Modeling the Effects of a Cyber-Attack on the Tactical Edge

Dr. Vikram Mittal, Mr. Gene Lesinski, and LTC Matthew Dabkowski
U.S Military Academy
Department of Systems Engineering
4th Floor, Mahan Hall
West Point, NY 10996
845-938-2700
Vikram.Mittal@usma.edu
Eugene.Lesinski@usma.edu
Matthew.Dabkowski@usma.edu

Keywords:
cyber-attack, combat modeling, IWARS

ABSTRACT: *Combat modeling involves opposing forces following set processes coupled with uncertainty to determine the winner. These models are built around traditional weaponry and tactics; however, cyber-attacks do not follow the traditional rules. Moreover, due to the very nature of a cyber-attack, it is difficult to model their effects, especially as it relates to a tactical mission. This study provides a simplified method to model the impact of a cyber-attack on a dismounted Army squad. Different pathways for the attack are identified. This method then assumes that the cyber-attack was effective and looks at the change in soldier performance as a result of the attack. In particular, it looks at the degradation of a soldier's ability to shoot, move, and communicate. This degradation can then be modelled in the Infantry Warrior Simulation (IWARS) to capture the changes in performance metrics to include survivability and lethality. Two case studies are presented. The first looks at the degradation of a soldier with a hacked Facebook account that received personal misinformation. The second looks at a jammed surveillance drone that provides the soldiers with the wrong information.*

1. Introduction

Ground combat is won through the appropriate arraying of ground forces coupled with the use of "force multipliers," which are intended to give one side an advantage. These force multipliers have evolved over time. Napoleon had his artillery. Clausewitz had his aircraft support. The modern United States Army has air and sea assets that can enhance its ground forces' lethality, survivability, and situational awareness. As militaries have become increasingly networked, a new force multiplying weapon has emerged—cyber weaponry.

The use of cyber weaponry to augment tactical ground forces has been somewhat limited [1]. American forces were able to gather increased situational awareness by exploiting their adversaries' use of commercial networks [2]. Meanwhile, Russian hackers used cellphone networks to pinpoint and track Ukrainian Army units [3]. These trends would lead one to expect that future near-peer wars would integrate cyber-attacks as a force multiplier to provide a tactical edge to ground forces.

Combat modeling attempts to predict the outcome of a force-on-force engagement by treating war as a formal system, consisting of entities and processes that are united by common objectives [4]. The entities consist of the combatants and weapons. Methodologies have been developed for many traditional weapons, primarily bursting and non-bursting munitions [5]. However, due to the wide range of possible cyber-attacks, it is difficult to create models that show the effect of a cyber-attack on a combat engagement.

This study outlines a method to build a combat model for a tactical mission that incorporates a cyber-attack. The model architecture separates the cyber-attack from the mission, and models the mission assuming that the cyber-attack was completely effective or ineffective. This paper limits itself to the combat modeling of tactical engagements where the goal of a cyber-attack would be to disrupt the mission.

2. Cyber Attacks on the Tactical Edge

Quite simply, no city has ever been taken by an aircraft carrier. Though air and sea power provide a decisive edge to a military, ground combat is "the foundation of military victory" [6]. Ground combat at its most fundamental level involves the allocation and coordination of small units in completing a set mission [7]. These tactical missions can range from setting an ambush to performing a direct attack on a fortified position.

The small units completing these tactical missions are an easy target for cyber-attacks, and the consequences from these cyber-attacks can be substantial when applied to multiple small units simultaneously [8]. Though cyber-attacks at higher echelons are possible, higher echelons have access to cyber defense resources and secured data networks, making effective cyber-attacks more difficult. Tactical units, operating at the "tip of the spear," do not have these resources; moreover, their communication networks are much more exposed, making them more vulnerable [1].

