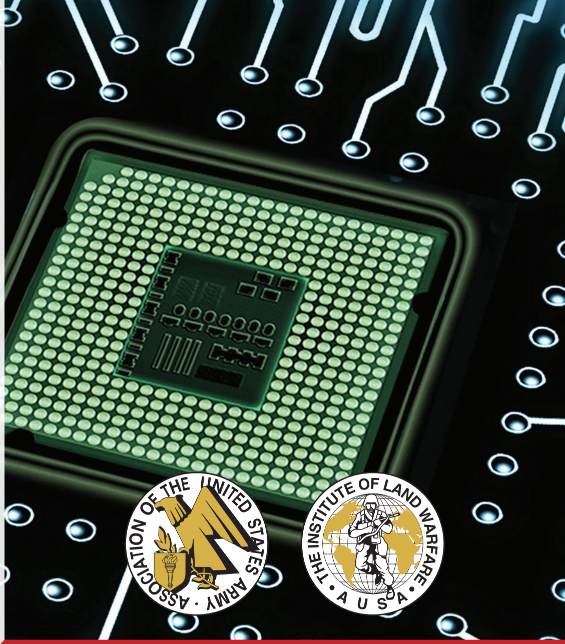
ILW SPOTLIGHT 17-3

Securing the Army's Weapon Systems and Supply Chain against Cyber Attack

by LTG Larry Wyche, USA Ret., and Mr. Greg Pieratt

PUBLISHED BY THE INSTITUTE OF LAND WARFARE
AT THE ASSOCIATION OF THE UNITED STATES ARMY



NOVEMBER 2017

> *From leaders, to providers, to cyber warriors, to users, each Soldier provides a critical link in cybersecurity. . . .*
>
> Major General Patricia Frost,
> Director of Army Cyber Operations[1]

Nearly two decades into the 21st Century, the United States finds itself immersed in a security environment of unprecedented complexity; one defined by re-emerging nationalism, religious radicalism, uncertainty and volatility. America faces a number of existential threats, ranging from the emergence of several capable regional peer competitors to the extension of war into cyber and space domains.[2] The offensive cyber capabilities of America's enemies continue to evolve and have now reached the point that the Army's weapon systems, the industrial controls used to manufacture them and the supply chain employed to sustain them are vulnerable to compromise.

The United States has an immense array of military forces ready to defend the nation and its allies. To sustain its globally-deployed forces and rapidly replenish combat losses, the Department of Defense (DoD) possesses a materiel capacity second to none. Likewise, the Army, as an integral part of the larger joint force, maintains strategically positioned, forward-based stocks around the globe. The Army is also able to reach back and draw upon a vast industrial enterprise. This includes: the Army's Organic Industrial Base (OIB), made up of 23 unique manufacturing and production facilities that repair and recapitalize equipment, manufacture service parts and produce many of the nation's munitions; the larger Defense Industrial Base, encompassing both organic components and more than 100,000 private sector companies and their subcontractors who perform under contract; and a multitude of commercial service providers who supply the energy, communications, transportation and utilities required to execute military operations.

Underpinning the efforts of this prodigious undertaking is the Single Army Logistics Enterprise (SALE), one of the largest and most complex enterprise resource planning (ERP) systems ever fielded. Synchronizing over 80 separate databases, SALE captures global resource requirements and provides world-wide asset visibility, all in real time.

ISSUE

The U.S. Army's weapon systems, the industrial controls used to manufacture them and the supply chain employed to sustain them are vulnerable to compromise by adversary offensive capabilities.

SPOTLIGHT SCOPE

- Addresses the potential impact of cyber threats to the Army's supply chain and the corresponding vulnerability of many of its most important systems.
- Describes potential sabotage venues, countermeasures and recommendations for a policy roadmap to secure the Army's supply chain.

INSIGHTS

- The first shots of the next war could likely be fired in cyberspace.
- The Army should apply the same level of effort that it invests in safeguarding its networks and information systems toward protecting its armaments and its ability to sustain them.
- Continued implementation of rigorous quality standards, blind buys, the use of tamper-proof packaging and serial number control, software assurance and the establishment of trusted foundries can substantially reduce the opportunities for infiltration by potential adversaries.

[1] Patricia Frost and Matthew Hutchinson "Top 10 Questions for Commanders to Ask About Cybersecurity," *Small Wars Journal*, 8 December 2015.

