, the communication denial system imposed a large physical burden on the soldier due to the weight of the system, and the

communication intercept system imposed a large cognitive load on the soldier.

The results of this study indicate that if the Army can only adopt one tactical cyber capability for fielding to its infantrymen, they should proceed with an RF localization capability. Additionally, the simulations indicate the importance of not increasing a soldier's physical and cognitive load, which can potentially offset any benefit from a new capability.

6 CONCLUSIONS

As the complexity of the world increases, militaries are required to perform more complex operations. In doing so, the soldier system, defined as the soldier, equipment, and their mission sets, increases in complexity. Therefore, the addition of new equipment onto a soldier requires a systems level analysis that involves having soldiers using the equipment in an operational environment. Since this is not feasible for equipment, especially in the conceptual design phase, simulation will play a crucial role in this analysis.

Several combat simulations are available, though many have historically been used for training purposes; regardless, they can be modified to account for new soldier capabilities. This paper outlines a methodology for performing such an analysis.

The paper then presented a case study that performs a trade space analysis on different tactical-cyber capabilities given to dismounted soldiers. This analysis used the combat simulation package IWARS to compare changes in soldier performance with the additional of different new tactical cyber capabilities.

This methodology was developed primarily to perform the analysis on tactical cyber trade-space presented in the case study. Future works will look at expanding this methodology to other tactical equipment including biomechanical enhancements, future weapons, and autonomous systems.

REFERENCES

- Almohammad, A., & Speckhard, A. (2017). *ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics*. International Center for the Study of Violent Extremism.
- Brantly, A., & Collins, L. (2018, November 29). *A Bear of a Problem: Russian Tactical Cyber Operations*. Retrieved December 1, 2019, from <https://mwi.usma.edu/bear-problem-russian-tactical-cyber-operations/>
- Congressional Research Service. (2018, September 4). *Electric Grid Cybersecurity*. Retrieved October 20, 2019, from <https://fas.org/sgp/crs/homesecc/R45312.pdf>
- Headquarters, Department of the Army. (2016). *FM 3-21.8: The Rifle Infantry Platoon and Squad*. Washington DC: Department of the Army.
- Hill, R. R., & Miller, J. O. (2017). A history of the United States military simulation. *2017 Winter Simulation Conference* (pp. 346-364). IEEE.
- Hodson, D. D. (2017). Military simulation: A ubiquitous future. *Winter Simulation Conference* (pp. 4024-4025). IEEE.
- INCOSE. (2015). *Systems Engineering Handbook*. Hoboken: Wiley.
- Leemans, R., & Mittal, V. (2018). A Systems Approach for Analyzing operational Energy Requirements for the Warfighter. *IEEE Systems Engineering Conference*. Orlando.
- Liu, H., Zhang, X., Su, X., Li, X., & Xu, N. (2013). Mobile localization based on received signal strength and Pearson's correlation coefficient. *IEEE 10th Consumer Communications and Networking Conference*.
- McDonnell, J. (2015). A Soldier System Engineering Architecture Modeling and Systems Approach. *NDIA Systems Engineering Conference*. Orlando, FL.
- Mittal, V. (2019). Operational Analysis for Dismounted Soldiers. *Proceedings of the 8th Annual World Conference of the Society for Industrial and Systems Engineers*. Baltimore, MD.
- Page, E. H. (2016). *Modeling and Simulation, Experimentation, and Wargaming-Assessing a Common Landscape*. Mitre.
- Porche, I. R., Paul, C., Serena, C., Clarke, C. P., Johnson, E.-E., & Herrick, D. (2018). *Tactical cyber: building a strategy for cyber support to corps and below*. Santa Monica: RAND Corporation.
- Samaloty, N., Schleper, R., Fawkes, M. A., & Muscietta, D. (2007). Infantry Warrior Simulation (IWARS): A Soldier-Centric Constructive Simulation. *Phalanx*, 40(2), 29-31.
- Shanker, T., & Richtel, M. (2011, January 16). In new military, data overload can be deadly. *The New York Times*, p. 2011.
- Shirey, R. (2000). *Internet Security Glossary*. GTE/BTN Technologies.
- Tolk, A. (2012). *Engineering principles of combat modeling and distributed simulation*. Hoboken, NJ: Wiley.
- Washburn, A., & Kress, M. (2009). *Combat Modeling*. New York: Springer.
- Wilson, J. R. (2016, October 2). How Military Harvests Technology from the Commercial Sector. *Military and Aerospace Electronics*.