Chapter

On Telecommunications Thorn Path to the IP World: From Cybersecurity to Artificial Intelligence

Manfred Sneps-Sneppe

Abstract

The chapter is devoted to the discussion of the telecommunications development strategy. Communication specialists all around the world are facing the problem: how to shift from circuit switching to packet switching. The same problem is the main challenge for the US Department of Defense. We discuss the Defense Information System Network move from circuits to packets, namely, "Joint Vision 2010" doctrine - 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 describe some packet switching shortcomings during the implementation of Joint Vision 2020, namely, 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. The JEDI cloud strategy has based on Artificial Intelligence Initiative. We conclude that the long-term channel - packet coexistence seems inevitable, especially in the face of growing cyber threats.

Keywords: circuit switching, packet switching, joint vision 2010, advanced intelligent network, joint vision 2020, SS7, IP, AS-SIP, softswitch, defense information systems network, defense red switched network, artificial intelligence

1. Introduction

The chapter is devoted to the discussion of the telecommunications development strategy. Communication specialists all around the world are facing the problem: how to shift from circuit switching to packet switching. 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,"- is the AT&T view [1]. Really, the DoD has one aging network based on circuit switching point-to-point circuits. This "old" technology requires an expensive support of hardware and additional upgrades with difficulties carried on in the IP era.

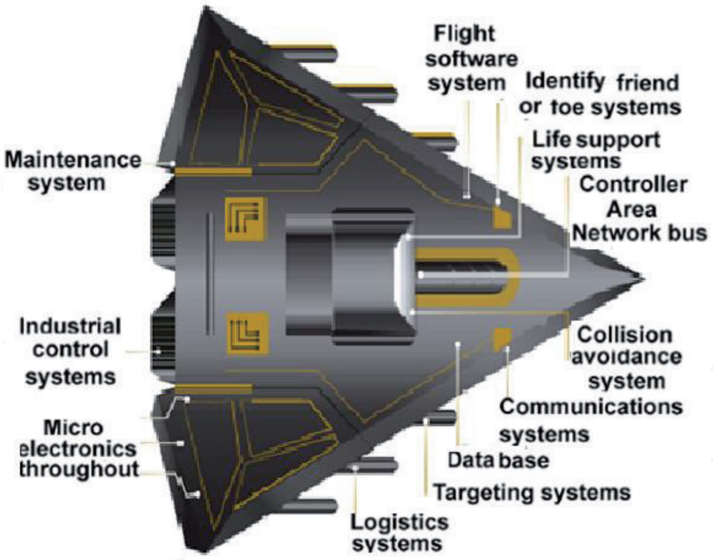
Flight software system
Identify friend or toe systems
Life support systems
Controller Area Network bus
Maintenance system
Industrial control systems
Micro electronics throughout
Collision avoidance system
Communications systems
Data base
Targeting systems
Logistics systems

Figure 1.
Software and information technology systems in aircraft (shown for classification reasons) [2].

Cyber threats are another hard obstacle in a move to IP world. In October of 2018, the Government Accounting Office (GAO) has reported [2], the United States weapons systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities. DoD weapon systems nowadays are more and more software dependent (**Figure 1**). We observe the weapons, from ships to aircrafts; use more software than even before. For example, the aircraft F-35 Lighting II software contains eight million lines of code [3].

The rest of paper is as follows. Sections 2 and 3 are about DoD's strategies "Joint Vision 2010" and "Joint Vision 2020," respectively. In Sections 4 and 5, we consider the target DISN infrastructure and Joint regional security stacks. In Section 6, the up-to-date JEDI Cloud Strategy and Artificial Intelligence Initiative have given in short. In the concluding Section 7, we point out rather unsuccessful US Army Regulator fights for IP technology. It is exampled by Defense Red Switch Network using 40 years old ISDN technology.

