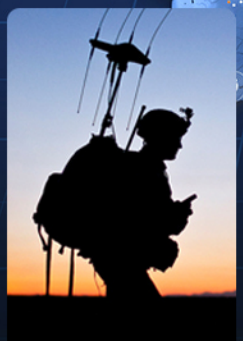
Office of the Army Chief Information Officer/G-6

SHAPING THE ARMY NETWORK: 2025-2040

March 2016



CIO/G-6

ENABLING SUCCESS For Today and Tomorrow

U.S.ARMY

CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to: Architecture, Operations, Networks and Space (SAIS-AON), CIO/G-6, ATTN: Mr. Edwin Payne, 107 Army Pentagon, Washington, DC 20310-0107

Executive Summary

Shaping the Army Network: 2025-2040 provides the long-term strategic direction for Army enterprise network modernization within the context of the Army Operating Concept. Using the IT baseline described in the Army Network Campaign Plan as a starting point, the intent is to guide development of science and technology requirements to get to "what's next" in the evolution of the Army's network.

The Army of 2025 and beyond will largely be located within the continental United States (CONUS), with a smaller deployed footprint. These CONUS-based forces must be ready to respond globally and rapidly for planned operations and unforeseen contingencies. The Army will fight as part of a joint, interagency and multinational force with a dynamic set of mission partners, enabled by a network that allows interoperability with governmental and non-governmental agencies and coalition members.

The battlefield and the Army of 2025-2040 will be shaped by so-called leap-forward technologies. We have made great progress toward the current vision of 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. However, the Army must continue to seek and evaluate emerging technologies in order to constantly modernize our network and maintain our technological edge.

The network capabilities and technologies required to meet the operational requirements of 2040 are grouped into five focus areas: dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; and cybersecurity and resiliency.

Each of the focus areas is described in detail, informed by an analysis of the latest information technology trends and forecasts, many of them potentially game-changing for the Army and the society we serve. One development the military must closely watch is the growing availability of ever-increasing data processing power and faster transmission speed at lower cost. This trend gives resource-poor states, criminal organizations and even individuals access to capabilities traditionally monopolized by advanced countries. The military also must determine how to harness the power of emerging technologies, such as supercomputing and data analytics.

The pace of innovation in information technology is increasing the pace of operations, and our adversaries' ability to influence our operating environment. The Army's success in 2040 will depend on our retaining overmatch in both security and capability to provide freedom of action within the cyber domain while denying it to our adversaries.

Delivering network capabilities to the Army is a team effort. This document serves as a guide to provoke thought and a means to inform and shape research, development and experimentation in government, industry and academic entities. Together, we must ensure that the Army maintains its technology edge far into the future.

Robert S. Ferrell
Lieutenant General
Army Chief Information Officer/G-6

Table of Contents

Battlefield 2040 Operational Scenario

Technology consistently impacts warfare. There have been significant advances in warfare and equipment since coalition forces launched Operation Desert Storm to retake Kuwait in 1990. Some of these advances include: the proliferation of drones both for attack and reconnaissance; the ability to know where every combat vehicle is located on the battlefield through Blue Force Tracking; the evolution of mission command (MC) software (from acetate map boards to large screen displays); and new communications gear that allows Soldiers to communicate beyond the line of sight. All of these improvements have significantly influenced Army operations in Iraq and Afghanistan. As innovation accelerates, even greater change will emerge over the next 25 years.

> "The U.S. Army's differential advantage over enemies derives, in part, from the integration of advanced technologies with skilled Soldiers and well-trained teams."
>
> **The U.S. Army Operating Concept**
> ***Win in a Complex World 2020-2040***
> **October 2014**

This operational scenario portrays one of many potential scenarios involving future technologies. It is not intended to be all-inclusive, but rather to demonstrate how advanced technology may influence future operations.

Warfare in the Year 2040

National intelligence agencies, working in coordination with joint, inter-organizational and multinational partners, use advanced artificial intelligence (AI) algorithms to monitor information feeds from a variety of sources, correlate findings with previously collected information and uncover a plot to develop an advanced biomedical toxin. This toxin, when used in conjunction with dispersal bombs, is capable of producing mass casualties and is nearly impossible to detect. The plot is led by a criminal gang called the Xipe Totec (XT) in cooperation with the local authorities of the sprawling mega-city of Sogals, on the island nation of Attica.

Source: http://wallpaperswide.com/tom_clancys_ghost_recon_future_soldier_3-wallpapers.html

To further develop the situation, a focused plan is created to identify specific individuals who are responsible for this activity, and determine precisely where the toxin is being produced. Through the multinational effort, national intelligence agencies are able to pinpoint the headquarters of this operation to a 10 city-block area. Relations with the government of Attica are poor and the government has limited control in Sogals; however, an agreement for a limited operation is obtained.

Given this intelligence, the national command authority directs a regionally aligned Joint Task Force (JTF), led by the Army, to immediately conduct a battalion-sized raid to neutralize the site and secure the toxin. The JTF is supported by sea-based naval logistical support and Air Force airborne intelligence and surveillance assets. Rules of engagement and the area's dense civilian population limit the use of kinetic weapons and emphasize the isolation and neutralization of the area through cyberspace operations. JTF command and staff are concerned that maneuver within the megacity is

impossible and any ground incursion will easily cause a flurry of social media that would eliminate any hope of surprise. After completion of a risk assessment of air and ground force insertion options, a decision is made to establish a limited airhead in a remote area that will facilitate access into the country's infrastructure, yet is close enough to conduct a final air assault to neutralize the site. Regionally aligned forces evaluate alternative approaches and identify an area that will accommodate an airhead and facilitate surprise to provide freedom of movement and logistical support for the attacking force.

Intelligence agencies, with the assistance of multinational partners, monitor the area both visually and electronically, providing the JTF commander intelligence on the local situation. Pathfinder assets establish a clandestine site, deploying autonomous ground and air robots that assist in the reconnaissance of the drop zone. This tactical information is automatically uplinked and combined with national overhead observation and signals intelligence (SIGINT) in a CONUS-based mission database (MDB). An advanced data-to-decisive-action collection architecture and algorithms electronically filter the raw intelligence in the CONUS-based MDB, generating anticipatory and actionable intelligence that is used to update the airborne force en route to the airfield and provide enhanced situational awareness (SA) to the Soldiers on the ground.

The "go ahead" is given, and the airborne assault initially takes the airhead and secures the area for the follow-on airlifted force. Ground protection robots are included in the airborne drop and immediately provide 360 degrees of security. Marine Corps tiltrotor aircraft deploy and arrive soon after the initial airborne assault. An expeditionary command post is established, along with secure communications with CONUS. The resiliency of the network prevents disruption by advanced cyber threats. Cyber teams employing remote software gain access to local cellular, landline and Internet communications networks. This software rapidly discovers available communication paths that enable real-time monitoring of XT communications, edge sensors and localized Internet of Things platform IT (PIT) devices, such as traffic or security cameras in the area. The communications paths are also used to leverage social media to support the eventual attack; and to provide backup to the attack force's communications, allowing for the dynamic transport of information over the available commercial infrastructure.

A micro-drone swarm is deployed over the suspected headquarters and laboratory area to establish persistent measurement and signatures intelligence (MASINT) to detect the biological agent; to map the details of the road network; and to provide a video feed to capture facial images that pattern-matching software can compare to known XT operatives and supporters. Quantum gravity sensors are deployed to detect any tunnels between the suspected XT cell locations. This information is also used to identify and crawl social networking sites to generate a human terrain analysis of the area and identify non-threatening areas (medical clinics, schools, commercial transportation terminals) to avoid collateral damage. As the information in the CONUS-based MDB grows, algorithms searching the data determine that the XT has a sophisticated ability to burst message traffic masked within the local communications system. SIGINT is focused to identify characteristics of this traffic, and network-mapping software is used to identify focal points of activity, such as possible command cells. The analysis is also able to identify any XT decoy activities used to confuse anyone monitoring their communications. Through comprehensive cyber electromagnetic activity (CEMA) preparation of the battlefield, key physical and cyber terrain are identified, and specific objectives to capture the XT leadership and secure their biomedical facility are set.

For the operation to be a success, surprise is paramount. Extensive operational and cybersecurity measures are taken to mask JTF operations. Sentiment algorithms are used to monitor social network

feeds and look for keyword hits that gauge the mood of the local populace and detect any indication that the operation is compromised. The battalion task force conducting the operation is ready. Rodent microbots are deployed to map the interior of the target buildings. This information, along with the information accumulated in the CONUS-based MDB, allows simulation software to create a virtual representation of the objective area and exploratory modeling of alternative ingress and egress routes. Soldiers, using their combat multi-capable helmet with a hands-free heads-up display attached to the simulation, are able to conduct a collective rehearsal of the raid, identify possible pitfalls and leverage the simulations' updated models to assess alternative courses of action, which have been electronically stored for quick reference. Tasks and timelines are established and electrically monitored so that predictive software can identify potential problems as the attack unfolds.

The raid begins. The identified XT control cells and the bio lab are hit initially with a tactical cyberspace attack. All communications within the building are isolated and spoofed to appear as a local overload of the system, causing a lack of service. Armed unmanned aerial vehicles (UAVs) are deployed to provide overhead coverage to identify and eliminate rooftop threats. Leaders on the tiltrotor aircraft are continually advised of the ongoing developments in the target area. Tailored information is streamed to each leader through a direct neural interface, forming a visual picture of the objective. The tiltrotor aircraft arrives at the buildings, hovering at 15 feet, which allows Soldiers outfitted with robotic exoskeletons to jump to the rooftop.

Soldiers follow routes of least expected resistance through the building (as determined by real-time data) to secure their objectives. XT combatants are identified through facial recognition software and marked by a red glow in the Soldier's visor. XT combatants who resist are neutralized using a combination of microwave emitters and chemical smoke grenades that, when used with an electrostatic discharge initiator, create a debilitating voltage shock wave. As the Soldiers designated to secure the bio lab arrive at their objective, they are notified that MASINT has detected that a key element of the biomedical toxin has been moved to a new location. The direct neural interface allows the Soldiers to coordinate a revised plan to secure the toxin. The plan is quickly approved, distributed and executed.

On the street, crowds are gathering as the operation unfolds. A preplanned public service announcement is released to warn residents. The announcement, which contains both audio and text messages, is burst-transmitted to cell phones in the area. Social network monitoring begins to show a high level of anxiety and hostility toward the Army's incursion into the city. With the XT leadership in custody and the biomedical toxin secured, the battalion begins its withdrawal. The few friendly casualties stabilize their wounds by using their individual broad-spectrum antibiotics trauma kits and are immediately evacuated on semi-autonomous drones to nearby medical personnel. As necessary, injured XT combatants are treated and remain in place. The battalion consolidates at the airfield lodgment; all personnel are accounted for and immediately redeploy. Mission accomplished.

The technologies and the Soldiers' use of them described in this operational scenario are imaginable and believed to be entirely feasible by 2040. The remainder of this document will describe many of the potential technologies employed within the scenario.

Acknowledgement to Sergeant Major Richard Russo, the author of *The Gotham Division and Staff Sergeant Parker: Imagining the Future of Urban Warfare*, for many of the ideas in this scenario.

Introduction

It is fully anticipated that the information, warfighting and kinetic technologies described in the operational scenario will continue to evolve over the next quarter-century. Commercial information technology (IT) developers are expected to out-pace government programs as affordability and availability of enhanced technologies secure a place within the global market. The militarization of these technologies is inevitable, as our adversaries will leverage every technological advantage they can muster. Greater availability of these advanced commercial and militarized technologies will decidedly alter the training and professional development programs that prepare our Soldiers, the tactics, techniques and procedures (TTPs) that our Soldiers will use in future conflicts, and the systems and processes used throughout the enterprise, from the industrial base to home station to the farthest tactical edge. This future warfare environment requires that the Army continue to invest in leading-edge and disruptive technologies, as well as education and professional development programs, in order to maintain technology overmatch in an increasingly complex, data-saturated environment.

