Shaping the Army Network: 2025-2040 (STAN)

What is it?

Shaping the Army Network: 2025-2040 provides long-term strategic direction for modernizing the Army's network and information technology. Taking the Army Operating Concept and analysis of current technology trends and forecasts, STAN was crafted to inform and shape research, development and experimentation in the government and private sectors. The overall objective is to build a secure, integrated, standards-based environment that ensures uninterrupted global access to the network, and enables collaboration and decisive action throughout all operational phases regardless of location. To meet these requirements, STAN focuses on capabilities and technologies in five areas: dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; and cybersecurity and resiliency.

What has the Army done?

Shaping the Army Network uses the network baseline of 2020, set in the Army Network Campaign Plan Mid-Term Implementation Guidance, as a starting point to analyze "what's next?" The Chief Information Officer/G-6 collaborated with other Army organizations, government agencies, industry and academia to develop STAN. The dialog regarding the direction of science and technology exploration, and research and development efforts will continue.

What continued efforts does the Army have planned for the future?

Shaping research and investments to ensure that the proper capabilities are available for Soldiers at the right place and time is an enormous task. The Army will continue its partnership with other government organizations, industry and academia to guide future technology development. As new technologies are designed and implemented, the Army will reexamine doctrine, policy, tactics, techniques and procedures to make sure the efficacy of any new capability is maximized.

Why is this important to the Army?

The Army's ability to remain the most lethal land force in the world will depend upon its ability to respond to the environment and sustain an operational advantage over all adversaries. The technology evolution cycle continues to quicken and many capabilities that once were limited to advanced state actors are now available to small, less sophisticated, non-state groups and individuals. STAN's focus on the long-range future – 10 to 25 years from today – is key to overcoming these conditions and keeping the Army on pace with, and even ahead of, the technology curve. Only by actively pursuing truly innovative, game-changing capabilities will the Army maintain its dominance on land and in cyberspace.

Resources

Army CIO/G-6 Website; http://ciog6.army.mil/
Shaping the Army Network: 2025-2040;
http://ciog6.army.mil/Portals/1/Shaping%20the%20Army%20Network%202025-2040.pdf
Army Network Campaign Plan;
http://ciog6.army.mil/Portals/1/ANCP/ANCP%20PRINT%206%20FEB%2015.pdf

References to any commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute an endorsement, recommendation, or preferential treatment by the U.S. Army.

Shaping the Army Network focuses on five (5) capability areas: dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancements; robotics and autonomous operations; and cybersecurity and resiliency.

Dynamic transport, computing and edge sensors: *Provide real-time information that can be exploited locally, combined, repurposed and/or transmitted for further analysis and exploitation, depending on the commander's needs.*

- software-defined, programmable network fabric with software-based control of devices
- network control fabric that allows rapid deployment and modification of computing, storage, operational and business functions based on a commander's information needs
- software-reconfigurable cryptographic devices
- adaptive bandwidth allocation technologies to maximize capacity
- computing infrastructure that learns from operational information requirements, then anticipates future application and data needs in response to mission changes

Data to decisive action: *Shorten the time needed to gather and validate data, transform them into high-quality information and present them in a way that best supports operational decisions.*

- intuitive and transparent methods of accessing data
- data synchronization technologies
- flexible, dynamic and reliable analytic platforms and advanced processing capabilities

Human Cognitive Enhancements: *Improve and augment human cognitive, intellectual and decision-making abilities and effectiveness.*

- model-based, course-of-action planning and decision tools
- automated, model-based fusion and analysis that exposes relationships and patterns, and allows operators to understand the projected impact of their actions
- dynamic situational and option awareness, and advanced collaboration tools
- multi-modal sensory prostheses to amplify the normal human spectrum (optical, acoustic)

Robotics and Autonomous Operations: *Fundamentally reshape the force along four axes: improve protection and safety, both kinetically against a physical adversary and virtually against digital intrusion and attack; decrease manpower and logistics requirements, and shrink the footprint; extend and amplify influence and reach; and increase lethality.*

- unmanned systems that expand the operational envelope, ease the human physical burden and workload, and reduce human exposure
- unmanned systems, integrated into unit infrastructure and with autonomous capabilities, that can interpret and react to dynamic threats in predictable, coordinated ways
- robotic "swarms" that extend coverage and provide overmatch through distributed and coordinated attack
- netted sensors that can self-mobilize and self-heal

Cybersecurity and Resiliency: *Provide Soldiers and leaders decision-quality knowledge without interruption, minimize threat of internal and external attacks, and remediate quickly when they do occur.*

- collective intelligence mechanisms that corroborate or substantiate data based on provenance and prior use
- intelligent cyber-physical systems that continuously assess trustworthiness of operator commands, anticipate threats and reconfigure themselves to evade or curtail such threats
- adaptive identity and access management that uses risk-based authentication, where transactions replace identity as the focus of decision making
- fully homomorphic encryption that allows computation of sensitive data to be outsourced to untrusted platforms, such as cloud providers, without exposing the sensitive data
- secure computation protocols that allow parties to compute a function based on their joint inputs without disclosing the individual inputs to each other
- automatic self-healing and self-protecting capabilities, including "self-destruct" to prevent system and data capture
- agents that reconstruct damaged data from traces left in the network or at endpoints

References to any commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute an endorsement, recommendation, or preferential treatment by the U.S. Army.

Army Chief Information Officer/G-6
107 Army Pentagon I Washington, DC 20310
CIOG6.ARMY.MIL