2. Joint vision 2010

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

The new DoD Doctrine [4] had issued by General J. Shalikashvili in 1995. This is the keystone document for Command, Control, Communications, and Computer (C4) systems up to now. At that time, "Joint Vision 2010" doctrine met a strong criticism from the US GAO side [5]. The GAO pointed out that the military services are operating as many as 87 independent networks. DISA initiated a similar data call after GAO survey and identified much more - 153 networks throughout Defense.

General J. Shalikashvili had met the technological uncertainty and the controversial requirements. Under these conditions, DISA (Defense Information Systems Agency) has made a very important decision - to use the "open architecture" and commercial-off-the-shelf (COTS) products only for military communication networks. The decision was – to use widely tested developments of Bell Labs, namely, the telephone signaling protocol SS7 and the Advanced Intelligent Network (AIN). These products were rather 'old' at that time: SS7 protocols had developed at Bell Labs since 1975 and defined as ITU standards in 1981.

The details regarding the transition to SS7 and AIN we found in a paper [6] from Lockheed Martin Missiles & Space – the well-known Defense contractor.

SS7 is an architecture for performing out-of-band signaling. In supports the call establishment, routing, and information exchange functions as well as enables network performance. In own order, the Advanced Intelligent Network was originally designed as a critical tool to offer sophisticated services such as "800" calls and directory assistance. The functional structure of the SS7 makes it possible to create the AIN by putting together functional parts: Service Control Point, Service Switching Point, the Service Creation Environment, Service Management System, Intelligent Peripheral, Adjunct, and the Network Access Point. **Figure 2** describes the AIN components that operate in the worldwide military telecommunication network, as well

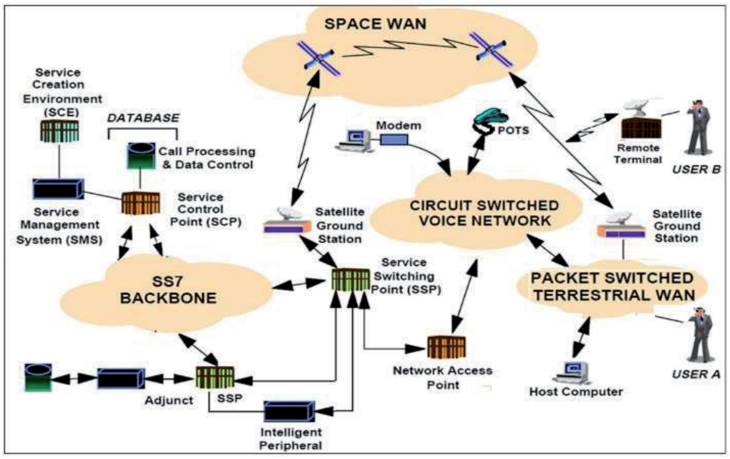
SPACE WAN
Service Creation Environment (SCE)
DATABASE
Call Processing & Data Control
Modem
POTS
Remote Terminal
USER B
Service Management System (SMS)
Service Control Point (SCP)
Satellite Ground Station
CIRCUIT SWITCHED VOICE NETWORK
Satellite Ground Station
SS7 BACKBONE
Service Switching Point (SSP)
PACKET SWITCHED TERRESTRIAL WAN
Adjunct
SSP
Network Access Point
Host Computer
USER A
Intelligent Peripheral

Figure 2.
Advanced intelligent network military service architecture [6].