Shaping the Army Network 2025-2040 is informed by an analysis of technology trends and forecasts, for a commander-focused Army network that is tailored to formation, echelon and mission in the 2025 to 2040 time frame. It supports the Army Strategy and the Army Campaign Plan, and builds upon the Army Operating Concept. It serves as a guiding document to provoke thought and a means to inform and shape research, development and experimentation by both government and industry entities to ensure that the Army maintains a technology edge in future conflict. The required capabilities described in Section 2, and the later discussions of potential solutions, apply to both tactical and institutional network operations.

The projected technology developments described in this document may not all come to pass. In fact, given the rapid pace of scientific advancement, the technology Soldiers eventually employ likely will differ from what is presented here. Therefore, investment strategies will likely need to be adjusted in the future as they will be influenced by global economics and still-unforeseen leap-ahead discoveries. The Army has a significant task to shape research and investments to ensure that the proper capabilities are available for our Soldiers at the right place and time to enable mission success. Furthermore, as a consequence of the development and deployment of these and other emerging capabilities, the Army will have to develop and implement new doctrine, policy and TTPs.

Given that predicting the long-range future for IT and how the Army will employ it can be difficult, this vision is based upon and extrapolates existing Army vision, strategy, doctrine, requirements and operating concepts, including the 2015 Army Network Campaign Plan and the supporting 2015-2016 Near-Term and 2017-2021 Mid-Term Implementation Guidance. In addition, both U.S. and internationally based commercial and academic projections for IT advancements were leveraged to develop five key technology areas, which will guide development of the future network: dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; and cybersecurity and resiliency. The vision addresses Network 2040, from the dismounted Soldier at the farthest tactical edge to supporting forces at home station.

This document is organized as follows: Section 2 discusses the projected operational environment and required capabilities to set the context for what the future network must enable; Section 3 describes what the network of 2025 is expected to look like, and serves as the baseline from which the network of 2025 to 2040 will be built; Section 4 contains a description of the network of 2040, including the capabilities that it will provide and the future technologies that may enable it; and Section 5 provides a set of concluding remarks. Annex A maps these required capabilities to their associated Joint

Capability Areas and Mission Command Focused End States. Annex B details the Mission Command Focused End States that set the conditions for the Army to transition to the Force 2025 and Beyond "Network After Next." Annexes C and D list acronyms and references.

Operational Environment and Required Capabilities 2025-2040

To achieve the Army Vision and remain the world's most lethal land force, the Army must continually examine, understand and respond to the environment in which it operates. The Army of 2025 and beyond will sustain a smaller force yet will maintain asymmetric overmatch through innovation and adoption of advanced network systems and processes.

The Army of 2025 and beyond will be largely CONUS-based with a smaller footprint of deployed forces; however, all forces will be prepared to respond globally and instantaneously to any validated threat. The Army will continue to fight jointly with a large and dynamic set of mission partners, and must operate seamlessly with other federal agencies and foreign governmental and non-governmental agencies, indigenous organizations and non-combatants.

> "The Army of 2025 and Beyond will effectively employ lethal and non-lethal overmatch against any adversary to prevent, shape, and win conflicts and achieve national interests."
>
> **The Army Vision**
> ***Strategic Advantage in a Complex World***
> **July 2015**

U.S. adversaries will include state and non-state military, criminal and terrorist elements, all of whom will present blended physical and cyber threats. Nontraditional combatants and battlefields will continue to emerge as a result of threats from these adversaries, continued urbanization and the spread of advanced cyberspace and counter-cyberspace capabilities. The proliferation and availability of commercial technology may allow adversaries to obtain an operational advantage. Technology, including weapons of mass destruction, advanced sensors, augmented humans, autonomous processes and automated decision making, will permeate the battlefield. The speed at which data are dispersed will create an information-rich environment; however, information quality may be low and extraction of mission-relevant content may be challenging. Misinformation will be used as a weapon.

The Army's ability to remain the most lethal land force in the world will depend upon how well it responds to this operational environment and whether it can sustain both operational and technological advantages over its adversaries. The material presented here is unconstrained by design and forms a baseline for discussion of future required capabilities that emerge as a result of threats, opportunities and evolving concepts of operations. Competitor and adversary investments in available and emerging technologies between now and 2040 are expected to place current U.S. technology overmatch at risk. These findings should inform Army science and technology, IT and network investment strategies; training and professional development of Soldiers and commanders at all echelons; operational TTPs; and sustainment of the organic and commercial industrial base. It also is critical that the findings inform adjustments to Signal Regiment and cyber workforce organization and structure as new capability solutions and operating concepts are deployed. The required capability areas covered here and the technologies discussed further in Section 4 include dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; and cybersecurity and resiliency.

Dynamic Transport, Computing and Edge Sensors

In 2040, Army operations will require that the network be continuously available across all echelons and in all environments – from the dismounted Soldier at the farthest tactical edge, from the squad through the Brigade Combat Team, while stationary or on the move, and when deployed and at home station.

> "Improvements to mission command will facilitate the decision making of leaders and Soldiers across all tactical echelons for Unified Land Operations in support of the Joint Force and allies. The Army will develop and field a robust, integrated, tactical mission command network, linking command posts and extending out to the tactical edge and across platforms."
>
> **Army Posture Statement 2015**

Forces must have the ability to organize and deploy with little notice, and must have the capability to fight upon arrival, fully informed and cognizant of the threat as well as the status of friendly forces and joint, inter-organizational and multinational partners. They must remain in full communication and coordination with higher-echelon command, whether that command element is forward-deployed or at home station. As part of an agile Joint force, individuals and units must be able to automatically connect, disconnect and reconnect to the network, and aggregate or disaggregate with known and emerging joint, inter-organizational and multinational partners, whether friend, non-combatant, government or non-governmental agents. In all operational scenarios, forces must maintain full interoperability and synchronization with a dynamic set of mission partners in all terrains, from megacities, to canopied jungles, to open plains, to remote rugged mountain and arctic landscapes.

Once deployed, commanders and Soldiers must retain the capability to remain mobile, without sacrificing mission command effectiveness, therefore enhancing agility, speed and discriminatory decision-making effectiveness at all levels. The network must also enable the commander to sustain high-tempo operations, and provide extended operating ranges to enable the forward line of troops, which will move with greater speed towards the objective, to maintain situational awareness and mission command performance. The network must support disconnected operations, which may include autonomous operation of a small group of Soldiers or subordinate units fully capable of performing missions while remaining undetected and disconnected from higher echelons. In addition, command posts must be able to set up, operate, tear down and move within threat timelines; and account for potential degradation of network connectivity during movement, setup or steady-state operations.

To achieve these objectives, the network must evolve to support: *dynamic transport*, which provides the commander access to strategic, tactical and locally available information by dynamically discovering and utilizing organic and commercially available resources; *dynamic computing*, where the computing infrastructure learns from operational information requirements and anticipates future needs to dynamically deploy applications and information on demand or in response to mission changes; and *the growth of networked edge devices*, which will provide real-time information that can be exploited locally, combined, repurposed and/or transmitted for further analysis and exploitation, depending on the needs of the commander.

Data to Decisive Action

Data to decisive action includes a wide range of domains and technologies that share a common goal: to decrease the time it takes to gather data, transform them into high-quality information, validate them and present them in a way that best supports operational decisions. The primary benefit to the commander is the ability to bring individuals and teams together to develop insights and draw conclusions from the information available.

As future Soldiers become increasingly comfortable and familiar with the challenges of the pervasive and ubiquitous information environment, evolution of battlefield processes and tools must be coupled with significant advances in the systematic ability to analyze and extract applicable, effective, timely, complete, authentic and trusted information to support decision processes. Augmenting Soldiers with advanced data-to-decisive-action capabilities increases effectiveness and reduces cognitive burden.

Commanders and Soldiers must have sophisticated processing and analytic computing capabilities in order to understand, cope with, sort and apply significant increases in information. The faster flow of information to the point of need requires innovative and advanced system-based tools that structure the information to enable an accelerated data to decisive action framework. This framework will provide enhanced situational awareness, as well as option awareness: the perception and comprehension of the relative desirability of the available options, and their underlying factors, tradeoffs and tipping points, which explain that desirability. Better common operating pictures and less technological complexity are essential to achieve this outcome.

Systems and processes must also be adjustable to focus information availability for maximum effectiveness while simultaneously seeking to minimize distractions generated by excessive data and information that are not applicable to the task at hand. The ability to transform data to decisive action is critical to success on an increasingly automated and information-saturated battlefield. Soldiers, teams and commanders must be able to make accurate and effective battlefield decisions. Therefore, they must be equipped with large-scale, collective, self-organizing and autonomous decision agents, machine- and application-directed information discovery, and synchronization and integration applications that overcome data flow imperfections to achieve mission command and success on the battlefield of 2040.

Human Cognitive Enhancement

The Army must leverage technology to improve and enhance human cognitive, intellectual and decision-making abilities and effectiveness. Human-machine interaction and teaming are critical enablers to overcome an increasingly complex information environment.

Future force reductions, coupled with the radical increase in both threat and friendly use of autonomous and semi-autonomous systems and potential robot “swarms”, require the identification and adoption of cognitive aids to augment Soldiers’ and commanders’ situational and option awareness. The projected increase in information and operational tempo (OPTEMPO) in all phases of operations requires that commanders have immediate knowledge of the status of Soldiers and units under their command. In addition, commanders must be able to synthesize this information and apply assets effectively to execute complex operations in the face of an innovative threat. These cognitive aids will also enable collaboration by distributed teams analyzing the operational environment.

Advances in human and cognitive sciences, and improvements in machine-machine and human-machine interaction, must be leveraged and incorporated into training programs to enhance Soldier, commander and unit performance. Scalable self-organization and collective decision-making tools, similar to how the Intelligence Community leverages a large number of information sources to develop “anticipatory intelligence”,[1] must be employed. In addition, tailored application of models,

[1] ***The National Intelligence Strategy of the United States of America 2014***, June 2014, p7. “Anticipatory intelligence is the product of intelligence collection and analysis focused on trends, events, and changing conditions to identify and characterize potential or imminent discontinuities, significant events, substantial opportunities, or threats to U.S. national interests.”

simulations and dynamic planning capabilities is necessary to increase Soldier, commander and partner agility, and to improve cognition and effective decision making.

Robotics and Autonomous Operations

Commanders and Soldiers must have the capability to employ, manage and defend against individual, integrated collections, teams or swarms of robots that can act under human control, independently or collaboratively. Robotic missions may include management and protection of communications and information networks, and provision of decision-quality information. Advanced technologies, such as robotic swarms, may necessitate even greater network capacity and dictate that fewer Soldiers manage, control and operate a significantly higher number of operational assets. Data analysis tools are essential to make sense of the volume of data and to translate the data into usable information.

The Soldier, the robot and the network will have to co-evolve to manage this new complexity. Robotics must mature from today's single, heavy platforms designed for specific tasks toward coordinated teams and agile swarms with applicability across a wide spectrum of battlefield missions. Robotics will become a critical element of an agile, dynamic and mobile network that will move and fight with the Soldier as part of the unit's network and operational infrastructure, providing connectivity and continuity within and across all elements. The Army also must be able to adapt and enhance robotics to support unit defense, both kinetically against a physical adversary and virtually against digital intrusion and attack. These new required capabilities, coupled with more intelligence and competence under uncertainty, will help achieve and maintain the Army's overmatch in a technologically evolving future.

Cybersecurity and Resiliency

Cyber attacks on U.S. systems, by both internal and external threats, continue to increase in frequency, severity and innovation. Automatic reconfiguration and redundant communication and collaboration must be integrated into a common operating environment (COE) to provide Soldiers and leaders decision-quality knowledge without interruption. In addition, the threat of internal and external attacks must drive changes in how the Army assesses and grants access to networks and information, as well as the development of offensive and defensive cyber capabilities.

> "Low-cost and global proliferation of malware have lowered barriers to entry and have made it easier for smaller, malicious actors to strike in cyberspace."
>
> **Secretary of Defense Ashton Carter**
> **16 September 2015**

Automatic self-healing and self-protecting capabilities must be able to defend against all weapon systems that could impact the continuity and resiliency of the network. This includes the capability to "self-destruct," thereby preventing data and system capture by a potentially successful attacker; to back up data; and to allow remote locations to operate from back-ups to maintain continuity of operations.

