DEPARTMENT OF THE ARMY
UNITED STATES ARMY CENTRAL
1 GABRESKI DRIVE
SHAW AIR FORCE BASE, SC 29152-5202

ACCG

30 January 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Central Fiscal Year (FY) 17-18 Cyberspace Strategy for Unified Land Operations

1. Rapid growth in information and communications technology affects every aspect of our lives. Improvements in speed, connectivity, and access to the cyberspace domain bring both incredible opportunities and significant risks. To prevent conflict, shape security environments, and win wars while operating as part of a Joint Force with multiple partners requires a proficient cyber force operating effectively in and through cyberspace to meet service and joint requirements.

2. The USARCENT FY17-18 Cyberspace Strategy for Unified Land Operations presents the USARCENT vision, major objectives, and end states while linking ends, ways, and means to integrate all USARCENT activities supporting or conducting operations in cyberspace.

3. This strategy projects to 2018 and provides strategic direction to drive investment, workforce, facility, and doctrinal changes within USARCENT to successfully operate in cyberspace and achieve mission success.

4. I request that each of you read and internalize the contents of this strategy. We will measure progress resulting in adjustments to end states and objectives as necessary using scheduled USARCENT forums.

5. The point of contact for this memorandum is (b)(6)

(b)(6)

GARRETT.MICHAEL.XAVIER.1062399771

MICHAEL X. GARRETT
Lieutenant General, USA
Commanding

Encl

ACCG
Subject: United States Army Central Fiscal Year (FY) 17-18 Cyberspace Strategy for Unified Land Operations

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
U.S. Central Command
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Cyberspace Command and 2nd Army
U.S. Army Criminal Investigation Command
U.S. Army Intelligence and Security Command
U.S. Army Corps of Engineers
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Commander, 33th Theater Signal Command (TSC)
Commander, 513th Military Intelligence Brigade
Commander, 1st Theater Sustainment Command
Commander, ASG- Kuwait
Commander, ASG- Qatar

CF:
Director, Office of the Chief Army Reserve
Director, Army National Guard

Executive Summary

DoD, the US Army and US Army Central (USARCENT) acknowledge the need for a renewed approach to warfighting. In the early stages of war, fighting was conducted primarily on land, with innovation and the introduction of ship building, warfare transitioned to include fighting at sea. Eventually aircraft were integrated as warfighting platforms. Today computers and the Internet provide opportunities to our adversaries which require a renewed approach to warfighting.

In order to deter current and emerging threats, USARCENT requires integrated and synchronized cyberspace forces, capabilities, facilities, and partnerships to combat cyberspace threats within the USARCENT AOR (Central Asian States Area (CASA), Arabian Peninsula (AP) and the Levant). These forces are also necessary to execute and modernize the USARCENT Campaign Plan, conduct Theater Security Cooperation and achieve Regional Security Cooperation. The USARCENT Cyberspace Strategy supports and nests with the Department of Defense Cyber Strategy (April 2015, The Army Cyberspace Strategy for Unified Land Operations 2025 (March 2016), The Army Campaign Plan, HQDA Strategic Effort #12, the Army Network Campaign Plan Near Term Implementation Guidance FY16-17) and the Army Cyber Command and Second Army Campaign Plan 2015-01, Rev 1.

Purpose: To provide CG USARCENT's vison, purpose and direction on the integration of Cyberspace operations into the USARCENT plans, operations and exercises. The USARCENT Cyberspace Strategy is aligned across five primary lines of effort which include the following:

LOE 1: Build the USARCENT Cyberspace Workforce. This LOE constitutes USARCENT main effort and consists of three (3) major objectives. First, USARCENT must integrate existing cyberspace talent within USARCENT staff and subordinate units. Second, program and track the arrival and integration of Career Force 17 (Cyberspace) Officers, Warrant Officers, and Enlisted Soldiers in order to formalize the manning and integration of Cyberspace Operations at Echelons Corp and Below (ECB). Third, educate and develop the USARCENT Total Force (Active, Guard, Reserve), DA Civilians and contractors on cyberspace capabilities, integration and proper cyberspace user hygiene.

LOE 2: Conduct Cyberspace Operations. To operate effectively in cyberspace, USARCENT and its subordinate units must integrate and synchronize Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO) and Department of Defense Information Network (DoDIN) Operations with our partners across the USCENTCOM AOR. A key task in this LOE is identifying organic cyberspace capabilities and capability gaps. Once those capabilities and gaps have been identified provide our findings and perspectives to TRADOC, ARCYBER and HQDA to enhance Army doctrine and current and future policies. Paramount to this LOE is that all USARCENT weapons systems, communication networks, and utilities remain ready and resilient to cyberspace vulnerabilities as detailed in the Army Cyber Resiliency Plan.