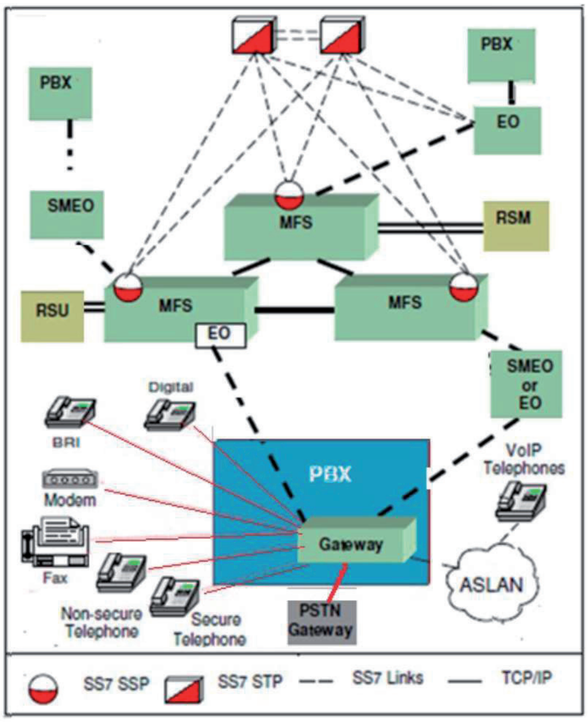

Figure 3.
The simplified DISN view: The current state [7].

as how they are deployed in SS7 backbone, the space Wide Area Network (WAN), circuit switched voice network and the packet switched terrestrial WAN.

To illustrate the current DISN architecture (**Figure 3**) we refer to the certification of Avaya PBX by DISA Joint Interoperability Test Command in 2012 [7]. The SS7 network is some kind of the nervous system of DISN up to the resent time. It connects the channel mode MFS (MultiFunctional Switches) and many others network components. That is, within the DISN network, the connections have established by means of SS7 signaling. All new terminal equipment what appears is largely IP type, nevertheless SS7 network retains its central place.

3. Joint vision 2020: all-over-IP

Just a few years later as "Joint Vision 2010" had introduced, namely, in 2007 the next Pentagon strategy "Joint Vision 2020" appeared. Pentagon published a fundamental program [8]. There we find the most important point: DISN have been built on basis of IP protocol (**Figure 4**). IP protocol should be the only means of communication between the network's transport layer and all available applications. The following 10 years have shown it is an extremely hard challenge.

To implement Joint Vision 2020, the most important step is the replacing of channel switching electronic Multifunctional switches (MFS) by packet switching routers. The transition to IP protocol has based on the use of Multifunctional SoftSwiches (MFSS) and new signaling protocol AS-SIP (Assured Services Session Initiation Protocol). MFSS operates as a media gateway (MG) between TDM circuits switching and IP packet switching components. During the transition phase, MFSS operates under the control of the media gateway controller (MGC). Communications control protocol H.248 has used between MG and MGC. As shown in **Figure 5**, MFSS should be pure packet switch besides DRSN 'island' using ISDN protocol.

A few words about SIP signaling. The SIP protocol widely used now for internet telephony is not able to provide secrecy during transmission (under cyber warfare conditions) and to provide priority calls. Therefore, the Department of Defense ordered to develop one new secure AS-SIP protocol [10]. The AS-SIP protocol turned out to be extremely difficult. AS-SIP uses the services of almost 200 different RFC standards while ordinary SIP uses only 11 RFC standards.

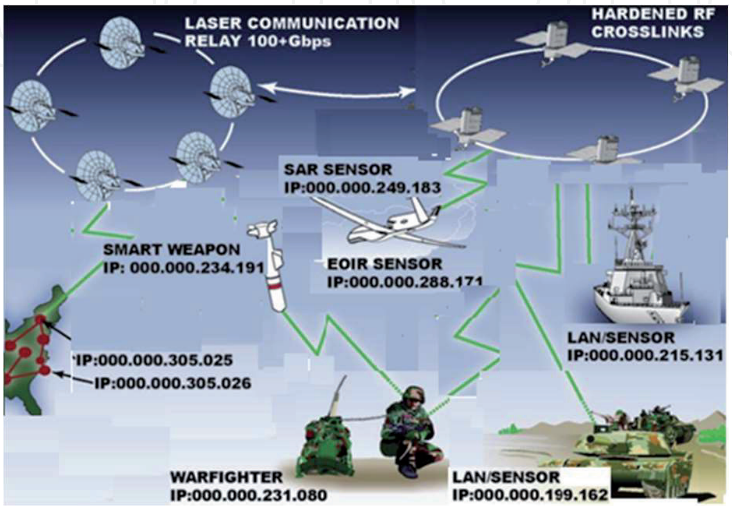

Figure 4.
Joint vision 2020: Each warfare object has own IP address.

