New Defenses for the Hybrid Battlefield

Paul Maxwell
Army Cyber Institute
UNITED STATES

paul.maxwell@westpoint.edu

ABSTRACT

Defenses used in military operations today are not prepared for the attacks that modern technology can mount. The destruction caused using drones, electronic warfare, and others means was demonstrated to be extremely lethal in recent engagements such as Syria, Armenia, the Ukraine. There are techniques readily available to help protect NATO forces against these threats and others that require additional research and development. To prepare for the modern battlefield, NATO forces must alter their training and equipment or risk significant attrition. This paper will explore the threats of the hybrid battlefield and make recommendations on how to update our tactics to protect against them. As our forces re-focus from counter-insurgency operations to peer-competitors, our training and operations need to evolve. Merely dusting off the Cold War field manuals and reverting to training center high-intensity scenarios is not sufficient for the hybrid battlefield. The changes proposed can and should be implemented quickly to defeat these existing and emerging threats.

1.0 INTRODUCTION

The modern battlefield is continuing to evolve as new threats emerge creating what has been coined 'hybrid warfare.' In conflicts such as those in Syria, Saudi Arabia, Armenia, and the Ukraine, weapons are being introduced or used in novel ways. Drones are performing attacks *en masse* or individually as munition delivery systems or flying bombs [1]–[3]. Electronic warfare is experiencing a resurgence with signal jamming and Position Location System (PLS) spoofing [4], [5]. Information warfare is gaining prominence as botnets spread misinformation and cyber-attacks target critical infrastructure [6]. Given these threats, NATO forces must rethink their defenses to protect their combat power and maintain their freedom to maneuver.

Current military field manuals are filled with techniques and tactics designed for the battlefields of yesterday. Camouflage is designed to conceal forces from mainly human eyes. Tactical obstacles are focused upon canalizing, turning, or blocking manned ground vehicles and personnel. Information operations are stuck in old media such as flyers and loudspeaker broadcasts. On top of these old tactics is layered two decades of battlefield superiority that has made forces careless about controlling their electromagnetic emissions. Peer competitors and lower-rated adversaries are all poised to use technologies that have an asymmetric advantage often with a relatively low cost. If we do not adapt our defenses to these new threats, then our current military superiority will evaporate.

To protect our forces, we must focus on the largest threats. Pre-World War I, digging fighting positions with overhead cover was not common because artillery was not the casualty producer that it became. Tactics evolved in this case to counter the threat. The reported quick destruction of combat formations in the Ukraine and Armenia-Azerbaijan by drone supported forces suggests that one of our biggest threats are targeting systems. As such, camouflage tactics need to evolve to counter Artificial Intelligence (AI) based targeting systems. Protecting our forces may also involve erecting Position, Navigation, and Timing (PNT) defenses to evade PNT-

guided munitions. Engineering efforts may shift to constructing obstacles focused on drones both aerial and ground based. Renewed efforts will need to be made to reduce electromagnetic emissions for protection from direction finding assets and jamming systems. And finally, information warfare will need to focus on operations security and deception by preventing leaked intel and tricking online data mining systems into drawing incorrect conclusions. In the following section, various technologies will be examined to propose potential actions needed to protect our forces.

2.0 DEFENDING AGAINST MODERN TECHNOLOGY ON THE HYBRID BATTLEFIELD

There are a multitude of technological advances over the past twenty years. Some of these advances are beginning to produce systems capable of inflicting massive damage on military forces. Defenses and training must evolve to counter the threat that these technologies present.

2.1 Artificial Intelligence

Artificial Intelligence has been studied for several decades. However due to hardware and software improvements, advances in the last ten years have resulted in very capable systems, some of which are in production today. AI is already used for image recognition, written and verbal word generation, outcome predictions, sentiment analysis, and more. These automated tools can help enemy forces with target identification (visually, electronically, and audibly), intelligence gathering, course of action development, resource allocation, war gaming, and information attacks. Though it is unclear if any of these technologies were used in the operations in Armenia-Azerbaijan, Syrian, or elsewhere, it is inevitable that this technology will enter the battlefield. Systems using AI will target our forces with a speed not previously experienced thus making us very vulnerable to their attacks.

Despite the claimed prowess of AI systems and the threats they may pose, they are extremely vulnerable to adversarial attacks. Actions such as adding noise (often imperceptible to humans) to an image will cause advanced recognition systems to fail. Many researchers to include an AI team at Google Brain have demonstrated how these attacks can cause AI systems to fail in their primary mission [7]. The team at Google Brain reports that all of the published attempts to make AI systems resilient against these attacks have proved vulnerable. This is unlikely to change in the near term as the ability to design systems that approach human levels of resilience and capability is an enormous research challenge.