2.1 Vulnerability Points

Figure 1 shows the communication equipment carried by a standard US Army rifle squad as dictated in [9]. Most near-peer competitors will carry similar equipment. A standard rifle squad is made up of nine soldiers. The squad leader will typically carry a GPS for determining their position and a reachback radio to communicate with its higher unit. Some squad leaders will carry a controller for operating a Raven or a similar-sized unmanned aerial vehicle (UAV); these devices are typically used for surveillance. The Squad Leader will also carry a device to communicate with his squad and track its position; dismounted soldiers would use Nett Warrior, and mounted soldiers would use Blue Force Tracker. Additionally, though it is not authorized, a Squad Leader will often carry a commercial cellphone, which serves as an emergency communication device and a method to access non-official networks (e.g., access Facebook) [10].

The squad is organized into two fire teams, each consisting of three soldiers and a leader. Each team leader would carry either a Nett Warrior or Blue Force Tracker device to allow them to communicate with the squad leader. Similar to the squad leader, they could also be carrying a commercial cellphone. The members of the fire team are not authorized any communications equipment; however, they could possibly be carrying a cellphone as well. Even if a soldier is not actively carrying a cellphone, they will likely have some access to the internet before and/or during the mission.

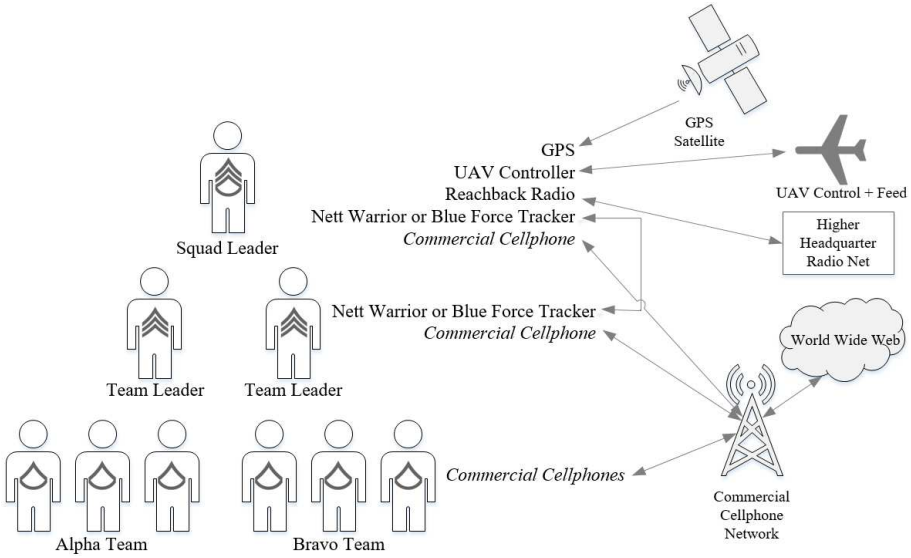

Figure 1. Communication equipment carried by a US Army Rifle Squad that can be exploited by a cyber-attack.

2.2 Effects of a Cyber-Attack on Tactical Mission

Table 1 lists the actions and effects of a cyber-attack. The first four items on the table—the reach-back radio, Nett Warrior or Blue Force Tracker, the UAV Controller, and the GPS—can all be spoofed or jammed. Spoofing involves providing false information to the user in such a way that they believe it to be true. Jamming denies or degrades usage of that communication channel to the user. Spoofing is difficult since these radio frequencies are encrypted; however, the jamming process can be accomplished through a number of tools that are commercially available [11]. Note that partial jamming of a system can mimic spoofing. For example, by increasing the noise on the UAV video feed, the enemy could camouflage their visual signature in the noise, causing the user to think that a path is free of enemies. Additionally, the radios can be intercepted. Interception allows for the enemy to have an increased awareness of friendly actions and intent.

