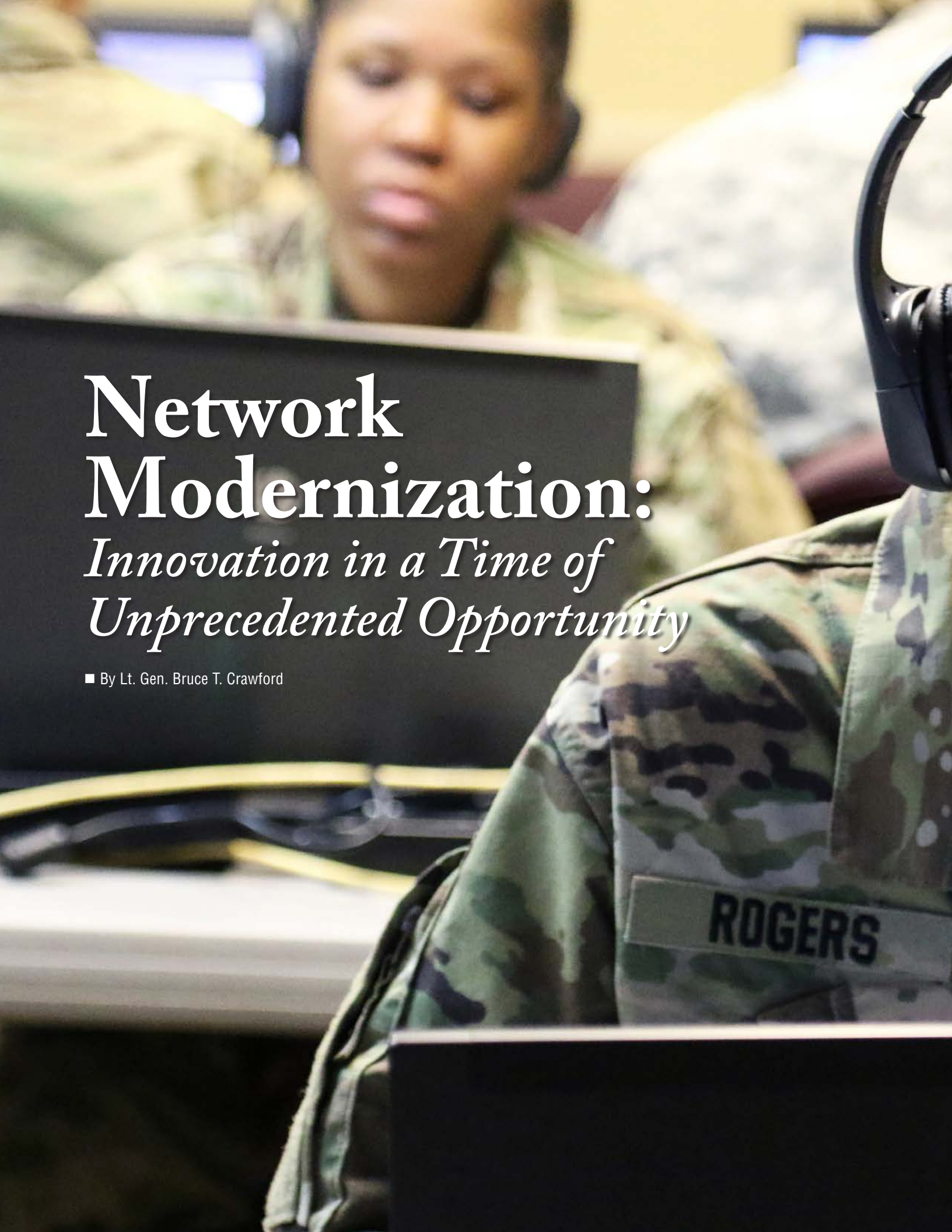

Network Modernization:
Innovation in a Time of Unprecedented Opportunity

■ By Lt. Gen. Bruce T. Crawford

First Lt. John R. Rogers, 642nd Regional Support Group, takes part in virtual convoy training on Feb. 24, 2018, at his unit's headquarters in Decatur, Ga. (Photo by Sgt. 1st Class Gary A. Witte)

The Army's current networks do not meet the requirements of operational commanders, so the Army is modernizing its tactical, enterprise, and intelligence networks to increase its warfighting capabilities.

It has been well-documented that advances in technology will heavily influence the character of future warfare. Artificial intelligence, information technology (IT), advanced robotics, more efficient and automated uses of the available spectrum, and the ability to leverage investments by commercial industry in low-earth-orbit meshed satellite constellations have the ability to be game-changers in the way we fight.

A Time for Introspection

During the past year, the Army has been on an introspective, intellectual journey to modernize its networks. This effort is clearly the largest of its kind in over 30 years.

To put this in perspective, the last time the Army took on a task of this magnitude, the internet was just beginning to take shape, there was no cybersecurity, software-defined capabilities existed only in laboratories, and the intent and capability of peer adversaries as threats to our networks were virtually unknown.

After a year of assessment, the Army concluded that its current network does not meet the requirements of operational commanders in a highly contested and congested environment against a near-peer adversary. After 16 years in a static, uncontested environment, given the evolution of the threat and advancements in technologies, it is clear that the time for redirection is now.

The Army also concluded that its existing network is too complex, too fragile, and insufficiently mobile. It lacks scalability and is not expeditionary or interoperable with joint and interagency partners.