A directed-energy weapon (DEW) is an example of a potential future system with an unusual application and impact. While DEWs may broadly target network and physical infrastructure initially, they may also evolve to enable targeting of specific military and commercial communications and network nodes, devices and infrastructure. The network must also protect against network node and device "micro-targeting," which involves targeting specific echelons, organizations or individual command positions or devices within the operating force. As these and other technologies continue to evolve into increasingly disruptive defensive and offensive threats, the Army must continue to improve the network's resilience and resistance posture to ensure continuous operations in an increasingly volatile environment.

These technology recommendations cannot be considered in isolation. Network operations, visibility, maintenance, training that emphasizes enhanced technology skills and sustainment requirements must be balanced with modifications to Signal Regiment and overall Army force structure. In addition, the evolution of specific applications, systems and platforms, to include their spectrum and power requirements, will require adjustments to how the Signal and Cyber workforces prepare for operations as part of both the operating and generating forces.

Network 2025

This section presents a description of the Army's planned (i.e., programmed) Network 2025. It will serve as the baseline from which Network 2040 will be built. Although many of the foundational services and initiatives currently under development are scheduled to be completed by 2025, they depend on sustained resourcing. Additionally, certain current and emerging challenges will remain either partially or completely unfulfilled by the 2025 baseline. These challenges and opportunities are summarized in Section 3.3.

Operational Tenets Driving Network 2025 Design

The Network 2025 design is driven by a set of key operational tenets that can be gleaned from a review of Army and Joint documents. Many of these concepts are also expected to be applicable beyond 2025. Some of the relevant tenets include:

CONUS-Based: An Army that is largely CONUS-based but able to project to meet global demands.

Fight on Arrival: An Army that can maintain continuous communications and operates upon arrival without a long build-up period or staging to establish network connectivity.

Distributed Operations: An Army that can operate over vast areas of operations, spanning political borders, continents and geographical combatant command boundaries.

Reduced Force Size: An Army that can maintain its operational readiness with fewer resources and Soldiers.

Interoperability: An Army that can produce unity of effort with a large, dynamic set of mission partners.

Regional Alignment: An Army that contains units aligned to geographic regions to enable mission preparation and engagement in Phase 0 operations.

Blended Threats: An Army that can respond with both kinetic and non-kinetic weapons to a mixture of state and non-state military, criminal and terrorist elements, all of whom will present blended physical and cyber threats.

Maintain Overmatch: An Army that can sustain IT overmatch when commercial investments and technologies continue to outpace those of the military, setting conditions for a potential enemy IT advantage.

Network 2025 Technical Overview

Figure 1 provides a high-level overview of the planned Network 2025. It depicts a single network that enables Soldier, civilian and mission partner connectivity through a global, secure environment.

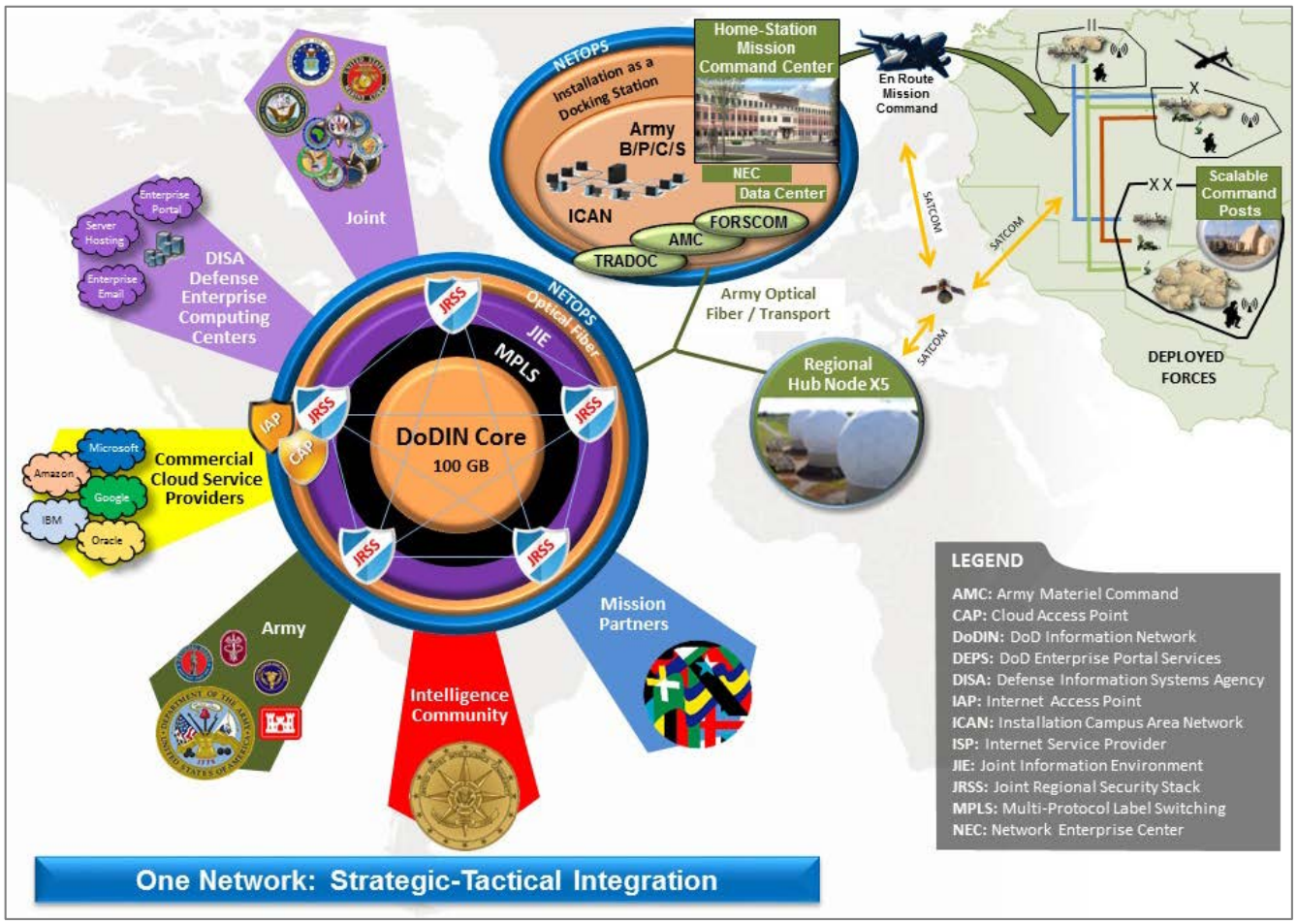


Figure 1. End-to-End Network

Deployed units will be supported by a mobile, tactical network built on a family of tactical satellite and terrestrial radios that will provide voice, situational awareness, and command and control (C2) across the force, down to the individual Soldier. A tailorable command post will support expeditionary operations, allows units to fight upon arrival and enable longer-term, more fixed operations.

Mission command applications will comply with the COE, improving interoperability across the force, allowing more agile delivery of new capabilities to the warfighter and reducing network life-cycle costs.

Deployed units will be connected to the larger enterprise through global Regional Hub Nodes (RHN). RHNs will provide an interface to the Department of Defense Information Network (DoDIN) core optical fiber network and enable enterprise-level services, such as email, collaboration, portal and Voice over Internet Protocol (VoIP), that must be extended to the tactical user. Commercial and Defense Information Systems Agency cloud and computing centers will provide worldwide access to data to fulfill Soldiers' needs, regardless of operational status or location.

The DoDIN optical network will form the backbone to connect the generating and operating forces. Multiprotocol Label Switching (MPLS), a virtual network-traffic management system, will maximize capacity at most installations to enable both business and warfighter mission area functions. Home-Station Mission Command Centers (HSMCC) at each division and corps headquarters will enable distributed operations, linking deployed forces with their CONUS-based headquarters. The network

will be protected by a consolidated set of Joint Regional Security Stacks (JRSS) that simplify and improve resistance to threats.

Remaining Network 2025 Challenges and Opportunities

While Network 2025 will provide significant advances in capability relative to today's network, there are numerous capability solutions that will not be fully fielded by 2025. This is partially due to the size of the Army and the length of time it takes to incrementally equip the total force with a new capability. As a result, units and installations frequently will have different levels of modernization. In addition, many of today's known required capabilities will not be deployed by 2025 because the technology will not have fully matured or because budget constraints will limit development and fielding. To close these gaps and achieve the operational capabilities required by 2040, research, aligned to several of the major capability and technology areas addressed within this vision, must continue.

Dynamic Transport, Computing and Edge Sensors

Mission Partner Interoperability: Executing operational missions in collaboration with a dynamic set of mission partners will remain a significant challenge. Current efforts, such as the Mission Partner Environment, will improve interoperability but the Army expects that effective information awareness, sharing and segmentation by user, mission and geographical area will remain an area for development beyond 2025. Additionally, techniques to enable organic over-the-air interoperability at the tactical edge, other than through a cellular phone, will remain a work in progress.

Constraints of Bring Your Own Network (BYON) and Bring Your Own Device (BYOD): Network 2025 will still predominantly be based on bringing government-furnished, unique devices to the theater. While this provides the most secure solution, development of military-unique information technologies will continue to significantly lag behind the pace of commercial sector advancements. The Army must continuously assess and adapt commercial developments to augment and enhance organic systems and prevent loss of IT overmatch.

Challenging Environments: The Army must be able to operate in many environments that will continue to inhibit network performance. The ability to maintain communications and position, navigation and timing in urban, canopied and arctic environments will remain a focus of research programs as the Army progresses to Network 2025.

Data to Decisive Action

En Route Mission Command: The Army is currently fielding a capability solution for the Global Response Force that will integrate IT on a C-17 to enable units to maintain situational and option awareness while in transit to the theater. This solution, while capable, is only focused on a small subset of the Army. To address the requirement across the entire force, the Army needs a solution that can be cost-effectively implemented and operated while on any mode of deployment transportation.

Situational Awareness and Option Awareness: While the network must enable the Army to operate across a full spectrum of missions, the majority of mission command applications still focus on maintaining awareness of just blue and red forces. Operating across all Joint Phases (0-5) will require mission command systems to maintain situational and option awareness of network operations and readiness levels, in addition to battlefield awareness of cyber, electromagnetic warfare (EW) and

environmental and economic shaping factors. Mission command systems must also portray how the battle damage assessment may change as a function of time.

Cybersecurity and Resiliency

Cyberspace Operations and Network Resiliency: The Army's posture against an EW attack must mature to address known, emerging and unknown future threats. Development and utilization of radio technologies that employ anti-jam and low probability of intercept/detection features are necessary to support network defense. The warfighter must also be able to visualize and respond to both EW and kinetic threats to the network, and to sustain effective operations in disconnected, intermittent and limited bandwidth (DIL) environments. Network operations must be able to selectively isolate, then reconnect systems and platforms, to effectively counter imminent threats. Units must be able to continue operations in DIL, EW and contested environments, then re-synchronize critical mission-specific data upon re-connection to the network in order to ensure an updated common operating picture for the commander.

Command and Control/EW Mutual Interference: Numerous developmental efforts are under way that offer the potential to better integrate and converge command and control and EW functions, and ensure that systems can handle interference, dynamic access, signal interception and geolocation, which can impact specific operations. Current significant initiatives include the radio frequency hardware and software convergence effort, which will integrate radios and jamming devices into a common chassis and enable spectrum use coordination between devices; and dynamic spectrum access technology that automatically detects intentional and unintentional interference and avoids the use of those channels for communication. While these technologies are promising, they are still maturing and will require a synchronized effort to ensure compatibility across vehicle fleets and platforms.

Network 2025-2040

This section presents a view of the technologies that may enable development and fielding of effective network capability solutions between 2025 and 2040. The Army will focus investment in mitigation of known and unknown threats, as well as in revolutionary technologies that could change the way U.S. forces or their adversaries fight.

The required capabilities identified in Section 2, combined with the network modernization challenges and opportunities discussed in Section 3, should inform S&T investment in the near and mid terms across a wide range of network and functional areas (e.g., reconnaissance, battlespace awareness, medical support and treatment, fire support, etc.). The remainder of this section discusses technology associated with these five areas: dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; and cybersecurity and resiliency.