Since soldiers will have access to the World Wide Web through either cellphones or computers before/during the mission, an online cyber-attack is possible [10]. Though there are numerous mechanisms to attack a soldier's cyber presence, the typical goal is to exploit data on the World Wide Web to decrease morale or create a lack of focus. This can take the form of exploiting personal information (e.g., stealing a person's identity and draining their bank account) or misinformation (e.g., hacking a Facebook account and convincing a soldier that his spouse is leaving him).

3. Model Architecture

Most existing combat models (e.g., IWARS, JCATS, OneSAF) do not have the capability to model a cyber-attack as part of a tactical operation. Therefore, it is necessary to combine these models with other modeling tools to build a combat model of a cyber-compromised tactical mission.

Figure 2 shows the process for a cyber-attack and how each step can be modelled independently. The first step is the detection of a communication channel that can be exploited. The probability of detection ($P_{detection}$) is based on the resources available to the exploiting forces and the strength/type of signal [12]. After detection, the exploiting force will attempt to exploit the signal, and there is an associated probability of exploitation ($P_{exploited}$). Based on the level of encryption and the scenario, the exploiting force could choose to intercept the signal to enhance their situational awareness, spoof the signal to change their adversary's course of action, or jam the signal to deny capabilities to their adversary [13].

Table 1. Actions and effects that can be taken through the exploitation of the different communication equipment carried by a rifle squad

Target	Action	Effects	How to Model Effects
Reach-back Radio	• Intercept • Spoofing • Jamming	• Increase in enemy SA • Misinformation • Incomplete/delayed transmissions • Inability for reachback resources (e.g., call for fire)	• Sudden change in mission profile • Diminish/eliminate reachback resources
Nett Warrior or Blue Force Tracker	• Intercept • Spoofing • Jamming	• Increase in enemy SA • Misinformation • Incomplete/delayed transmissions • Decrease in friendly SA	• Increase in enemy common operating picture • Use confusion matrix to mistake red forces for blue forces
UAV Controller	• Spoofing • Jamming	• Misinformation • Decrease in situational awareness	• Diminish/eliminate UAV resource
GPS	• Spoofing • Jamming	• Reduced ability to navigate • Inability for targeting	• Diminish/eliminate call for fire resource • Friendly forces take wrong routes
Soldier (Social Media)	• Exploitation of personal information • Misinformation	• Decreased morale • Lack of focus	• Increase in target acquisition time • Smaller field of regard • Target classification confusion

If the cyber-attack is not successful, the combat scenario is modeled as normal. However, if the cyber-attack is successful, the model designer must determine the impact of the cyber-attack. Table 1 provides guidance as to how to model the effects of a cyber-attack on a dismounted rifle squad. For example, if a UAV feed is jammed, the simulation can be run with the exploited team not having a UAV asset.

The two simulations are run separately to generate different metrics; these metrics are often tied to survivability (e.g. number of blue force survivors) and lethality (e.g. number of red force killed). The survivability and lethality metrics from the two scenarios can be combined, based on the probability of a successful cyber-attack ($P_{success} = P_{detection} \times P_{exploited}$). The end results can be used to identify the potential outcome of a cyber-compromised mission.

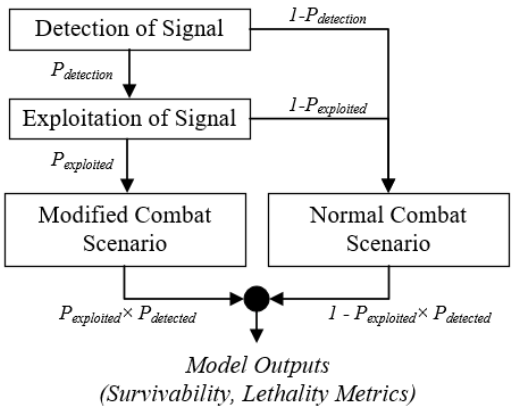

Figure 2. Architecture of a tactical combat model integrated with a cyber-attack

The probabilities of detection and exploitation can be difficult to determine. Often, $P_{detection}$ is close to 1 for most modern militaries since they currently have assets for detecting these signals. However, the $P_{exploition}$ is based on the signal integrity and security, as well as the type of attack. For example, $P_{exploited}$ for a jamming attack on an encrypted signal would be higher than that for a spoofing attack. The combat modeler can simply use values of 0 and 1 for $P_{success}$ and ignore the contributions from $P_{detection}$ and $P_{exploited}$. The results vary linearly between the two, allowing the combat modeler to identify the change in the combat scenario with and without a successful cyber-attack.