Military tactics need to evolve to protect against AI systems using their vulnerabilities. For example, current vehicle and personnel camouflage patterns are designed to fool the human eye. What works well against the eye does not work as well against an AI image recognition system. AI systems are showing to be as good as or better than humans in recognizing images and that ability is sure to increase with more research effort. To protect personnel and systems against these threats, camouflage should be reimagined to defeat AI systems. Researchers have shown that techniques such as attaching appliques with various patterns or shapes and putting text with an object [8]–[12] can easily fool AI systems. Adding ‘noise’ of this type to camouflage patterns can help defeat AI recognition systems while still maintaining their optical functionality. Defenses of this type should be designed to be updated periodically to account for retrained AI models thereby prolonging their effectiveness.

AI targeting systems may take other forms such as acoustic recognition systems. Microphones are prolific especially in urban environments and AI models can be developed to classify objects based on their acoustic

signatures. To defend against these systems, militaries can acoustically alter their systems' signatures or they can attempt to deceive detectors by generating false signatures (aka noise generators). Research work on defeating voice recognition systems [13]–[15] show that acoustic systems can be fooled by modifying the emitted sounds or through transmission of signals inaudible to humans. One could imagine tactically deployed noise generators that emit inaudible frequencies that attempt to deceive AI detection systems thereby providing protection to friendly forces.

2.2 Position, Navigation, and Timing Defenses

With each technological advance, military reliance on Position, Navigation, and Timing (PNT) information increases. Besides basic navigation, many systems rely on PNT data for their functions. Communications systems rely on the timing for synchronization, smart weapons rely on positioning data for targeting guidance, and the robots of the future battlefield (and drones on the current battlefield) will use the data for navigation and localization. Accordingly, our forces are at risk from the loss or spoofing of PNT data. Attacks on PNT can affect maneuver operations and communications while localized denial or spoofing of PNT signals may offer protection against enemy systems. The Russians and others have been linked to GPS denial and spoofing attacks on land [16] and at sea [4], [17] for defensive and offensive purposes. The work of [18] demonstrates that drones are susceptible to PNT attacks as well using low cost, Commercial-off-the-Shelf (COTS) tools.

Defenses against PNT attacks mostly center around pre-PNT training. Education for troops on basic navigation techniques and how to recognize PNT attacks is needed. Techniques for synchronizing time-reliant systems without PNT is necessary. Adding back-up technologies for navigation such as advanced inertial systems and potentially celestial-based systems can help too. The enemy knows our reliance on PNT systems and has the means to deny or spoof this data and thus we cannot ignore this threat.

From an offensive perspective, militaries need to develop tools that can deny/spoof PNT for protection purposes. High value systems could have protective devices deployed around them to deceive smart munitions, unmanned vehicles, and other threats. Once a unit establishes its defensive position and has confirmed its location, the need to receive PNT data is reduced. Actively denying or spoofing that data can then provide additional threat protection. Additionally, altered PNT data may be used to create canalization lanes that lead enemy forces away from friendly units or into pre-determined engagement areas. No matter the technique chosen, PNT defenses and mitigations must be added to our toolkit and training.

2.3 Electronic Warfare Concerns

Twenty plus years of battlefield technological overmatch have resulted in a battlefield that is littered with electro-magnetic (EM) emissions. The cold war training on how to keep your EM signature low and therefore protect your forces has been replaced by constant, high-power transmissions, an increase in electronic tools used, and a loss of knowledge on how to shape and direct necessary emissions. As the focus returns to peer and near-peer conflict, emphasis needs to return to reducing force EM signatures. As shown in the conflicts in the Ukraine, Armenia-Azerbaijan, and other places, large sources of EM emissions can be easily targeted for destruction or jamming [5], [19].

To defend against EM-based attacks, cold war type lessons should be reintroduced to military training. Techniques such as always transmitting on the lowest possible power setting, using directional antennas when possible, and entering radio-listening silence at key moments should be trained once more. Despite these efforts though, the increasing proliferation of always-on, electronic devices on the battlefield will create a signature profile that good discipline cannot hide. Each electronic device creates a magnetic field and emits radiation in