LOE 3: Identify and Develop Cyberspace Capabilities. As the Army continues to identify and resource cyberspace capability gaps for cyber materiel and capability development, USARCENT must advocate our requirements in order to become the premier ASCC for the integration of Cyberspace Operations. To do so, we must identify and develop the required Cyberspace Operational Need Statements (ONS) and understand the Joint Capabilities Integration and Development (JCIDS) process so that our capability gaps may be resourced. In addition, USARCENT must formalize a relationship with ARCYBER and Assistant Secretary of the Army (Acquisition, Logistics and Technology (ASA(AL&T)) to ensure that our cyberspace requirements are met and nested with the FY17 cyberspace capability development efforts which include Cyberspace Mission Command Platforms, Development of the Persistent Training Environment (PTE) and Cyber Training Ranges, Cyberspace Situational Awareness, Big Data Cyberspace Analytics, Deployable and Tactical DCO Infrastructure, and Insider Threat mitigation.

LOE 4: Invest in Facilities, Systems and Infrastructure. The training, education, development, and integration of cyberspace operations within the USARCENT staff and with our partners requires a training facility. In addition, USARCENT needs to gain greater awareness of IMCOM led forums which determine and drive resourcing cyberspace requirements on Army Installations. Also essential is that the USARCENT staff ensure the resiliency, readiness and reliability of relevant Platform Information and Technology (PIT), Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems across the USARCENT AOR.

LOE 5: Develop Partnerships. Cyberspace Operations at their core are successful due to networks and interconnectivity. For USARCENT to be successful in Unified Land Operations the USARCENT staff must understand and interoperate with our partners. Cyberspace is no exception. To achieve mission success, we need to gain greater awareness of the capabilities, limitations and initiatives of our Joint, Interorganizational and Multinational (JIM) partners and strive for interoperability and synchronization. This requires integration of cyberspace objectives into FY 17/18 exercises, inclusion of cyberspace related talking points into engagements and development of “Spheres of Influence” for consistent and deliberate dialogue with our partners regarding the evolving cyberspace threat. The ultimate goal is to ensure our partners understand the importance of cyberspace operations and its relation to our collective effects to improve regional security.

THE U.S. ARMY CENTRAL CYBERSPACE STRATEGY FOR UNIFIED LAND OPERATIONS FY 17-18

> *"Cyber professionals – resourced with the right infrastructure, platforms and tools – are the key to dominance in cyberspace."*
> *LTG Edward Cardon - Commander, U.S. Army Cyber Command*
> *House Armed Services Committee Testimony, March 2015*

LOE 1: BUILD THE WORKFORCE

This LOE constitutes USARCENT's main effort and requires application and integration of Cyberspace planners across the three mission sets of Cyberspace Operations. Cyberspace is a warfighting domain which is and will continue to be contested militarily. Cyberspace operations, enabled by our global network, can affect both the virtual and the physical worlds. As such, USARCENT staff must view our network as a warfighting platform and ensure the readiness of personnel and equipment. An important aspect to this effort is understanding that USARCENT can access and leverage skillsets across the Army's Total Force (AC, USAR, ARNG) to address emerging cyberspace threats. The two primary focus areas in support of this LOE are:

1.1 Identify, align and integrate existing cyberspace talent within USARCENT staff and subordinate units.

1.2 Program and track the arrival and integration of Career Force 17 (Cyberspace) Officers, Warrant Officers, and Enlisted Soldiers in order to formalize the manning and integration of Cyberspace operations at Echelons Corp and Below (ECB).

Major Objective 1.1: *Identify, Develop and Retain the Cyberspace Workforce*

To execute the USARCENT mission it is important we have the right skill sets in the right jobs at the right time. To ensure we have the right personnel we must first look internally and identify personnel with experience in the Cyber Mission Force and align them against current or emerging capability gaps. These Soldiers and Civilians need to understand our networks, the TTPs of our adversaries, and be capable of adapting faster than our adversaries. In addition, our cyberspace planners need to coordinate with USARCENT and CFLCC maneuver elements.

Major Objective 1.2: *Educate and Develop the USARCENT Total Force*

Critical to execution and integration of cyberspace operations is the need to educate the force on Joint and Army policy on Cyberspace operations. Courses such as the Army Cyberspace Operations Planners Course, Cyberspace Operations Planners Seminar, Joint Cyberspace Analysis Course (JCAC), Joint Network Attack Course (JNAC), and Cyberspace 300/400 are important to establishing cyberspace proficiency. MTTs should be programmed to ensure that USARCENT staff is trained to meet this objective. Additional conditions to achieve this include home station training designed to meet current force needs in the cyberspace domain and the development and integration of

Cyberspace Objectives into FY17/18 exercises.