[2] U.S. Army Training and Doctrine Command (TRADOC), Field Manual (FM) 3.0, *Operations* (Washington, DC: Government Printing Office, 2017), pp. 1-6–1-10.

The recent expansion of military operations into the cyber domain places this breakthrough at risk. War is about human behavior. Operational success goes to those militaries who are forward-thinking, able to learn rapidly, adapt and react quickly and who can manage risk in a rapidly changing environment. In a few short years, America's competitors have modernized and learned from U.S. joint force operations. They have also revolutionized their cyber capabilities. Adversaries now possess the ability to disrupt economic systems, command and control, infrastructure and logistics operations and even to negate the effects of America's weapon systems. In fact, worldwide cyber capabilities have advanced to the extent that the next conflict could well be decided in cyberspace. The Army's senior leadership has warned: "The first shots of the next actual war will likely be fired in cyberspace, and likely with devastating effect."[3]

This new strategic reality is addressed in the President's Executive Order of 11 May 2017, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The order requires a presidential report on "cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks."[4]

The United States has made significant headway in the integration of cyber into its operations while continuing to develop and enhance both offensive and defensive military capabilities. Since the activation of the U.S. Cyber Command (CYBERCOM) and the U.S. Army Cyber Command (ARCYBER) in 2009, priority of effort has been to protect DoD and Army networks and information systems against interruption and exploitation—and rightly so. After significant investment of time and resources, the Army has made substantial progress toward the achievement of this aim.

The United States has made significant headway in the integration of cyber into its operations while continuing to develop and enhance both offensive and defensive military capabilities.

However, the cyber capabilities of America's enemies are much more expansive and they continue to evolve. **The Army's weapon systems and the supply chain that supports them are now more vulnerable than ever. To counter this threat, the same level of effort invested in safeguarding the Army's networks and information systems must now be committed toward protecting its armaments and its ability to sustain them.**

A Troubling Possibility

Imagine a scenario in which the United States finds itself engaged in conflict against an aggressor who launches a surprise invasion of an allied nation. U.S. forces are deployed and make contact with enemy forces. Without warning, strange things begin to happen:

- ground-launched anti-tank missiles fail to function;
- the enemy takes control of U.S. satellites;
- anti-aircraft missiles miss their targets; and
- U.S. artillery explodes over friendly forces.

In the Continental United States, the 23 manufacturing arsenals, depots and ammunition plants of the Army's OIB swing into full gear to support the fight. As they work around the clock to repair equipment, manufacture service parts and produce munitions, they begin to encounter problems which severely degrade their operations:

[3] Nikki Ficken, "AMRDEC Workshop Promotes Cybersecurity Awareness," *Army News Service*, 7 April 2016.

[4] President Donald J. Trump, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Presidential Executive Order, 1 May 2017.

- diagnostics provide false readouts or order the wrong parts;
- errors appear in shipping manifests and commodities are loaded onto the wrong ships going in the wrong direction; and
- cyber attacks on the water systems and power grids of Army installations disrupt the manufacture of equipment, munitions and materiel or delay the deployment of forces.

Firmware provides guidance for weapon systems and allows industrial controls to conduct diagnostics and perform precision machining.

Subsequent investigation reveals that the failure of the Army's weapon systems, along with its inability to sustain them, occurred through a combination of altered firmware (the proprietary software used to control weapon systems), and compromised electrical components and integrated circuitry, all of which were introduced into the supply chain months or years before. The attack may have been a manifestation of one of the enemy's latest tactics, the zero-day attack, in which adversaries exploit a critical but undiscovered flaw in a weapon system's firmware and so cause irreparable damage.[5, 6, 7]

The danger is acute, and the damage resulting from a cyber attack on the Army's logistics enterprise could be catastrophic. The Army's program executive offices, program managers and Army Materiel Command's research, development and engineering centers are working in collaboration to prevent such a catastrophe, but are under-resourced. The incidents described below illustrate the scope of this threat.