various frequencies. Though many of these signals may not be detectable with current technology at long distances, advances in AI, antennas, and signal processing may eventually result in a new threat. A technique to defend against this threat may be to create a Faraday cage [20] like system around key nodes such as tactical operations centers. These systems can dampen or eliminate EM emissions from devices contained therein. Militaries should investigate shelter materials that provide this protection. Another technique may be in the deception arena. Forces can create sources of EM radiation with patterns that mimic actual forces to deceive the enemy. This can work in either singular role to focus an enemy on one false location or in a flooding-type role where the enemy has more targets to decipher than time and resources allow. Finally, jamming capabilities need to be reintroduced to the force and in higher quantities and availability. Often jamming tools were limited to higher echelons and limited in number. Tactical units can benefit from jamming devices to combat attackers. The ability of small units to protect themselves against Unmanned Aerial Vehicles (UAVs) in a manner similar to how Russia attempted to defend against Turkish drones [21] will be invaluable on the future battlefield. The ability to deny communications channels to the enemy should no longer be the domain of operational and higher-level units only.

2.4 Unmanned Vehicles

Unmanned Vehicles (UVs) whether aerial, ground, or maritime present new challenges to our forces. These vehicles operate, navigate, communication, and maneuver differently than the opponents we train against. Their size can be much smaller than manned vehicles and they can operate in larger quantities than normal. In the past, an attack by aerial vehicles was often limited to small sorties of one to two vehicles. UAV swarms can number in the dozens of vehicles thereby overwhelming the defender with targets. Loitering munitions can lie in wait with little observable signature for extended periods until they find a suitable target. As such, our defenses against these threats must evolve.

Often, engineered defenses focus on ground-based threats. Obstacles, such as trenches, wire, and berms, focus on defeating ground threats whether on foot or in vehicles. Smaller ground UVs and UAVs can easily avoid or circumvent these traditional obstacles. Accordingly, these obstacles need to have their design updated to account for these new threats. For small ground threats, that may mean different wire configurations or differently shaped trenches. For aerial threats more creative solutions are required. One solution mentioned previously may be to use PNT spoofing to channel UAVs into engagement areas where they can be destroyed/disabled. Another possibility may be to create physical or even electronic UAV barriers (aka fences). Low-cost physical fences that are difficult for UAV collision avoidance systems to detect could be erected near friendly forces potentially ensnaring the threat. More extensive and easier to deploy drone fences such as those being developed in [22] can also be used to cordon off defensive positions. These fences take advantage of the UAVs dependence on PNT and other technology to find their targets. Systems such as these are already being tested for airport protection.

Another defense against UAVs that could develop is air-to-air UAV combat systems. Currently, the defenses against UAVs all center around electronic attack, physical ground-based attacks (e.g., shotguns, nets), or animal aerial attacks [23]. As with traditional, manned aerial vehicles, UAVs first developed with an intelligence role followed later by the attack role. For manned aircraft, the air-to-air combat mission developed last. As of yet, there is very little work in this role for UAVs other than a competitive, aerial battle environment for entertainment [24]. Work should be done to develop UAVs (and potentially ground UVs) whose sole purpose is to attack and defeat other UAVs. UAV fighter craft can be developed as cheaply as their offensive opponents, produced in the same quantities, and as easily controlled. These aircraft would possess the same speeds and capabilities as their opponent and provide another layer of protection to ground forces.

No matter the choice of defenses used against UVs, they must be prolific and therefore available at the small unit level. Expensive defenses that require advanced training and that are limited in quantity leave the majority of forces exposed to the UV threat.

2.5 Defending in the Information Domain

Nations and their militaries are beginning to awaken to the threat of misinformation, disinformation, and influence operations. Propaganda and deception have long been a part of many militaries' strategies, but the network effects enabled by modern communications platforms has changed the way information affects society. Research such as [25], [26], demonstrate the effects of information attacks and illustrate how they will continue to grow in magnitude. AI and technical tools like botnets amplify these attacks by creating realistic products and then spreading them with a speed that cannot be matched by humans.

Defeating these attacks is not simple and technology has not yet evolved to handle it. Techniques to verify message authenticity or provide non-attribution are still being researched. Even when completed, these techniques may fail to be effective given that humans are still involved and may not noticed or understand these defenses.

One potential way to combat these attacks is to develop information networks that can support distribution of friendly messages. Our forces should develop their own content distribution networks to include botnets and other tools. Militaries must be able to create messages and distribute them as quickly and as effectively as our adversaries. Relying on traditional distribution methods is inadequate and will not reach the intended audiences. This may include things such as obtaining access to various media platforms and targeted advertising lists. We must reimagine how we reach the target audiences with our messages in a rapid manner.

2.6 Fighting with/against the Internet of Things

Another technological threat to our forces is from the expanding Internet of Things (IoT) and the communications technologies that enable them. In all but uninhabited environments, networked devices persist. These frequently possess numerous sensors and the ability to communicate. The presence of these devices creates an environment where surveillance is persistent and the ability to maneuver un-noticed no longer exists. As such, militaries must develop techniques to counter these sensors and/or their ability to communicate.