> *Computerized traffic, public safety systems and electronic banking will be among the new terrorist targets. It might be that the spectacular attack in the future will lie not in how many people you kill or injure, but in how effectively you can paralyze major urban areas by changing a few ones and zeros, or potentially disrupt the functions of financial systems.*
> ***General Joseph Votel, Commander USCENTCOM–April 2015***

LOE 2: OPERATIONS

To operate effectively in Cyberspace, USARCENT and its subordinate units must integrate and synchronize Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO) and Department of Defense Information Networks (DoDIN) Operations with our partners across the USCENTCOM AOR. To achieve this goal, USARCENT supports the Army through the coordination and synchronization of all USARCENT cyberspace stakeholders and activities ensuring our formations and networks provide effective support to Joint and Army operations. USARCENT works to achieve the following four major objectives to reach this end state.

2.1 Conduct Cyberspace Operations

2.2 Identify USARCENT Cyberspace Capabilities and Capability gaps

2.3 Provide operational perspectives to enhance Doctrine and Policy

2.4 Ensure Operational readiness of Warfighting platforms, Communications networks, Platform Information Technology (PIT), Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems

Major Objective 2.1: *Conduct Cyberspace Operations*

The USARCENT conducts cyberspace operations to (1) secure Department of Defense terrain in the cyberspace domain, (2) defend against and remove threats from friendly cyber terrain and, as authorized, (3) support combatant commands to achieve effects in support of their operations. USARCENT coordinates with HQDA resourcing forums and organizations to ensure that USARCENT can operate across the three mission sets of cyber operations.

Major Objective 2.2: *Identify USARCENT Cyberspace Capabilities and Capability Gaps*

In order for USARCENT to conduct Cyberspace Operations it is important that we provide tools and capabilities which enable our cyberspace workforce to combat current and emerging cyberspace threats. To accurately identify and align these capabilities, the USARCENT staff must coordinate with ARCYBER and the Cyber Center of Excellence to leverage the intellectual knowledge and resources of these organizations to identify capability gaps in current USARCENT tools, resources and skill sets. Once identified, the

USARCENT staff must program and align funding to resource these identified gaps.

Major Objective 2.3: *Provide Operational Perspectives to Enhance Doctrine and Policy*

The US Army develops and updates doctrine and policy to enable effective Cyberspace operations to include enhancing cybersecurity. In FEB 2016, CG USARCENT directed the standup of a USARCENT Cyberspace Operational Planning Team (OPT) to develop a cyberspace strategy and conduct a review of OCO, DCO, and DoDIN impacts at the ASCC level. (USARCENT FRAGO 021830ZFEB16). Once complete the review will be forwarded to CG ARCYBER, HQDA G-3/5/7 (TR, OD), CG TRADOC and CG Cyber Center of Excellence (CoE) for integration into Army wide findings on Cyberspace integration.

Major Objective 2.4: *Ensure Operational Readiness of Warfighting Platforms, Communications Networks, Platform Information Technology (PIT), Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems*

In support of the Army Resiliency Plan – *"Cyber Strong"*, USARCENT aligns manpower, resources and command focus to ensure combat readiness and mission assurance of weapon systems, warfighting and industrial platforms. In addition, coordinate with USCENTCOM JCC, HQDA and ARCYBER for SME support as directed in HQDA Army Cyber Resiliency Plan EXORD. Source document – *HQDA EXORD 168-16, 141733ZAPR16.*

> *Our cyberspace capabilities should be brought to a level where they are as trained and ready as any carrier strike group, squadron, marine air-ground task force, brigade combat team, or regional combat team. Our cyber teams require platforms, tools, training and infrastructure, just like maneuver elements in all other domains.*
> *Army Cyber and Second Army Campaign Plan 2015-01 Rev 1*

LOE 3: Capability Development

This LOE provides an opportunity for USARC ENT staff to identify and communicate Cyberspace materiel and capability development requirements within a forum of Army capability development SMEs. Historically, commanders have identified that the traditional cyberspace capability development process is too cumbersome to respond to present or emerging cyberspace warfighter requirements. At the direction of CSA38, the US Army Cyberspace Acquisition, Requirements and Resourcing (CARR) Working Group was developed in 2015 to address these needs. The CARR provides a proactive governance and management construct to rapidly develop Cyberspace capabilities with agility, flexibility, and accountability. The FY17 CARR Acquisition strategy includes the following priorities:

