ENVISTACOM

WHITE PAPER

Protecting the Protectors

BY: ALAN L. LEWIS, CP APMP

The mission of America's defense industrial base is to equip America's warfighters with mission-critical technology and solutions necessary to counter existing and emerging threats and protect military personnel, civilians, and vital infrastructure worldwide. That salient mission encompasses everything from Research and Development (R&D), engineering, and solution/product development to support functions such as human resources, training, and Information Technology (IT).

Leveraging expertise and strategic investment in people, processes, and technology to push the boundaries of what's possible and to offer America's defense customers relevant, innovative, yet practical solutions, enables them to meet the rigors of their missions and operations in both austere and peaceful environments. Adopting a 360-solution development approach that encompasses the current and future needs of the Department of Defense (DoD), centered on the military's strategy/goals, mission/tactics, enemy practices, and warfighter implementation offers the best assurance for highly effective solutions.

In this paper, we'll focus on some of the ways the defense industry can effectively incorporate system-protective measures for our protectors—the warfighters—from Safety in System-Level Design, Enemy Countermeasures, and Cybersecurity perspectives.

SAFETY IN SYSTEM-LEVEL DESIGN

Actively investing in smarter, more efficient, and operationally safe Satellite Communications (SATCOM) systems is one way to provide for the warfighters' safety. Below are four areas that will enable defense agencies to meet this challenge.

Next Generation SATCOM Antenna Technology: Traditionally, customers have chosen larger SATCOM antennas because of their innate ability to acquire signals; however, the constant trade-off between physical size of the dish versus power output versus bandwidth throughput (especially in Geostationary Orbit (GEO) and Medium Earth Orbit (MEO)) is driving SATCOM systems to be smaller and more power-efficient, while maintaining the same or similar performance capabilities. Modern antenna innovations have prompted a shift in thinking regarding the deployment of small aperture antennas to be acceptable, and often preferred, for certain applications. Investigating and developing next generation technology to provide an increased level of warfighter safety by reducing the antenna profile and requiring fewer individuals to operationally deploy the terminal in a substantially shorter timeframe is needed.

Transport Virtualization Ecosystem: An additional area of next generation technology that's being actively pursued in the defense industry is the development of a Transport Virtualization Ecosystem where commercial proprietary and DoD-owned modem waveforms are deployed as applications on Commercial Off the Shelf (COTS) High Performance Computing (HPC) hardware. This same COTS hardware can be simultaneously used for other adjacent transport virtualization applications like encryption (e.g., TRANSEC), intrusion detection/prevention, cyber sensors, WAN optimization, etc., minimizing the number of disparate appliance and associated power and cooling resources that need to be deployed in support of network operations. The underlying technology helps make future communications inherently more resilient and secure through activities like "wave hopping," which effectively hardens the network against jamming and hacking, making it more difficult for adversaries to interfere with communications. This capability prevents the enemy from detecting and interfering with electronic signals and posing a greater threat to military command and control. Patents on this underlying technology grant the right to exclude others from making, using, or selling it; essentially rendering the technology property of the inventor. This capability prevents the enemy from detecting and interfering with electronic signals and posing a greater threat to military command and control.

Portable Baseband Data Package: SATCOM systems are often susceptible to heat seeking radio detection and targeting type weapons. Developing the ability to deploy a portable baseband data package with the antenna and locating it up to 150 feet away from the baseband data package via coaxial Interfacility Link (IFL), and even farther via fiber optic IFL, addresses that susceptibility. During training exercises, operators may only need to be a short distance from the baseband, but while in-theater (hot zones), this capability also keeps the warfighter a safe distance away from the reflector which, because of RF signal emission, is often subject to enemy Direction Finding (DF), or Radio Direction Finding (RDF) (the method of measuring the direction from which an RF signal was transmitted), and is often the target of air to ground missiles. Warfighters can remotely and safely manage, maintain, operate, and shut down the equipment from either a technical control facility or simply in the field using an optimized Monitor and Control (M&C). The M&C software can be installed on a laptop connected to the baseband equipment up to 300 feet away via ethernet (or further distance away via fiber). Actively evaluating other secure wireless technologies to add greater operational capabilities for stand-off operations will also provide greater safety and flexibility to the warfighter.

Lightning Strike Protection: Because some dangers occur from natural, environmental events such as lightning strikes, to susceptible SATCOM terminals, engineering traditional ground rods for stationary solutions that connect the grounding system of electrical components to earth ground or using alternative grounding protection kits for highly mobile SATCOM systems will help prevent damage done by natural events. Either solution averts the danger away from SATCOM operators and the system's baseband equipment.