Defeating the sensors of IoT devices would be an enormous challenge given the numerous types of sensors (optical, audio, motion, magnetic field, etc.) and their various implementations. Some may be defeated using some of the techniques mentioned previously in the AI, PNT, EW sections. Though depending on these techniques may not be sufficient. Attacking the ability of the sensor platforms to communicate may provide a more reliable defense. Many of these systems rely on WiFi or cellular (e.g., 4G, 5G) networks to communicate. Jamming these networks at a local level could provide some operational security. Research such as [27], [28] demonstrate that these networks can be jammed and therefore help defend units. As mentioned previously, these types of systems must become more prevalent at the tactical level to allow the levels of defense necessary to defeat modern threats. Small numbers of systems at operational and strategic levels will be inadequate on the battlefield of today.

2.7 Satellite Defenses

For many years, militaries have used and defended against satellite observation technologies. Until recently, satellite launches were the domain of nation states and their numbers were few enough that militaries could track

their location and defend against unwanted observations. As an increasing number of launch companies grows, the number and types of satellites increases. As discussed in [29], their capabilities and the ability to access their data has grown as well. Soon, it may be difficult to avoid satellite observation from most places on earth as discussed in [30]. As a result, our defenses must consider this powerful intelligence capability.

Defending against this threat will be difficult. The most obvious method is through anti-satellite capabilities (i.e., missiles). This is an expensive and controversial tactic and one that may not be effective given the size (some cubesat are only a few feet in size) and number of the satellites in some of the proposed satellite networks. The ability to defeat all of these potential opponents seems questionable, other techniques need to be developed.

This is an area to conduct research and development in now. Some techniques may attempt to defeat the satellites sensors themselves. This might be done by blinding/jamming the sensors or through techniques to avoid them such as creating optical shields that prevent the ability to observe a given area. Other techniques may target the data processing elements of the satellites such as the algorithms or AI tools that identify items of interest from the petabytes of data generated. Finally, defenses may target the satellites' communications networks preventing them from sharing the information they have gathered. No matter the technique used, these systems should be designed and developed quickly and fielded in sufficient numbers to protect our forces.

3.0 CONCLUSIONS

The battlefield of today and the future has changed. Technology has advanced to a place where advanced tools and software that was once the domain of only advanced nation states is now available publicly and at low cost. Additionally, communications, computing power, and miniaturization has allowed sensor networks to proliferate and create an environment where everything is observable at all times. However, traditional military defensive training remains rooted in the experience of the recent counter-terrorism and cold war fights. Our tactics and tools necessary to fight and win on the modern battlefield must be improved to account for these modern threats. Failure to do so will result in the experiences seen by the Armenians and Ukrainians in their conflicts.

REFERENCES

[1] J. Kitfield, "Russian Drone Threat: Army Seeks Ukraine Lessons," *Breaking Defense*, Oct. 14, 2015. https://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/ (accessed Apr. 22, 2021).

[2] R. Dixon, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare," *Washington Post*, Nov. 20, 2020. Accessed: Apr. 22, 2021. [Online]. Available: https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

[3] B. Hubbard, P. Karasz, and S. Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran," *The New York Times*, Sep. 14, 2019. Accessed: Apr. 22, 2021. [Online]. Available: https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

[4] M. Burgess, "To protect Putin, Russia is spoofing GPS signals on a massive scale," *Wired UK*, Mar. 27, 2019. Accessed: Apr. 22, 2021. [Online]. Available: https://www.wired.co.uk/article/russia-gps-spoofing

[5] J. Gould, "Electronic Warfare: What US Army Can Learn From Ukraine," *Defense News*, Aug. 08, 2017.

https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine/ (accessed Apr. 22, 2021).

[6] "Significant Cyber Incidents | Center for Strategic and International Studies." https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed Apr. 22, 2021).

[7] SYNCED, "Google Brain's Nicholas Frosst on Adversarial Examples and Emotional Responses | Synced," Nov. 21, 2019. https://syncedreview.com/2019/11/21/google-brains-nicholas-frosst-on-adversarial-examples-and-emotional-responses/ (accessed Aug. 13, 2021).

[8] D. Heaven, "Why deep-learning AIs are so easy to fool," *Nature*, vol. 574, no. 7777, Art. no. 7777, Oct. 2019, doi: 10.1038/d41586-019-03013-5.

