On Paradigm Shift in Telecommunication Technologies: a Review of Pentagon's Approach

Manfred Sneps-Sneppe, Dmitry Namiot

Abstract -**The article is devoted to the discussion of the telecommunications development strategy. Communication specialists all around the world are facing the problem: shifting from circuit switching (CS) to packet switching (PS). The same problem is the main challenge for the U.S. Department of Defense. We discuss the Defense Information System Network move from circuits to packets, namely, "Joint Vision 2010" - the implementation of signaling protocol #7 and Advanced Intelligent Network, and "Joint Vision 2020" - the network transformation by the transition to Assured Services Session Initiation Protocol and Multifunctional SoftSwiches. We compare routers and switches and provide an example to illustrate the difficulties that complicate the transition from CS to PS and how to make this transition by hybrid CS+PS solutions. We describe some packet switching shortcomings during the implementation of Joint Vision 2020, namely, Joint Information Environment as a beautiful but unattainable dream, the failed GSM-O contract, and Joint regional security stacks failures. The Defense Department's newly released cloud strategy positions the general-purpose Joint Enterprise Defense Infrastructure (JEDI) cloud initiative as the foundation. The strategy emphasizes a cloud hierarchy at DoD, but JEDI cloud strategy leaves a series of unanswered questions relating to the interoperability of clouds that could spell disaster in the future. The JEDI cloud strategy has based on Artificial Intelligence Initiative. We conclude that the long-time channel-packet coexistence seems inevitable, especially in the face of growing cyber threats.**

Keywords: **circuit switching, packet switching, Joint Vision 2010, Advanced Intelligent Network, SS7, DISN, DRSN, hybrid packet-circuit solution, Artificial Intelligence.**

ABBREVIATIONS

AI - Artificial Intelligence
AIN - Advanced Intelligent Network
AS-SIP - Assured Services Session Initiation Protocol
ATM - Asynchronous Transfer Mode
CAS - Channel Associated Signaling
COE - Common Operating Environment
DISA - Defense Information Systems Agency
DISN - Defense Information Systems Network
DOD - Department of Defense
DODIN - Department of Defense Information Network
DRSN - Defense Red Switched Network
DSN - Defense Switched Network
DVS - video conferencing network (DISN VIDEO).
GAO - Government Accounting Office
GIG - Global Information Grid
ISDN - Integrated Services Digital Network
JEDI - Joint Enterprise Defense Infrastructure
JIE - Joint Information Environment
JRSS - Joint Regional Security Stack
MFS - MultiFunctional Switch
MFSS - Multifunctional SoftSwich
MLPP - Multi-Level Precedence and Preemption
MPLS - Multiprotocol Label Switching
NFV - Network Function Virtualization
NIPRNet - Non-classified Internet Protocol Router Network
PSTN - Publish Switch Telephone Network
RFC - Request for Comments
SS7 - signaling protocol #7
SIP - Session Initiation Protocol
SIPRNet - Secret Internet Protocol Router Network
SDN - Software Defined Network
UC - Unified Capabilities
TDM - time division multiplexing.

I. INTRODUCTION

This paper is an extension of work "The curse of software: Pentagon telecommunications case" that is published in the 2019 International Symposium on Systems Engineering (ISSE) proceedings [1]. It is devoted to the discussion of the telecommunications development strategy exampled by Pentagon's solutions in the area of information systems shifting from circuit switching (CS) to packet switching (PS). We point out several shortcomings due to a lack of software resources. Communication specialists are facing the same problem all around the world.

1.1. On U.S. Department of Defense obsolete networks: the AT&T view

"The DoD today still has analog, fixed, premises-based, time-division multiplexing (TDM) and even asynchronous transfer mode (ATM) infrastructure,"- is the AT&T view [2]. Really, the DoD has one aging network based on point-to-point circuits that require constant hardware maintenance and upgrades with difficulties be carried on in the IP era. The existing TDM environment is 30 years behind current commercial technologies, even the DoD's recent technologies - MPLS and JRSS - are already falling behind state of the art [3].

How to modernize the huge DoD's network? It involves more than 15,000 classified and unclassified networks, connecting more than seven million computers and IT devices, 10,000+ operational systems: 20% mission-critical,

The article received 20 Sep 2020.

Manfred Sneps-Sneppe - Ventspils University of Applied Sciences (email: manfreds.sneps@gmail.com)
Dmitry Namiot - Lomonosov Moscow State University (email:dnamiot@gmail.com).

67,000 servers in more than 770 data centers, and support to more than 6,000 locations, 600,000 buildings, and structures in 146 countries with a 170,000-person IT workforce (Figure 1).

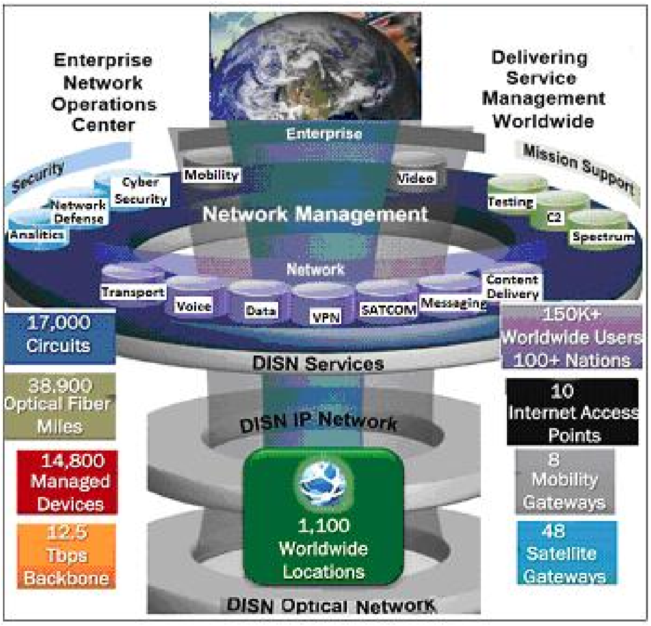


Fig. 1. DISN: $24 Billion Network Infrastructure [4]

In the case of large enterprises such as DoD, technology refresh periods are driven by operational cycles measured in five to ten year intervals. According to the AT&T view [2], the migrating to an NFV architecture is preferable. Such a network is built on the three pillars of SDN, NFV, and orchestration (Figure 2). AT&T refers to the orchestration component as Enhanced Configuration Orchestration Management and Policy (ECOMP). That is the AT&T point [2]. AT&T insists on a fully software-based DoD's network, but could it be implemented?

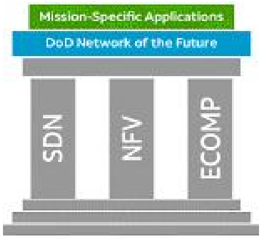


Fig. 2. Potential Foundation of DoD Network of the Future [2]

A. *Cyber threats: what GAO found*

Cyber threats are another hard obstacle in a move to the IP world. In October of 2018, the Government Accounting Office (GAO) has reported [5], the United States weapons systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities. Today DOD weapon systems are more software dependent than ever before (Figure 3). From ships to aircraft, weapons are becoming more advanced technologically and use more software and less hardware to control everything. For example, the F-35 Lighting II software (aircraft) contains eight million lines of code and controls everything from flight controls to radar functionality, communications, and weapons deployment [4].

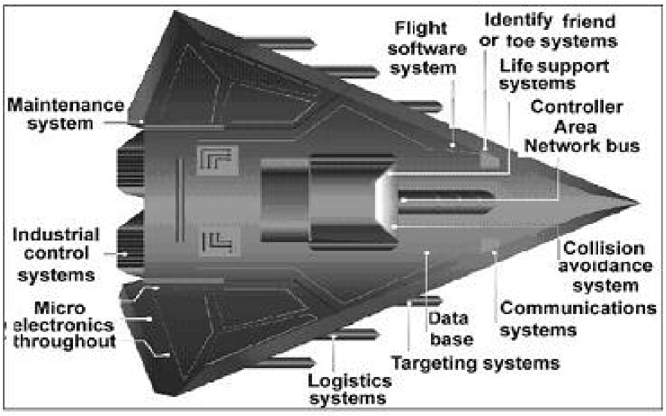

Flight software system
Identify friend or foe systems
Life support systems
Controller Area Network bus
Maintenance system
Industrial control systems
Micro electronics throughout
Collision avoidance system
Communications systems
Data base
Targeting systems
Logistics systems

Fig. 3. Embedded software and information technology systems in weapon systems (represented via fictitious weapon system for classification reasons) [5]

The USS Zumwalk (the latest US Navy ship) is powered by Linux and IBM blade servers running Red Hat Linux with six million lines of software code. It contains sixteen Raytheon built self-contained, mini data centers (the shipboard Internet) connecting all of the ship's systems (internal and external communications, weapons, sensors, etc.) over Internet protocols. The ship even has a classified wireless network that allows sailors to connect to the network and perform maintenance [5].

The situation with cyber threats remains critical. A January 2019 Department of Defense Inspector General report, summarizing state of the art, says Department components, including the services, collectively have 266 cyber vulnerabilities, mostly related to their ability to even identify potential threats [6].

The rest of the paper is as follows. Sections 3 and 4 are about DoD's strategies "Joint Vision 2010" and "Joint Vision 2020", respectively. In Section 5, we consider Army Unified Capabilities. A comparison of circuit switching versus packet switching has carried on in Section 6. Sections 7 and 8 are devoted to military software complexity considering Common Operating Environment and Single Security Architecture. In Sections 9 and 10, the up-to-date JEDI Cloud Strategy and Artificial Intelligence Initiative have given in short. In concluding Section 11, we point out a rather unsuccessful US Army Regulator fights for IP technology exampled by Defense Red Switch Network using 40 years old ISDN technology.

II. Joint Vision 2010: General Shalikashvili and Bell Labs Heritage

A. *On the initial Shalikashvili's doctrine*

The Defense Information Systems Network (DISN) is a global network. Its purpose is to provide services for the transfer of various types of information (speech, data, video, multimedia) for the effective and secure control of troops, communications, reconnaissance, and electronic warfare.

The DoD Doctrine [7] issued by General J. Shalikashvili[1]

[1] John Shalikashvili (1936 – 2011) is a man of extremely amazing fate. He served in every level of unit command from platoon to division. Served

in 1995 is the keystone document for Command, Control, Communications, and Computer (C4) systems up to now. “The development of DISN will be an evolutionary process that will support the military’s move into the 21st-century information age, and will replace the individual legacy communications systems with a seamless transport,” – has ordered General Shalikashvili at the beginning of his service as the Chairman of the Joint Chiefs of Staff.

In those years, the DISN architecture was ATM oriented (Figure 4). Recall in a few words about what is ATM - for young generation readers. Using ATM, information has segmented into fixed-length cells [6]. The ATM cell has a fixed length of 53 bytes. A cell is make up of a 'header' and a 'payload.' The payload (48 bytes) carries the information to be transmitted (voice, data, video) and the header (5 bytes) is for the addressing mechanism. ATM is a switched based technology with some packet switching features. ATM was invented in the early 1980's - a result of research carried on by AT&T and French Telecompany. ATM had standardized by ITU in 1988. ATM along with synchronous digital hierarchy (SDH) transport, in its own time, has was meant to form the basis of the public broadband ISDN (B-ISDN). The ATM era did not take place.

It is worthy to note. As mentioned above by AT&T, two highly important classified military networks have built on ATM switches: (1) JWICS (Joint Worldwide Intelligence Communications System), and (2) AFSCN (Air Force Satellite Control Network).

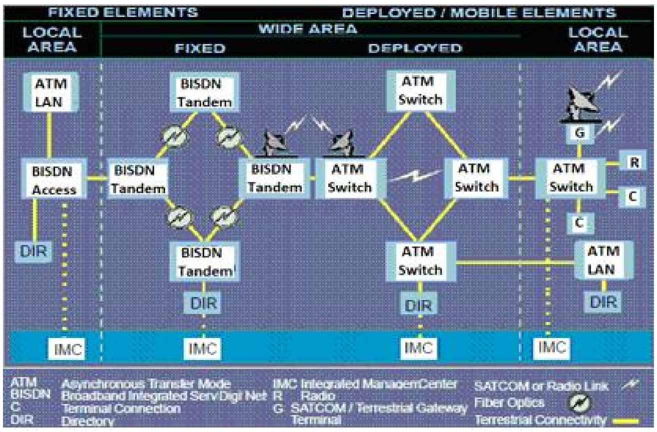


Fig. 4. Key Elements of the DISN Architecture (1995) [8]

"Joint Vision 2010" doctrine met strong criticism from the US GAO side just in 1998 [9]. The GAO pointed out the following:

“Although Defense has been implementing the DISN program for 7 years, numerous networks continue to exist without DISA’s knowledge. Our own survey found that the military services are operating at least 87 independent networks that support a variety of long-haul telecommunications requirements. DISA initiated a similar data call to the military services and Defense agencies after GAO survey and identified 153 networks planned or operating throughout Defense.”