Further, in its current state, the Army is not postured to acquire and rapidly integrate new technologies in a reasonable time frame or at a reasonable cost. And last but certainly not least, the Army concluded that it is likely entering a state of "perpetual innovation," a cascading series of future states that will be defined by consistent, disciplined innovation instead of an institutional mindset of modernizing toward a defined end state.

How Is This Effort Different?

The ongoing modernization effort is not limited to the tactical network. The Army is also developing plans to modernize its enterprise and intelligence networks and continue to build on the great work that is already in progress with its business mission area systems to further enhance warfighting capability.

The enterprise mission area includes capabilities that support hybrid cloud hosting capacity, post, camp, and station infrastructure, and core enterprise services and that reduce the cyberattack surface by regionalizing cybersecurity support concepts.

The business mission area supports network capabilities aligning human resources, logistics, acquisition, and financial services. The intelligence mission area supports specific network capabilities to enable the collection, analysis, production and distribution of intelligence.

What makes this effort different from past attempts to modernize Army networks is this effort takes on an institutional reform approach (from requirements to resourcing) instead of focusing solely on technology.

It also represents a fundamental change in the approach toward modernization because it is threat-informed and it institutes experimentation and demonstrations by actual units that take into account feedback from Soldiers, operational commanders, and the Army's combat training centers, which are the closest thing to actual combat.

This network modernization effort is intently informed by a congressionally mandated Institute for Defense Analyses study of Army networks and an assessment of strategy from the Director of Operational Test and Evaluation.

Enabling The Army's New Vision

The new Army Vision laid out by

the Secretary of the Army challenges us all to "build the Army of 2028 that is ready to deploy, fight and win decisively against any adversary, anytime, anywhere, in a joint, multi-domain, high intensity conflict, while simultaneously deterring others and maintaining our ability to conduct irregular warfare."

Given the current and future reliance on technology, we must posture ourselves now to deliver the network required to make this vision a reality.

Network Modernization Efforts

Over the past 12 months, the Army has invested quite a bit of intellectual energy outlining the characteristics, requirements, and attributes of its future state networks. In the near term, it is taking several tangible actions to make this vision a reality. Those actions include halting programs that do not meet the objective state and the needs of operational commanders and reinvesting those resources to fix capability gaps that enhance readiness, increase lethality, and enable the Army to fight and win against peer adversaries.

Additionally, the Army is pivoting to a more agile acquisition process of "find-try-adapt and buy" to leverage technology investments of commercial and defense industries quickly. These three pillars are all designed to keep pace with technological developments, stay ahead of current and emerging threats, and enable readiness in our formations as a part of the joint team.

These are the Army's priority focus areas:

- ☐ Developing a common operational environment.
- ☐ Consolidating 19 disparate battle command systems into a handheld, mobile, command post computing platform.
- ☐ Unifying all transport capabilities into a seamless standards-based architecture.
- ☐ Enhancing the mobility and survivability of our command posts from the enterprise level to the tactical level.
- ☐ Increasing joint and coalition interoperability.

The result of this modernization will be a network that successfully enables the Army to continue to "fight tonight" while simultaneously projecting the network it needs for the future.

People and Processes

Delivering the network the Army needs to fight and win demands institutional reform. This effort is also about identifying and overcoming challenges that hinder innovation and, ultimately, the ability to make Soldiers more lethal in preparing for and conducting war. The Army has taken an introspective look, acknowledged potential risks, and set forth a course correction to ensure continual strides to help foster a culture of innovation.

Retain, grow, and recruit the workforce. The Army's greatest asset is its people. The workforce continues to be critical to maintaining our advantage, and the Army will continue to focus on grooming its current IT workforce while simultaneously looking at ways to recruit the right talent to renew the force.

As the Army's IT network transforms to defend against emerging threats, the skill sets of the IT workforce must transform and adapt to new technology.

While emerging technologies have great potential to enhance the Army's posture and readiness, they also bring changes to IT roles and the skill sets required for the workforce. Efforts are currently underway to infuse the anticipated skill sets of the future into training and development opportunities for the workforce.

Encourage and incentivize creativity. Innovation will come from our Soldiers. Their ingenuity and creativity in engineering solutions should not be suppressed. Soldiers should always feel empowered and have a say in applying creative approaches from the field.

No problem is insurmountable when an environment of experimentation and exploration of new ideas is encouraged. This bottom-up (versus top-down) approach to creativity will continue to be cultivated to yield exponentially more innovative and viable solutions.

Identify and rapidly address prohibitive policy. Although several policy reform efforts are underway, the priority IT-related reform effort is optimizing the risk management framework (RMF). RMF is a process that requires some major adaptation to best support current and future technological integration.

RMF describes the process that communications systems (from all services) must undergo to identify cybersecurity vulnerabilities, assess risk, and achieve authorities to connect new technologies to networks. In its current state, this process impedes the rapid integration of new technologies.

The Army must pivot to a more agile implementation of RMF that moves from a focus on compliance to a more "risk-based," rapid integration mindset in order to maintain a competitive advantage against peer adversaries.

Modernizing the Army's networks is critical to maintaining overmatch against increasingly evolving peer adversaries around the globe. The implementation of the network modernization strategy is tangible evidence of the Army's commitment to be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere.

Lt. Gen. Bruce T. Crawford is the Army chief information officer/G-6. He has a bachelor's degree in electrical engineering from South Carolina State University, a master's degree in administration from Central Michigan University, and a master's degree in National Resource Strategy from the Industrial College of the Armed Forces.