4. Case Study 1

The first case study looks at a squad performing a presence patrol through the main street of a village. An earlier cyber-attack was directed at a member of the squad to reduce his combat effectiveness.

4.1 Scenario

A blue rifle squad is performing a daytime presence patrol through a rural town; their mission is to walk through the town and engage any red forces that they come across. The blue forces are moving down the main street, where the red forces are expecting them. They are moving in a squad file formation with the alpha team leader as the lead person. The alpha team leader is followed by the rest of alpha team, the squad leader, and bravo team. The blue forces are following simple rules of engagement that require them to clearly identify a target as being a member of the red forces prior to engaging.

A four-person, red unit is waiting on the main street for the blue forces. The red forces have a sniper stationed on top of a building that has a clear line of sight on most of the pathway. The remaining three red force members are at ground level and have set up an ambush along the route.

Prior to the mission, red forces launched a cyber-attack directed at the alpha team leader. They used the blue forces' Facebook site to get the e-mail address for the alpha team leader's spouse. Upon getting this information, the red forces sent the spouse a phishing e-mail to gain access to her computer. If the red forces gain access to the computer they can extract compromising files (e.g., embarrassing photographs) and place them in the public domain.

If the cyber-attack was effective, the alpha team leader would have degraded performance during the mission, having to spend significant time prior to the mission working through the issue with his spouse. Going into the mission, the alpha team leader would be tired and pre-occupied with this issue. As such, he will have a slower response time and a decreased field of view [14].

4.2 Model

A model was built in IWARS to replicate both the normal mission and a modified mission that reflects the cyber-attack. The model uses Fort Benning's McKenna MOUT site to simulate the town, with the blue force moving north along the main street. Both forces are wearing standard body armor and carrying M4 assault rifles. Since the mission occurs during daytime, neither unit is using night vision. The scenario map and the view from the sniper are shown in Figure 3. Each model was run 100 times to ensure an adequate number of iterations, based on convergence tests.

In the modified scenario with the cyber-attack, the alpha team leader would have a decreased ability to acquire and identify an enemy through a lack of focus and being sleep-deprived. IWARS models target acquisition through the ACQUIRE-TTPM methodology that is fully explained in [15]. The "unaided eye" is treated like any other visual sensor that has the ability to detect a target, and so the performance of this sensor can be degraded to capture the increased difficulty in target acquisition. IWARS uses a "confusion matrix" to handle target identification, and the parameters can also be modified to reflect the change in ability for the alpha team leader to differentiate a red agent from a civilian. These parameters can be used to create a new visual sensor that can be assigned to the alpha team leader.

When this scenario is run under the base condition, the alpha team leader, who is the lead person for the blue squad, detects the sniper and engages him. He communicates to the rest of the squad, and others engage the sniper until it is incapacitated. The blue squad then continues its movement into the town. When the blue squad enters the ambush site, they engage and incapacitate the red force. Since the blue force has numerical superiority over the red force, the blue force wins the bulk of the engagements.

When the modified scenario is run, the alpha team leader has a lower probability of detecting the sniper. By the time the sniper is detected, the sniper has engaged multiple members of the squad, allowing for more blue casualties. The blue forces then push through the ambush site and neutralize the enemy. Though the blue force still wins the engagement most of the time, they sustain heavier casualties than in the base scenario.