As it follows from DoD Response [9], dated May 5, 1997, the DISA experts attempted to save ATM solution. Nevertheless, two months later GAO [10] once more noted:

“C4ISR[2] architecture is critical to achieving information superiority. Creating the C4ISR Architecture in itself is not enough to build the Defense Information Infrastructure and its attendant systems. Past architecture efforts are not successful.”

DOD has had an official requirement for C4ISR interoperability and for a Department-wide architecture since 1967 when it encountered communications interoperability problems during the Vietnam War: “However, it has never adequately met that requirement, even though it experienced similar problems during military operations in Grenada, Panama, and the Persian Gulf. In 1987/12 and again in 1993/13 we reported that DOD had made little progress in meeting the requirement because it lacked centralized or joint managerial and funding control over individual service priorities, which often took precedence over interoperability priorities. We also reported that all of DOD's component commands, services, and agencies had been unable to agree on what such an architecture should accomplish or what it should consist of.”

B. *The fateful DISA decision*

In reality, at that time many shortcomings of military information networks had revealed. Firstly, this was the low level of integration of many hundreds of networks included in DISN, which significantly limits interaction within a single network and reduces effective unified management of all its resources. Under conditions of technological uncertainty and the requirements from General J. Shalikashvili side, DISA (Defense Information Systems Agency) has made a principled decision to build US military communications networks using the "open architecture" and commercial-off-the-shelf (COTS) products. As a result, the choice fell on the developments of Bell Labs, namely, on the telephone signaling protocol SS7 and the Advanced Intelligent Network (AIN). These products were rather ‘old’ for that time: SS7 protocols had developed at Bell Labs since 1975 and defined as ITU standards in 1981. Note that the very Bell System had dismembered in 1983. Honestly speaking, SS7 has been a huge success in the telecommunication industry and has deployed in all public telephone circuit switched networks by all carriers throughout the world. The key features of SS7 have found their way into other systems such as Global System for Mobile Communication (GSM), military communication, and even satellite signaling

The details regarding the transition to SS7 and AIN we found in a paper from Lockheed Martin Missiles & Space [11] – the well-known Defense contractor. At that time, military communication systems have started to merge traditional circuit-switched voice with Internet and Asynchronous Transfer Mode (ATM) as the backbone

as a United States Army Supreme Allied Commander Europe from 1992 to 1993. Shalikashvili was the first foreign-born man to become Chairman of the Joint Chiefs of Staff (from 1993 to 1997). He was born in Warsaw, Poland, in the family of émigré Georgian officer Dimitri Shalikashvili and his Russian origin wife Countess Maria Rüdiger-Belyaeva.

[2] C4ISR stands for C4 (Command, Control, Computers, Communications), Intelligence, Surveillance, and Reconnaissance.

networks. A critical role of SS7 issue is the interface for voice circuits with ATM.

Let us point out the key features of SS7 and AIN.

SS7 is an architecture for performing out-of-band signaling in support of the call establishment, routing, and information exchange functions of the Publish Switch Telephone Network (PSTN). It identifies functions be performed by a signaling system network and a protocol to enable their performance.

In its own order, the Advanced Intelligent Network (AIN) had originally designed as a critical tool to offer sophisticated services such as expert operator assistance and directory assistance. The functional structure of the SS7 makes it possible to create the AIN by putting together functional parts (Figure 5): Central Office (CO), Switching Point (SP), Signaling Transfer Point (STP), Service Control Point (SCP), and Service Switching Point (SSP).

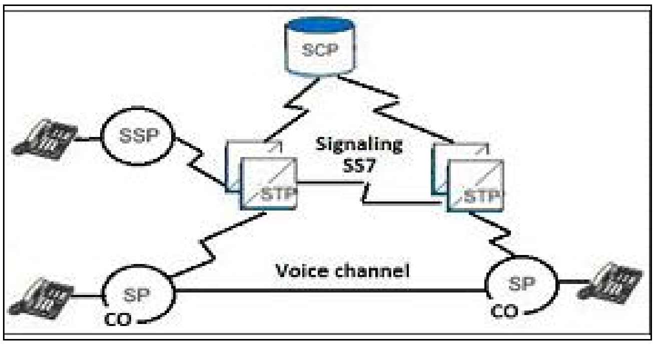


Fig. 5. Intelligent Network basics

Figure 6 describes the AIN components that operate in the worldwide telecommunication network, as well as how they are deployed in SS7 backbone, the space Wide Area Network (WAN), circuit switched voice network and the packet switched terrestrial WAN. The AIN components besides named above include the Service Creation Environment (SCE), Service Management System (SMS), Intelligent Peripheral (IP), Adjunct, and the Network Access Point (NAP).

The SCE provides the design and implementation tools needed to assist in creating and customizing services in the SCP. The SMS is a database management system used to manage the master database that controls the AIN warfighter services. These services include ongoing database maintenance, backup and recovery, log management, and audit trails. The Intelligent Peripheral (IP) services include the following:

- Tone generation
- Voice recognition
- Audio and data playback
- Voice or data compression
- Call control
- Recording
- DTMF tone detection and collection
- Many other tactical or strategic services such as personnel identifications

The Adjunct provides the same operation as the SCP, but has configured for one or fewer services for a single switch. The Network Access Point (NAP) is a switch that has no AIN functions. It has connected off a SSP and interfaces to trunks with SS7 messages. It will route the call to its attached SSP or AIN services based on the called and calling number received.

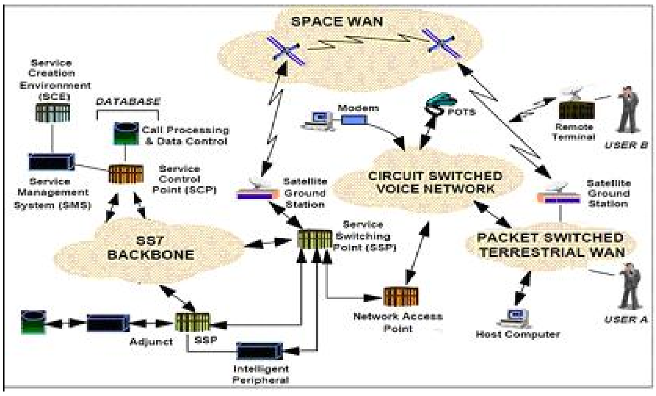


Fig. 6. Advanced Intelligent Network Military Service Architecture [11]

To illustrate the current DISN architecture (Figure 7) we refer to the certification of Avaya PBX by DISA Joint Interoperability Test Command in 2012 [12]. The SS7 network is some kind of the nervous system of DISN up to resent time connecting the channel mode MFS (Multi-Functional Switches). That is, within the DISN network, the connections have established by means of SS7 signaling. All new terminal equipment that appears is largely of IP type; nevertheless, SS7 network retains its central place. From this, we make an important conclusion: the presence of the SS7 network does not interfere the transition to IP protocols, but rather the opposite - it facilitates the transition to packet switching, makes it step by step.

C. *Shortcoming No1*

Lockheed Martin Missiles & Space was responsible for the AIN from the very beginning of the Joint Vision 2010 program [13]. New military equipment and new services are coming continuously that requires the continuous improvement of AIN. How to hire qualified professionals? In the long list of vacancies with Lockheed Martin, the first place took the search for analysts of multifunctional information systems. From the applicants' many skills were required: to develop new services for AIN and to work with equipment from CISCO, Juniper, etc. Even veterans with 28 years of experience were invited. Obviously, young professionals, who grew up in IP world, seem unable to support and develop existing AIN network, they have not knowledge in the area of circuit switching technologies.

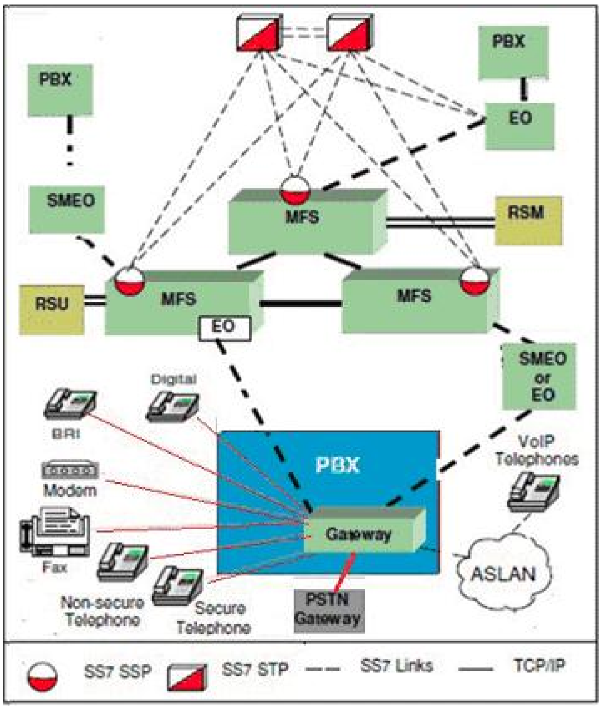


Fig. 7. The simplified DISN view: the current state [12]

III. Joint Vision 2020: All-over-IP

A. *Each warfare object has its own IP address*

Just a few years later as "Joint Vision 2010" had introduced, namely, in 2007 a new Pentagon strategy "Joint Vision 2020" appeared. Pentagon published a fundamental program [14], in which we find the most important point: Global Information Grid (GIG) must be built on basis of IP protocol (Figures 8 and 9). IP protocol should be the only means of communication between the transport layer and applications. It is an extremely hard challenge.

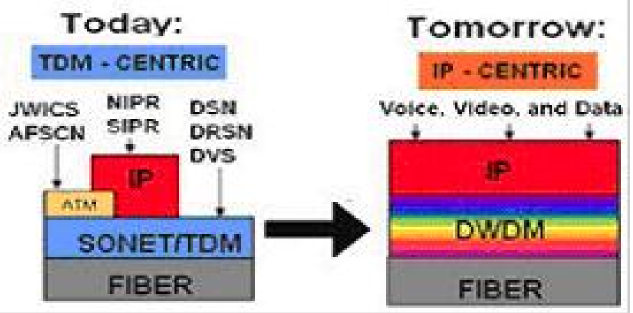


Fig. 8. DISN: from circuit switching to packet switching.

Up to now, the main military communications networks of the Pentagon are circuit-switched networks (Figure 8): (1) DSN - Defense Switched Network; (2) DRSN (Defense Red Switched Network) - for the top-secret government communications; (3) DVS - video conferencing network (DISN VIDEO). In addition, Figure 8 shows two highly important classified military networks mentioned above built on ATM switches: (4) JWICS and (5) AFSCN. There are also two widely known messaging networks: (6) SIPRNet (Secret Internet Protocol Router Network) and (7) NIPRNet (Non-classified Internet Protocol Router Network)[3].

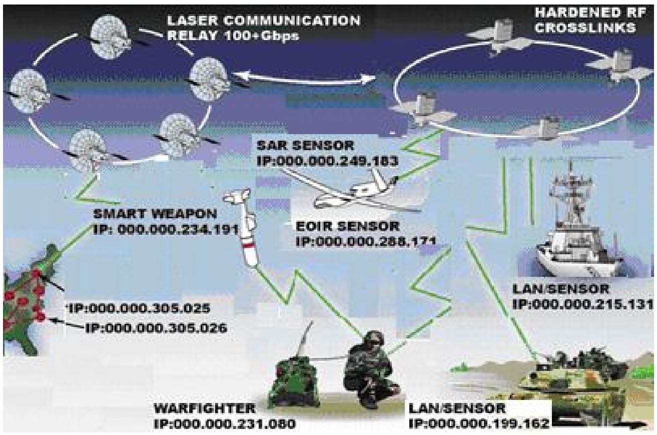


Fig. 9. Joint Vision 2020: Each warfare object has its own IP address.