In addition, another class of cross-cutting technologies, although not specifically expanded upon in this document, must be continuously assessed to determine how they can be adopted and adapted to enhance network operations. These include but are not limited to: nanotechnologies, micro air vehicles, drones and sensors, medical and casualty care, and protective materials to reduce Soldier risk and enhance situational and option awareness; artificial intelligence, which may significantly accelerate decision making and integrate diverse data in innovative ways; and transdisciplinary technologies, which identify and synthesize technologies developed within one discipline that, when

merged with developments in other disciplines, provide unexpected solutions to potentially intractable problems from the institutional base to the farthest tactical edge.

Dynamic Transport, Computing and Edge Sensors

Success on the information-saturated battlefield of 2040 depends upon a critical attribute of Network 2040: the ability to provide usable information to Soldiers, units and commanders, from home station to the farthest tactical edge, when and where needed, without interruption. Whether the Army can ensure availability of required information is contingent upon leveraging technologies that enhance data transport, computing and edge devices in all operational environments.

Dynamic Transport: With shrinking budgets and growing network capacity demand, the Army must focus on maximizing investment value and rationalizing investments in unique military/government solutions. To that end, the Army must investigate new approaches to ensure that sufficient organic network capacity, augmented by commercial technology, is available to meet the expanding requirements for mission data. The demand for global bandwidth is growing in the commercial sector; therefore, the Army should assume that the commercial market will increase global capacity and reliability to meet that need. It is likely that commercial network investments will outpace the Army's ability to generate organic capacity. As a result, the Army must focus research and development, as well as enhancements to existing programs of record, to leverage the expanded and enhanced commercial network capacity and integrate it with organic Army communications capabilities. As the nation's adversaries will have similar access to commercial assets, it is key that the Army be able to transparently discover, integrate and present a seamless network of both commercial and organic assets to the commander. The combined network will leverage commercial capacity growth and hardened organic assets to reduce the potential risk of adversary IT overmatch while providing a hardened network and services.

In order for the Army to capitalize on and leverage commercial network capacity in conjunction with enhanced organic systems, a dynamic transport architecture must be developed. This architecture will allow Army equipment to automatically and rapidly discover available network transport assets, provide options to the commander, connect to them, secure the transport and seamlessly integrate the available capacity into Army operations. This scenario is far different than the current mode of operation, which relies on pre-provisioning in a build-up phase or an extended organic system set-up upon arrival. As an example, future dynamic transport capability solutions should discover local cellular networks, commercial satellite networks or commercial aerial networks. While the focus of Network 2025 is to develop regional solutions with connections from the operational area to regional nodes, the focus for Network 2040 must be to transparently and securely leverage what is commercially available to augment organic Army assets based on what is operationally required.

Implementation of dynamic transport capability solutions will require the Army to develop a programmable network fabric (e.g., software-defined networking (SDN)), software-reconfigurable cryptographic devices and adaptive bandwidth allocation technologies to maximize connectivity. In this context, SDN is a network architecture that is more dynamic, manageable and adaptable because it implements software control of devices using open standards. The outcome will be an agile, cost-effective network that leverages available Army organic and commercial networking resources, which can be reconfigured rapidly using a more centralized command and control model. The centralized model must also support regional and redundant control options if control structures are disrupted. With dynamic transport increasingly leveraging commercial resources, cryptographic devices will need to be enhanced to match the new dynamic network. This will require the Army to drive research and

development toward extending SDN to cryptographic devices, which will necessitate influencing organizations beyond the Army.

Dynamic Computing: The future Army network will be a highly dispersed computing infrastructure consisting of and leveraging the computational capabilities of assets that span Soldier-carried devices, apparel, weapon systems, command post servers and higher-echelon systems. The computing infrastructure's systems and processes must adapt to the computing needs of the information and applications required by the commander, which in turn will require the computing infrastructure to interoperate with the underlying dynamic transport architecture. The outcome will be a network that can adapt to mission needs, as well as to underlying changes in the operating environment.

By 2040, the Army will have implemented a software-defined data center (SDDC) architecture, where all infrastructure components are virtualized and delivered as a service. Control of the data center is fully automated by software, meaning component configuration is maintained through intelligent software systems. This is in contrast to traditional data centers, where the infrastructure typically is defined by hardware and devices. The challenge for 2040 will be to extend the edge of the SDDC to include devices carried by the Soldier or contained in weapon systems and equipment not located in the data center. This will require an analytical capability to understand where computing is available, which functions are being used and which information is being processed, as well as a predictive capability to enable the network to adapt to emerging information demands. To manage the network, a resilient and secure control fabric must exist to rapidly deploy and modify computing, storage, operational and business functions based on a commander's information requirements.

The commercial sector is developing network function virtualization (NFV) as an architecture to design, deploy and manage network services. By implementing NFV, the Army will be able to reduce proprietary hardware requirements, and create and deploy network functions based on evolving operations. With dynamic computing and dynamic transport, the commander will be faced with making network decisions or understanding how automated reconfiguration impacts operations. The challenge for Army research is to develop visualization and control capability solutions to understand and shape a dynamic transport and computing network.

Growth of the Networked Edge Device: The number of devices at the network edge is growing. This includes devices on Army equipment and Soldiers, as well as sensors accessible in the area of operation (AO). Collected data must be available to Soldiers locally, as well as transported to rear-echelon fusion centers or operation centers for processing, exploitation and further dissemination. The availability of data will provide new opportunities for commanders to gain situational awareness and to combine data in creative ways. In addition, fusion and operations centers might find innovative uses for "dark data": data previously collected that, when combined with other, seemingly unrelated data, can provide novel insights into resolving complex operational scenarios.

The commercial sector describes the explosion of everyday objects that are network connected as the Internet of Things (IoT). For clarity, the DoD describes PIT as all DoD IT that receives, processes, stores, displays or transmits DoD information, which includes IoT devices. The IoT offers devices that are under machine control and have the ability to act as sensors and/or actuators. The Army has an opportunity to leverage IoT devices as a positive game changer for situational awareness and control of deployed assets. The challenge for the network of 2040 is to support the growth in new information, the game-changing opportunity to combine data in innovative ways, and the need to deliver raw and combined data locally, regionally and globally to a diverse set of users. The expansion of IoT devices will drive the need to strengthen machine-to-machine local wired or wireless networks, and the dynamic transport infrastructure. Therefore, the Army must focus research and development to create

a more robust machine-to-machine communication, discovery and caching architecture that can support connected, semi-connected or disconnected operations; and influence the development of standards that enable the Army's networks and interoperability. The network must optimize delivery of information between individual Soldiers, between units co-located in the AO, between units and higher levels of command, and among Army, joint, inter-organizational and multinational partners. This is a fundamental change from the current norm, which includes collecting information at the edge and transporting it to data centers for storage, analysis, exploitation and access. Instead, this new paradigm will enable a more agile force with the option to exploit information closer to the individual Soldier.

Data to Decisive Action

The process of going from diverse, disconnected data elements to an effective command decision requires an operationally focused framework. This need will drive several dramatic improvements in future Army systems and networks. The critical aspects of this paradigm shift can be distilled down to the concepts of accessibility, availability and interoperability as foundational imperatives. The emphasis will remain on enabling individual and team cognition in an information-rich environment.

Accessibility: Today's stovepiped analytical systems often hinder effective access to the right data at the point and time of need, and therefore represent a starting point for transformation rather than an acceptable end state. The technical complexity and fragility of current solutions must be replaced by a new generation of flexible, dynamic and reliable analytic platforms integrated throughout the networked global enterprise. Some of the challenges that currently hinder the Army include constraints in data availability and network transport capacity (particularly across the global wide area network (WAN)), complex standalone applications and a dependence upon skilled expertise to operate and maintain today's environment. Specifically, present-day limitations on data access impede effective mission execution for many organizations across the enterprise; at the same time, the demand for more data continues to increase in both breadth and depth. These forces are driving the move away from the constraints of large, monolithic equipment footprints that strictly confine implementations to heavily resourced data center facilities. The architecture of these costly and complex systems requires significant expertise and financial resources to transport large volumes of data across the currently restricted capacity of the global WAN and to build visualization capability solutions that fulfill the users' needs. An operational and technical architecture that is focused on a data-centric, rather than a system-centric, approach – the global mesh – will facilitate transparent access to required data irrespective of systems or sources.

To ensure accessibility at the point and time of need, the global mesh will leverage a single authoritative DoD identification system as the trusted global source for role-based access controls. This will simplify access controls and enable automatic segmentation of data as pre-defined roles will be set and the data will be tagged with these roles, down to the individual data element level, at the time of capture. Access to system functions, applications and data sources will be granted through a role attribute within a given user's identity profile, which will designate operational need for access and govern use of the analytic solution. This will allow users unfettered access to data sets and sources that are organic to their operational domain without requiring manual intervention or any system modifications by administrators. By leveraging a single DoD authentication resource, Joint partners and other dynamic mission partners will have access to data and analytics in a rapid and automated manner.

Availability: Evolving Big Data analytical tools are burdened by elaborate dependencies and configuration conflicts that result from developmental growing pains. These factors have contributed

to making this emerging capability less available to the broader operational community. These technologies are expected to mature and stabilize, ultimately enabling the Army to instantiate a scalable, hardware-agnostic, federated global mesh as depicted in Figure 2. In addition, numerous advances are expected to address and resolve many of the constraints, such as fragile applications, complex configurations, extensive dependencies between applications, and a requirement for expert knowledge to operate and maintain such systems, that presently inhibit effective use of these capability solutions.

Labor-intensive tasks that currently require significant expertise will become automated through mature, pre-defined code and reference libraries that enable a modular "plug-and-play" approach to analytic development. This will simplify the processes of connecting to a data source, standardizing the elements within the data stream and applying appropriate search tags and relationships to the data. Modularity and portability of pre-developed code elements will enable more effective application of machine learning to numerous components within the new solution. This will include the process of linking context from external references to the data elements, normalizing the data, identifying statistical baselines and deviations in the data streams, and presenting meaningful summary views through a customizable interface. Improvements in these key areas will enable greater adoption and integration of analytics within Army missions and across the operational environment.

