C4ISRNET

THE EVOLUTION OF WARFARE IN THE CYBER ERA

Sponsored by:

leidos

Cyber training exercises help integrate infantry ground units with cyber, signal and human intelligence collection capabilities, giving units on the modern battlefield a broader capacity to search out and isolate their enemies in real time.

CAPT. MEREDITH MATHIS / 2ND STRYKER BRIGADE COMBAT TEAM, 2ND INFANTRY DIVISION

THE EVOLUTION OF WARFARE IN THE CYBER ERA

By: Matt McLaughlin

On Feb. 24, 2022, Russian government hackers launched a cyberattack on the U.S. satellite company Viasat, using malware called AcidRain to erase data from modems and routers in Viasat's system. The attack, launched one hour before Russia's invasion of Ukraine, permanently disabled thousands of machines in the Viasat network, hampering communication by the Ukraine military.

The cyberattack was one of many that Russia has carried out against Ukraine over the last decade, including attacks on critical infrastructure in 2015 and 2016 that knocked out power in Ukrainian cities. Russian hackers also attacked businesses and other organizations across Ukraine in 2017 with Petya malware that resembled ransomware, wiping data from computers.

The attack on Viasat represents a significant milestone in cyberwarfare, as it targeted tactical elements used for military operations on the ground, whereas the earlier attacks were aimed at critical infrastructure and other businesses.

"The Russian attacks on Ukraine show how a U.S. near-peer power treats cyber in actual warfare," said Paul Butterfoss, vice president of cyber solutions with Leidos, a science and technology solutions leader in the defense sector. "We have a good understanding for how cyber is used in relative peacetime. It's the primary method of attack in the gray zone of asymmetric warfare. But we haven't had a lot of experience with how cyber is used in a full-scale, kinetic conflict. I think there's recognition that systems at the edge are vulnerable, but can they actually be exploited in real-time during battle? And how do we improve our integration of full-spectrum cyber capabilities with the other warfighting domains [air, land, sea, and space] as part of a kinetic conflict with a near-peer adversary?"

The state of U.S. military cyber

Cyberwarfare can be waged at multiple levels. In cyberspace, attacks that penetrate a network can be used to affect an adversary by influencing critical infrastructure such as power and utilities. At the tactical level, electronic warfare and electromagnetic effects can affect opposing troops, hampering their offensive or defensive efforts. A third level involves information and influence operations that can disrupt institutions such as elections or governments.

The U.S. military aims to build powerful offensive and defensive capabilities in each of these areas to maintain its information advantage and decision

dominance. As it engages in this effort, resilience has become a key concept. U.S. forces must maintain the effective operation of their own systems to achieve mission objectives. Deterrence is also a critical element, as projecting offensive strength can dissuade potential attackers.

Ultimately, the U.S. military intends to extend its dominance from traditional battlespaces into cyberspace, affecting communications, intelligence and information systems. Cyberattacks aim to degrade an opponent's information capabilities and thereby provide an operational advantage. By combining kinetic capabilities with cyberattacks, a force can more precisely and effectively destroy intended targets.

"Although destructive attacks are most attention-grabbing, Russia's main cyber activity in Ukraine has probably been intelligence collection," said James Andrew Lewis, senior vice president of the Center for Strategic and International Studies, in a June 2022 report. "Russian hackers have most likely sought to gather data to inform Moscow's prewar planning, kinetic targeting, occupation activities, influence operations, and future negotiations with Kyiv."

At the tactical level, the stakes are particularly high. U.S. troops on the battlefield don't have the luxury of waiting to reboot systems or find alternatives. Critical systems must operate as expected at the moment they are needed, and failure can cost lives.

In an era when news of information breaches seems constant, effective cybersecurity may seem unachievable. But results from the war in Ukraine suggest a different story. Ukraine has learned from years of weathering Russian cyberattacks, and support from Western allies, as well as the technology industry, has enabled it to improve its cybersecurity posture.

"The war has demonstrated that cyber defense is not a hopeless cause," said Nick Beecroft, a nonresident scholar in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, in a December 2022 interview.