B. *Multifunctional SoftSwitch*

For the implementation of Joint Vision 2020, the most important step is the replacement of channel switching electronic Multifunctional switches (MFS) by packet switching routers. The transition phase has based on the use of Multifunctional SoftSwiches (MFSS) and new signaling protocol AS-SIP.

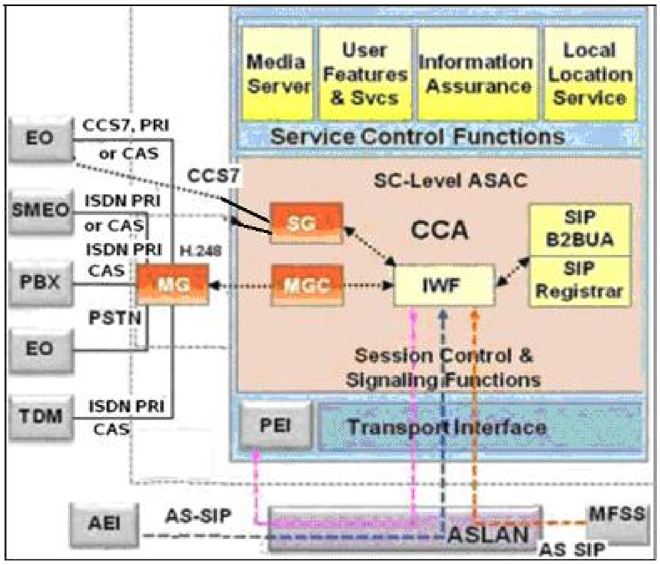


Fig.10. A reference model for Multifunction SoftSwitch: the first phase [15].

At the first phase (Figure 10), MFSS (see the left side) supplies the traditional telephony protocols CCS7, ISDN PRI, and CAS (Channel Associated Signaling) used for connections with the channel switching networks. Thus, MFSS will also needs to provide ISUP-SIP inter-networking function (IWF). A signaling gateway (SG) deals with all signaling protocols such as ISUP, CCS7/SS7, and CAS. MFSS operates also as a media gateway (MG) between TDM circuits switching and IP packet switching under the control of the media gateway controller (MGC) while communications control protocol like H.248 has used between MG and MGC. In the second phase (Figure 11), MFSS is pure packet switch besides DRSN 'island' using

[3] Currently, a new classification of DISN networks had introduced: the NIPRNet network has been renamed to SBU IP Data, SIPRNet to Secret IP Data, the JWICS intelligence network to TS / SCI IP Data and the government DRSN network to Multilevel Secure Voice.

ISDN protocol.

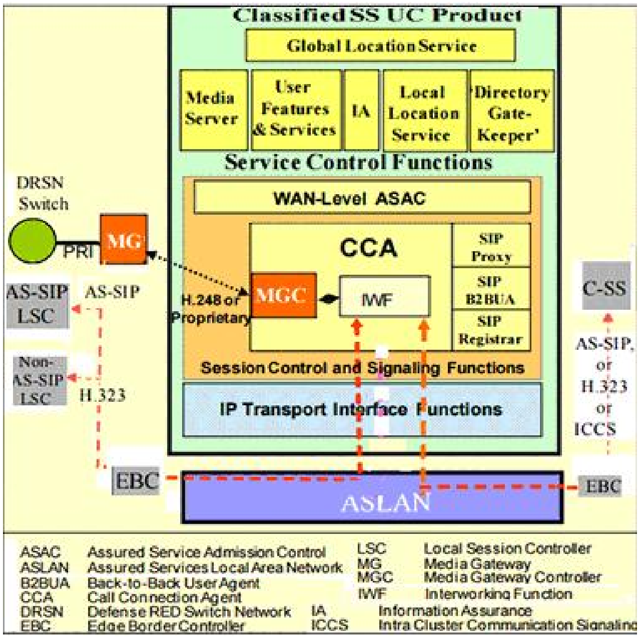

Classified SS UC Product
Global Location Service
Media Server
User Features & Services
IA
Local Location Service
Directory Gate-Keeper'
Service Control Functions
WAN-Level ASAC
CCA
MGC
IWF
SIP Proxy
SIP B2BUA
SIP Registrar
H.248 or Proprietary
Session Control and Signaling Functions
IP Transport Interface Functions
DRSN Switch
PRI
MG
AS-SIP LSC
AS-SIP
Non-AS-SIP LSC
H.323
C-SS
AS-SIP, or H.323 or ICCS
EBC
ASLAN
EBC
ASAC Assured Service Admission Control
ASLAN Assured Services Local Area Network
B2BUA Back-to-Back User Agent
CCA Call Connection Agent
DRSN Defense RED Switch Network
EBC Edge Border Controller
LSC Local Session Controller
MG Media Gateway
MGC Media Gateway Controller
IWF Interworking Function
IA Information Assurance
ICCS Intra Cluster Communication Signaling

Fig. 11. A reference model for Multifunction SoftSwitch: the second phase [15]

A few words about SIP signaling. The main drawbacks of the SIP protocol used for internet telephony are the difficulties in securing secrecy (under cyber warfare) and servicing priority calls, which is important for military applications as well as for emergency service. Therefore, by order of the Department of Defense, a secure AS-SIP protocol was developed [16]. The AS-SIP protocol turned out to be very cumbersome. If ordinary SIP uses 11 other RFC standards, then AS-SIP uses the services of almost 200 RFC standards.

Note the leading role of the Session Controller as an essential part of MFSS. The Service Control Function (SCF) entity provides a framework for creating service interactions. It provides a seamless transition for creating a new set of composite services. That includes UC-based AS-SIP services, 3rd and 4th generation (3G/4G) as well as traditional wireline and mobile wireless services, Web services, and other services applications into feature-rich advanced new services. The SCF functional entity uses, from one side, only a "single" AS-SIP protocol for communicating with the WAN SS, MFSS, or LSC and, from another, SCF is cooperating with as many as 19 servers and supports plenty of protocols: SOAP, HTTP, LDAP, SQL, RADIUS, etc. (Figure 12).

CISCO - the largest contractor of the Pentagon - has installed 22 softswitches at military bases around the world (Figure 13). There are two types of top-level softswitches: WAN SS = Wide Area Network SoftSwitch, MFSS = MultiFunction SoftSwitch. Starting in 2011, first one MFSS has installed in Stuttgart (Germany). Unfortunately, up to now, there is not open available information about any fully operating MFSS. Besides, there we see also four Global Network Support Centers (GNSC) - two in the US (at Scott Air Base and Hawaii), as well one - in Germany and one – in Bahrain [17].

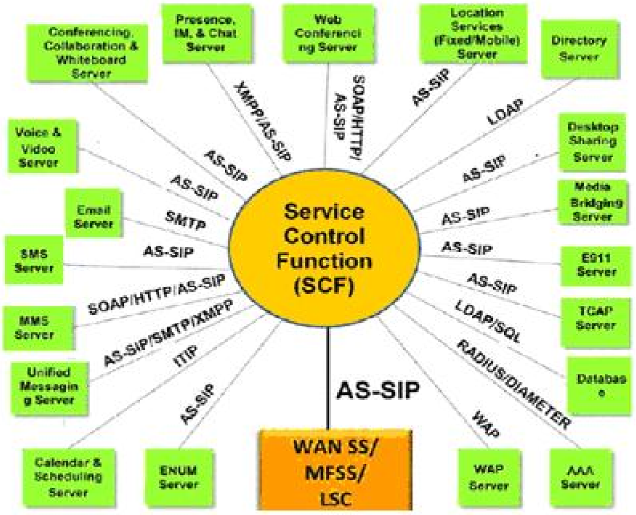


Fig. 12. Operational Concept of Open Protocol Standards used by Service Control Function Entity for Communications with Application Servers and Session Controller [15]

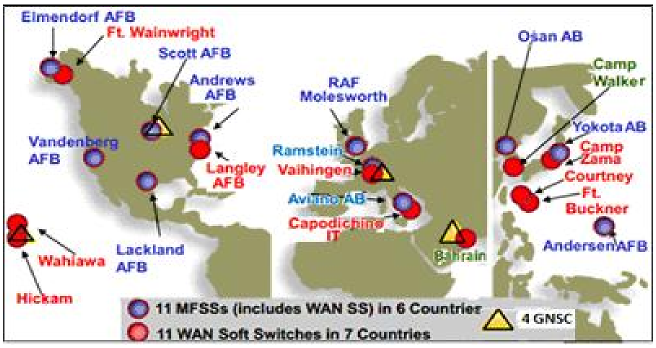


Fig. 13. DISN Joint Vision 2020: 22 SoftSwitches and 4 Global Network Support Centers [17]

C. The target DISN infrastructure

The target DISN infrastructure contains two level switching nodes: Tier0 and Tier1 (Figure 14). Top level Tier0 geographic cluster typically consists of at least three Tier0 SoftSwitches. As the distance between the clustered SoftSwitches must planned so that the return transmission time does not exceed 40 ms and propagation delay equals 6 µs/km thus the distance between Tier0 should not exceed 6,600 km. The classified signaling environment uses a mix of protocols: the existing vendor-based H.323 and AS-SIP signaling. The use of H.323 has allowed during the transition period to all DISN CVVoIP (Classified VoIP and Video). In addition, a unique MG capability exists as part of a Tier0 SS. Classified VVoIP interfaces to the TDM Defense RED Switch Network (DRSN) via a proprietary PRI.

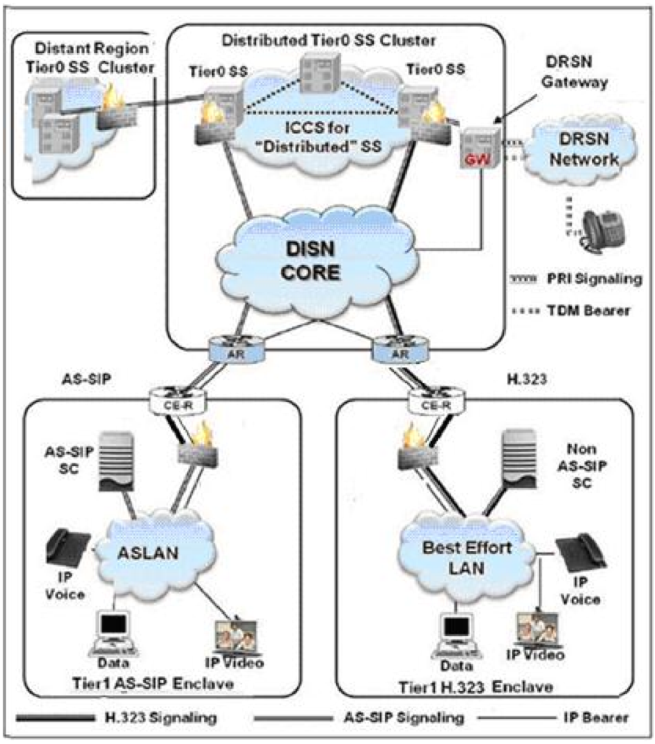


Fig. 14. DISN Classified VoIP and Video Signaling Design [18]

Summing up. It is still difficult to predict the time during which the DISN network will finally switch to the AS-SIP protocol. Obviously, TDM and ISDN equipment could stay for an unpredictable time, especially considering cyber-security threats.

IV. On Army Unified Capabilities

A. *Unified Capabilities*

The aim of "Joint Vision 2020" concept is to implement unified services, so called Unified Capabilities (Figure 15). Army Unified Capabilities (UC) have defined as the integration of voice, video, and/or data services delivered across secure and highly available network infrastructure [19].

The following are the basic Voice Features and Capabilities:

- Call Forwarding (selective, on busy line, etc.)
- Multi-Level Precedence and Preemption (Interactions with call forwarding, No reply at the called station, etc.)
- Precedence Call Waiting (Busy with higher precedence call, busy with Equal precedence call, etc.)
- Call Transfer (at different precedence levels, at same precedence levels)
- Call Hold and Three-Way Calling.