Cyber Breaches of USTRANSCOM and Army Weapon Systems

From 2008 to 2013, there were a number of documented incidents in which adversarial hackers used zero-day exploits and phishing attacks to break into the information systems used by contractors working for U.S. Transportation Command (USTRANSCOM), the unified combatant command responsible for moving U.S. troops and distributing military equipment around the world. Opposing militaries have long assessed that logistics and mobilization are potential U.S. vulnerabilities and have advocated cyber operations against America's command, control and logistics networks and weapon systems in the early stages of any potential conflict.[8, 9]

Congress investigated USTRANSCOM's operations during a one-year period from 2012–2013 and discovered evidence of approximately 50 attempted attacks on USTRANSCOM contractors. At least 20 of these attacks were successful, including a 2012 attack in which a regional competitor was able to compromise multiple systems aboard a commercial vessel contracted by USTRANSCOM.[10, 11]

In 2014, Senator James Inhofe, Ranking Member and Chairman of the SASC (Senate Armed Services Committee) Subcommittee on Readiness, stated, "We must ensure that cyber intrusions cannot disrupt our mission readiness."[12] To this end, $200 million was authorized in the 2016 National Defense Authorization Act; a follow-up report to Congress is required by 2019.[13, 14]

[5] FireEye.com, "What is a Zero Day Exploit?" May 2017.

[6] Lillian Ablon, "RAND Study Examines 200 Real-World 'Zero-Day' Software Vulnerabilities," RAND Corporation, 9 March 2017.

[7] Lillian Ablon and Timothy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and their Exploits* (Santa Monica, CA: RAND Corporation, 2017).

[8] Shannon Tiezzi, "US Senate: Chinese Hackers Targeting U.S. Military Contractors," The Diplomat, 19 September 2014.

[9] Bryan Kerkel, Patton Adams and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman for the U.S.-China Economic and Security Review Commission," 7 March 2012.

[10] U.S. Senate Committee on Armed Services Press Release, "SASC investigation finds Chinese intrusion into key defense contractors," 17 September 2014.

[11] Shannon Tiezzi, "US Senate: Chinese Hackers Targeting US Military Contractors."

[12] U.S. Senate Committee on Armed Services Press Release, "SASC Investigation Finds Chinese Intrusion into Key Defense Contractors," September 2014.

[13] 114th Congress, National Defense Authorization Act for Fiscal Year 2016, "Legislative Text and Joint Explanatory Statement," (Washington, DC: Government Printing Office, November 2015).

[14] Charles Fleischmann, "Cybersecurity and acquisition reforms in the FY 2016 National Defense Authorization Act," *Husch Blackwell*, 6 January 2016.

Near-peer competitors have also infiltrated a number of critical U.S. weapon systems, including the UH-60 Black Hawk Helicopter, the Patriot Missile System and the THAAD—terminal high-altitude air defense—Missile Defense System. Hackers installed remote access tool kits and downloaded blue prints, technical data and other proprietary information. Furthermore, they were able to insert a backdoor, repeatedly returning to collect system updates until they were ultimately detected.[15]

U.S. military shipping remains a target of adversarial cyber operations.

Means of Incapacitation

Adversaries are able to sabotage both weapon systems and the industrial controls used to manufacture them in several ways. The first is through the use of altered firmware, the software developed by the vendor to control the critical functions of weapon systems. To reduce development costs, firmware is often created from commercial off-the-shelf or even open-source software, making exploitation relatively easy. Once compromised, attackers can insert pass codes that give them system access at a later time. Firmware can also be embedded with remote code execution, enabling attackers to take control of the weapon system. Another tactic is a "man-in-the-middle" attack, in which the enemy pretends to be a legitimate part of the communication link and so is able to intercept and alter commands.

SABOTAGE AVENUES:

- altered firmware;
- remote code execution;
- "man-in-the-middle" attack; and
- malware in electronic components.

An alarming example of this technique was demonstrated in the exploitation of firmware implanted in hand-held scanners used by shipping, warehousing and delivery services. The scanners seemed innocuous, but they activated upon connection with a WiFi network. They initially transmitted technical details about the ships, shipping manifests and other critical corporate information to a potential opponent. In a subsequent phase, they transferred control of the entire network to their servers. Had the compromise not been discovered by a security company working with the U.S. Department of Homeland Security, it could have affected the shipping industry and Armed Forces. In one company alone, 16 of 48 scanners were infected.[16, 17]

Another, and likely the most nefarious challenge, stems from the electronic components found in missiles and smart munitions, helicopters, tanks, howitzers and other combat vehicles. These components are often built from commercial off-the-shelf circuitry, microchips and micro-controllers—a practice resulting from acquisition reform that was established prior to the 11 September 2001 terrorist attacks on the U.S. homeland. Used for navigation, flight control, avionics and propulsion control, high-speed communication and data transfer, these chips can be embedded with malware that can arrest or alter their function.[18, 19]

Securing the Army's Supply Chain

The Army faces a significant challenge in safeguarding its vast supply chain, from which it must sustain its weapons and equipment. Two of the most significant hazards are potential compromises to the ERP systems used within

[15] Aditya K. Sood and Richard Enbody, "U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers," *Georgetown Journal of International Affairs*, 19 December 2014.