Key U.S. cyber capabilities

The U.S. faces a massive challenge in fielding effective offensive and defensive cyber capabilities. As information technology plays an increasingly important role in modern life, the number of assets that could be targeted by a cyber adversary also increases. The integration of operational technology with IT to create Internet of Things systems adds to the scope and complexity of the situation. As more systems create, compile and analyze data while relying on automation to improve speed, accuracy and efficiency, the more vulnerable U.S. forces become to disruption by cyberattack.

"The cyber attack surface is approaching infinity," Butterfoss said. "And given the interconnected society that we live in, those attacks can quickly propagate, both in the civilian space and on the battlefield."

Further, the strategic advantage that the U.S. has enjoyed for decades has been eroding rapidly because of cyberwarfare. Adversaries such as Russia, China, Iran and North Korea have developed powerful cyberwarfare capabilities in an effort to close the gap with the U.S.

The security of the supply chain for U.S. forces has become an imperative in terms of cyberwar. This includes hardware manufactured by a foreign power with vulnerabilities that could be exploited at high-leverage moments, such as in combat. The software supply chain poses even greater challenges, as demonstrated by the 2019 and 2020 Russian cyberattacks on SolarWinds, a software company whose cloud-based system management tools were widely used across industries. The ubiquity of SolarWinds software led to thousands of organizations being affected, including government agencies such as the departments of State and Homeland Security, as well as companies such as Microsoft, FireEye, Intel and Cisco.

A Zero Trust approach to security

To address these issues, U.S. military systems must be built with trusted technologies and must be integrated into an overall security environment that protects data and minimizes vulnerabilities.

The Zero Trust approach to security has emerged as an essential element of efforts to improve the U.S. ability to defend itself in the context of cyberwarfare. A Zero Trust architecture requires all users who connect to an organization's network to be authenticated. Whether they reside within the network or access it remotely, users must be authorized to gain access to applications and data, and the security configuration of their systems must be continuously validated.

In May 2021, the Biden administration published an executive order that establishes a Zero Trust strategy for the federal government and requires agencies to develop a plan to implement a Zero Trust architecture.

The Defense Department published its DoD Zero Trust Strategy in October 2022, laying out a roadmap to improve the security of military devices, application, assets and services.

"Our adversaries are in our networks, exfiltrating our data, and exploiting the

Department's users. The rapid growth of these offensive threats emphasizes the need for the Department of Defense (DoD) to adapt and significantly improve our deterrence strategies and cybersecurity implementations," said DoD CIO John B. Sherman in a foreword to the document. "To meet these challenges, the DoD requires an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly as possible."

DoD will rely on the defense industry as it addresses this challenge. For example, Leidos uses its Zero Trust Readiness Level (ZTRL™) tool suite to simplify Zero Trust adoption for government organizations. The suite includes customizable dashboards that can assess an agency's plans and progress toward meeting the criteria established by DoD's Zero Trust Strategy and other guidelines.

The DoD also is developing and training its forces to meet the new challenges of cyberwarfare. The military services are engaging in Expeditionary Cyber initiatives that will leverage cyber operations, analysis, network management, platform design and sustainment. For example, the Army activated its Cyber Electromagnetic Activity (CEMA) battalion in October 2022. The battalion, the first of its kind in the Army, brings offensive cyberspace and electronic warfare capabilities.

A cyber warfare operations journeyman assigned to the 175th Cyberspace Operations Group of the Maryland Air National Guard monitors live cyber attacks on the operations floor of the 27th Cyberspace Squadron.

JOSEPH EDDINS / AIRMAN MAGAZINE

Defensive challenges and capabilities

DoD has considered cybersecurity a priority for decades and has made continuous efforts to improve its strategy in this arena. In February 2023, the department released its 2023-2027 DoD Cyber Workforce Strategy, which establishes how DoD intends to create a cyber workforce that meets its numerous, complex and evolving needs. The strategy sets out DoD's approach to address its shortcomings in workforce development, better manage its cyber workforce and stay at the forefront of technological advances.

The DoD's Zero Trust Strategy represents another major piece of the department's approach to cyber challenges. The strategy spells out how DOD will promote adoption of Zero Trust across all personnel, implement Zero Trust practices in new and legacy systems, deploy new technologies at least at the pace of industry and align other policies with Zero Trust principles.