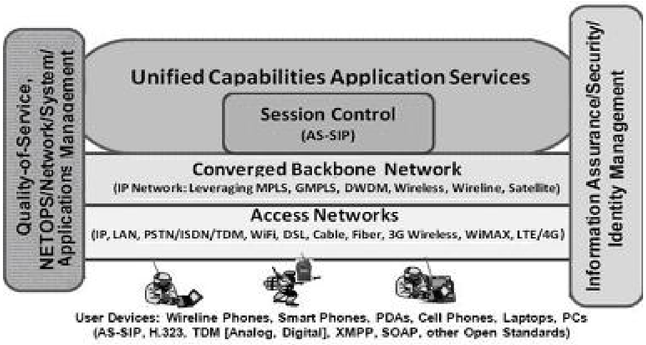
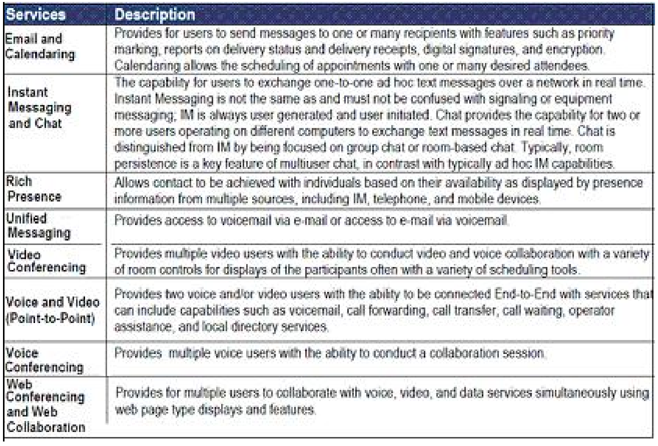

Quality-of-Service,
NETOPS/Network/System/
Applications Management
Unified Capabilities Application Services
Session Control
(AS-SIP)
Converged Backbone Network
(IP Network: Leveraging MPLS, GMPLS, DWDM, Wireless, Wireline, Satellite)
Access Networks
(IP, LAN, PSTN/ISDN/TDM, WiFi, DSL, Cable, Fiber, 3G Wireless, WiMAX, LTE/4G)
Information Assurance/Security/
Identity Management
User Devices: Wireline Phones, Smart Phones, PDAs, Cell Phones, Laptops, PCs
(AS-SIP, H.323, TDM [Analog, Digital], XMPP, SOAP, other Open Standards)

Fig. 15. Conceptual View of Army UC Reference architecture

The Unified Capabilities architecture (Figure 15) uses the IP for the wide-area backbone network. All access networks using different access technologies terminate to the IP/MPLS backbone network. The worldwide DISN backbone transport network will consist of both wireline (e.g. fiber) and wireless (e.g. satellite) networks. Access networks may contain many access technologies such as IP, LAN, PSTN/ISDN/TDM, Wi-Fi, DSL, Cable, and Fiber, 3G Wireless, WiMAX, and LTE/4G Wireless. The IP/LAN access technologies will work with the IP/MPLS network seamlessly. However, PSTN/ISDN/TDM needs appropriate gateways to interworking with the IP/MPLS network.

The Unified Capabilities services are covering communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to a single device, wired to wireless, non-real time to real-time, and scheduled to ad hoc. The capabilities have provided through a collection of services. A service has defined as a mechanism to enable access to a set of one or more capabilities' [18]. Services include email and calendaring, instant messaging and chat, unified messaging, video conferencing, voice conferencing, web conferencing (Table 1 and Figure 16).

Table 1: UC Service Descriptions [18].



Services	Description
Email and Calendaring	Provides for users to send messages to one or many recipients with features such as priority marking, reports on delivery status and delivery receipts, digital signatures, and encryption. Calendaring allows the scheduling of appointments with one or many desired attendees.
Instant Messaging and Chat	The capability for users to exchange one-to-one ad hoc text messages over a network in real time. Instant Messaging is not the same as and must not be confused with signaling or equipment messaging; IM is always user generated and user initiated. Chat provides the capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from IM by being focused on group chat or room-based chat. Typically, room persistence is a key feature of multiuser chat, in contrast with typically ad hoc IM capabilities.
Rich Presence	Allows contact to be achieved with individuals based on their availability as displayed by presence information from multiple sources, including IM, telephone, and mobile devices.
Unified Messaging	Provides access to voicemail via e-mail or access to e-mail via voicemail.
Video Conferencing	Provides multiple video users with the ability to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.
Voice and Video (Point-to-Point)	Provides two voice and/or video users with the ability to be connected End-to-End with services that can include capabilities such as voicemail, call forwarding, call transfer, call waiting, operator assistance, and local directory services.
Voice Conferencing	Provides multiple voice users with the ability to conduct a collaboration session.
Web Conferencing and Web Collaboration	Provides for multiple users to collaborate with voice, video, and data services simultaneously using web page type displays and features.

Fig. 16. Rich information services surrounding a soldier: not too much?

B. On priority calls

Let us take an attention to the AS-SIP protocol. The SIP, as a signaling protocol, does not support the ability to break into ongoing calls. It is critical to support Multi-Level Precedence and Preemption calls (e.g. emergency calls). For these reasons, a new protocol - Assured Services SIP protocol has invented. AS-SIP got many features for Unified Capabilities requirements.

The Multilevel Precedence and Preemption (MLPP) service is the key feature of AS-SIP. It allows properly validated users to place priority calls and preempt lower priority phone calls using the priority level that is associated with a call. This capability lets high-ranking personnel reach critical organizations and personnel during network stress situations (e.g., a national emergency or degraded network performance).

RFC 4542 [21] describes six precedence classes, in descending order:

Executive Override (or Flash Override Override): used when declaring the existence of a state of war and cannot be preempted.

Flash Override: used when declaring Defense Condition One or Defense Emergency and other national authorities the President may authorize and cannot preempted in the Defense Switching Network (DSN).

Flash: reserved generally for telephone calls pertaining to command and control of military forces essential to defense and retaliation, conduct of diplomatic negotiations critical to the arresting or limiting of hostilities, continuity of federal government functions essential to national survival, etc.

Immediate: reserved generally for telephone calls pertaining to situations that gravely affect the security of national and allied forces, reconstitution of forces in a post-attack period, etc.

Priority: reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of government operations.

Routine: designation applied to those official government communications that require rapid transmission by telephonic means but do not require preferential handling.

V. Circuit switching versus Packet switching

A. On basics of routers and switches

The challenge for Joint Vision 2020 lies in a confrontation of circuit switching and packet switching. Let us show a difference amongst these two technologies.

Packet switching. In order to understand the technological trends [22], one has to know the functions that packet and circuit switches do. Figure 17 shows the functional blocks of a packet switch, also called a router. When information arrives at the ingress linecard, the framing module extracts the incoming packet from the link-level frame. The packet then has to go through a route lookup to determine its next hop, and the egress port. Right after the lookup, any required operations on the packet fields have performed, such as decrementing the Time-To-Live (TTL) field, updating the packet checksum, and processing any IP options. After these operations, the packet has sent to the egress port using the router interconnect, which has rescheduled every packet time. Several packets destined to the same egress port could arrive at the same time. Thus, any conflicting packets have to be queued in the ingress port, the output port, or both.

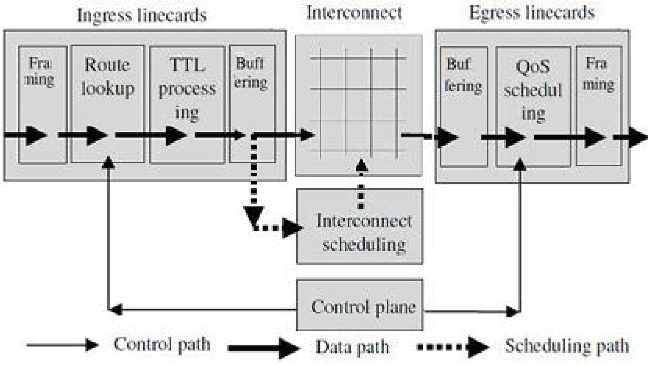


Fig. 17. The functionality of a packet switch [22]

In the output linecard, some routers perform additional scheduling that is used to police or shape traffic, so that quality of service (QoS) guarantees have assured. Finally, the packet has placed in a link frame and sent to the next hop. In addition to the data path, routers have a control path that has used to populate the routing table, to set up the parameters in the QoS scheduler, and to manage the router in general. The signaling of the control channel is in-band, using packets just as in the data channel. The control plane might obtain the signaling information through a special port attached to interconnect.

Circuit switching. The main distinction between a router and a circuit switch is when information may arrive to the switch. In packet switching, packets may come at any time, and so routers resolve any conflicts among the packets by buffering them. In contrast, in circuit switching information belonging to a flow can only arrive in a predetermined channel, which has reserved exclusively for that particular flow. No conflicts or unscheduled arrivals occur, which allows circuit switches to do away with buffering, the online scheduling of interconnect, and most of the data-path processing.

Figure 18 shows the equivalent functions in a circuit switch. As one can see, the data path is much simpler. In contrast, the control plane becomes more complex: it requires new signaling for the management of circuits, a state associated with the circuits, and the off-line scheduling of the arrivals based on the free slots in the interconnect. An important difference between a router and a circuit switch is the time scale in which similar functions need performed. For example, in both types of switches the interconnect needs to be scheduled. A packet switch needs to do it for every packet slot, while a circuit switch only does it when a new call arrives.

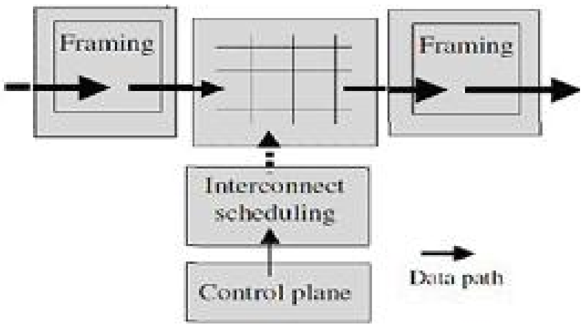


Fig. 18. Functionality of a circuit switch [22]

A comparison of a router and circuit switch. Let us recall an example coming from Stanford University [5]. Compare the switches of equal throughput. It is reasonable to expect that since packet switches do much more work, it would come at the price. Compare two high capacity switches: packet switch Cisco CRS-1 and Ciena TDM switch; the former consumes 7 times the power and costs 10 times more (to multiple cost numbers with $1000 to get absolute values). Note that the throughput in both cases is equal to 10 million telephone calls (64 Kbps x 10 M = 640 Gbps). The software running in a typical transport switch has based on about three million lines of the source code, whereas Cisco's Internet Operating System (IOS) has based on eight million, up to three times more.

Summing up it is worth to note the software for circuit switch is much simpler and cheaper than for packet switch.

B. *Network optimization for unified packet and circuit switched networks*

In unified future network architecture coming from Stanford University [23], backbone routers have replaced with less expensive hybrid optical-circuit/electrical-packet switches that have both circuit switching and packet switching capabilities. These hybrid switches are logically connected in a fully meshed network where each hybrid switch implements an IP node, and where each IP node is logically connected to each and every other IP node via a single direct circuit-switched hop. This unified packet and circuit-switched network then can managed using a single converged control plane. Figure 19 depicts this unified fully meshed IP network architecture. The actual underlying optical transport network can dynamically allocated to provide different circuit capacities. Thus, it implements each logical connection in the full-mesh. For example, a logical connection from San Francisco (SF) to New York (NY) may implemented as an optical circuit-switched path via Seattle and Chicago.