[16] John P. Mellow, "Target Fiasco Shines Light on Supply Chain Attacks," *TechNewsWorld*, 3 February 2014.

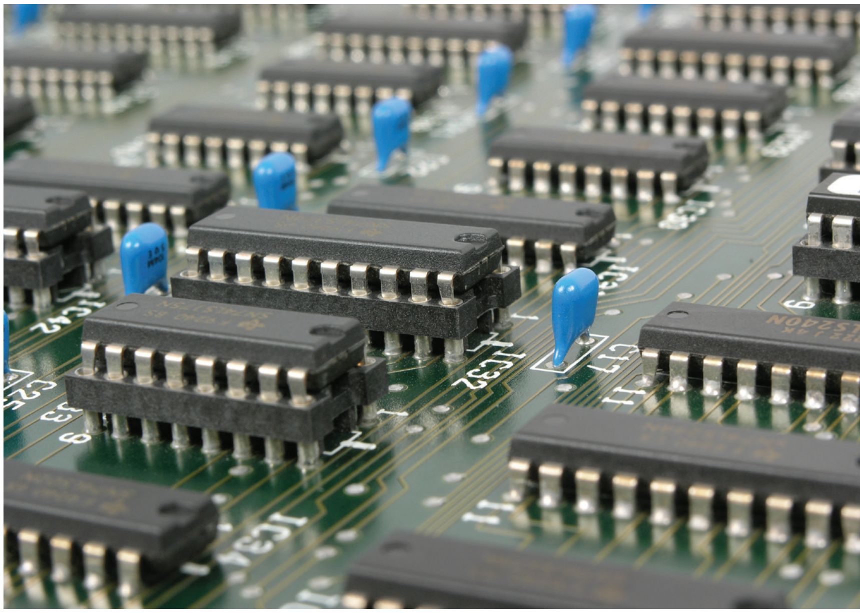
[17] Aditya K. Sood and Richard Enbody, "U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers."

[18] *Ibid.*

[19] Said company was Trap X Security, a San Mateo-based cybersecurity firm.

the OIB and the introduction of counterfeit or sabotaged components into the inventory.[20]

A leading enterprise risk intelligence company estimates that up to 80 percent of breaches to ERP systems originate in the supply chain. At any given time, the Army conducts business with over 11,000 Tier 1 suppliers, known as prime vendors, who provide the raw materials, equipment and repair parts needed to support worldwide operations. In order to attain real-time asset visibility, the Army must enable its suppliers to access its systems. This introduces vulnerability, as each one of these Tier 1 suppliers also has hundreds (if not thousands) of Tier 2 and 3 suppliers supporting them. A single Bill of Materiels used in the repair of one of the Army's missile systems contains parts produced by over 2,000 vendors at all tiers. Subcontractors, who may lack the sophisticated firewalls and security measures used by the government, present a softer target to potential adversaries. Once inside the ERP, adversaries can alter schedules, manipulate parts lists or engage in a litany of other destructive actions.



Counterfeit and sabotaged microchips and components pose a significant threat to the supply chain.

Countermeasures

A number of countermeasures have been developed to secure the Army's supply chain and thwart adversarial efforts. Many of these are already integrated into individual weapon systems' Program Protection Plans.