Figure 3. Scenario map (left) and view from the sniper (right) for Case Study 1

4.3 Results

The results from the simulations are shown in Table 2. "Winning" the scenario means that all enemies were incapacitated or having a lower percentage incapacitated than the enemy at the end of the run. Note that a draw would occur if both sides had equal percentages incapacitated.

As expected, an effective cyber-attack reduced the percentage of blue wins and increased red wins. Additionally, more blue forces were killed following the cyber-attack. Though the alpha team leader was killed in almost every scenario, since he did not notice the sniper early enough, the sniper was able to engage and hit multiple members of the squad before being incapacitated. Losses from the sniper resulted in a reduction in firepower for the blue squad as they go through the ambush site, resulting in more blue casualties.

Table 2. Case Study 1 results based on 100 simulation runs

	% Wins		Average Deaths (*Std. Dev*)		
	Red	Blue	Blue	Red	Civilian
Baseline	13%	82%	5.13 (*1.74*)	3.78 (*0.41*)	0.22 (*0.44*)
Cyber Attack	27%	56%	6.16 (*1.78*)	3.46 (*0.58*)	0.29 (*0.50*)

Figure 4 shows the average number of red and blue deaths as a function of the probability of an effective cyber-attack. These values are the weighted average of the two scenario outputs. The probability of an effective cyber-attack is the product of the probability of detection and the probability of exploitation. As the probabilities increase, the number of red deaths decrease and the number of blue deaths increase. Hence blue forces should attempt to minimize the probability of an effective cyber-attack. In this case, the probability of detection can be reduced by the unit not having a Facebook page or making the site private. The probability of exploitation can be reduced by having spouses take information assurance training to make sure they do not fall victim to phishing e-mails.

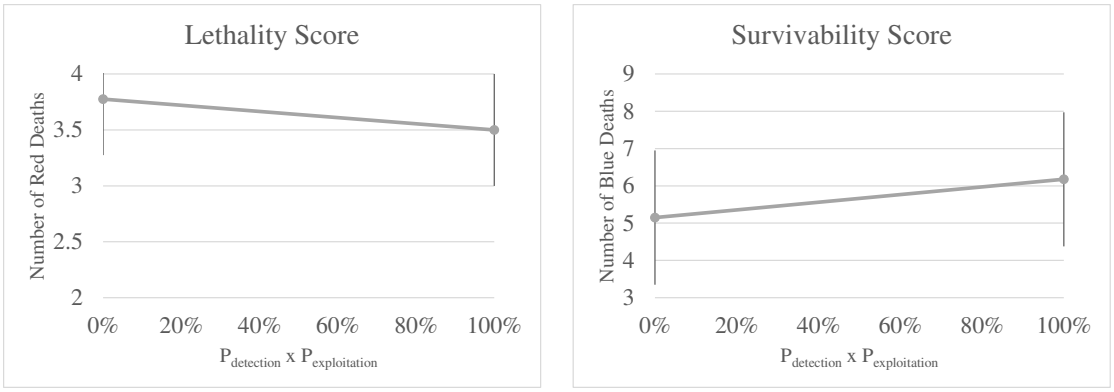

Figure 4. Lethality and survivability metrics based on the percentage of an effective cyber-attack for Case Study 1, set to be the product of the probability of detection and probability of exploitation.

5. Case Study 2

The second case study is similar to the first case study in that a blue rifle squad is moving through a town where red forces have set an ambush. However, for this case study, the blue squad has an unmanned aerial vehicle (UAV) for performing reconnaissance; the red force can detect and exploit the UAV.

5.1 Scenario

The blue rifle squad has wrapped up an operation north of the town and must move through the town back to its vehicles. There are two paths through the town that the blue rifle squad can take. Since the blue forces know that there is expected enemy activity, they decide to use a UAV to detect the location of red activity. After flying the UAV down the main street, they decide whether to take the main street or a side street. It is preferable for them to take the main street because it is a shorter walk to the vehicles.