Figure 2: Preparing the Canvas

ENEMY COUNTERMEASURES

On the battlescape, enemies use tools like reconnaissance aircraft, Unmanned Aerial Vehicles (UAV), drones, radar, and satellite imagery to carry out real-time surveillance. Providing protective countermeasures to the warfighter by developing and/or incorporating equipment to conceal the warfighter's location, capabilities, and/or vulnerabilities can prevent or mitigate these types of surveillance activities.

For instance, tenting/canvas covers for many systems offer a simple, flexible, and low cost solution in this regard. This functionality not only hides the terminal visually (i.e., shapes and light), but can also be designed to camouflage the thermal signature, sound, and magnetism emanating from the equipment. The covering helps prevent casting of shadows and disrupts equipment outlines by mimicking the surrounding terrain color and texture depend on the area of operation). Textiles may also help conceal the equipment from night vision instruments. Coverings help protect the terminal from the elements, such as sand, wind, water, dust, direct sunlight, and heat thus extending equipment life and ensuring operational performance when needed by the warfighter. Components with blackout lights and/or a cover that hides the lights (vehicle lights, equipment LEDs/LCDs, etc.), will greatly improve concealment when operating in-theater or adverse environments.

Additional tools include implementing low-heat signature radiating devices into many solutions. Electronics and power sources (generator, Uninterrupted Power Supply (UPS), etc.) contribute to an overall heat signature. High Performance Amplifiers (HPAs) and integrated Block Upconverter (BUC)/Solid State Power Amplifiers (SSPAs) using Gallium Nitride (GaN) technology can effectively diminish the heat signature, thereby providing increased power efficiency for many devices. These improvements can provide tangible Size, Weight and Power (SWaP) enhancements. Additionally, employing low-to-no heat producing generators, battery-operated, and solar powered solutions will all reduce the heat signature of SATCOM systems.

Figure 3: Securing Against Cyber Attacks

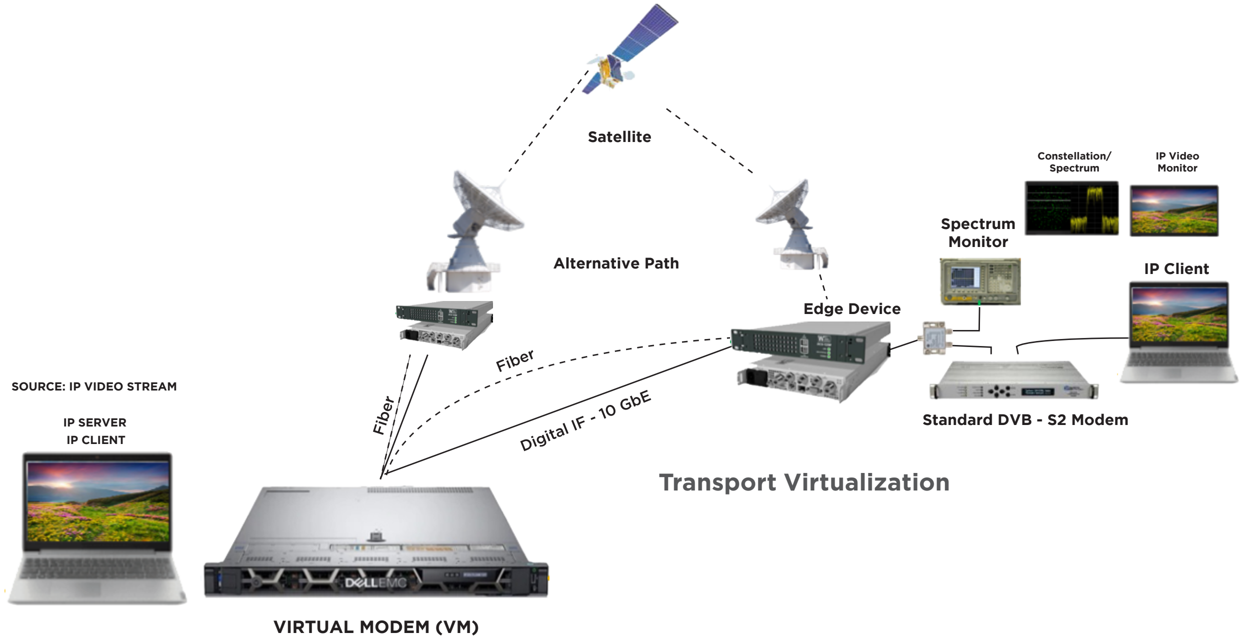
CYBERSECURITY

As the DoD's systems and networks become more interconnected and collaborative, greater and faster access to mission-critical data is made possible. Warfighters rely on these communications systems (including SATCOM) for in-theater situational awareness. Commanders rely on these systems to make quick, agile mission decisions. The timely transfer of vital orders and bi-directional dissemination of perishable information is essential during combat or training exercises. This increased interconnectedness, however, gives the enemy a larger attack surface on which to execute electronic and cyber exploits against our networks, sensors command and control, and IT infrastructure. The volume of cyber-based attacks are increasing exponentially, and hostile actors' methods and tools are becoming more sophisticated.