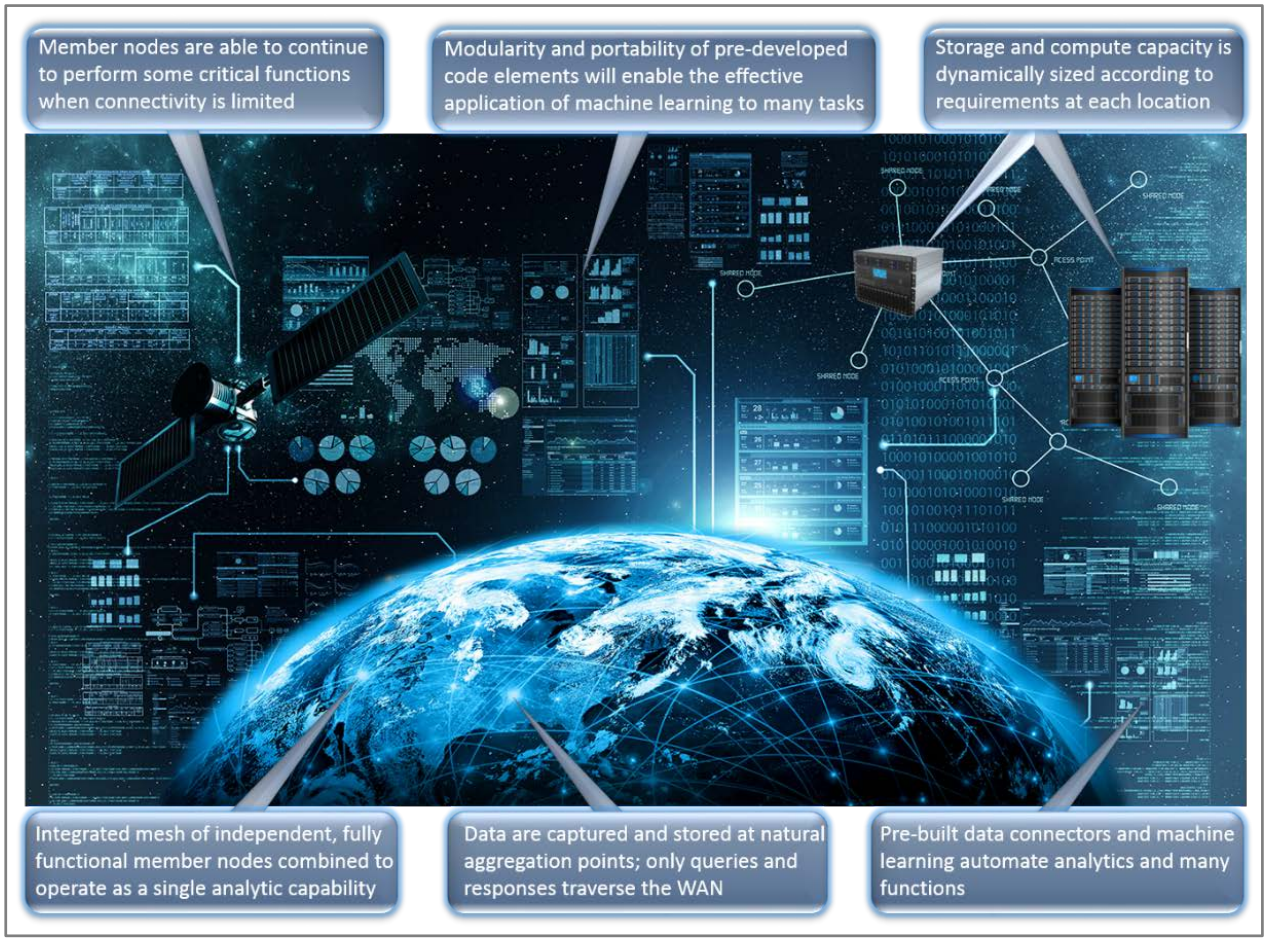


Figure 2. Overview of global analytic mesh and member nodes

Global data analytics will prove critical to a wide range of Army missions and warfighter functions, from detecting network-based attacks through subtle anomaly identification, to optimized large-scale mission planning that leverages diverse streaming data and sensor sources. Collected data will span all

types and classification levels, and will support tactical mission command systems, strategic operations and a variety of context-enriched information. Effective integration of a broad range of analytics within the network operations domain will leverage advances in machine learning to automate many of the common functions that today require dedicated personnel, thus freeing up future staff to focus on those missions that can only be performed using human skill and intelligence. Such an implementation will require agile and tailored development of cross-domain solutions to provide unidirectional data ingest. These robust solutions will be sized to the needs and demands of the supported user environment, and tailored to the workload and capacity requirements of mission-driven use cases at each echelon and geographic location.

In addition to the right data being available in all operational scenarios and locations, user-facing interfaces will provide intuitive and transparent access to data without requiring specialized skills in computer science or statistics. With data now more accessible and available, pre-defined code libraries will accelerate the process of analytic development and facilitate identification of subtle relationships across and within diverse data sets. This functionality will enable development of customized views, providing operational pictures that are tailored by user and role. The user-defined operational views will fuse a wide range of sensors and sources to create a meaningful dashboard. This will enable non-technical operators to select data feeds and sources, apply built-in and self-defined analytics, and arrange outputs within a personalized interface, supporting a full spectrum of user needs, including the ability to rapidly establish performance monitoring on a variety of geographically dispersed systems. The solution will also enable advanced users to identify “zero day” cyber threats within a defended environment – in advance of any adversary activity.

The key technologies that will enable this global dynamic mesh include: a distributed and logically federated network that minimizes transport of data across the WAN; scalable and modular analytics that maximize interoperability within the Army and between Joint partners; and the ability to establish role-based access controls to quickly size member instances of the global mesh appropriate to the supported mission.

Interoperability: The global capability solution described above will address limitations in current implementations, which are based upon the concept of central monolithic clusters that require moving the data to the system. Instead, the global mesh will be composed of individual member nodes placed at key data aggregation points. A node in this context is a dynamic, appropriately sized, wholly self-contained, fully functional, analytics application stack residing on a cluster of computing and storage capability. Some nodes will have the ability to function for brief periods with reduced or no connectivity to the global mesh. Advances in data synchronization technologies will be required to support the level of data consistency that is critical for certain systems and commander decisions while still allowing for disconnection from and reconnection to enterprise networks and data sources.

The majority of the nodes within the global mesh will be permanent strategic instances collecting data specific to the geographic location and mission to which each is assigned. These nodes will be configured to execute analytics on locally stored data as requested by other enterprise nodes. This architecture will support the concept of moving the code or query to the data rather than moving the data themselves. This new environment will be possible by including data interoperability in future systems’ foundations.

This environment will also minimize the need to transport large volumes of data across the WAN by collecting and storing data at existing aggregation points nearest to where the data are generated. To achieve this federated functionality, each instance will be consistently configured in terms of inter-system protocols, data standards for indexing and storage, and role-based user access controls. Any

enterprise-level node can then transmit a single analytic query for a given type of data that has been collected at multiple global locations; each member node will then execute the query on its locally stored data, returning only the answer back across the WAN to the requesting node and user.

As the Army becomes more agile and mobile, enabled by new technologies such as SDN and dynamically positioned services, analytic capability solutions must likewise adhere to these very same operational imperatives. This means that the effective solution must be both scalable and modular in terms of storage capacity, memory and computing power. Agility is critical to support the warfighter on the move, providing maximum functionality with a minimum physical footprint. Satisfying this need will require both flexible software applications and modular hardware components. Improvements supporting this capability will result in logical separation of operating systems and applications from specific hardware dependencies, allowing storage, computing, memory and networking capacity to be independently scaled. This feature of the enterprise solution will support dynamic and rapid adjustments by node, as well as targeted sizing of each node to meet the specific needs of the supported location. The anticipated improvements that will enable these capability solutions span hardware and software, including more memory and storage capacity at lower costs, stable code baselines and improvements in code interoperability, auto-generated code and modular applications, abstraction of the application from hardware dependencies and linear performance scalability as a function of physical resources.

Human Cognitive Enhancement

The analytics noted earlier will provide the situational and option awareness data necessary to meet mission requirements on the battlefield of 2040. Furthermore, to improve option awareness, historical and background information from mission knowledge databases, multi-intelligence feeds, and human and system communications from across the network regarding plans, status and outcomes will be integrated into visualizations of options in the decision spaces available. Key sources of these data will include instrumented Soldiers equipped with multi-modal sensory prostheses that monitor individuals (to include teammates, adversaries, non-combatants and surroundings), networks, systems and attributes of the environment in real time. Such prostheses will capture data beyond the range of human senses, simultaneously mapping those data back to other senses for use by the warfighter, like night vision goggles map invisible infrared spectra back into those that are visible to the human eye.

Technologies such as health and fitness monitors will evolve beyond measuring heart rate into devices that continuously take electrocardiograms (EKGs), respiration rates and levels of chemicals in the blood (hormones and neurotransmitters), and monitor joint and muscle effort, neurological activity (through EKGs) and possibly brain function as inferred from electroencephalograms of electrical brainwave activity. Optical sensors will capture visible and non-visible electromagnetic spectrum (EMS), such as infrared and ultraviolet light, and acoustic sensors will enable detection of even faint sounds beyond the normal sound spectrum and at a great distance. Sensors will monitor chemical and biological data and measure radiation, temperature, pressure and magnetic fields. This information will be fused, enhanced through automated analytics and incorporated into model-driven information displays that will enable a range of advisory services, including enhanced situational awareness, dynamic planning and option awareness, communication and coordination, mission simulation, human-machine interfaces, and model-based fusion and analysis, as described below.

Enhanced Situational Awareness: The network's shared common operating picture will be enriched with background information gathered from all connected systems and enhanced by real-time analytics that expose relationships and patterns, and provide insight into their potential causes and predicted effects. Soldiers and distributed teams will be able to view people, systems and terrain with identities,

histories and relevance to current and future tasks. In this way, the scenario assault team may gain situational awareness from their teammates' reactions in real time. Displays also will help users maintain understanding of their current task and how it relates to the larger mission (such as when the key toxin ingredient in the Battlefield 2040 Operational Scenario was moved), bolstering human working memory by keeping track of next steps and information gaps.

Dynamic Planning and Option Awareness: Model-based, course-of-action planning and decision tools will provide users in-depth analysis of the full space of courses of action, characterizing costs and benefits to the mission in terms of quantitative and qualitative measures. Operators will be able to understand the projected impact of their actions, both on their own tasks and on the mission as a whole. Such option awareness analysis would be essential in the Battlefield 2040 Operational Scenario to decide which component will lead the assault, the limits on kinetic actions and where the airhead should be located. Further, each of these decisions could be revisited in real time as new data update the decision spaces. The system will be capable of anticipating when decisions or replanning/retasking is required based on ongoing mission assessments (troop/asset health and status, updated threat laydown, etc.), then will initiate processing and user interactions as appropriate. In this way, even as Soldiers move through the building toward their bio-lab objective, routes may change in real time in response to the bio-sensors' monitoring teammate reactions.

Communication and Coordination: Situational and option awareness functions will be tightly coupled with workflow management, collaboration, coordination and communication services. Users will receive model-generated tasking that not only describes their own responsibilities but also characterizes interdependencies across the mission. Advanced collaborative tools will enable individuals, as part of widely distributed teams, to interact effectively in spite of their physical separation. Proactive anticipatory communications will meet identified information needs before users must actively request inputs.

Mission Simulation: By substituting real-time feeds for historical or synthetic ones, Soldiers will be able to rehearse upcoming operations using the same tools they access during combat. Virtual environments will provide troops opportunities to practice perceiving, interpreting and responding to events, including establishing key information to be communicated at critical points within the mission and developing familiarity with terrain and objectives.

Human-Machine Interfaces: The anticipated stream of multi-modal (visual, auditory, haptic) information can only be managed and exploited to gain decision advantage through the utilization of automated fusion and analysis technologies that transform and reinterpret feeds, into both near- and far-term operational goals and plans, and transmit these forecasts and visualizations of decision spaces to consumers across the network. Moreover, information must be prepared and disseminated at an appropriate level of abstraction for the user, just in time for use (as determined by ongoing analysis of users and needs), and conveyed in order of priority within the context of current mission tasks and operational conditions. While the same data might have use at the individual Soldier, brigade and corps level, the goals at each level, and therefore the interpretation of those data, will be different.

Such systems will also require next-generation human-machine interfaces capable of mediating mixed-initiative communications, where both people and machines actively participate in a dialog, each contributing what is best suited at the most appropriate time. Doing so effectively constrains automated processing and allocates cognitive work across people and automation. Furthermore, advances in digitally enhanced, multi-modal, augmented reality interfaces will enable efficient transmission of information to the modality best suited to communicating it to people. These appropriately timed communications will draw attention to key information (by modulating salience),

to communications from teammates or to entities or other features in the physical world. In addition to selecting the best modality, the automation will present information in formats that improve processing speed and accuracy and facilitate entity and situation recognition. These interfaces could potentially employ techniques that actually alter neural function to improve processing, for instance through the skull using trans-cranial magnetic stimulation or direct electrical stimulation that uses neural implants. The timing of stimuli could be in response to operational contexts that the automation recognizes, such as changing routes through buildings or responding to the moved toxin ingredient in the Battlefield 2040 Operational Scenario. Alternatively, they could be triggered by the automatic sensing of a human internal state, such as mental or physical fatigue, or physiological responses that indicate pre-conscious recognition of stimuli or detection of anomalies.

Model-based Fusion and Analysis: This kind of analysis and presentation of information will require a network of interrelated models that enable different sources of data to be mapped to common concepts that can be connected, reasoned over and translated across levels of abstraction at each echelon and for each coalition partner. For example, by modeling mission plans and courses of action in terms of the forces involved in specific operations, the system will be able to generate automated support for planning (such as the assault and airhead location in the Battlefield 2040 Operational Scenario), situational and option awareness, team coordination (such as when assault teams move through the buildings in the Battlefield 2040 Operational Scenario) and pre-mission simulation and training that are tailored to Soldiers' needs and synchronized across the enterprise. Alberts & Hayes (2007) suggest that such a mature, dynamically adaptive planning environment requires a shift from shared information to shared understanding (situational and option awareness), which necessitates dynamic real-time transformation and interpretation of data across frames of reference.[2]

Robotics and Autonomous Operations

Robotics may represent one of the most significant and game-changing technologies for the Army since the development of the tank in World War I. Robotics have already altered the nature of warfare, from the introduction of small robots that can counter improvised explosive devices (IEDs) to large missile-carrying drones that can penetrate deep across borders and accurately strike hostiles in otherwise inaccessible, complicated hideouts. This infusion of both physical and cyber (i.e., bots and botnets) robotics will continue to shape the profile of all Army components and units. As these systems evolve, they will slowly become an organic part of the Army. Future robotic systems will migrate from being tools that augment specialized operations to being the essential core of fighting units, providing a key element of a unit's infrastructure and operational capability. The robot will become as crucial to the warfighter as the radio and the rifle are now. These systems are on an accelerated evolutionary path that will quickly shift from sophisticated tool to dedicated work animals to operational assistants. Like the Soldier, these systems will bring ability, experience and connectivity that will change the way the Army conducts future warfare.