Meanwhile, the red forces have set up an ambush along the main street. Two red forces are on either side of the road and will engage the blue forces as they turn onto the main road. However, if the blue forces take the other path, the red forces will attempt to move and engage the blue forces while moving, resulting in decreased effectiveness.

The red forces are able to perform a cyber-attack on the UAV as it flies overhead. Upon detecting the UAV, they decide to use a jamming signal to increase the noise in the UAV video feed. The video feed has enough noise to prevent the detection of the red forces. However, the jamming signal is not strong enough to cause the blue forces to lose trust in their data. Since the blue forces do not see the red forces on the UAV feed, they proceed down the main street; if they had, they would have diverted down the side street.

5.2 Model

Similar to the case study, a model was built in IWARS to replicate both the normal mission and a modified mission that reflects the cyber-attack. Again, the model uses the McKenna MOUT site map to simulate the town, but this time with the blue forces moving through the town from north to south. The blue forces and red forces are wearing standard body armor and carrying M4 assault rifles. The blue forces have a UAV that is controlled by the squad leader. The scenario map and the view from the UAV are shown in Figure 5. Convergence testing again found that 100 runs would be an adequate number of runs.

In the normal scenario, the squad leader detects the red forces and opts to take the side street to avoid the red forces. The red forces then proceed to move from their ambush site and attack the blue force on the side street. Since they are moving, they lose their defensive advantage and hence are more vulnerable. In the modified scenario, the signal noise prevents the squad leader from detecting the red forces, and he heads down the main street.

Figure 5. Scenario map (left) and view from the Blue Force UAV (right) for Case Study 2

5.3 Results

The results from the simulation are shown in Table 3. This analysis used the same definition for "winning" as the first case study. With the baseline, the blue force always wins, since the blue force has numerical superiority and both forces are engaging while moving. However, following the cyber-attack, the red force wins a small number of the attacks by forcing the blue force into the kill zone. Though the number of wins are low, they impose significantly more casualties on the blue force.

Figure 6 shows the average number of red and blue deaths as a function of the probability of an effective cyber-attack, which is determined from the weighted average of the two scenario outputs. As expected, as the probability of an effective cyber-attack increases, the number of blue deaths increases while the number of red deaths decrease. With the current scenario, the probability of an effective cyber-attack is high. Since low-flying UAVs emit noise, the red forces should be able to readily detect it. Additionally, jamming equipment is commercially available and results in the degraded video performance of the UAV. Moreover, most UAVs do not have a method to detect or overcome jamming. The usage of a quieter UAV, a jamming detector, or increasing the signal transmission power could result in a less effective cyber-attack.

Table 3. Case Study 2 results based on 100 simulation runs

	% Wins		Average Deaths (*Std. Dev*)	
	Red	Blue	Blue	Red
Baseline	0%	100%	3.07 (*1.21*)	4.0 (*0.0*)
Cyber Attack	4%	89%	5.21 (*1.61*)	3.82 (*0.41*)