Establishing trusted identities to govern access to critical systems poses a major challenge to any enterprise implementing Zero Trust, but for DoD it can be a matter of life or death. For example, at the tactical level, warfighters must be able to validate that command, control, communication and intelligence are

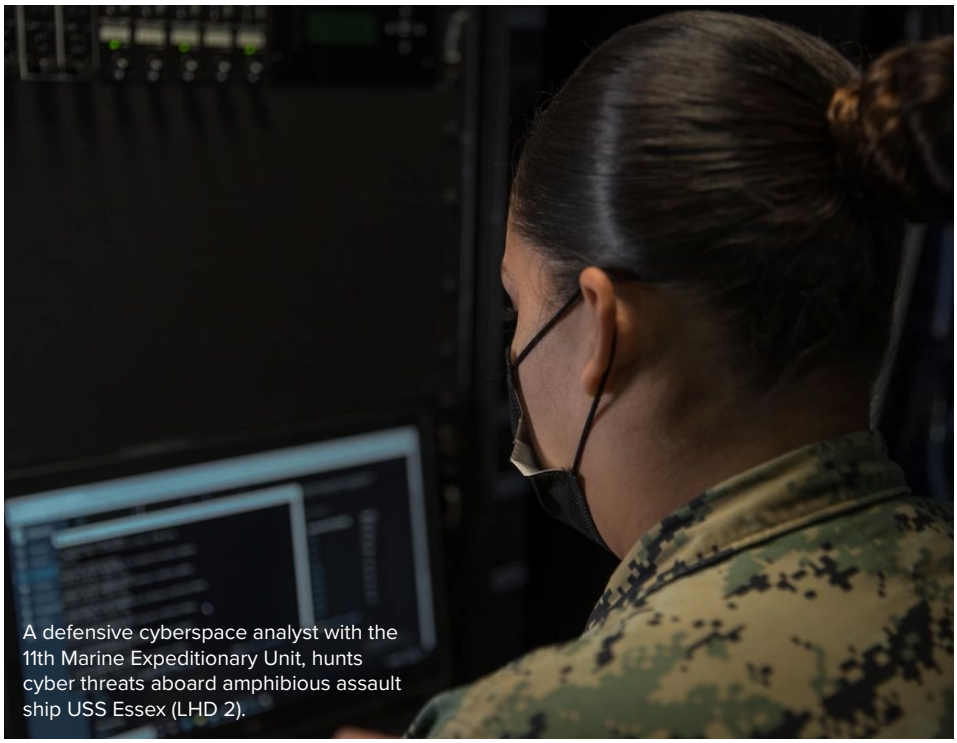
trusted and legitimate. As technology such as deep fakes creates the potential for disinformation, trust is even more challenging to establish.

"When you hear someone's voice over the radio and it sounds like your commander, is it actually your commander?" Butterfoss said. "That's one of the hard problems we are working to solve. It's challenging enough addressing deep fakes and other deception techniques in the enterprise when you have massive amounts of compute resources. It gets exponentially more difficult at the edge, especially when bullets are flying."

Zero Trust also requires detailed visibility into the systems it governs. Military personnel must know where systems and information reside, how they are operating and what they need to maintain effective operation. Security orchestration and automated response (SOAR) solutions enable this capability while speeding up and improving the accuracy of response to certain cyberthreats.

In fact, automation capabilities enabled by artificial intelligence and machine learning hold significant promise as a force multiplier for DoD, even beyond the cyber arena. The automated nature of these technologies also reduces the burden on IT personnel to handle rote tasks and allows them to focus on more challenging issues.

Effective cyber defenses, enabled by Zero Trust and other elements of DoD's cybersecurity strategy, will establish and improve the resilience of a variety of tactical elements, including position, navigation and timing systems, command and control, and key weapons systems. At the strategic level, these defenses will help DoD deal with threats such as insiders who seek to compromise Defense information systems.



A defensive cyberspace analyst with the 11th Marine Expeditionary Unit, hunts cyber threats aboard amphibious assault ship USS Essex (LHD 2).

U.S. MARINE CORPS PHOTO BY SGT. JENNESSA DAVEY

Going on the offensive in cyberspace

As world powers such as the U.S., Russia and China develop offensive cyber capabilities, the concept of deterrence has emerged as an essential element of their approaches to cyberwarfare, much as it has served as a key tenet of nuclear warfare for the last 70 years.