As robotic technologies are adopted by the warfighter, new tasks and methodologies of employment will naturally evolve. The capability and capacity of the network must grow to embrace and enable these emerging technologies. Old TTPs, which must account for human vulnerabilities, will be reexamined, allowing relaxation of the physical constraints that are based on Soldiers' current physical abilities. Robotic-centric TTPs, which could fundamentally change concepts of operations and tactics, may be adopted instead. As these systems gain new capability and credibility, and are employed by

[2] Brehmer (1991). Organization for decision making in complex systems. In J. Rassmussen, B. Brehmer & J. Leplat (Eds.), *Distributed decision making: Cognitive models for cooperative work* (pp. 335-347). Chichester, U.K.: Wiley.

the warfighter, new focus, applications and use criteria will change the very nature of the way battles are prosecuted.

The Army anticipates that robotics will fundamentally reshape the force along four major axes: protection and safety; manpower reduction and logistics; influence and reach; and lethality. Each area presents different challenges to the future network and will have to co-evolve and adapt to support future robotic capability solutions and manned-unmanned teaming.

Protection and Safety: Whether for safety (reduction of accidents and mishaps) or protection (mitigation of harm from an adversary), robotics will continue to reduce human exposure to dull, dirty and dangerous tasks, therefore increasing the overall effectiveness of the fighting unit. In dangerous tasks, such as IED disruption and neutralization, robotics are already proving their utility as a lifesaver. Even without sophistication, small robotic systems provide Soldiers essential stand-off distance from explosives and ambush. The next generation of counter-IED robots (advanced explosive ordnance disposal robotic systems) will increase this operational capability by adding and automating complex manipulations, raising the dexterity of these systems. Extending this dexterity to vehicles will enable rapid route clearance in hostile environments. Convoys are another inherently dangerous operation as personnel are vulnerable in clustered, predictable and slow-moving vehicles. Driverless trucks can reduce the inherent exposure to danger by removing the need to man each vehicle. This flexibility also changes the role of the warfighter from navigator to supervisor, mitigating the need to focus on maneuvering and freeing the attention of the Soldier to focus on the fight. Reducing human vulnerability also reduces the logistics burden. Vehicle armor intended to protect the crew cab can be redesigned or optimized to cut weight and volume, potentially increasing the efficiency of logistics. Additionally, resources dedicated to protecting personnel in vehicles can be reallocated to the mission of transporting materials and supplies. Experimentation with driverless convoys through the Army's Autonomous Mobility Appliqué System program is currently under way.

Robotics can mitigate dull and dirty tasks as well. They can increase the effectiveness of units in roles that are tedious, such as perimeter security, observation and overwatch, where diligence is essential but attention to detail is fatiguing. This utility will be integrated into the Common Robotics System – Individual, with interchangeable sensor payloads that provide cameras, radar and non-lethal means. This greater awareness will also extend to the battlefield. Today, unattended ground sensors (UGS) provide rudimentary but critical information from systems placed in strategic locations. Future robotic systems will mobilize these sensors to develop sensor nets that can self-mobilize and self-heal to maintain coverage, relieving the cognitive load of oversight.

Robotic advancement, coupled with a strong network, will continue to blur the lines between specialized robots designed for a specific task to generalized platforms capable of executing multiple tasks. The vehicle used to drive troops to the front will become the overwatch for the base. Paired with advances in "smart" components, such as cell phones, lights, routers and cameras, all components in a unit will work together to maintain awareness, enhance safety and provide layers of protection to the unit. Even when not actively employed, these components will be part of a larger network of connected and embodied sensors, enabling a dynamic and heavy version of today's concept of the IoT. To support this multi-functionality, the future network must be stable, pervasive and available across the entire enterprise, down to the individual Soldier and components. Customer, consumer and Soldier will need to handle these complexities in a different manner and may require additional considerations, such as repairability, replaceability and service level agreements. In the past, if basic components – like a lightbulb – broke, nobody had to call tech support. With the IoT, the infusion of ubiquitous,

smart and connected components will have to be evaluated to make sure they deliver on their value propositions.

Manpower Reduction and Logistics: Robotics may also address the growing pressure to reduce the overall footprint of the Army, not only by assuming tactical roles on the front lines but by supporting operations to sustain them. One of the major factors in an army's effectiveness is its ability to feed, arm and fuel its troops in theater. This includes moving materiel, as well as protecting it and the personnel handling it. The greater the number of forward-deployed personnel, the greater the tail. Therefore, a significant role for robotics is to move humans out of vehicles and away from screens in order to reduce the footprint and costs associated with manned sustainment operations. Every support role fulfilled by a robot reduces the need for and burden of a forward-deployed human counterpart, consequently reducing the need to supply and protect that human. Through effective employment, robotics may enable the Army to fight more with a smaller deployed footprint.

In addition to reducing personnel, robotics will ease the physical burden and workload of those remaining. A Soldier is less effective if fatigued from heavy effort. Robotics can relieve this burden by filling the role of a pack mule, transporting heavy loads where traditional vehicles are not capable and where, historically, Soldiers had to carry their own supporting equipment. Exploration of this concept is already under way, with medium-sized all-terrain vehicle robots like the Squad Multipurpose Equipment Transport, which is able to transport (in either guided or autonomous modes) the bulk of supplies for a squad across unstructured terrain. Even more impressive concepts are being explored with four-legged robots (Robotic Wingman) that can carry man-sized loads over rough terrain by walking with the Soldier.

The concept of unmanned transport also extends to the air domain. Demonstrations are under way for utilizing unmanned helicopters for aerial cargo lift and carry. These large systems utilize Apache-sized helicopters to lift, transport and deliver large loads, without human direction, over and around inhospitable routes and under hostile fire. As robotics evolve, this concept will expand to include large-vessel lift and lightweight continuous quadcopter operations that can resupply the individual dismounted Soldier even during a live mission.

Future robotics efforts may break the need to organize transport in long cargo trains for protection. By reducing personnel threats, transport may take on a more continuous and distributed supply methodology, like a heavy version of industry's United Parcel Service (UPS), where deliveries are made on an as-needed basis. Empowering a smart network that can track assets across an entire enterprise may support a less structured supply methodology, like Amazon's KIVA robots, where the warehouse inventory is on mobile robots that optimize their movement to dynamically fulfill individual orders.

Robotics may also shape future staging and battle preparations. Robotics could enable concepts like remote marshalling, where robotic assets and supporting supplies marshal in remote areas, managing and maintaining their own resources until called upon. These systems could be mobile and handle their own protection and organization in a configuration similar to what carrier groups provide the Navy. Equally possible is that these same resources could be distributed over large areas and regions near volatile borders, with the ability to come together as a cohesive unit when needed.

Critical to enabling such directed and autonomous robotics capability solutions, and the reduction of support infrastructure and personnel, is a strong and healthy network that supports the heavier oversight and connectivity load for coordination, tracking, logistics and planning.

Influence and Reach: In addition to improving safety and reducing cost, robotics will expand the envelope of effective warfare through novel platforms and methodologies of employment. New robotic systems will continue to expand the duration, range and coverage of today's warfighter, to include moving into domains previously inaccessible to manned systems. Already robotics are increasing the duration of critical operational capabilities, such as surveillance, overwatch and network connectivity. Technologies and systems like Global Hawk allow nearly continuous standoff observation of large areas of influence, with flight times nearing 20 hours and ranges of thousands of miles. New research programs, like the Defense Advanced Research Projects Agency's Vulture program, are looking to expand flight duration from hours to weeks. On a more tactical level, medium-size UAVs, such as the Reaper, have expanded operational envelopes beyond traditional borders and bear a significant burden in the war on terrorism. As these assets become more integrated, they will enhance the efficacy of manned units. Even now, the Army is investigating the effectiveness of augmenting manned attack helicopters with dedicated UAVs (manned-unmanned teaming) to act as a coordinated entity with superior awareness and influence. Unmanned technology will continue to spread to individual units and even the dismounted Soldier, with small, lightweight aerial vehicles like hand-launched UAVs and quadcopters.

Robotics will also expand the operational envelope of ground warfare. Development of effective walking machines has extended robotic reach into rough, unstructured terrain, allowing the warfighter to carry heavier loads. Unmanned ground systems provide unprecedented persistence, awareness and responsiveness over large areas. Small crawling and flying robots, such as those being developed by the Army's Soldier-Borne Sensors program, promise reach into tight areas, such as bunkers, caves and constricted urban zones. Robotics also will increase the range and duration of current standalone solutions, and the effective AO for existing units, through collaboration between robots via hierarchical teams or ad hoc swarms.

While future robotics will not need constant and high-bandwidth connections for tactical control, contact and communication will remain essential to coordinate effectively with them as they move into previously unreachable or contested areas. The network must become dynamic to achieve and maintain connectivity in the face of a potential adversary and under less-than-ideal environmental conditions.

Lethality: Robotics will continue to provide the Army greater lethal and non-lethal overmatch.[3] Coupled with autonomy and intelligence, robotic systems will be able to react at speeds greater than the decision loops of all but the most sophisticated adversaries. Not only will these systems be able to competently navigate and maneuver in potentially hostile environments but they will be able to develop their own understanding of situations and derive appropriate responses, even when communication with the warfighter is contested or denied. Already there are signs that future warfare may be initiated and waged silently, without ever making direct contact with an adversary, through cyber and EW attacks. Robotics offer alternate means of delivering lethal and non-lethal force.

Lethality will come in different scales, as well. Large armor will continue to play a role in the future as envisioned by the Army's heavy assault vehicle, the Armored Robotic Wingman. This platform brings much-needed firepower to the front lines. Smaller platforms, such as hand-launched aerial vehicles, will provide dismounted Soldiers critical tactical situational and option awareness. Lethality will be achieved not just through size but also numbers. Swarms offer great potential in a distributed and coordinated attack. Coordinated swarming, such as small lightweight UAVs or fast and agile

[3] Lethality of robotics and autonomous systems will comply with DoD Instruction 3009.09, Autonomy in Weapon Systems.

ground vehicles, can quickly overwhelm today's most sophisticated defenses while overcoming and adapting to loss of individual members.

As robotics move into an active combat role, connectivity, coordination and contingency will become increasingly critical. The robot and network of the future will have to support new rules of engagement in the face of an aware and active adversary. While autonomy may mitigate the need for lock-step authority, these robots will still be part of a coordinated fighting unit and must be able to provide real-time assessments, actionable intent and potential contingency alternatives. Security of the platform, the network and the data will remain paramount as the capability for lethality grows, but may be mitigated by machines that are more introspective and self-aware.

With advances in artificial intelligence, robotic systems will start to become real assets in understanding and interpreting the current battle picture, and will begin to share decision making and action with the fighting Soldier. Robots that can interpret and react to dynamic threats in predictable and coordinated ways will move robotics from simple tools and faithful pack animals towards assistants that can share awareness in a fight.

Cybersecurity and Resiliency

Each of the revolutionary technologies described in Section 4 raises the question: How can these technologies be integrated into Army networks, systems and operations while managing the risks associated with their potential compromise by an advanced adversary, the unanticipated consequences of interactions among new and existing technologies, or cascading effects due to failures or instability?

> "Network dominance and defense are an integral part of our national security … With the evolving cyber environment, the Army has been proactively adapting to cyber threats and vulnerabilities by transforming processes, organizations and operating practices."
>
> **Army Posture Statement 2015**

Network 2040 includes the means by which data are transported from one location to another, regardless of which entity owns or controls specific transport methods or components. These means are supported by the following five constructs (each of which is discussed below): achieving data quality assurance; design principles for directed self-organization; intelligent cyber-physical systems; adaptive identity and access management; and novel forms of encryption.