While still early in their deployment, many already show significant promise. Efforts include:

- **Isolating critical functions and building fail-safes:**
  - ▹ Each weapon system component is developed for a specific application—each component has certain functions critical to its performance. Once identified, redundant or fail-safe methods can be developed to ensure that systems' functionality cannot be interrupted.[21]
- **Rigorous standards for inspection and receipt:**
  - ▹ Instituting and enforcing tough quality standards for inspection upon receipt from vendors is effective in ensuring that all electrical components, integrated circuitry and circuit boards contain no malicious code and that they function as designed and intended.[22]
- **Substitution:**
  - ▹ In a number of systems, there are components which perform similar functions and can be used interchangeably. In the event that counterfeit parts are discovered, similar but reliable components can be substituted.[23]
- **Sourcing, i.e., buying from trusted foundries:**
  - ▹ Computer chips are manufactured in semiconductor plants, referred to in the industry as "foundries." The Army must ensure that its

COUNTERMEASURES:

- isolating critical functions and building fail-safes;
- rigorous standards for inspection and receipt;
- substitution;
- sourcing, i.e., buying from trusted foundries;
- "blind buys";
- software (firmware) assurance; and
- separation kernels, or "wrappers," for commercial off-the-shelf and open-source software.

[20] Jill Scharr, "China-Made Handheld Barcode Scanners Ship with Spyware," *tom's guide*, 15 July 2014.

[21] John L. Freudenthal, "Program Protection: Design for Maintenance, Metrics and Best Practices," U.S. Army Research, Development and Engineering Center, April 2017.

[22] *Ibid.*

[23] *Ibid.*

suppliers are sourcing from trusted foundries that enforce rigorous quality and inspection standards to prevent counterfeiting and the insertion of malware. This can be challenging, however, as the cost of opening a microchip foundry exceeds $5 billion. Suppliers may be tempted to source their chips from cheaper third-party factories, many of which are either located in territories belonging to potential adversaries or controlled by them in other locations within Asia, increasing the likelihood of tampering.[24]

There are also documented instances of legitimate components being replaced with counterfeit ones while in distribution. Tamper-resistant packaging makes this more difficult. The addition of lot and serial numbers to the packaging not only makes components easier to track, but also serves as a deterrent to counterfeiting.[25]

Tough quality standards and rigorous inspection upon receipt are effective countermeasures.

- **"Blind Buys":**
  - ▹ Purchases may also be made from multiple low-risk suppliers who are not aware of the component's end use. This makes it more difficult for adversaries to target weapon systems with malware.[26]
- **Software (firmware) assurance:**
  - ▹ Much of the firmware in use is based on Microsoft Windows or built on products that are. The U.S. Army Communications-Electronics Command and the U.S. Army Communications-Electronics Research, Development Center are continually pioneering new methods to ensure that firmware runs as designed and is free from vulnerabilities that occur either through design or are accidentally programmed into it. Thousands of programs and applications have been vetted thus far.[27]
- **Using separation kernels, or "wrappers" for commercial off-the-shelf and open-source software:**
  - ▹ Many of today's software systems are designed with such tight project time restrictions that redesigning existing software from scratch is almost impossible. To limit engineering costs and to meet project schedules, it is common practice to reuse software to the greatest extent possible. This poses a problem when it comes to building in adequate security measures. The solution comes in the form of a separation kernel, which allows multiple software applications to run on the same hardware platform, but guarantees that those applications remain separated and cannot affect one another, thus preventing the spread of malware.[28]

Where does the Army go from here?

- **Streamlining Acquisition Processes and Strengthening Contracts:**
  - ▹ Many of today's challenges can be traced to the rapid explosion of technology and the inability of the government's acquisition

[24] *Ibid.*

[25] *Ibid.*

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

processes to keep pace. Efforts are underway to streamline the acquisition processes of the Army. Work is underway to develop tighter contracting language that will provide stricter accountability and tougher penalties for suppliers who take short-cuts to better their bottom lines. Quality standards and remedies for non-performance must also be well-articulated and strict. This will remain an area of opportunity in the future.

- **Testing, Evaluation and War-Gaming:**
  - ▹ Appreciating the rapid speed at which enemy cyber tactics and techniques evolve, the Army has established "red" teams whose mission is to employ the newest enemy cyber doctrine and methods against Army and Joint organizations to discover vulnerabilities. Red-teaming and testing of key weapon systems and critical components in the laboratory has enabled the Army to enhance survivability and reliability. This initiative should be expanded to include larger numbers of weapon systems. Conclusions drawn in laboratory settings must also be war-gamed and validated during exercises. This will enable leaders at all levels to think through the ramifications of system failures and so to develop alternate solutions.
- **Bolstering the National Industrial Security Program (NISP):**
  - ▹ The NISP was established to ensure that U.S. defense contractors safeguard classified information in their possession while performing work for the government. With over 13,000 contractor facilities in both private industry and academia cleared for access, there is ample opportunity for a systems breach. The government must balance between need-to-know and the "open campus" approach designed to inspire creativity and innovation while assessing vulnerability and risk. Reinforced information security awareness, accompanied by a greater number of oversight visits, is also in order.
- **Export Controls:**
  - ▹ In early 2015, the Bureau of Industry and Security (BIS) within the Department of Commerce (DoC) published a rule impacting the export of cybersecurity items—including weapon systems, infrared technology, high-end radar, intelligence, surveillance and reconnaissance systems, intrusion software and network communications surveillance systems. This new rule raises an alarming question. How does the U.S. government, including DoD and the Army, manage compliance in light of an ever-increasing security assistance portfolio and the global technology "explosion"? This is another area of opportunity that requires close collaboration between the BIS, the DoC, DoD and the Army.[29]