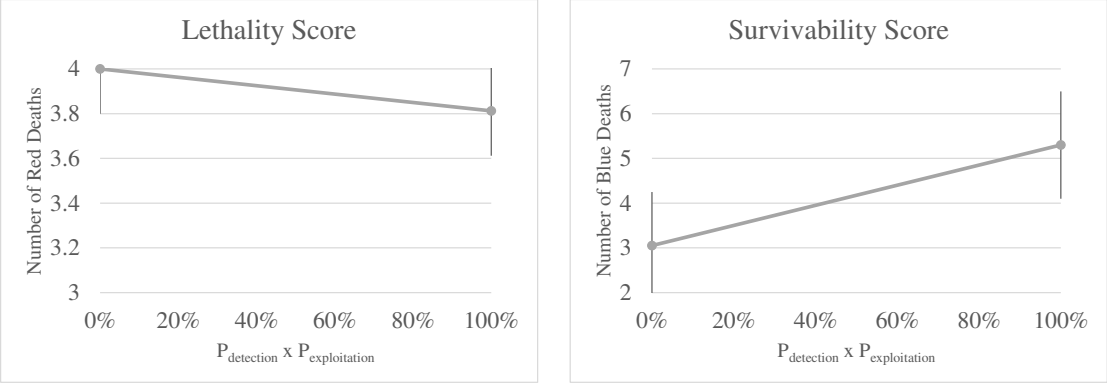

Figure 6. Lethality and survivability metrics based on the percentage of an effective cyber-attack for Case Study 2, set to be the product of the probability of detection and probability of exploitation.

6. Extending Technique to More Complex Missions

The missions modeled in the two case studies are somewhat simplistic; more complex missions can be modelled similarly. A more complex mission would have multiple cyber-attack activities. As such, different models can be run to capture each effect, and each of the models would have a certain probability of occurring. The sum of the probabilities for each scenario should sum to 1. Similar to the simple missions, these probabilities can be determined from estimating the probability of an effective cyber-attack based on detection and exploitation; however, other parameters play a role as well.

For example, in the first case study, the red forces performed a cyber-attack to decrease the combat effectiveness of the alpha team leader. Additionally, they could perform a cyber-attack where they spoof the blue reachback radio and order the blue squad to not fire at the sniper who is located in a protected area. The probability of an effective cyber-attack through this means is much lower than the Facebook + phishing e-mail attack, since this attack would require breaking into encrypted channels. Table 4 gives approximate probabilities for each of the four associated scenarios, as well as the lethality and survivability metrics for each scenario. By using the probabilities, the overall metrics for the scenario can be determined.

Table 4. Case Study 1 Scenario with a second cyber-attack (spoofing of radio signals)

		Average Deaths (*Std. Dev*)		
	Probability	Blue	Red	Civilian
Baseline	0.74	5.13 (*1.74*)	3.78 (*0.41*)	0.22 (*0.44*)
Facebook/Phishing Attack	0.20	6.17 (*1.78*)	3.46 (0.58)	0.29 (*0.50*)
Radio Spoofing Attack	0.05	5.86 (*1.72*)	2.32 (*0.51*)	0.62 (*0.60*)
Both Attacks	0.01	6.45 (*1.37*)	2.08 (*0.89*)	0.76 (*0.68*)
Overall	1	5.39 (*1.74*)	3.63 (*0.45*)	0.26 (*0.46*)

7. Conclusions and the Way Forward

Modern nations are integrating cyber-attacks to create an advantage for combat units. Though higher echelons have cyber-security capabilities, squad elements are particularly vulnerable. While traditional combat modeling software can use agent-based models to model the outcome of small-unit engagements, they lack the capacity to model a cyber-attack.

This paper introduced a simple model architecture to model a small unit performing a mission in a cyber-compromised environment within IWARS. It identified pathways for a cyber-attack for today's networked soldier; these attacks would cause a change in the model related to the agents' actions and behaviors. By running the model with and without these changes in actions and behaviors, a combat modeler can gain insight into the effects of a cyber-attack on a mission. The metrics for the two models can then be combined by taking into account the probability of each event occurring.

Two case studies were presented to demonstrate this process. The first involves a social media attack on the point-man for a presence patrol. The second involved jamming a UAV to convince a blue squad to take a road that puts them into a kill zone. In both case studies, the cyber-attacks resulted in an increase in blue deaths and a decrease in red deaths.

8. References

[1] I. Porche, C. Paul, C. Serena, C Clarke, E. Johnson, D. Herrick, "Tactical Cyber: Building A Strategy For Cyber Support To Corps And Below." DTIC, 2016. [Online]. Available: https://www.dtic.mil/DTICOnline/downloadPdf.search?collectionId=tr&docId=AD1031235/. [Accessed 10 June 2018]

[2] U.S. Army Cyber Command, "Integration of Cyberspace Capabilities into Tactical Units." Army Knowledge Online, 2018. [Online]. Available: https://www.army.mil/article/163156/. [Accessed 8 March 2018].