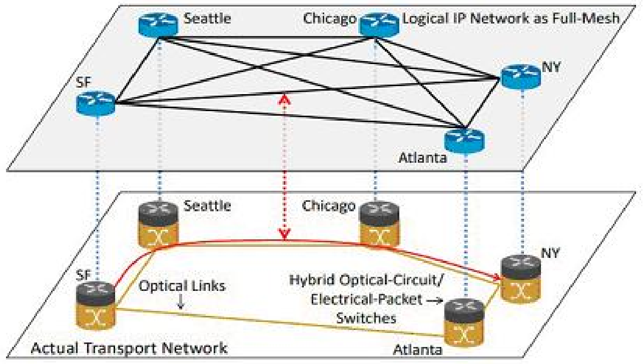


Fig. 19. IP network logically as a full-mesh, with logical connections implemented over an optical circuit-switched transport network and logical routers [23]

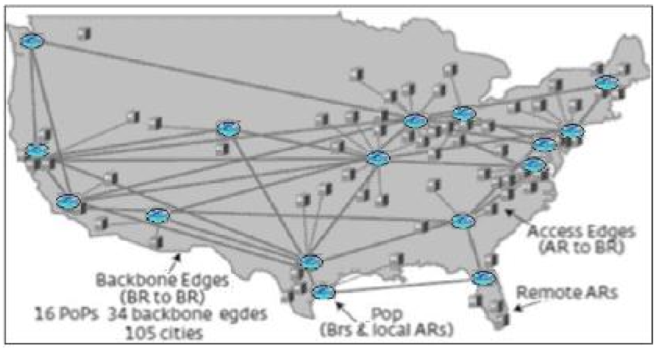

Access Edges (AR to BR)
Backbone Edges (BR to BR)
16 PoPs 34 backbone egdes 105 cities
Remote ARs
Pop (Brs & local ARs)

Fig. 20. AT&T US IP core network: 16 PoPs across the U.S. are aggregating the traffic from 89 other cities [23]

The efficiency of Unified Packet and Circuit Switched Network has proven by data of AT&T US IP core network (Figure 20). Two architectures had compared: (1) traditional All-IP version used MPLS backbone routers (BR) and (2) the hybrid packet and circuit core with hybrid MPLS-OTN (packet optical) switch, replacing BRs in core PoPs with hybrid MPLS-OTN switches (Figure 21). The overall number of core ports have reduced significantly in IP-and-DCS (Dynamic Circuit Switching) when compared to the reference design (from 2564 to 1480). As a result, nearly 60% in overall Capex savings achieved when compared to the reference IP-over-WDM design. Most of these savings come in the backbone switches, which see an 85% reduction in cost. A key problem that must be solved in this unified architecture approach is the allocation of optical circuits between adjacent IP nodes in the logical full-mesh (i.e., between every pair of ingress and egress nodes).

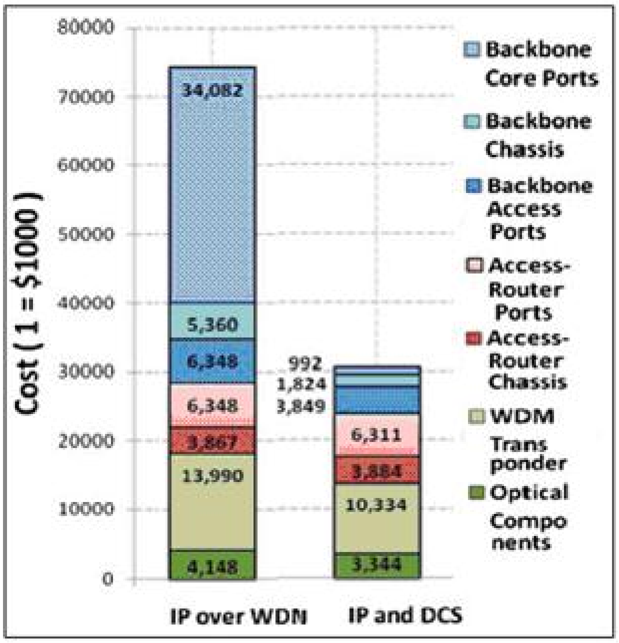


Fig. 21. Capex results for two AT&T US IP core network designs [23]

Summing up. These results have led to the following:

(1) Packet switching will continue to exist at the edge of the network. The packet-switched network should ideally gather traffic from disparate sources, and multiplex it together.

(2) At the core of the network, the circuit switched transport network should remain as a means to interconnect the packet switched routers, and as a means to provide high reliability and performance guarantees.

VI. On military software complexity

A. *Common Operating Environment*

The Common Operating Environment (COE) Architecture is a key component for the planned Army Enterprise Network Architecture [24]. The Computing Environment (CE) is a logical grouping of systems with similar characteristics (deployment, environmental, transport dependencies, form factors, etc.) used to organize the COE. A CE comprises the necessary hardware, operating system, libraries, and software required to run applications within the COE containing as much as 189 primary military systems (Figure 22), namely:

(1) Data Center, DC: consists of 65 primary systems;

(2) Command Post, CP: consists of 26 primary systems;

(3) Mounted, MC: Operating and run-time systems, native and common applications, and services. Consists of 6 primary systems;

(4) Mobile/Hand Held, MHH: consists of 10 primary systems;

(5) Sensors: for specialized, human-controlled, or unattended sensors. Consists of 38 primary systems;

(6) RT/Safety Critical/Embedded, RTSCE: Consists of 44 primary systems.

Coordination of work between these six units requires a very strong, clearly standardized discipline. It is required to meet the requirements for fifteen control points (!) of the common operating environment for 189 (!) interfaces totally.

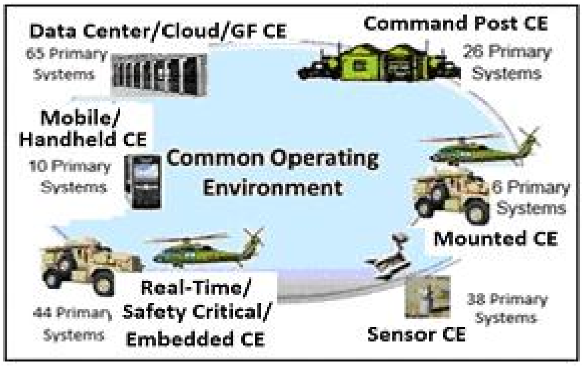


Fig. 22. COE focuses on six CE containing 189 US Army primary military systems [24]

Control Points are the primary COE mechanism to facilitate interoperability. Each of six CEs has interfaces with 5 other CEs, yielding 30 combinations. Each CP captures both directions of the interfaces, thus 15 Control Points (Figure 23). Control Point Specifications should be complete and comprehensive. The Control Point Specification includes sufficient interface details so that implementers can use this document for development and testers can use it for interface test and verification.

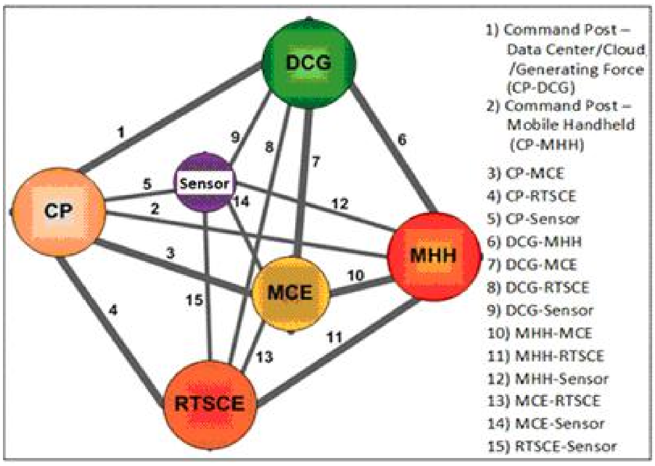


Fig. 23. 15 potential Control Points for COE [24]

The idea of COE per se is attractive one but a giant volume of software be developed arises a reasonable doubt – could the common COE architecture be implemented whenever.

B. *Army Tactical Control Points*

Let us consider a particular case of COE, namely: the current Army approach to information technology implementation and management. Seamless integration must exist across the Army Enterprise Network and between computing environments. Tactical Control points facilitate the integration of mission environments (Figure 24) and serve as intermediaries between mission environments and the corresponding computing environments [25].

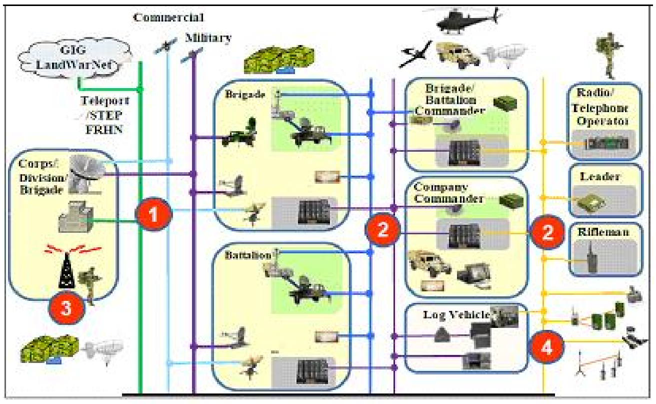


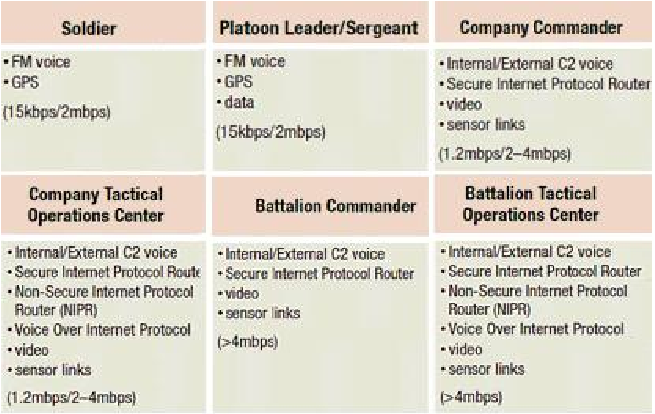
Fig. 24. The Army Tactical Network and Control Points: 1 – Enterprise to TOC/Command Post, 2 – Enterprise/Command Post to Platform/Soldier/Sensor, 3 – Enterprise/Command Post to Soldier, 4 – Platform/Soldier to Sensor [25]

Control points have placed to enforce the following requirements (Figure 25):

(1) Interoperability of Structured Data (e.g., databases, geospatial data, spreadsheets) and Unstructured Data – Data that have no defined data model (e.g., documents, presentations, pictures, audio, video);

(2) Security;

(3) Gateways - to evaluate the request according to its filtering rules (e.g., by IP address or protocol).



Soldier	Platoon Leader/Sergeant	Company Commander
• FM voice • GPS (15kbps/2mbps)	• FM voice • GPS • data (15kbps/2mbps)	• Internal/External C2 voice • Secure Internet Protocol Router • video • sensor links (1.2mbps/2–4mbps)
Company Tactical Operations Center	**Battalion Commander**	**Battalion Tactical Operations Center**
• Internal/External C2 voice • Secure Internet Protocol Route • Non-Secure Internet Protocol Router (NIPR) • Voice Over Internet Protocol • video • sensor links (1.2mbps/2–4mbps)	• Internal/External C2 voice • Secure Internet Protocol Router • video • sensor links (>4mbps)	• Internal/External C2 voice • Secure Internet Protocol Router • Non-Secure Internet Protocol Router (NIPR) • Voice Over Internet Protocol • video • sensor links (>4mbps)

Fig. 25. Army communication capabilities [25]

Consider in more detail Control Point 2 (Enterprise/Command Post to Platform/Soldier/Sensor). This provides the interface to/from the enterprise standard/protocol by the following means.

- Interoperability: authentication via PKI, LDAP or Active Directory; the messaging – VMF; geospatial data standard is VMF/MIL-STD 2525C.
- Security: encryption – NSA/NIST-certified solutions; key management – EKMS/KMI-compliant solutions; end-point protection – Host-Based Security System (HBSS); enterprise service management – Remedy/ITSM, IP Management/SPECTRUM (configured to roll up data at control points); and patch management – manual.
- Gateways: the enterprise/command post server is responsible for the translation of XML/SOAP to/from VMF.

The COE implementation is for a rather long-time period.

C. *Capability Set 13*

Army network modernization is moving through a sequence of capability sets. Capability Set 13 (CS 13) is the package of 2013, which allows utilizing advanced satellite-based systems — by data radios, handheld devices and uses the latest mission command software. CS 13 allows transmitting voice/chat communications and situational awareness data [26]. On patrol vehicles configured with components of CS 13, leaders will be able to exchange information and execute mission command using mobile communications technologies. CS 13 level patrol vehicles can work on move, rather than having to remain in a fixed location to access the network (Figure 26).

Fig. 26. A command Post (version CS-13, 2012) [26]

In 2013, the GAO had supervised Capability Set 13 project and pointed out some negative features [28]:

"The Army's network modernization strategy focuses on addressing four factors that Army leaders believe are at the root of the Army's network challenges: (1) a lack of common technical standards, (2) unsynchronized acquisition timelines, (3) no visibility at the enterprise (top) level, and (4) test and acquisition processes that they believe result in the fielding of outdated technology."

A major component of CS21 (of financial year 2021) is the Integrated Tactical Network (ITN) [20]. The approved ITN components for CS21 include single-channel commercial radios with advanced networking waveforms, high capacity line-of-sight radios, voice and data gateways, tactical cross domain solutions, small aperture satellite terminals, expeditionary servers, variable height antennas (via a quadcopter drone), etc. Thus, CS21 contains a series of tactical improvements according to the current technological achievements.