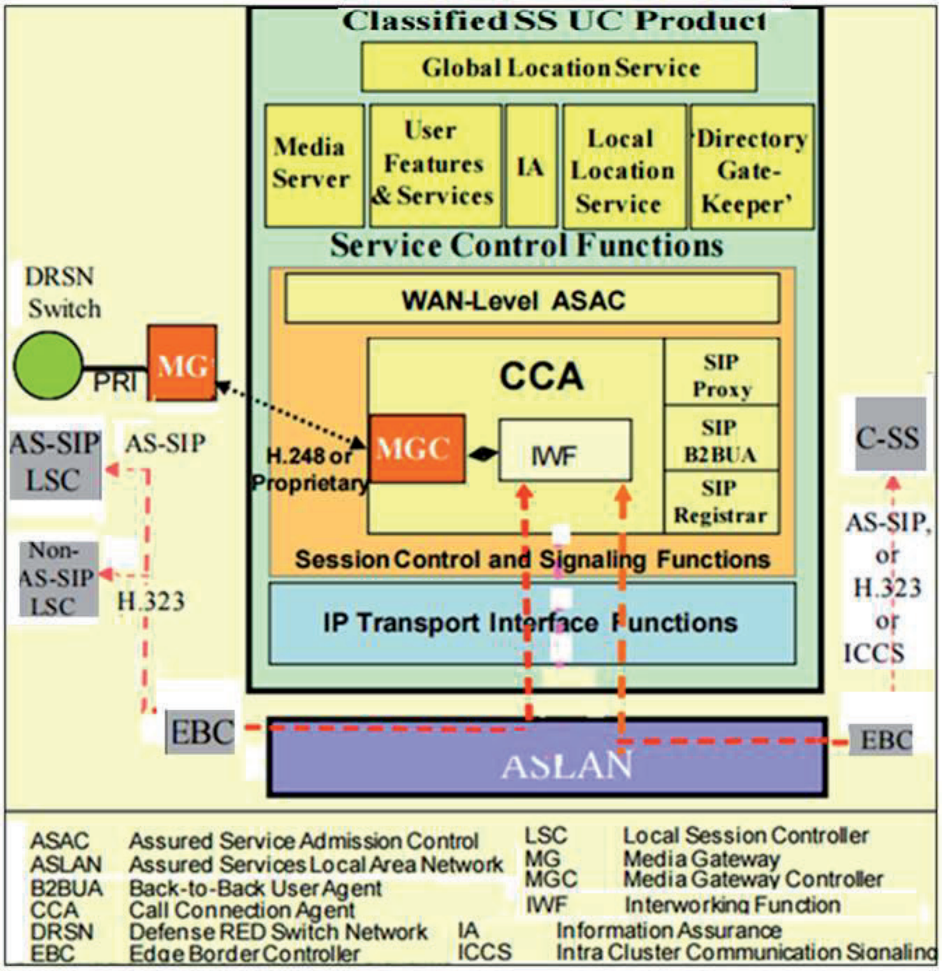
Classified SS UC Product
Global Location Service
Media Server
User Features & Services
IA
Local Location Service
Directory Gate-Keeper'
Service Control Functions
WAN-Level ASAC
CCA
SIP Proxy
SIP B2BUA
SIP Registrar
MGC
IWF
H.248 or Proprietary
Session Control and Signaling Functions
IP Transport Interface Functions
DRSN Switch
PRI
MG
AS-SIP LSC
AS-SIP
Non-AS-SIP LSC
H.323
EBC
ASLAN
C-SS
AS-SIP, or H.323 or ICCS
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

Figure 5.
Reference model for multifunction SoftSwitch [9].