- Cyberspace Analytics
- DCO Infrastructure
- Cyberspace Mission Command and Platform/ Battle Command Suite
- Persistent Training Environment and Cyber Training Ranges
- CPT Deployable Kits and Tool Suites

- Forensic Malware
- Cyber Situational Analysis

USARCENT Staff must align capability development requirements with the CARR Annual Plan IOT accelerate USARCENT resourcing requirements. The two focus areas in support of this LOE are as follows:

3.1 Identify and Amplify USARCENT Capability Development Requirements

3.2 Update USARCENT Cybersecurity Technology and Systems

Major Objective 3.1: *Identify and Amplify USARCENT Capability Development Requirements*

To ensure that USARCENT does not create a "hollow" cyberspace workforce, the staff needs to review, identify, acquire and integrate systems, tools and requirements which enable "Freedom of Movement" within Cyberspace for USARCENT and our partners. These capabilities need to minimize friendly vulnerabilities while simultaneously exploiting those of our adversaries and provide attribution to adversary cyberspace effects. The following are essential components for successful completion of this major objective:

a) Understanding the HQDA Cyberspace Capability Development process

b) Understanding the technological challenges of future warfighting and

c) Programming the required resources which enable survivability and mission success in cyberspace degraded environments.

The USARCENT G-2, G-3 and G-6 must take the lead across the staff to enable transformation of our existing systems and provide the tools and capabilities which ensure mission success.

Major Objective 3.2: *Update USARCENT Cybersecurity Technology and Systems*

The rapid pace of innovation in information technology continues to increase the reach and tempo of our operations, simultaneously these technological innovation also provide opportunities for our adversaries to negatively impact our operations. Adding to this complexity is the requirement that we operate as part of a Joint, Inter-organizational and Multinational force reliant on a network which provides assured interoperability. To maintain our technological advantage our system must remain secure and resilient. Operational tenets which drive the Network 2025 design must be integrated into our network design today. As a result USARCENT Networks must provide the following capabilities:

- *Fight on Arrival Capability*
- *Support to Distributed Operations*
- *Ensure Operational readiness with a reduced force size*
- *Provide Mission Partner Interoperability*

- *Maintain IT overmatch*
- *Provide Situational Awareness*

LOE 4: Facilities Systems and Infrastructure

As the USARCENT Staff advises the Command on facilities, systems and infrastructure in need of development or upgrade, the staff must remain aware of the need for cyberspace resiliency and utility in warfighting. Informed decisions must be made to ensure that USARCENT initiatives such as the Combined Land Operations Center (CLOC), expanded SCIF facilities, Cyber Ranges, Logistical Hubs (APODs, SPODs), and others are designed to be resilient in cyberspace degraded environments. The investment in our facilities, systems, and infrastructure of today will enable our training and warfighting efforts over the next 20-30 years. As a result, USARCENT integrates cyberspace resiliency as a prime planning consideration as USARCENT invests in warfighting facilities and capabilities. Doing so ensures that we are judicious stewards of our nations dollars and ensures that our forces maintain freedom of movement in cyberspace degraded environments. USARCENT must also engage with HQDA and IMCOM to expand the aperture of the IMCOM led Quarterly Cyberspace Installation Summits beyond CONUS based Army facilities. This forum guides and informs DoD Cyberspace investments on Army installations and needs to ensure that USARCENT's CONUS based non-Army locations and USARCENT's OCONUS facilities are included in their decision making. In addition, as the Army begins to integrate cyberspace planners into operational and tactical units, the USARCENT staff needs to ensure that facilities are designed to ensure smooth integration of these warfighters and their requirements. The two focus areas in support of this LOE are as follows:

4.1 Ensure Readiness and Reliability of SCADA systems throughout the USARCENT AOR

4.2 Review and Develop Cyberspace Training Facilities for Partner Nation Training and Interoperability

Major Objective 4.1: *Ensure Readiness and Reliability of SCADA systems throughout USARCENT AOR*

The threat of SCADA networks places the health and welfare of USARCENT Soldiers and the USARCENT mission at risk. Without reliable power, communications, heating/cooling sources the ability of USARCENT to execute our wartime mission becomes slowed and unreliable. As a result, USARCENT includes verbiage into contracts which impact our SCADA systems which ensures that the systems have scheduled, periodic reviews for cyberspace vulnerabilities. These reviews need to be conducted on a no less than annual cycle, with identified vulnerabilities mitigated within 30 days of announcement or discovery. USARCENT commanders must empower their staff to meet these timelines and address these vulnerabilities. These efforts ensure that USARCENT supports and implements the HQDA led "policy to implementation" approach to cybersecurity of our warfighting and industrial platforms.