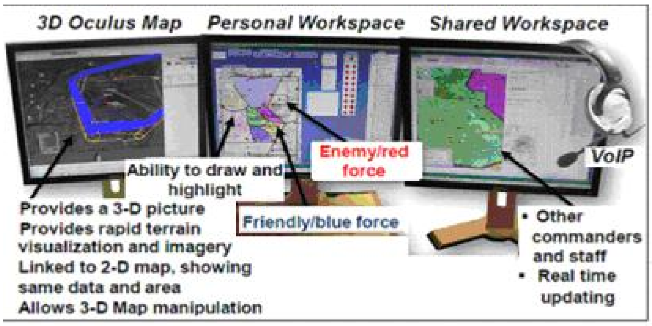

3D Oculus Map
Personal Workspace
Shared Workspace
Enemy/red force
VoIP
Ability to draw and highlight
Provides a 3-D picture
Provides rapid terrain visualization and imagery
Linked to 2-D map, showing same data and area
Allows 3-D Map manipulation
Friendly/blue force
• Other commanders and staff
• Real time updating

Fig. 27. Command Post of the future [27]

Summing up. As GAO concluded in 2013, Army is moving ahead but its network strategy is still evolving. Honesty speaking it seems impossible to modernize the software for as much as 189 US Army primary military systems, but some improvements of Army network have made continuously. We point out some doubts relate to

Command Post of the future (Figure 27): it is too complicated for the nearest time.

VII. CYBERCOM TAKES THE DISN CONTROL BUT UNSUCCESSFULLY

A. Single Security Architecture

In October 2010, the U.S. Army Cyber Command had set up. USCYBERCOM is now a part of the Strategic Command along with strategic nuclear forces, missile defense and space forces [29]. One of Cyber Command key tasks is Joint Information Environment based on Single Security Architecture (Figure 28).

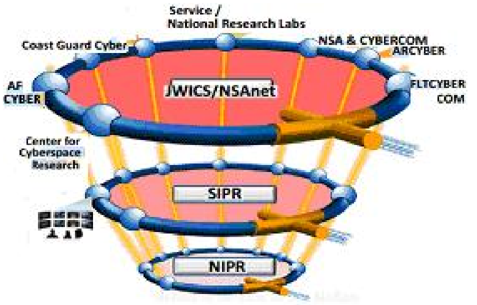


Fig. 28. Three levels of Single Security Architecture (SSA) [30]

It is worth noting the U.S. Cyber Command activities significantly slow down the transition to IP world. Cyber Command shall receive UC network situational awareness from as much network components as DoD Component Network Operations, Security Centers (NOSCs), and the DISA Network Operation Center (NOC) infrastructure. It should provide Operational Directive Messages to the DoD Components to meet mission needs. Thus, DISA and the other DoD Components shall be responsible for end-to-end UC network management. The solution of cyber defense tasks radically changes all plans for the DISN network (Figure 29).

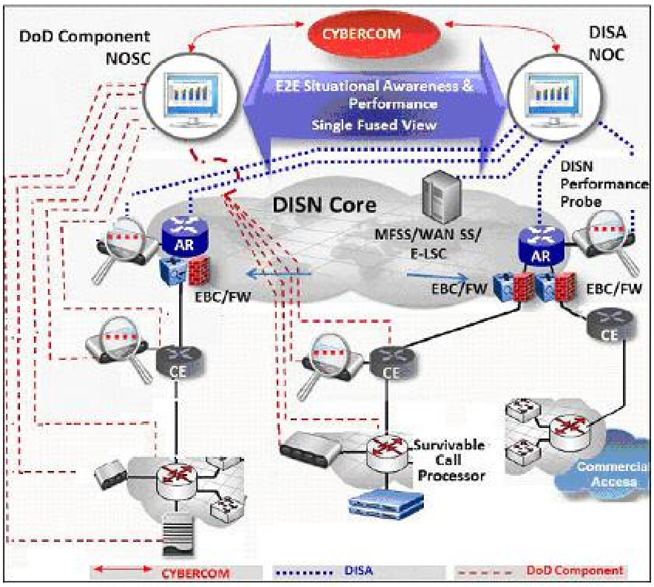


Fig. 29. CYBERCOM Construct for UC Network Operations [18]

B. Joint regional security stacks

The very concept of the Joint Information Environment (JIE) is extremely complex, and the requirements of cybersecurity make it even more difficult. The essence of the JIE concept is to create a common military infrastructure, provide corporate services and a unified security architecture. According to SSA, Joint regional security stacks (JRSS) are the main components of the JIE environment providing a unified approach to the structure of cybersecurity as well as protecting computers and networks in all military organizations.

JRSS is a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding, and provides a lot other network security capabilities. JRSS equipment, in fact, are IP-routers with a complex set of cyber-protection software. For example, the typical physical NIPR JRSS stack is comprised of as many as 20 racks (Figure 30). Currently, JRSS stacks have installed for the NIPRNet. It has planned also to install the stacks for the SIPRNet. The first JRSS stack had installed and successfully operated at the military base of San Antonio, Texas. In 2014, 11 JRSS stacks had installed in the United States, 3 stacks in the Middle East and one in Germany. The total amount of works includes the installation of 23 JRSS stacks on the NIPRNet service network and 25 JRSS stacks on the secret SIPRNet network (Figure 31). By 2019, it have planned to transfer to these stacks cybersecurity programs, which have now deployed in more than 400 locations [29].

Fig. 30. The physical NIPR JRSS stack - 20 racks [31]

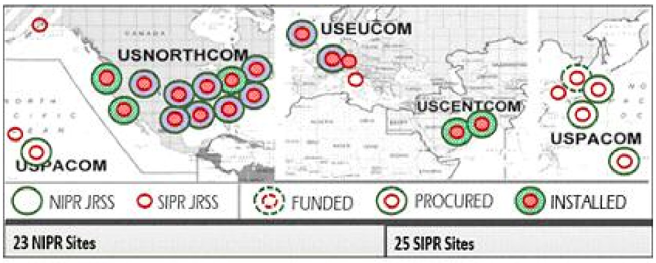


Fig. 31. 10. JRSS Current and Planned Deployments [32]

The DISN and DoD Component enclaves provide the two main network transport elements of the DODIN as shown in Figure 32 with the JRSS role.

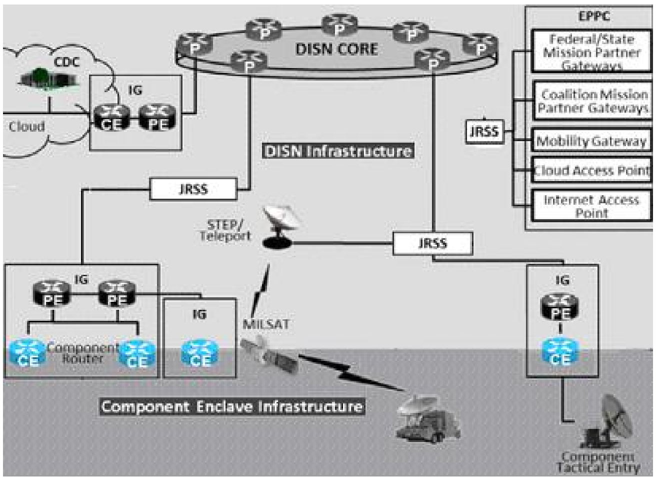


Fig. 32. The leading role of JRSS in DODIN Transport [33]

C. *Shortcoming No 2. GSM-O project*

In June 2012, Lockheed Martin won the largest tender for managing the DISN network (Global Services Management-Operations, GSM-O). The key task of the GSM-O contract is the modernization of the management system for cybersecurity requirements. The cost of work was a huge amount - 4.6 billion dollars for 7 years.

In 2013, the GSM-O team began to study the status of the four GIG network management centers that are responsible for the maintenance and uninterrupted operation of all Pentagon computer networks. There are 8,100 computer systems in more than 460 locations in the world, which in turn have connected by 46,000 cables. The first deal was to consolidate the operating centers - from four to two (Figure 33) by expanding the centers at the AB Scott (Illinois) and Hickam in Hawaii, but closing the centers in Bahrain and Germany.

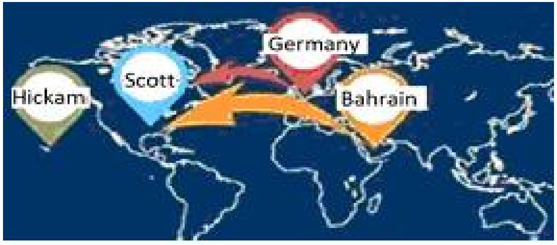


Fig. 33. The GSM-O goal to consolidate the operating centers - from four to two

In 2015, the telecommunications world was shocked by the news: Lockheed Martin is not coping with the upgrade of the DISN network management and sells its division “LM Information and Global Solutions” to the competing firm Leidos. The failure of the work was most likely due to the inability to recruit developers capable of combining the "old" circuit switching equipment with the latest packet switching systems as well as taking into account the new cybersecurity requirements [34].

D. *Shortcoming No3. The crucial JRSS failure*

During several last years, the GAO has been paying attention to Pentagon’s budget, particularly to JRSS budget. The JRSS will replace about 1,000 non-standardized network security stacks, currently scattered around the world, with 48 of the new standardized stacks at 25 locations, “reducing the number of avenues for cyberattack” [35].

July 2016. A report GAO-16-593 [36] required more control over the Nevertheless Chief spending of funds for JRSS. The GAO report states:

"The Department of Defense (DOD) plans to spend almost $ 1 billion by the end of this fiscal year to implement just one JIE element. However, the department did not fully determine the scope of JIE or its expected cost. Officials said that the JIE cost estimate is complicated because of the size and complexity of the department's infrastructure and the approach to implementing JIE. However, without information on the expected costs of JIE, the ability of officials to monitor and make effective decisions about resources is limited. "

November 2016. Defense Department Chief Information Officer Terry Halvorsen is attacking the GAO [37], they do not understand what the Joint Information Environment is: "What we tried to say to the GAO is that in this case do not measure JIE - you should measure its components." JIE consists of various programs, such as JRSS security stacks and partner country environments. JRSS, for example, aims to consolidate 1,000 legacy network security stacks to 48 standardized stacks at 25 worldwide locations. There are specific metrics to measure there, Halvorsen said.

February 2017. Nonetheless, DOD’s response in the GAO audit indicates it will take steps to address all GAO’s recommendations regarding JIE. Nevertheless, Chief Information Officer Halvorsen resigned.

January 2018. Under the pressure of GAO critics, the Pentagon’s chief weapons tester said the DoD should stop deploying its new network security platform JRSS. The Pentagon’s weapon tester said that during a test last year the version of the program in use by the Air Force did not help protect the network [38].

February 2018. Despite the GAO critics, DoD continues the JRSS initiative. DOD stood up 14 of the 25 security stacks planned across the network in the U.S., Europe, and Pacific and southwest regions in Asia. The final security stack has planned for completing by the end of 2019 [39].

Could be fulfilled the Pentagon's grandiose plans? The complexity of the task, in particular, characterizes the set of requirements for potential JRSS developers, named in the invitations to work for Leidos. Requires work experience of 12-14 years and knowledge of at least two or more products from ArcSight, TippingPoint, Sourcefire, Argus, Bro, Fidelis XPS, Niksun FPCAP, Lancope, NetCool, InfoVista, and Riverbed. Note that each of these companies provides its complex software for cyber defense. How to combine them? How to hire such high-level software developers and for work in top-secret environment?

More importantly, is the project worth be doing? Why? The crucial JRSS failure is extremely important: JRSS is too S-L-O-W. It sounds like a sentence on the fate of the JRSS project [40].

During the press conference on May 17, 2018, DISA officials acknowledged some performance issues for tools that military units are storing inside the JRSS. The JRSS is an early phase of a planned Defense Department-wide computer cloud. In general, digital tools that the services put into the cloud are still functioning and are not losing any data, but it is taking too long for data to transfer from the cloud to the user, namely, JRSS is too slow [41].

E. Could Leidos cope with GSM-O II?

In October 2018, the Defense Information Systems Agency has released a final solicitation for the potential 10-year, $6.52B Global Solutions Management-Operations follow-on contract for telecommunications and information technology services. GSM-O II is a single award contract designed to provide a full global operations and sustainment solution that has needed to support DODIN/DISN [42].