The aim of "Joint Vision 2020" concept is to implement unified services based on Unified Capabilities concept. Army Unified Capabilities (UC) have defined as the integration of voice, video, and/or data services. These services have delivered across secure and highly available network infrastructure [11].

The following are the basic Voice Features and Capabilities:

- Call Forwarding (selective, on busy line, etc.)
- Multi-Level Precedence and Preemption (MLPP)
- Precedence Call Waiting (Busy with higher precedence call, busy with Equal precedence call, etc.)
- Call Transfer (at different precedence levels)
- Call Hold and Three-Way Calling and many others.

The Unified Capabilities services are covering a plenty of 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, etc. A collection of services include email and calendaring, instant messaging and chat, unified messaging, video conferencing, voice conferencing, web conferencing (**Figure 6**).

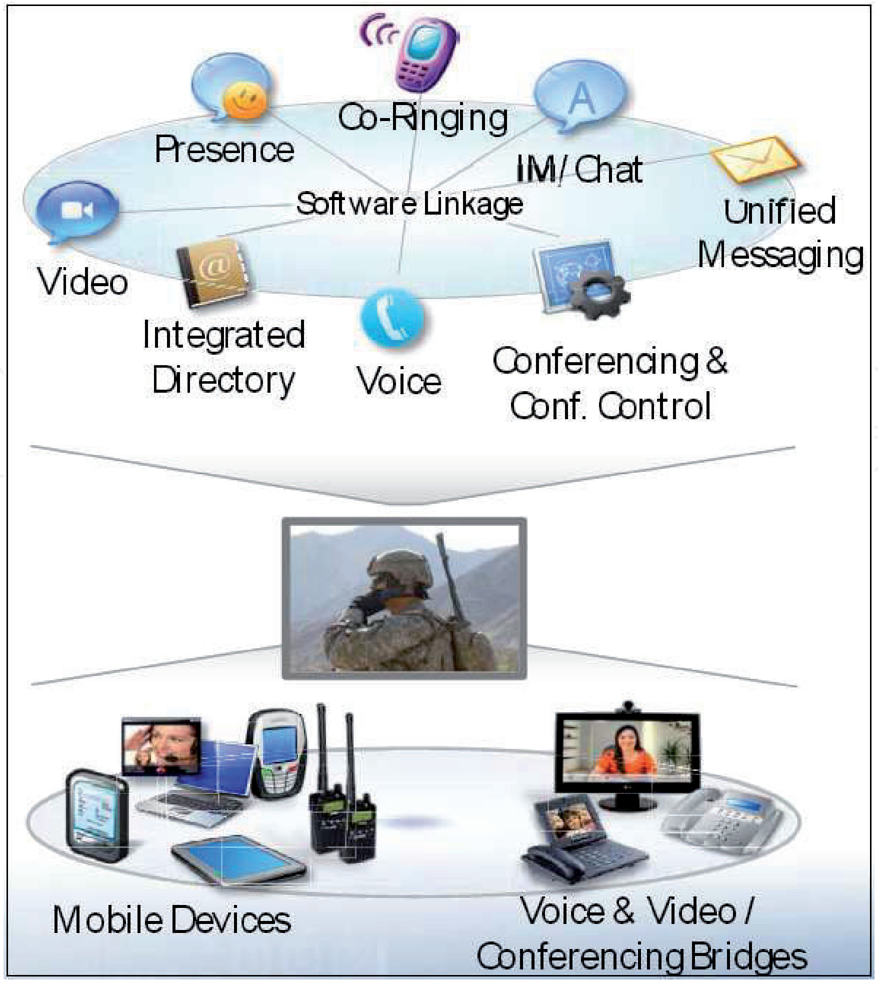

Figure 6.
Rich information services surrounding a soldier: not too much?