Secretary of Defense Lloyd J. Austin III has stated that integrated deterrence among the domains of warfare, including the cyber domain, is part of the foundation of the U.S. National Defense Strategy. As with conventional or nuclear warfare, the concept of proportionate response is important in the context of cyberwarfare. For example, lethal attacks on the U.S. or its citizens may lead to a lethal response. However, identifying the actions that demand a response in the cyber domain and establishing an appropriate response remains a challenge.

In many cases, the cyberwarfare that has been carried out until now has greatly affected civilian populations. The U.S. military is still determining what offensive capabilities are acceptable to use, under what circumstance they should be used and the extent to which they may be employed. Balancing these factors will require thoughtful consideration by military and civilian leaders and likely will continue to change as the nature of cyberwarfare evolves into the future.

As the conduct and scope of cyberwarfare evolves, the U.S. also needs to develop the skills and numbers of its cyber warriors. Science, technology, engineering and mathematics education in general will remain an important focus, as will specific training in cyberwarfare. Further, the U.S. must determine how it will rely on automation as it conducts cyberwarfare. Automated systems enable greater effectiveness and efficiency, but this must be balanced with human judgment.

In 2022, the Army announced that it would establish an office to oversee offensive cyber and space capabilities. The Program Manager Cyber and Space office will test and field tools such as aerial jamming pods, biometric information systems, and battlefield navigation tools.

The future of U.S. military cyber

As the nature of cyberwarfare evolves, the U.S. will continue to advance its offensive and defensive capabilities. This will involve the participation of industry as well as government agencies and military forces. The involvement of private companies in the cyber defense of Ukraine demonstrates how this likely will take place going forward, according to the Carnegie Endowment's Nick Beecroft.

"The war has exposed the huge role of the private sector in defending digital networks at national scale," Beecroft said. "Commercial entities have morphed from vendors to vital agents of defense and foreign policies."

The role that Zero Trust Architecture has played in U.S. cyber defenses also will grow. The implementation of Zero Trust is a process that will change over time as technology advances and the tactics of U.S. adversaries evolve.

Implementing Zero Trust will be a continuous process in the face of evolving circumstances. Additional Zero Trust enhancements will be incorporated in subsequent years. For example, advances in biometric technologies will improve defensive capabilities in cyberspace by more accurately and effectively establishing a user's identity.

Many new and enhanced technologies will affect cyberwarfare in the future. Quantum computing is expected to become commercially available over the next decade, which will have massive impact on the use of encryption technologies to protect data. Quantum tools could easily crack data encrypted using current methods, so cyber defenses will need to use new approaches — including quantum-safe encryption — to secure systems and data. Quantum networks will also affect the way military forces communicate and transmit data, enabling new capabilities while improving the speed and precision of operations.

Automation will also play an important role in the future of U.S. cyber. Powered by AI and ML, automated systems will be able to detect and respond to attacks without human intervention. On the tactical level, this will help U.S. forces become more dynamic and reconfigurable, enabling rapid change to deal with new factors on the battlefield and in cyberspace.

Advances in technology also will yield new capabilities in deception on the battlefield. U.S. forces will need tools that can determine if the targets they are aiming at are, indeed, real. They'll also employ offensive deception to fool adversaries, costing them time and effort and forcing them to expose operational assets.

"Things are changing and evolving within our environments, and we need to be the masters of that change, which includes leaving things behind that are legacy, and figuring out how we make those changes beneficial, from a capability perspective," Butterfoss said. "We have a lot of legacy systems that we're still supporting, and yet, we still talk about all these future technologies that we want to bring in. Having them all in one environment together becomes the struggle. We need a way to push through change." C4

About C4ISRNET:

C4ISRNET is dedicated to the technologies of communications, defense and intelligence IT, unmanned systems and sensors, GEOINT, and cyber. It's the networked capabilities of these technologies that have transformed the enterprise of warfare. Defense and intelligence officials rely on C4ISRNET for information on advanced weapons platforms, sensor systems, and command-and-control centers that provide information advantage, battlefield dominance, speed of command and mission effectiveness. To stay informed, visit c4isrnet.com.

About Leidos:

Leidos is a Fortune 500® technology, engineering, and science solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, civil, and health markets. The company's 45,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $14.4 billion for the fiscal year ended December 30, 2022. For more information, visit www.Leidos.com.
23-LEIDOS-0419-26303