A cyber approach, capabilities, and methods to counter cyber threats ensures networks containing sensitive information regarding capabilities, locations, operations/missions, plans, etc. remain secure, thus protecting the warfighter. Maintaining robust cyber hygiene practices can ensure optimum system health and strengthen online security. For basic "cyber housekeeping" we must lean on the National Institute of Standards and Technology's Cybersecurity Framework (NIST) guidance and Department of Defense Cybersecurity Analysis and Review (DoDCAR), a framework that performs threat-based, cybersecurity assessments on architecture. Additionally, MITRE ATT&CK, a globally accessible, centralized repository of known techniques and attacks that adversaries use to exploit systems should be used in tandem with other cyber hygiene practices.

SATCOM designers must work to protect the most vulnerable components of the SATCOM ecosystem – the satellite to ground link, or the transmission element. The satellite to ground link is vulnerable to kinetic attack, jamming, interception, or other degradation; therefore, actively developing new techniques and technologies to counter these challenges is important. Three of the greatest SATCOM vulnerabilities include credential compromise, Denial of Service (DoS), and attacks on supply chain.

SATCOM Vulnerabilities	Mitigation Techniques
Credential Compromise	When the enemy targets credentials, humans are leveraged as the weak link because breaking into the command and control planes yields much greater access than just a point in the data plane. Hiding the traffic in the noise makes it more difficult for malicious actors to target communications.
Denial of Service (DoS)	The enemy often employs DoS, a situation in which the attacker renders a network unavailable to users through disruption of service. Virtualizing the system (and the roaming techniques) helps the warfighter thwart DoS attempts.
Attacks on Supply Chain	The supply chain is fraught with counterfeit parts, materials, and assemblies. Malicious malware or backdoors may be installed on devices before they are even delivered to a customer. Hardest hit by these forgeries are dedicated government assets such as Global Broadcast Service (GBS) and Advanced Extremely High Frequency System (AEHF). As the government builds additional SATCOM infrastructures, these threats must be prevented. Industry leaders continuously work to strengthen their suppliers' cybersecurity posture and protect our development environment by: • tracking clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns • using automated tools to continually assess our vendor's networks • ensuring a viable patch management is in place and executed • employing methods for verification of distributed binaries through hash checking with our suppliers, and other integrity checking mechanisms • scanning all downloads for malicious signatures and testing software updates prior to deployment



Transport Virtualization

Transport Virtualization Ecosystem (mentioned earlier) allows rapid development of solutions interoperable within the warfighter's operational architecture and Cyber-Resilient within the theater. By having a true virtual development environment, defense industry engineers must develop cutting edge secure communications capabilities, like quantum-based communications for quantum key distribution (QKD), making eavesdropping by rogue actors virtually impossible. These capabilities can be tested with other components within the virtualization of network capabilities (i.e., modems, routers, switches, etc.). This enables the Cyber Test and Evaluation (T&E) teams and developers to not only harden the system, but also evaluate adversarial attack tactics and techniques in a controlled, repeatable scientific manner.

CONCLUSION

Let's face it—accelerated communications requirements in response to ever-evolving enemy tactics, along with the increasing fluidity and complexity of the battlescape, make communications more critical now than ever before. DoD SATCOM systems provide the near instantaneous data exchange between the warfighter and command and control centers contributing to their importance, thus, enabling warfighters to conduct missions safely and reliably.

Technology capabilities that enable the collection of intelligence and distribution of orders safely, rapidly, and continuously is paramount. Warfighters gain and preserve an edge over the enemy by imposing their will on the offensive and defensive decision-making cycle. Ongoing innovation based on the warfighter's evolving needs and their mission-critical work involving the defense of our nation will ensure they're always at the top of their game.

Alan L. Lewis, CP APMP, is a Senior Proposal Manager at Envistacom, LLC. He has more than 25 years of capture/pursuit management, process development and improvement, and marketing communications experience in the public and private sectors. Alan can be reached at alewis@envistacom.com.

Thanks to my Envistacom colleagues, Dexter Campbell, Director, Army and USMC Programs; Dewell Mitchell, Director of Sales Engineering; Steve Reeder, Sr. Architect (Cyber & Engineering); and Jennifer Harris, Freelance Proposal/Technical Writer for their insights and contributions to this whitepaper.

Photo credit: (p.1) Cpl. Destiny Dempsey • (p.2-3) Sgt. Jack Adamyk and Staff Sgt. Jonathan Snyder, respectively

The appearance of U.S. visual information does not imply or constitute DoD endorsement.