4. The target DISN infrastructure

The target DISN infrastructure contains two level switching nodes: Tier0 and Tier1 (**Figure 7**). Top level Tier0 nodes interconnect as geographic cluster and a cluster typically contains at least three Tier0 SoftSwitches. The distance between the clustered SoftSwitches must planned so that the return transmission time does not exceed 40 ms. As propagation delay equals 6 μs/km thus the distance between Tier0 should not exceed 6600 km. The classified signaling environment uses a mix of protocols including the vendor-based H.323 and the AS-SIP signaling. The use of H.323 has allowed only during the transition period to all IP protocol based DISN CVVoIP (Classified VoIP and Video). Classified VVoIP interfaces to the TDM Defense RED Switch Network (DRSN) via a proprietary ISDN PRI as a temporary exception.

In October 2010, the US 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 [13]. One of Cyber Command key tasks is to build Joint Information Environment (JIE) and to implement Single Security Architecture (SSA).

It is worth noting the US Cyber Command activities significantly slow down the transition to IP world. Cyber Command shall receive UC network situational awareness from all network agents including DoD Network Operations Security Centers (NOSCs), and the DISA Network Operation Center (NOC) infrastructure (**Figure 8**). Thus, DISA and the other DoD Components shall be responsible for end-to-end UC network management providing the strong cybersecurity requirements. The solution of cyber defense tasks radically changes the all DISN network modernization plans.

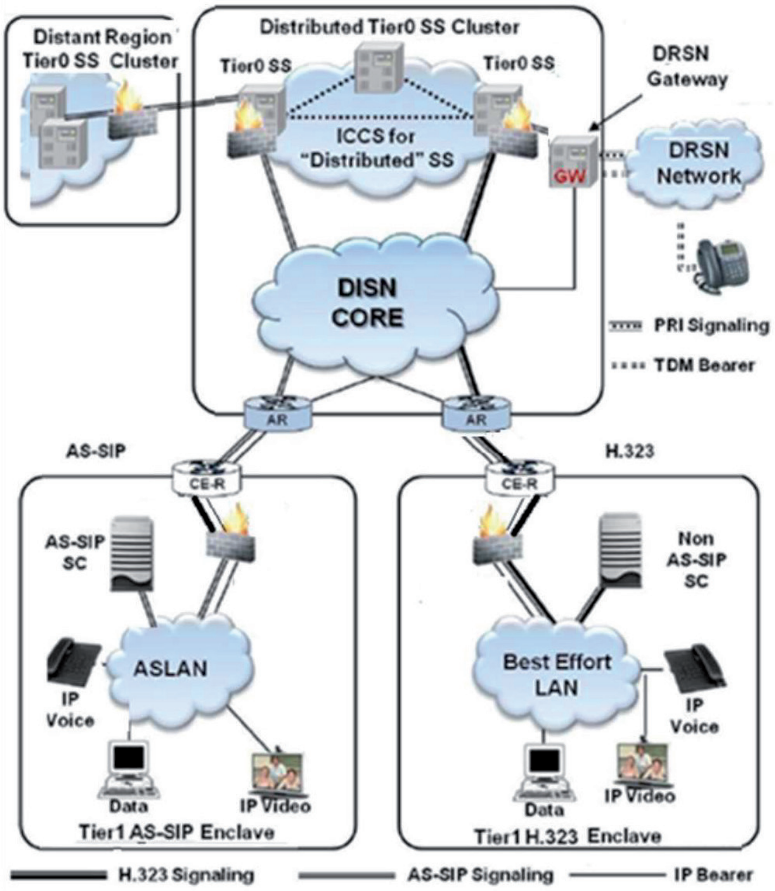

Figure 7.
DISN classified VoIP and video signaling design [12].