Achieving Data Quality Assurance: A resilient network ensures that data are provided to the correct decision makers in the timeframe required to support mission decisions, with qualities that decision makers can determine, despite the presence of advanced adversaries within the network or at the endpoints from which data are obtained or consumed. The desired qualities are related to correctness in the form of precision, accuracy and time-binding, along with accountability or assurance in the form of provenance, intended use or limitations, known dissemination and tamper evidence. The presence of these qualities is crucial to the human cognitive and autonomous or semi-autonomous environments described in the preceding sections. These qualities must be ensured despite the fact that adversaries seek to influence decisions by manipulating the data that decision makers use through modification, fabrication, delay or destruction.

Decision makers should have the ability to understand the qualities of the data offered or considered for use in the data-to-decisive-action cycle. While data tagging and metadata binding will be relevant, other mechanisms used to ensure these qualities may include autonomous agents that accompany data or prepare the way for data use, specifically by defending against manipulation. Defense from manipulation may include changing the order in which facts are perceived, collective intelligence

mechanisms that corroborate or substantiate data based on their provenance and prior uses, and agents that reconstruct damaged data from traces left in the network or at endpoints.

Design Principles for Directed Self-Organization: Network resiliency, and the mission resilience it supports, will be achieved by applying a set of design principles derived from research on and lessons learned from resilience in other systems, to include biological[4] systems. Autonomous or semi-autonomous agents will self-organize network services, based on the direction of mission owners and their representatives. Directions will reflect mission and organizational priorities for security and resiliency objectives, presented in intuitive ways. Self-organization of network services will take individual resource limitations into consideration (e.g., devices with size, weight and power limits, and damage or destruction of specific nodes or pieces of equipment), directing collective behaviors to provide required operational capabilities.

Security design principles for Army-controlled resources will continue to include separation, isolation, encapsulation, ensuring that critical security checks cannot be bypassed, layering, modularity, hierarchical trust and hierarchical protection. Resiliency design capabilities include the ability to: make architectural changes[5] or update information without disrupting ongoing operations; determine, with a specific level of confidence, the properties of information, network components or endpoints; separate information, define sub-networks and isolate endpoints based on mission, security properties or criticality; and learn from events in order to better anticipate potential future disruptions. In addition, experimental or conceptual application of resiliency design principles and continued research into socio-technical systems will lead to new or modified design strategies that enable Army-controlled resources to participate in broader networks within acceptable risk tolerance.

Intelligent Cyber-Physical Systems (ICPS): Network 2040 will be equipped with ICPSs. Intelligence will allow groups of cyber physical systems (CPS), such as ground robots and unmanned vehicles, to automatically exhibit group decision making and coordinate their actions autonomously (i.e., without operators) to ensure mission success. Intelligent architectures, based on hardware root-of-trust mechanisms, including encryption and root-kit detection hardware digital rights management, allow for continuous evaluation of the trustworthiness of the system's state and operations. To mitigate insider threats and operator sabotage, a CPS will continuously assess the trustworthiness of operator commands. This will be done by validating them against mission context, required safety envelopes and ongoing performance data, as well as by seeking corroborating authorizations from trusted parties when operator actions are suspect. CPS will have resilient, cyber-security analytics mechanisms to anticipate incoming cyber threats and reconfigure themselves to undertake maneuvers to evade or minimize such threats. They will also have the ability to communicate lessons learned in cyber protection to their peers so as to rapidly improve the overall group security posture.

Adaptive Identity and Access Management: Network 2040 will support multiple risk-aware and context-aware authentication and access control mechanisms – mechanisms that adapt to circumstances and adjust access decisions based on an assessment of the risk involved. Adaptive approaches include risk-based authentication (RBA), where transactions replace identity as the focus of decision making; for example, "Should we let this transaction take place?" replaces "Have we identified this person?" RBA systems evaluate context information, including but not limited to related actions, historical activities of the entity, time of day, data context, Internet Protocol addresses of requestors and providers, and client type. Requiring that a user be at or near a geographic location, i.e., geolocating

[4] For example, history has shown that viruses are more prone to spread and cause widespread harm (death) in homogenous populations than in more heterogeneous populations with a diverse immune system. In the cyber world, this translates to a diverse set of applications and operating systems that are abler to survive a malware attack than a homogenous set.
[5] Examples would include changes to network connections, dynamic relocation of key services, etc.

the user, would be applied in certain cases. With further refinement, the system would evaluate user behaviors – not just simple things, such as keystroke timings, but behaviors with a strong personality or psychological component. This could include observing activities under stress or predicting a user's next actions.

Encrypting, decrypting or signing data requires access to cryptographic keys. How well those keys are secured and the confidence that, when shared, they are shared with the correct party are critical. Key sharing could be housed in pieces of equipment or personal effects, or at designated geographical locations, and transmitted to cryptographic devices via secure communications channels.

Novel Forms of Encryption: Several fundamental changes in cryptography will extensively affect defensibility of the network.

Fully homomorphic encryption will allow arbitrary computations to be performed on encrypted data. This, in turn, will enable computations of sensitive data to be outsourced to untrusted platforms, such as cloud providers, without exposing the sensitive data.

Secure multiparty computation (SMC) protocols will allow parties to compute a function based on their joint inputs without disclosing the individual inputs to each other. For example, coalition partners may each provide pieces of information that would jointly determine targets without disclosing the details of their imagery or methods. Increasingly efficient methods are available for SMC, such as the SPeedZ protocol.[6]

Quantum computation is a major concern for Network 2040 as it poses a threat to current public key algorithms, such as digital signature algorithms used in identification and authentication protocols, and public key cryptography used in web transactions. Promising post-quantum approaches are being matured, to include hash-based digital signature schemes and public-key encryption schemes.

Contrary to the challenges of quantum computing, quantum key agreement offers a physically guaranteed method for key exchange. Two parties who share a line-of-sight connection can agree on advanced encryption standard keys, with a guarantee that the adversary learns nothing about the key. For Network 2040, this enables high levels of security for key exchanges.

Taken together, implementation of the five cybersecurity and resiliency constructs described above will mitigate the threat to current and future systems and will increase the assurance that the missions that depend upon those systems and networks will be able to achieve their desired outcomes.

Conclusion

The battlefield of the future will contain complexities that must be addressed and overcome. For instance, most of the world's population will dwell in mega-cities. Weapon systems, disruptive technologies and conflict within these complex environments will create scenarios that the Army can partially predict, although with an understandable level of uncertainty. The Army's current network carries with it a significant support burden and does not provide the mission flexibility and resiliency that emerging threats will demand in 2025 and beyond.

The commander of 2040 will be able to leverage other units' assets and even commercial communication systems and networks in the area of operations as if they were his or her own. Personnel and equipment readiness will be informed by networked sensors that feed analytic capabilities. These capability solutions will be supported by data-to-decisive-action software, which

[6] SPDZ (SPeedZ) protocol: Multiparty computation protocol; processing and performing computations on classified data without revealing the specifics of the data to any of the active participants.

will enable situational awareness, logistics resupply, over-the-air fixes and administration of bio-medical antidotes, to name a few.

Machine learning will enable recurring tasks, like the battle update brief, to be compiled automatically and delivered to the commander, leaving the staff more time to assess, plan, adapt to and overcome the enemy. The operational autonomy enabled by networked sensors will allow robotics to be tightly coupled to the commander's mission, without the one-to-one joystick command and control required today.

As force structure is further reduced, in conjunction with the continued convergence and automation of network management functions, valuable technical personnel will increasingly be available to support offensive and defensive cyber operations and the co-option of commercial networks and sensors found in the AO. Many of these components are already under development. Research in this area must be nurtured and guided to meet the needs and missions of future commanders.

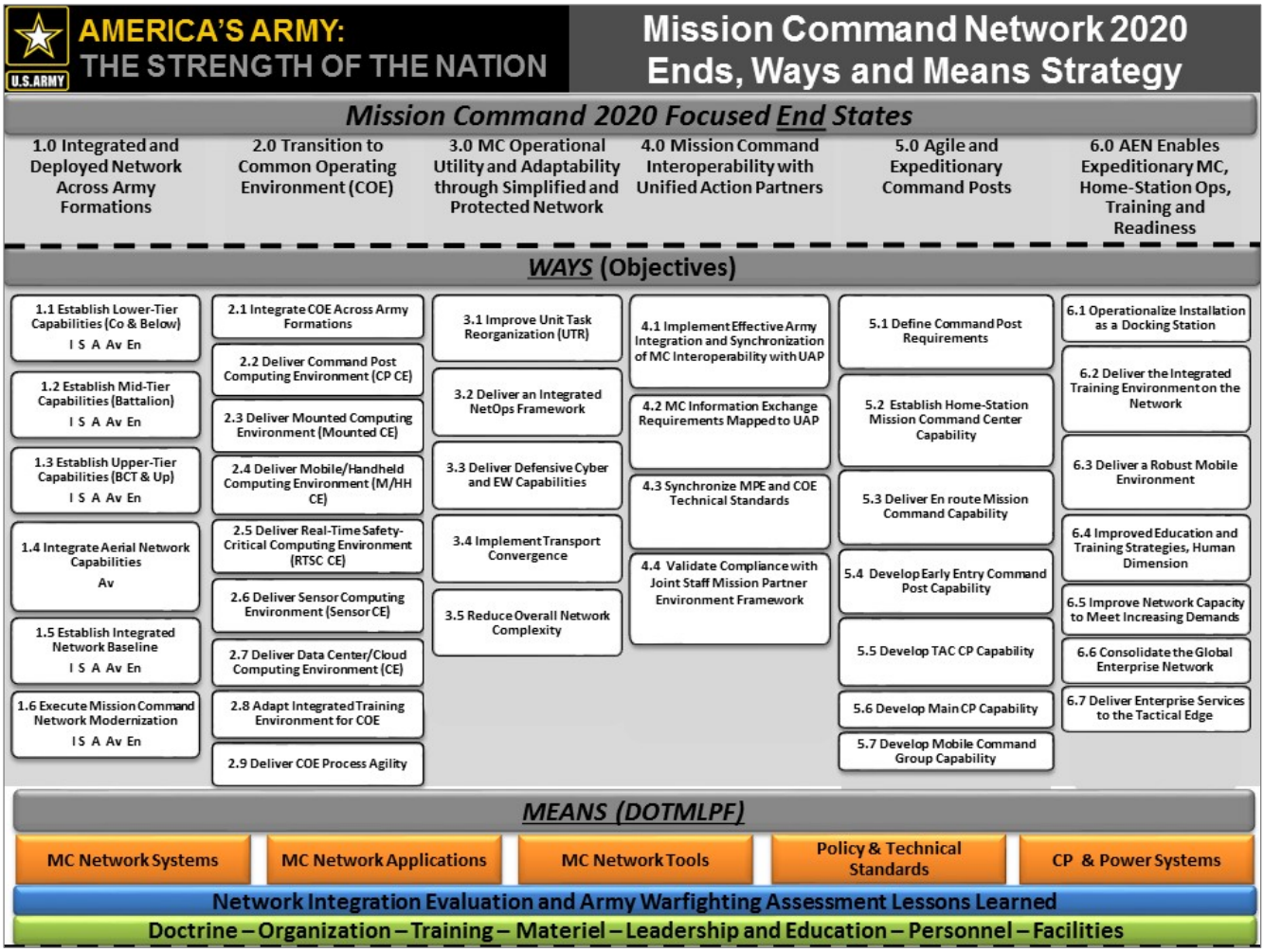
This document focuses on game-changing technologies of the future and is intended to guide network investments, not because the Army must keep up with technology but because the missions of 2040 demand it.