Major Objective 4.2: *Review and Develop Cyberspace Training Facilities for Partner Nation Training and Interoperability*

To demonstrate our commitment to cyberspace security and cyberspace interoperability with our regional partners, the USARCENT staff must review, identify, and program funding and manpower to develop a cyberspace training facility at Camp Buehring. This facility will support the integration and training of our regional cyberspace planners and also serve to highlight the impact of cyberspace vulnerabilities to military C2, financial and energy sectors. Concurrently, the USARCENT staff will review the need for development of a cyberspace training facility in theater for US use. This facility must be connected to the National Cyber Range and leverage capabilities of the DoD Persistent Training Environment to maximize on the benefit of virtual capabilities to increase staff awareness and facilitate the integration of cyberspace operations.

The nation's cybersecurity requires a collaborative approach with a range of interagency and industry partners contributing authorities, capabilities, and insights to protect US infrastructure and information, deter attacks, and deter adversaries in cyberspace. By working together we improve our collective knowledge about what is happening across the cyberspace domain and protect our networks.

USCYBERCOM Commanders Intent- Powered through Partnership

LOE 5: Partnerships

The value of partnerships and establishing allies is essential to the success of warfighting and is an essential component to the USARCENT mission and Theater Security Cooperation in the USARCENT AOR. However, challenges remain which are unique to cyberspace operations and hinder the development of strong cyberspace partnerships. The USARCENT staff must identify ways to overcome these challenges. Several of which are as follows: fear of exposing capabilities with Middle East Stabilization Force (MESF) partners, deconfliction of Cyberspace topics with OSD (Policy) and the USCENTCOM Joint Cyberspace Center (JCC), over classification of information, lack of awareness of our regional partners Cyberspace capabilities, concern of two way information sharing with commercial entities, and regional commercial partners fear of association with DoD elements. USARCENT staff must develop creative and innovative strategies to leverage and enhance cyberspace partnerships within our AOR, doing so enhances incident response actions, bolsters hardening of our collective networks, and aligns capabilities against a common cyberspace threat. The two focus areas in support of this LOE are as follows:

5.1 Partner across DoD, Commercial and Regional Cyberspace Planners

5.2 Increase Cyberspace Interoperability with Partner nations and DoD Joint Cyberspace Planners

Major Objective 5.1: *Partner across DOD, Commercial and Regional Cyberspace Planners*

USARCENT has been a long term proven partner with our allies in the Middle East. However, we have not leveraged resources to engage our regional partners on cyberspace operations. To fully operationalize cyberspace at the ASCC level, USARCENT needs to integrate cyberspace operations into plans, exercises, and bi- lateral / multi-lateral engagements. Initiatives such as the Regional Land Power Network, Land Force Symposiums, and Leader Development Conferences need to serve as a forum to bring USARCENT and our regional partners to the table to discuss current and emerging cyberspace capabilities and how best to integrate these capabilities to support Regional Security Objectives.

Major Objective 5.2: *Increase Cyberspace Interoperability with Partner Nations and DoD Joint Cyberspace Planners*

To enhance and sustain Theater Security with our regional partners, the USARCENT staff must develop and integrate Cyberspace Objectives into future plans and exercise, beginning with FY17. These objectives must address the need for interoperability and provide a candid assessment of our capability to interoperate with our regional partners and Joint cyberspace planners. To effectively execute this MO, USARCENT staff (G-2, G-3, and G-6) must engage and nest with the USCENTCOM JCC to program and align skillsets and resources to engage our regional cyberspace partners during multilateral and bilateral exercises.

REFERENCES

The DoD Cyber Strategy, U.S. Department of Defense, April 2015.
Army Cyberspace Strategy for Unified Land Operations 2025, HQDA G-3/5/7, January 2016.
Army Network Campaign Plan 2020 and Beyond, Implementation Guidance, Near Term 2015- 2016, Army CIO G-6, 6 February 2015.
FM 3-12 "Cyberspace Operations", U.S. Army Training and Doctrine Command. *FM 3-38 "Cyber Electromagnetic Activities*, Headquarters Department of the Army, February 2014.
Shaping the Army Network: 2025-2040, CIO G-6, March 2016
Army Campaign Plan FY 2014, FRAGO 1
Army Cyberspace Command (ARCYBER) Campaign Plan, 2015-01, Rev 1 United States Army Central Command (USARCENT) Campaign Plan 2016
United States Army Central Command (USARCENT) Theater Campaign Support Plan 16-01 (2017-2022)
Cyberspace Acquisition Requirements and Resourcing (CARR) Annual Plan FY 2016 The Army Cyberspace Resiliency Plan December 2015