The key GSM-O II Attributes are:

- Cybersecurity defense of the DISA enterprise infrastructure to include the DISN backbone, cyber automation and defensive cyber operations.
- Joint Regional Security Stacks aids in the support required to integrate, maintain and modernize systems to support and enhance the mission.

Leidos is the incumbent on the initial $4.6B GSM-O program and has received approximately $1.9B in obligations through the current contract. Leidos inherited the contract from Lockheed Martin’s former information systems and global services business, which merged with Leidos in August 2016 [43]. Now we are looking for the Leidos success. It is yet unclear and 10-year period, of course, is a rather long time. Could Leidos cope with GSM-O II?

VIII. JEDI CLOUD STRATEGY AND ITS CRITICS

The Defense Department's newly released cloud strategy positions the general-purpose Joint Enterprise Defense Infrastructure (JEDI) cloud initiative as the foundation [44]. The strategy emphasizes a cloud hierarchy at DOD, with JEDI on top. Fit-for-purpose clouds, which includes MilCloud 2.0 run by DISA, will be secondary to the commercially run JEDI general-purpose cloud.

During testimony at a Senate Armed Services cybersecurity subcommittee hearing Jan. 29, 2019, DOD CIO Dana Deasy said that DoD needs to stop debating over mission-specific tools and focus entirely on implementation. Note some unexplainable rush with the JEDI project forgetting about recent shortcomings with JRSS deal.

April 10, 2019. The Department of Defense confirms that Amazon and Microsoft are the winners. Oracle and IBM are officially out of the race for a key $10 billion defense cloud contract as Amazon and Microsoft move ahead. Note Amazon was in the best position to win the government contract and has considered the favorite by most.

Could be the JEDI Cloud Strategy successful? A key technological difficulty for the JEDI project is interoperability of clouds (Figure 34). The interoperability of a technology (getting different parts to function in combination) can divided into three main categories: internal, external, and iterative. Unfortunately, in each category, the Pentagon’s JEDI cloud strategy leaves a series of unanswered questions that could spell disaster in the future [45].

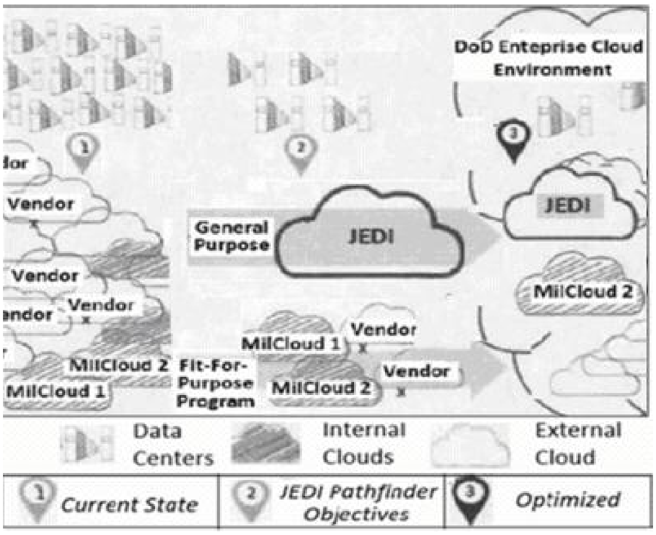


Fig. 34. DoD Pathfinder to Hybrid Cloud Environments [44]

For internal interoperability, the strategy lays out the correct goal, common data and application standards such as tagging, transport protocols, and interfaces will be developed to navigate DoD away from custom approaches. However, it does not mention the enormous logistical hurdles to this data-normalization process.

First, both the military’s legacy IT systems and the 500+ clouds already used within the Pentagon will each need to have their data formatted and migrated onto the JEDI platform.

The second unanswered question regards the JEDI cloud’s external interoperability. This sounds simple on paper, but the reality is far more uncertain. In a future conflict situation, would America’s allies need to use the same cloud provider (e.g., Microsoft or Oracle) and the same data-formatting practices as the DoD? The strategy does not discuss these long-term concerns including security flaws.

IX. ARTIFICIAL INTELLIGENCE INITIATIVE

The Defense Innovation Unit (DIU), launched in 2015, is a DoD organization founded to help the U.S. military make faster use of emerging commercial technologies. DIU is staffed by civilian and both active duty and reserve military personnel. The organization has headquartered in Silicon Valley (Mountain View, California) with offices in Boston, Austin, and some more. The Joint Artificial Intelligence Center is a focal point of the DoD Artificial Intelligence Strategy [46]. The DoD has created this Cloud Strategy to strengthen the security and resilience of the networks and systems that contribute to the Department's military advantage.

Taking into account the potential magnitude of AI’s impact on the whole of society, and the urgency of this emerging technology race, President Trump signed the executive order “Maintaining American Leadership in Artificial Intelligence” on February 11, 2019, launching the American AI Initiative. This was immediately followed by the release of DoD’s first-ever AI strategy [47].

The DoD strategy identifies how artificial intelligence can manage the understanding of all the Department’s data to free information from the current system of “disjointed stovepipes.” This is really one great idea - artificial intelligence, if it happens to be successful. Could it have more success than JRSS initiative?

X. Don’t touch what works

A. US Army Regulator fights for IP technology but unsuccessfully

The similar kind harsh sentence of the DoD’s activities flows from the Army Regulation document [27] of 2017 regarding Telecommunications Systems and Services. The Army regulator recognizes that there is ‘old’ equipment on the network: time-division multiplex equipment, integrated services digital networking, channel switching video telecommunication services. According this document, all these services will use IP technology. Name the few of instructive claims:

4–2.d. Commands that have requirements to purchase or replace existing Multilevel Secure Voice (previously known as Defense Red Switched Network (DRSN)) switches will provide a detailed justification and impact statement to the CIO/G–6 review authority.

4–2.e. The moratorium on investment in legacy voice-switching equipment and the requirement to submit requests for waivers to purchase voice-switching equipment applies to all TDM voice-switching equipment that is not capable of providing unclassified and/or secret IP voice services. The Army will migrate as soon as practical to an almost-everything-over-Internet Protocol architecture, to include Unified Capabilities (UC) and collaboration, with an end state of end-to-end IP.

4–4. All Army organizations will cease investment in (non-emergency) integrated services digital network (ISDN) supported technology, equipment, and transport. All Army organizations will transition from ISDN to a compatible IP-supported technology or service including, but not limited to, video, facsimile, voice, and other network capabilities.

7–4. Secret IP voice is the Army-preferred means of providing secret-only voice communications. The latest UCR will provide guidance for the implementation of secret IP voice capabilities. The UCR requires that classified IP voice migrates to multivendor equipment using the Assured Services Session Initiation Protocol (AS–SIP).

As we have mentioned above citing the AT&T view [2], the DoD today still has analog, fixed, premises-based, time-division multiplexing and even asynchronous transfer mode infrastructure and could remain for the unpredictable period according to the well-known software developers slogan: Don’t touch what works.

B. Defense Red Switch Network

No reason to be surprised that the Defense Red Switch Network (DRSN) uses 40 years old ISDN technology, the more – in conditions of cyberwar. DRSN is a dedicated telephone network, which provides global secure communication services for the command and control structure of the United States Armed Forces and the NATO Allies (Figure 35). The network has maintained by DISA and has secured for communications up to the level of Top Secret.

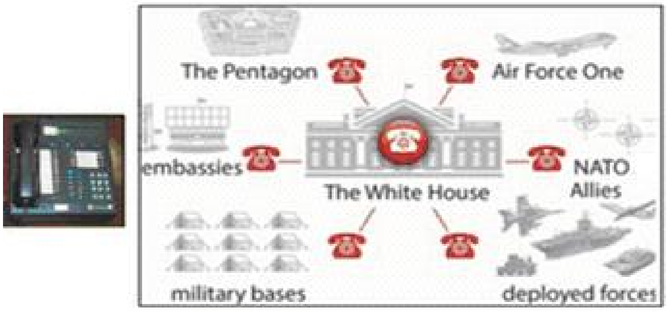


Fig. 35: Secure Terminal Equipment, STE; note slot in the front for Crypto PC Card (left). The DRSN architecture (right) [48]

"Red Phone" (Secure Terminal Equipment, STE) connects to the network via ISDN line and operates at a speed of 128 kbps. Note the slot at the bottom right serves for a crypto-card and four buttons at the top - to select the priority of communications. Special DRSN security features include Automatic Number Identification (ANI), Security Access Levels, Automatic Security Authentication (ASA) and Push-to-Talk Handset. The STE is the primary device for enabling secure communications over the Defense Switched Network (DSN). It may be used for secure voice, data, video, or facsimile.

C. The DISA dizzying projects

Under the industry pressure, the DISA administration is oriented officially to the today’s top technologies: Software Defined Network and Network Function Virtualization (Figure 36).

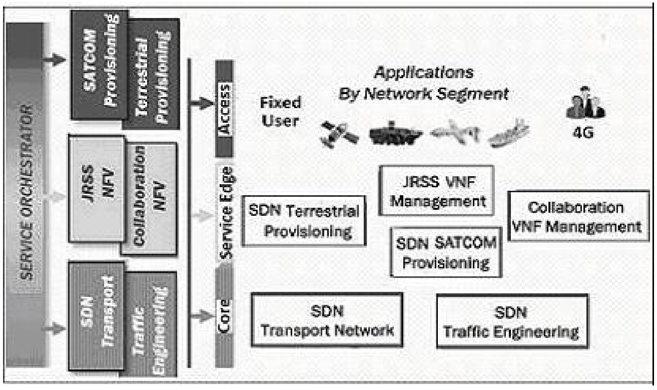
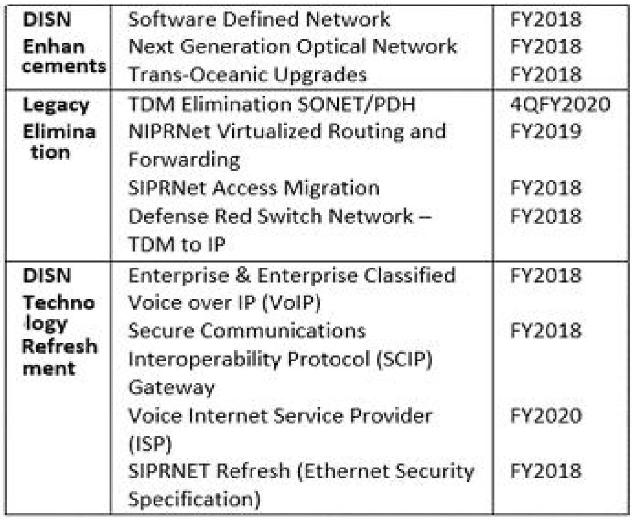


Fig. 36: The newer DISN architecture (the excerpt from slide 8 [4]): Software-Defined Network (SDN) & Network Function Virtualization (NFV)

Regarding the newer DISA projects [4], the obsolete TDM technology has changed by IP technology in the nearest years (Table 2).

Honestly speaking, these DISA projects look unlikely to implement in such a short time (they may be even harmful essentially - due to growing cyber threats).

Table 2. DISA Top Priorities (the excerpt from DISN Infrastructure Network Portfolio [4])



DISN Enhancements	Software Defined Network	FY2018
	Next Generation Optical Network	FY2018
	Trans-Oceanic Upgrades	FY2018
Legacy Elimination	TDM Elimination SONET/PDH	4QFY2020
	NIPRNet Virtualized Routing and Forwarding	FY2019
	SIPRNet Access Migration	FY2018
	Defense Red Switch Network – TDM to IP	FY2018
DISN Technology Refreshment	Enterprise & Enterprise Classified Voice over IP (VoIP)	FY2018
	Secure Communications Interoperability Protocol (SCIP) Gateway	FY2018
	Voice Internet Service Provider (ISP)	FY2020
	SIPRNET Refresh (Ethernet Security Specification)	FY2018

Summing up, the most fundamental question about the ubiquitous DISN transition to IP technology arises.

XI. Conclusion

Communication specialists all around the world are facing the same problem: shifting from circuit switching (CS) to packet switching (CS). The same problem is the main challenge for the U.S. Department of Defense. The DoD today still has analog, fixed, premises-based, time-division multiplexing (TDM) and even asynchronous transfer mode (ATM) infrastructure. The nowadays DoD's strategy is the move to a fully software-based network, but could it be implemented? Cyber threats are another hard obstacle in a move to IP world.