Summary

The U.S. military possess a materiel capacity second to none. The Army, as an integral part of the larger joint force, is able to draw upon strategically positioned, forward-based stocks and also reach back to a vast industrial enterprise to sustain its globally-engaged units, rapidly replacing combat losses. Underpinning this effort is one of the largest and most comprehensive ERP systems ever fielded. Army logisticians are now able to see global

POLICY ROADMAP FOR THE FUTURE:

- streamlining acquisition processes and strengthening contracts;
- testing, evaluation and war-gaming;
- bolstering the National Industrial Security Program; and
- export controls.

[29] Kay Georgi, "Cybersecurity and export controls? Not for now in the U.S.!" *Military Embedded Systems Newsletter*, 16 June 2016.

resource requirements and world-wide asset distribution in real time.

The expansion of military operations into the cyber domain, combined with the accelerated ability of America's enemies to disrupt economic systems, command and control, infrastructure, logistics and weapon systems, place DoD's materiel advantage at risk. The next conflict could well be decided in cyberspace.

Since the activation of CYBERCOM and ARCYBER, the U.S. Military has made headway in developing both offensive and defensive cyber capabilities and has achieved significant gains in safeguarding DoD and Army networks and information systems against interruption and exploitation. Concurrently, the offensive cyber capabilities of America's enemies continue to evolve and mature and have now reached the point that the U.S. Army's weapon systems, the industrial controls used to manufacture them and the supply chain employed to sustain them are vulnerable to compromise.

Cyber operators on mission in the 780th Military Intelligence Brigade operations center at Fort Meade, Maryland. ARCYBER announced on 2 November that all 41 of its active duty Cyber Mission Force teams were validated as having achieved full operational capability in September 2017, more than a year ahead of schedule.

The danger is acute, and the damage resulting from cyber attack on the Army's weapon systems could be catastrophic. While the Army's program executive offices, program managers and Army Materiel Command's research, development and engineering centers are working in collaboration to prevent such a catastrophe, they are under-resourced for the level of effort required. To negate this threat, a whole-of-government or even inter-allied approach is needed. The same level of effort invested in securing DoD and Army networks and information systems should be committed toward protecting its armaments and its ability to sustain them.

Countermeasures, while effective, are still early in their deployment. This too, remains an area of opportunity. **Through the continued implementation of rigorous quality standards, blind buys, the use of tamper-proof packaging and serial number control, software assurance and the establishment of trusted foundries, the opportunities for counterfeiting and infiltration by adversaries can be substantially reduced.**

Refined and expanded policy tools have demonstrated potential when it comes to safeguarding the Army's weapon systems, industrial controls and the supporting supply chain. Stricter security and continued dialogue on the "open campus" concept can diminish the ability of adversaries to access and compromise weapon systems. Tighter contracting language, stricter accountability and tougher penalties for suppliers who take-short cuts should also limit counterfeits and malware-loaded microchips. Testing and war-gaming will build confidence in existing and future weapon systems and enable commanders at all levels to think through the consequences of systems' failures and develop alternate methods.

The task of securing the Army's weapon systems and the supply chain that sustains them will require extensive resources and the commitment of time and effort, but there really is no choice. Army readiness and America's defense depend upon it.

The Association of the United States Army is a private, non-profit educational organization that supports America's Army—Regular Army, Army National Guard, Army Reserve, retired Soldiers, government civilians, wounded warriors, veterans, concerned citizens and family members.

Interested in becoming a member of AUSA? See the benefits of membership and join online at:

www.ausa.org/membership