[3] D. Voltz, "Russian hackers tracked Ukrainian artillery units using Android implant: report." Reuters. Dec 2, 1016.

[4] A. Washburn and M. Kress, *Combat Modeling*, Springer, 2009.

[5] "Munition Delivery Accuracy," *IWARS 5.1 Methodology Guide.* April 2014.

[6] R. Peters, "Boots on the Ground: War's Enduring Requirement," *New York Post.* March 22, 2003. [Online]. Available: https://nypost.com/2003/03/22/boots-on-the-ground-wars-enduring-requirement/. [Accessed 10 June 2018].

[7] Association of the United States Army, "The U.S. Army Squad: Foundation of the Decisive Force," October 11, 2011, [Online]. Available: https://www.ausa.org/publications/us-army-squad-foundation-decisive-force. [Accessed 5 June 2018]

[8] F. Yildiz, "Modeling the effects of cyber operations on kinetic battles." Naval Postgraduate School Department of Operations Research, 2014.

[9] Program Executive Officer (PEO) Soldier, *Soldier System Integration Dismounted Baseline Version 2.0 for the Soldier System*. 2017.

[10] N.J. Shallcross, "Social Media and Information Operations in the 21st Century," *Journal of Information Warfare,* 16(1), 2017.

[11] S.P. LeBlanc, A. Partington, I. Chapman, and M. Bernier. "An overview of Cyber Attack and Computer Network Operations Simulation," *Proceedings of the 2011 Military Modeling & Simulation Symposium,* April 2011..

[12] C.L. Krishna and R.R. Murphy. "A Review on Cybersecurity Vulnerabilities for Unmanend Aerial Vehicles," *Safety, Security, and Rescue Robotics, 2017 IEEE Internal Symposium.* Oct 2017.

[13] K. Harmann and C. Steup. "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," *Cyber Conflict (CyCon), 2013, 5th Internal Conference, IEEE,* June 2013.

[14] T.M. McLellan, G.H. Kamimori, D.G. Bell, I.F. Smith, D. Johnson, & G. Belenky, "Caffeine Maintains Vigilance and Marksmanship in Simulated Urban Operations with Sleep Deprivation," *Aviation, Space, and Environmental Medicine* 76, 1, 39-45, 2005.

[15] US Army Material Systems Analytsis Activity, *Physical Knowledge Acquisition Document: Target Acquisition and Misidentification (ACQUIRE-TTPM-TAS),* Nov 2012.

Author Biographies

LIEUTENANT COLONEL MATTHEW DABKOWSKI is currently the program director for the Systems Engineering program in West Point's Department of Systems Engineering. He is a career Army officer with a background in Infantry and operations research / systems analysis. He is a graduate of the West Point Class of 1997 with a degree in Operations Research. He holds an MS in Systems Engineering and a PhD in Systems and Industrial Engineering from the University of Arizona. Lieutenant Colonel Dabkowski's research interests focus on network science, decision analysis, and applied statistics.

GENE LESINSKI is currently an Assistant Professor in the West Point Department of Systems Engineering. He retired from the Army after 23 years with a background in Infantry. He is a graduate of the West Point Class of 1985 with a degree in Civil Engineering. He holds an MS in Systems Engineering from UVA. Mr. Lesinski's research interests focus on computational intelligence, system design, and system architecture.

VIKRAM MITTAL, Ph.D. is currently an Assistant Professor in the West Point Department of Systems Engineering. He holds a BS in Aeronautics from Caltech, a MSc in Aerospace from Oxford, and a PhD in Mechanical Engineering from MIT. Dr. Mittal's research interests focus on M&S, robotics, and energy.