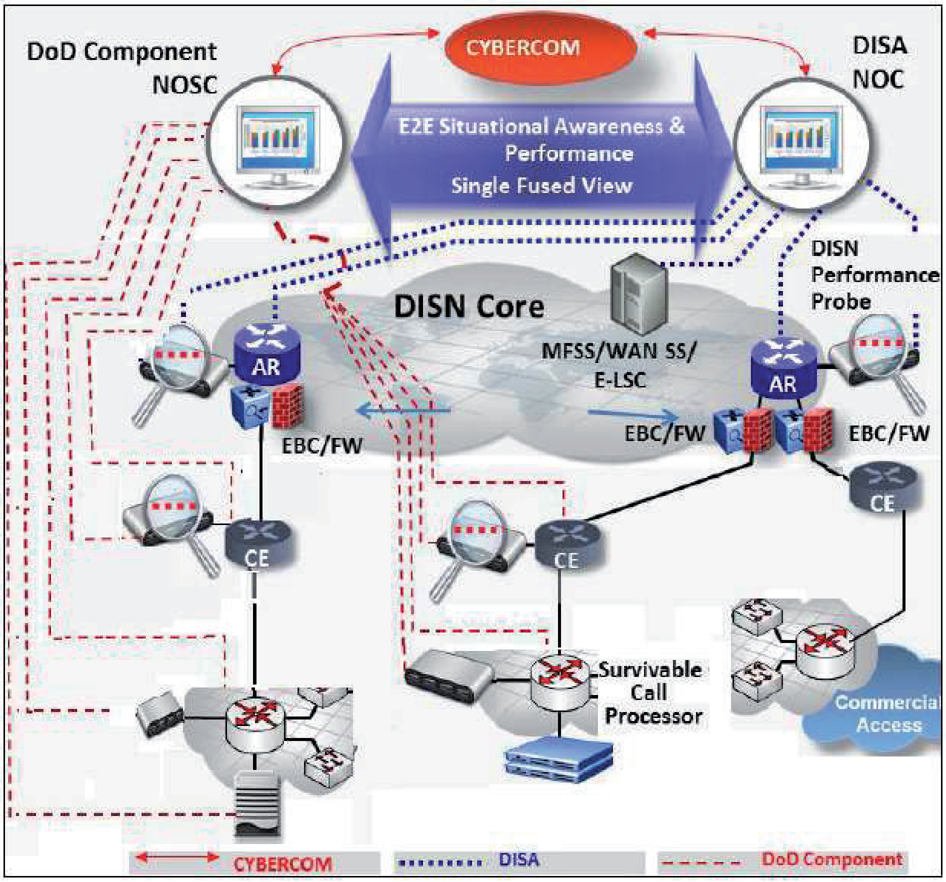

Figure 8.
Operational construct for unified capabilities network operations [12].

5. Joint regional security stacks

The essence of the Joint Information Environment concept is to create a common military infrastructure, provide corporate services and a unified security architecture. The very concept of JIE is extremely complex, and the requirements of cybersecurity make it even more difficult. 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 information networks everywhere in military organizations.

JRSS performs many functions as a typical IP-router providing cybersecurity: firewall functions, intrusion detection and prevention, and a lot other network security capabilities. JRSS equipment contains a complex set of cyber-protection software. For example, the typical NIPR JRSS stack is comprised physically of as many as 20 racks containing cyber-protection software and in real time testing information streams. Currently, JRSS stacks have installed for the NIPRNet (Non-classified Internet Protocol Router Network). It has planned also to install the stacks for the SIPRNet (Secret Internet Protocol Router Network). 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 9**). By 2019, it has planned to transfer to these stacks all cybersecurity programs. In nowadays, these programs are located in more than 400 places over the world [13].

The DISN and DoD Component enclaves provide the two main network transport elements of the DODIN (Department of Defense Information Network) with the interconnecting JRSS role as shown in **Figure 10**.

5.1 Shortcoming with the GSM-O project

On June 2012, Lockheed Martin won the largest tender for managing the DISN network - Global Services Management-Operations (GSM-O) project. The essence of the GSM-O contract was to modernize DISN management system taking into account the USCYBERCOM security requirements. The cost of work was 4.6 billion dollars for 7 years.