[9] K. Eykholt *et al.*, "Robust Physical-World Attacks on Deep Learning Visual Classification," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, USA, Jun. 2018, pp. 1625–1634. doi: 10.1109/CVPR.2018.00175.

[10] J. Vincent, "Magic AI: these are the optical illusions that trick, fool, and flummox computers," *The Verge*, Apr. 12, 2017. https://www.theverge.com/2017/4/12/15271874/ai-adversarial-images-fooling-attacks-artificial-intelligence (accessed Apr. 10, 2020).

[11] S. Thys, W. Van Ranst, and T. Goedemé, "Fooling automated surveillance cameras: adversarial patches to attack person detection," *ArXiv190408653 Cs*, Apr. 2019, Accessed: Aug. 03, 2021. [Online]. Available: http://arxiv.org/abs/1904.08653

[12] B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018, doi: 10.1016/j.patcog.2018.07.023.

[13] Q. Wang, B. Zheng, Q. Li, C. Shen, and Z. Ba, "Towards Query-Efficient Adversarial Attacks Against Automatic Speech Recognition Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 896–908, 2021, doi: 10.1109/TIFS.2020.3026543.

[14] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, "SurfingAttack: Interactive Hidden Attack on Voice Assistants Using Ultrasonic Guided Waves," presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020. doi: 10.14722/ndss.2020.24068.

[15] T. Chen, L. Shangguan, Z. Li, and K. Jamieson, "Metamorph: Injecting Inaudible Commands into Over-the-air Voice Controlled Systems," presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020. doi: 10.14722/ndss.2020.23055.

[16] C. Sebastian, "Getting lost near the Kremlin? Russia could be 'GPS spoofing,'" *CNNMoney*, Dec. 02, 2016. https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/index.html (accessed Aug. 03, 2021).

[17] "Year-long ocean cruise finds GNSS interference," *GPS World*, Mar. 13, 2019. https://www.gpsworld.com/year-long-ocean-cruise-finds-gnss-interference-everywhere/ (accessed Aug. 03, 2021).

[18] J. Aru Saputro, E. Egistian Hartadi, and M. Syahral, "Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test," in *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*, Oct. 2020, pp. 95–100. doi: 10.1109/ICITAMEE50454.2020.9398386.

[19] J. Detsch, "The U.S. Army Goes to School on Nagorno-Karabakh Conflict," *Foreign Policy*. https://foreignpolicy.com/2021/03/30/army-pentagon-nagorno-karabakh-drones/ (accessed Apr. 22, 2021).

[20] E. Kuczynski, "What is a Faraday Cage?" https://www.signalsdefense.com/blog/what-is-a-faraday-cage/ (accessed Aug. 03, 2021).

[21] S. Bryen, "Russia knocking Turkish drones from Armenian skies," *Asia Times*, Oct. 26, 2020. https://asiatimes.com/2020/10/russia-knocking-turkish-drones-from-armenian-skies/ (accessed Apr. 22, 2021).

[22] D. Dixon, "New drone apps, technology create invisible fences," *The Florida Times-Union*. https://www.jacksonville.com/metro/business/2017-07-29/new-drone-apps-technology-create-invisible-fences (accessed Aug. 03, 2021).

[23] "Trained Police Eagles Attack Drones On Command," *Popular Science*, Feb. 02, 2016. https://www.popsci.com/eagles-attack-drones-at-police-command/ (accessed Aug. 13, 2021).

[24] T. Moynihan, "Combat Drones That Are Built for Bashing Into One Another," *Wired*. Accessed: Aug. 03, 2021. [Online]. Available: https://www.wired.com/2015/10/game-of-drones/

[25] K. Hartmann and K. Giles, "The Next Generation of Cyber-Enabled Information Warfare," in *2020 12th International Conference on Cyber Conflict (CyCon)*, May 2020, vol. 1300, pp. 233–250. doi: 10.23919/CyCon49761.2020.9131716.

[26] A. Stoica, "From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment," vol. 1, no. 1, p. 9, 2020.

[27] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *ArXiv210100292 Cs*, Jan. 2021, Accessed: Aug. 03, 2021. [Online]. Available: http://arxiv.org/abs/2101.00292

[28] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2020, pp. 1010–1015. doi: 10.1109/CCWC47524.2020.9031175.

[29] "New Earth Surveillance Tech Is About to Change Everything, Including Us." https://www.vice.com/en/article/wxebk5/new-earth-surveillance-tech-is-about-to-change-everything-including-us (accessed Aug. 03, 2021).

[30] "Open-source intelligence challenges state monopolies on information," *The Economist*, Aug. 07, 2021. Accessed: Aug. 16, 2021. [Online]. Available: https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information