The DoD Doctrine "Joint Vision 2010" issued in 1995 by General J. Shalikashvili and enhanced by DISA in 1998 contains a principled decision: to build US military communications networks using the "open architecture" and commercial-off-the-shelf (COTS) products. At that time, the choice fell on the developments of Bell Labs, namely, on the telephone signaling protocol SS7 and the Advanced Intelligent Network (AIN). Lockheed Martin was responsible for the AIN from the very beginning of the "Joint Vision 2010" program. New military equipment and new services are coming continuously that requires the continuous improvement of AIN. How to hire qualified professionals? Young professionals, who grew up in IP world, seem unable to support and develop existing AIN network, they have not knowledge in the area of circuit switching technologies. It is an event pointed out as Shortcoming No1.

Just a few years later as "Joint Vision 2010" had introduced, namely, in 2007, a new Pentagon strategy "Joint Vision 2020" appeared announcing the extremely important point: DISN must built on basis of IP protocol. For the implementation of "Joint Vision 2020", the key important step is the replacement of channel switching electronic Multifunctional switches (MFS) by packet switching routers. The transition phase has based on the use of IP oriented Multifunctional SoftSwiches (MFSS) and new signaling protocol AS-SIP. It is still difficult to predict the time during which the DISN network will finally switch to the AS-SIP protocol. A comparison of router and circuit switch has carried on by an example coming from Stanford University: the software for circuit switch is much simpler and cheaper than for packet switch. Thus, TDM and ISDN equipment could coexist with IP equipment for an unpredictable time.

The aim of "Joint Vision 2020" concept is to implement unified services, so called Unified Capabilities. The Unified Capabilities architecture uses the IP for the wide-area backbone network. The Common Operating Environment Architecture is a key component for Army Enterprise Network Architecture. The idea of COE per se is attractive one but a giant volume of software be developed, especially considering USCYBERCOM requirements on cyber-security. Cyber Command key task is to build Joint Information Environment on principles of Single Security Architecture. This giant project arises a reasonable doubt. Could be implemented these ambitious ideas whenever? Our doubts have based on two more shortcomings.

The first one. In June 2012, Lockheed Martin won the largest tender for managing the DISN network: Global Services Management-Operations (GSM-O). The first deal was to upgrade the DISN management system, namely, to consolidate the operating centers - from four to two. In 2015, the telecommunications world was shocked by the news: Lockheed Martin is not coping with the upgrade of the DISN network management and sells its division "LM Information and Global Solutions" to the competing company Leidos. The failure of the work was most likely due to the inability to recruit developers capable of combining the "old" circuit switching equipment with the latest packet switching systems as well as taking into account the new cybersecurity requirements

The second shortcoming relates to Joint regional security stacks (JRSS) as a foundation of Single Security Architecture. The JRSS will replace about 1,000 non-standardized network security stacks, currently scattered around the world, with 48 of the new standardized stacks at 25 locations, reducing the number of cyberattacks. The crucial JRSS failure is extremely important: JRSS is too S-L-O-W. It sounds like a sentence on the fate of the JRSS project as a whole.

The Defense Department's newly released cloud strategy positions the general-purpose Joint Enterprise Defense Infrastructure (JEDI) cloud initiative as the foundation. The strategy emphasizes a cloud hierarchy at DoD, but JEDI cloud strategy leaves a series of unanswered questions relating to interoperability of clouds that could spell disaster in the future.

The JEDI cloud strategy has based on Artificial Intelligence Initiative. Underscoring the potential magnitude of AI's impact on the whole of society, and the urgency of this emerging technology race, President Trump signed the executive order "Maintaining American Leadership in Artificial Intelligence" on February 11, 2019, launching the

American AI Initiative.

Summing up the analysis of DoD's telecommunication strategy, we apply to the Army Regulation document of 2017 regarding Telecommunications Systems and Services. The Army regulator recognizes that there is old equipment on the network: TDM and ISDN equipment, channel switching video telecommunication services, etc. These services should use IP technology but all these changes require a huge number of programmers, which is difficult to implement. No reason to be surprised that the Defense Red Switch Network (DRSN) uses 40 years old ISDN technology.

In conditions of cyberwar, the very move to internet technologies in telecommunications seems doubtful..

REFERENCES

[1] M. Sneps-Sneppe, D. Namiot, "The curse of software: Pentagon telecommunications case" in 2019 International Symposium on Systems Engineering (ISSE), October 2019. DOI: 10.1109/ISSE46696.2019.8984557.

[2] "The Defense Network of Tomorrow—Today," An AT&T Whitepaper, 2018.

[3] "DoD Network of the Future Powered by Commercial Networks and Innovation," Web Link " http:// att.com/gov/defense 2017/".

[4] Ch. Osborn, "Defense Information Systems Network (DISN). An Essential Weapon for the Nation's Defense," InfrastructureDirectorate, 16 May, 2018, Web Link "www.disa.mil› Symposium/".

[5] GAO-19-128, "Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities," Report to the Committee on Armed Services, U.S. Senate, US Government Accountability Office, October 2018.

[6] D. Grazier. "What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks? An Obvious Solution Being Ignored," January 31, 2019, Web Link https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a-generation-of-weapons-vulnerable-to-cyberattacks/.

[7] "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," 30 May 1995. Web Link "http://waffenexporte.de/NRANEU/others/jp-doctrine/jp6_0(95).pdf/".

[8] L. Bowman, R. Riehl, S. Shah, "Defense Information System Network (DISN) asynchronous transfer mode (ATM) goal architecture and transition strategy," in IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201), 19-21 Oct, 1998, Boston, USA. DOI: 10.1109/MILCOM.1998.722548.

[9] GAO/AIMD-98-202, "Defense Networks. Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals," US General Accounting Office, July 30, 1998.

[10] GAO/NSIAD/AIMD-98-257, "Defense Information Superiority: Progress Made, But Significant Challenges Remain," Letter Report, 08/31/98.

[11] W. W. Chao, "Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters," in MILICOM, 1999. IEEE.

[12] DISA, "Special Interoperability Test Certification of Avaya S8300D with Gateway 450 (G450)," Joint Interoperability Test Command (JITC), 17 Apr, 2012.

[13] "DARPA names Lockheed Martin to build intelligent network," March 24, 2005. Web Link "http://www.militaryaerospace.com/articles/2005/03/darpanames-lockheed-martin-to-build-intelligent-network.html/".

[14] U.S. Department of Defense, "Global Information Grid. Architectural Vision," Version 1.0, June 2007.

[15] "US Army Unified Capabilities (UC) Reference Architecture (RA)," Version 1.0, 11 Oct, 2013.

[16] US Department of Defense, "Assured Services (AS) Session Initiation Protocol (SIP), Errata-1," July 2013, Web Link http://www.defense.gov/news/newsarticle.aspx?id=122949/.

[17] "Cisco LSC Overview," Web Link "https://www.cisco.com/web/strategy/docs/gov/Cisco_LSC_Overview_Jan2011.pdf/".

[18] US Department of Defense, "Information Enterprise Architecture Unified Capabilities. Reference Architecture," Version 1.0, January 2013.

[19] US Department of Defense, "Unified Capabilities Master Plan (UC MP)," October 2011.

[20] K. Bailey, "Army finalizes design for modernized network capability set," April 30, 2020. Web Link "http://www.army.mil/article/235174/army_finalizes_design_for_modernized_network_capability_set/".

[21] F. Baker, J. Polk (Cisco Systems), "Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite", RFC 4542, May 2006.

[22] P.M. Fernandez, "Circuit switching in the internet," Dissertation, Stanford University, June 2003.

[23] S. Das, G. Parulkar, N. McKeown, "Rethinking IP core networks," in Journal of Optical Communications and Networking, 5(12):1431–1442, 2013.

[24] US Department of Defense, "Definitions and Guidance for the Common Operating Environment. Annex B to LandWarNet 2020 and Beyond Enterprise Architecture," Version 2.0, 1 Aug, 2014.

[25] "Common Operating Environment Architecture. Appendix C to Guidance for 'End State' Army Enterprise Network Architecture," U.S. Army CIO/G-6, 1 Oct, 2010.

[26] "CS-13 Introduces New Networking Capabilities," December 5, 2012. Web Link "http://defense-update.com/20121205_cs-13-introduces-new-networking-capabilities.html/".

[27] Army Regulation 25–13 Information Management, "Army Telecommunications and Unified Capabilities. Headquarters Department of the Army," Washington, DC, 11 May, 2017.

[28] GAO-13-179, "Army networks. Size and Scope of Modernization Investment Merit Increased Oversight," January 2013.

[29] D. Metz, "Joint Information Environment Single Security Architecture (JIE SSA)," DISA, 12 May, 2014, Web Link http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/.

[30] "Cyber Situational Awareness - Big Data Solution," Web Link "https://docplayer.net/2357634-Cyber-situational-awareness-big-data-solution.html/".

[31] S. Meloni, "The Future of the Joint Information Environment (JIE)", Sept 24, 2014. Web Link http://blog.immixgroup.com/2014/09/24/the-futureof-the-joint-information-environment-jie/.

[32] "JRSS Deployments," Web Link https://c.ymcdn.com/sites/alamoace.site-ym.com/resource/resmgr/2017_ace/2017_speakers/2017_AACE_Keynote_Presentations/doc_keynote_Yee.pdf /.

[33] DoD Instruction 8010.01. "Department of Defense Information Network (DODIN) Transport," September 10, 2018. Web Link http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/.

[34] A. Corrin, "Leidos-Lockheed merger changes the face of federal IT," in Federal Times, February 5, 2016, Web Link "https://www.federaltimes.com/it-networks/2016/02/05/leidos-lockheed-merger-changes-the-face-of-federal-it/".

[35] "Cyberscoop," Web Link https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/.

[36] GAO-16-593, "Joint Information Environment: DOD Needs to Strengthen Governance and Management," Jul 14, 2016.

[37] "Pentagon Tech Chief Says He'll 'Take the Hit' for GAO Criticism of JIE," Nov 02, 2016. Web Link http://www.nextgov.com/cio-briefing/2016/11/pentagon-tech-chief-says-hell-take-hit-gao-criticism-jie/132882/.

[38] M. Gruss, "The debate about whether DISA's new security system is ready for primetime", Febr 7, 2018, Web Link https://www.c4isrnet.com/show-reporter/afceawest/2018/02/08/the-debate-about-whether-disas-new-securitysystem-is-ready-for-primetime/.

[39] L.C. Williams, "DOD CIO: JRSS set for 2019 completion," Mar 05, 2018, Web Link "https://fcw.com/articles/2018/03/05/jrss-completionmiller. aspx/".

[40] L. C. Williams, "Is it time to rethink JRSS?" Feb 01, 2019, Web Link "https://defensesystems.com/articles/2019/02/01/jrss-pause-report-williams.aspx/".

[41] J. Marks, "The Pentagon Has a Big Plan to Solve Identity Verification in Two Years," in NEXTGOV, May 17, 2018, Web Link "https://www.defenseone.com/technology/2018/05/pentagon-has-big-plan-solve-identity-verification-two-years/148280/".

[42] Jane Edwards, “DISA Issues Final RFP for $6.5B GSM-O IT. Telecom Support Recomplete Contract,” October 16, 2018, Web Link “https://www.govconwire.com/2018/10/disa-issues-final-rfp-for-6-5b-gsm-o-it-telecom-support-recompete-contract/”.

[43] “Global Solutions Management – Operations II,” DISA, May 2020, Web Link “https://“disa.scott.ditco.mbx.it-requirements@mail.mil/”.

[44] L. C. Williams, “DOD cloud strategy puts JEDI at the center,” Feb 05, 2019, Web Link https://defensesystems.com/articles/2019/02/06/dod-cloud-strategy.aspx/.

[45] T. Keelan, “The Pentagon’s JEDI cloud strategy is ambitious, but can it work?” March 21, 2019, Web Link https://www.c4isrnet.com/opinion/2019/03/21/the-pentagons-jedi-cloud-strategy-is-ambitious-but-can-it-work/.

[46] US Department of Defense, “DoD Cloud Strategy Readiness for Artificial Intelligence (Al),” December 2018.

[47] US Department of Defense, “Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity,” February 12, 2019, Web Link https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf/8.