Annex A: Joint Capability Area (JCA) Alignment

Joint Capability Areas	Mission Command	Shaping the Army Network: 2025-2040			
Net-Centric JCA & Enhanced Operations JCAs	**Focused End States**	**Technology Areas**	**Operational & Environmental Trends**	**Required Capabilities**	**2025-2040 Technologies**
6.1 Information Transport **6.3 Net Management** Enhance 2.5 Battlespace Awareness, Data Dissemination & Relay Enhance 5.1.1 Establish & Maintain Unity of Effort with Mission Partners	**1.0 Integrated and Deployed Network across Army Formations** **3.0 MC Operational Utility and Adaptability through Simplified and Protected Network** **4.0 MC Interoperability with Unified Action Partners**	**Dynamic Transport, Computing and Edge Sensors**	▪ Reduced force structure. ▪ Increased data/information management at all echelons. ▪ Information sharing with a dynamic set of mission partners.	Dynamic access to information when needed via secure & unsecure channels.	Dynamic transport architecture and programmable network fabric.
				Augmented MC continuously available from tactical edge to home station.	R&D to leverage commercial capacity.
				Agile force automatically connects, disconnects, organizes, aggregates forces.	Implement dynamic computing and virtualization infrastructure.
				Remain mobile without sacrificing MC capabilities.	Leverage and adapt Internet of Things.
				Connect with known & emerging coalition and government agencies.	Networked edge sensors and devices and data available to individual Soldiers.
6.2 Enterprise Services **6.3 Net Management** Enhance 2.1 Planning and Direction Enhance 2.3 Processing / Exploitation Enhance 5.2.2 Develop Knowledge and SA	**3.0 MC Operational Utility and Adaptability through Simplified and Protected Network**	**Data to Decisive Action**	▪ Increased OPTEMPO and accelerated decision cycles. ▪ Proliferation of commercial technology to adversaries. ▪ Surge of autonomous devices/data may result in information overload.	Decrease time to gather, transform, validate and present data.	Eliminate stovepiped solutions; scalable, globally distributed data & storage.
				Enable all-source trusted information and advanced decision-support tools.	Flexible, dynamic and reliable storage and analytic platforms.
				Advanced computing capability; cope in an information-saturated environment.	Leverage machine learning to generate tailored decision-support products.
				System-based tools to maximize data effectiveness and minimize distractions.	Global mesh of data analytics via dynamic storage, computing, memory.
				Capability to understand, cope, sort and apply significantly more information.	Simplified, scalable, tailorable and modular systems and access.
6.2 Enterprise Services **6.3 Net Management** Enhance 2.5 Battlespace Awareness, Data Dissemination & Relay Enhance 5.3 Planning Enhance 5.4 Decide	**3.0 MC Operational Utility and Adaptability through Simplified and Protected Network** **6.0 Enables Distributed MC, Home-Station Ops, Training and Readiness**	**Human Cognitive Enhancement**	▪ Information-saturated environment. ▪ Quality of that information will be questionable. ▪ Misinformation as a weapon.	Increase cognitive capability; overcome 'noise'; improve decision making.	Integration of operation and Soldier status data for enhanced SA and OA.
				Commanders' SA and OA augmented by hybrid cognitive architecture.	Dynamic planning and OA data tailored to augment specific user requirements.
				Enable scalable, enhanced, machine-machine and human-machine interfaces.	Sensory prostheses, instrumented Soldier & systems (imagery, sensors, robotics).
				Integrated, enhanced humans, robotics & systems; anticipatory intelligence.	Human-machine interfaces fuse visual, audio, haptic information; build options.
				Monitor Soldier status and predict operational trends and alternatives.	Enhanced battlefield operations models enable automated planning support.

6.2 Enterprise Services **6.3 Net Management** Enhance 2.2 Collection	**3.0 MC Operational Utility and Adaptability through Simplified and Protected Network** **6.0 Enables Distributed MC, Home-Station Ops, Training and Readiness**	**Robotics and Autonomous Operations**	▪ Emergence of autonomous and self-organizing robotics, to include independent and "swarm" operations.	Employ robotics to reduce force risk and increase operational protection.	Network-enabled manned-unmanned systems and teams.
				Expand reach of SA and OA without risk of exposure.	Connected network of robotics & sensors become operations and TTP enablers.
				Automate performance of selected battlefield tasks (e.g., logistics).	Robotics augment/replace humans in logistics, protection, battle tasks.
				Enable mobile network operations and operational flexibility under uncertainty.	Robotics' autonomy, mobility, sensing, manipulation extend influence and reach.
				Network ability to manage autonomy-enabled systems, teams, swarms.	Autonomous systems, platforms, swarms enhance combat operations, reduce risk.
6.4 Information Assurance **6.3 Net Management**	**3.0 MC Operational Utility and Adaptability through Simplified and Protected Network**	**Cybersecurity and Resiliency**	▪ Constant, blended cyber threats from state and non-state actors.	Advanced defensive cyber ops: self-healing, reorganization, resistance, resilience.	Dynamic, hardened systems protect data, survive kinetic and cyber attacks.
				Sustain network and operations while under attack.	Predict, assess and interdict network incursions before threat activation.
				Simplified, resistant, resilient network degrades without catastrophic failure.	Self-organizing network services ensure continuity of operations, data provision.
				Automatic reconfiguration, redundancy; ensure continuous operations.	Autonomous, intelligent cyber-physical systems decision making, cyber defense.
				Anticipate threat actions; detect and respond before compromise.	Adaptive identity and access management reduces insider threats.

Annex B: Mission Command Focused End States



Annex C: Acronyms

TERM	DEFINITION
AI	Artificial Intelligence
AJ	Anti-Jam
AMC	Army Materiel Command
ANCP	Army Network Campaign Plan
AO	Area of Operations
ARNG	Army National Guard
ARW	Armored Robotic Wingman
ATV	All-Terrain Vehicle
BYOD	Bring Your Own Device
BYON	Bring Your Own Network
C2	Command and Control
CEMA	Cyber Electromagnetic Activities
CIO/G-6	Chief Information Officer/G-6
COE	Common Operating Environment
CONUS	Continental United States
CPS	Cyber-Physical Systems
CRS-I	Common Robotic System – Individual
DARPA	Defense Advanced Research Projects Agency
DEPS	DoD Enterprise Portal Service
DEW	Directed Energy Weapon
DIL	Disconnected, Intermittent or Low bandwidth
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EEG	Electroencephalogram
EKG	Electrocardiogram
EMS	Electromagnetic Spectrum
EOD	Explosive Ordnance Disposal
EW	Electromagnetic Warfare
FORSCOM	U.S. Army Forces Command
FY	Fiscal Year
HSMCC	Home-Station Mission Command Center
HUD	Heads-Up Display
ICPS	Intelligent Cyber-Physical Systems
IED	Improvised Explosive Device
IP	Internet Protocol
IR	Infrared
IT	Information Technology
IoT	Internet of Things
JCA	Joint Capability Area
JIE	Joint Information Environment
JRSS	Joint Regional Security Stack
JTF	Joint Task Force
LPI/LPD	Low Probability of Intercept / Low Probability of Detection
MASINT	Measurement and Signatures Intelligence
MC	Mission Command
MDB	Mission Database (e.g., CONUS-based Mission Data Base)
MEDCOM	U.S. Army Medical Command
MPE	Mission Partner Environment
MPLS	Multi-Protocol Label Switching
MUM-T	Manned-Unmanned Teaming
NEC	Network Enterprise Center
NFV	Network Function Virtualization

NIA	National Intelligence Agency
OA	Option Awareness
OPTEMPO	Operational Tempo
PIT	Platform IT
PNT	Position, Navigation & Timing
POR	Program of Record
RBA	Risk-Based Authentication
RF	Radio Frequency
RHN	Regional Hub Node
S&T	Science & Technology
SA	Situational Awareness
SBS	Soldier-Borne Sensors
SDN	Software-Defined Networking
SDDC	Software-Defined Data Center
SIGINT	Signals Intelligence
SMC	Secure Multiparty Computation
SMET	Squad Multipurpose Equipment Transport
SPDZ	SPeedZ Protocol
STS	Socio-Technical Systems
SWaP	Size, Weight and Power
TRADOC	U.S. Army Training and Doctrine Command
28TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground Sensors
UPS	United Parcel Service
USACE	U.S. Army Corps of Engineers
USAR	U.S. Army Reserve
USARPAC	U.S. Army Pacific Command
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XT	Xipe Totec (Notional entity in the Operational Scenario)

Annex D: References

20YY Preparing for War in the Robotic Age, Robert O. Work and Shawn Brimley, Center for a New American Security, January 2014.

Army Directive 2013-02, Network 2020 and Beyond: The Way Ahead, 11 March 2013.

Army Network Campaign Plan 2020 and Beyond, Army CIO/G-6, 6 February 2015.

Army Network Campaign Plan 2020 and Beyond, Implementation Guidance, Near-Term 2015-2016, Army CIO/G-6, 6 February 2015.

Army Network Campaign Plan 2020 and Beyond, Implementation Guidance, Mid-Term 2017-2021, Army CIO/G-6, 6 February 2015.

Army Posture Statement, 2015.

Army Strategic Planning Guidance, 2015.

Army Warfighting Challenges (AWFC), Information Paper, U.S. Army Training and Doctrine Command, Army Capabilities Integration Center, 10 July 2014.

The Army Vision: Strategic Advantage in a Complex World, 11 May 2015.

TRADOC Pamphlet 525-3-1: The Army Operating Concept: Win in a Complex World 2020-2040, 7 October 2014.

Augmenting Human Intellect: A Conceptual Framework, Douglas C. Engelbart, October 1962.

Autonomy in Weapon Systems, DoD Instruction 3009.09, 21 November 2012.

Breakthrough Technologies for National Security, Defense Advanced Research Projects Agency, March 2015.

Capstone Concept for Joint Operations: Joint Force 2020, Joint Chiefs of Staff, 10 September 2012.

Complex Operational Decision Making in Networked Systems of Humans and Machines, The Committee on Integrating Humans, Machines and Networks; National Research Council, 2014.

DARPA Robotics Challenge (DRC), Orlowski, Christopher, PHD, MAJ, U.S. Army; http://www.darpa.mil/program/darpa-robotics-challenge as of 3 December 2015.

The DoD Cyber Strategy, U.S. Department of Defense, April 2015.

DoD Research and Engineering Enterprise [Strategy and Planning Document], Assistant Secretary of Defense (Research & Engineering), 1 May 2014.

Force 2025 and Beyond: Unified Land Operations; Win in a Complex World, U.S. Army Training and Doctrine Command, 7 October 2014.

Initial Capabilities Document (ICD) for Networked Enabled Mission Command (NeMC), U.S. Army Training and Doctrine Command, 1 December 2011.

Legged Squad Support System (LS3), Orlowski, Christopher, PHD, MAJ, U.S. Army; http://www.darpa.mil/program/legged-squad-support-system as of 3 December 2015.

Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report, Kott, Alexander; Alberts, David; Zalman, Amy; Shakarian, Paulo; Maymi, Fernando; Wang, Cliff; and Qu, Gang; Army Research Laboratory Report ARL-SR-0327, June 2015.

The Megacity, Operational Challenges for Force 2025 and Beyond, U.S. Army Training and Doctrine Command Unified Quest 14, Army Capabilities Integration Center, 8 May 2014.

Memorandum: Required Capabilities for FY14 Capabilities Developments, including Capabilities Needs Analysis (CNA) 17-21, U.S. Army Training and Doctrine Command, 4 November 2013.

The Mission Command Network, Vision & Narrative, U.S. Army Combined Arms Center, 16 June 2015.

The National Intelligence Strategy of the United States, June 2014.

The National Military Strategy of the United States of America 2015, June 2015.

Planning: Complex Endeavors, David S. Alberts & Richard E. Hayes, The Command and Control Research Program (CCRP) (Future of Command and Control), April 2007.

Science and Technology Lines of Effort for a Future Expeditionary Army, U.S. Army Training and Doctrine Command, 16 September 2014.

Strategic Trends Analysis, The Landscape of Future Conflict, U.S. Army Training and Doctrine Command Unified Quest 14, Army Capabilities Integration Center, 8 May 2014.

Technology and Capability Objectives for Force 2025 and Beyond, Information Paper, U.S. Army Training and Doctrine Command, Army Capabilities Integration Center, 4 August 2014.

TRADOC Capabilities Needs Analysis (CNA) Critical Capability Gaps 2016-2020, U.S. Army Training and Doctrine Command, 15 September 2014.

The United States National Security Strategy, February 2015.