In 2013, the GSM-O team began to study the current state of the DISN management. There are four management centers: two centers in the US - at the AB Scott (Illinois) and Hickam (Hawaii) and two more - in Bahrain and Germany. They are responsible for the maintenance and uninterrupted operation of all Pentagon computer networks. The work is very laborious: there are 8100 computer systems in more than 460 locations in the world, which in turn have

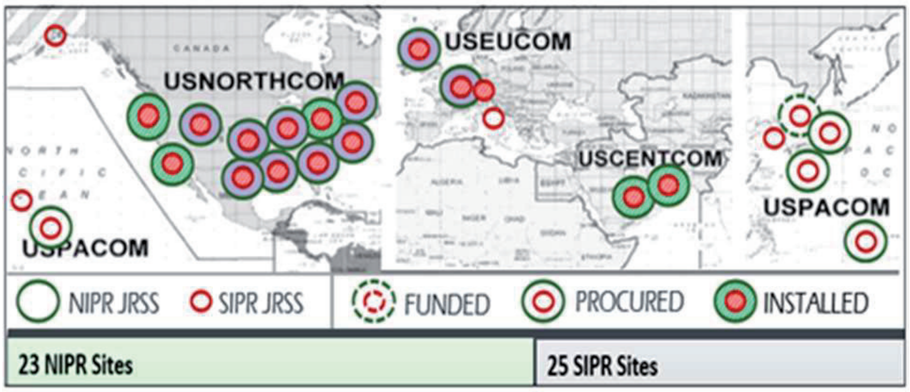

Figure 9.
JRSS current and planned deployments [14].

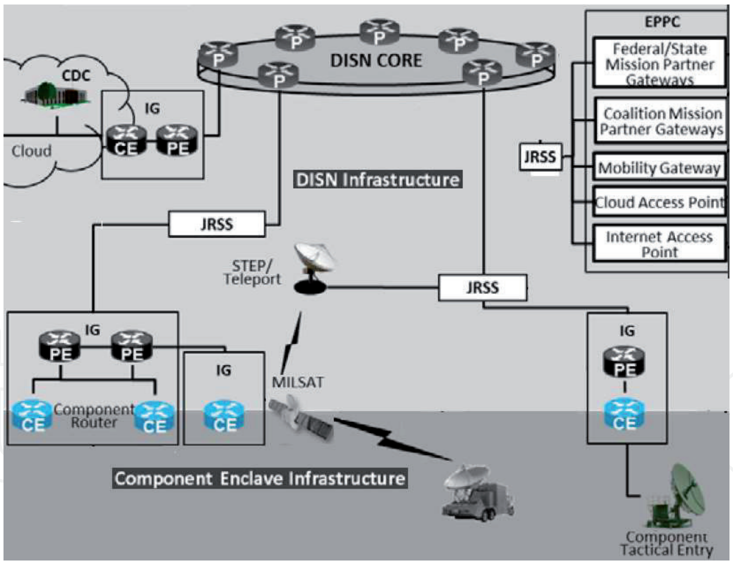

Figure 10.
The leading role of JRSS in DODIN transport [15].

connected by 46,000 cables. The first deal was to consolidate the operating centers - from four to two, namely, to expand the US centers by closing the centers in Bahrain and Germany.

In 2015, the telecommunications world had shocked by the news: Lockheed Martin is not coping with GSM-O project, not able to upgrade of the DISN network management. Lockheed Martin has sold its division “LM Information and Global Solutions” to the competing firm Leidos. One can assume that the failure of the work was most likely due to the inability to recruit developers. New generation of software makers are not familiar with the ‘old’ circuit switching equipment and are not capable to combine it with the latest packet switching systems. The more, they should take into account the never cybersecurity requirements [16].

5.2 The crucial JRSS failure

This failure is much more scandalous. During several last years, the GAO criticized Pentagon’s budget, particularly paying attention to JRSS budget. Many tests regarding JRSS effectiveness were unsuccessful, they were not able to reduce the number of cyber threats [17].

Despite the strong 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 [18].

Could be fulfilled this Pentagon’s grandiose JRSS plan? The complexity of the task, in particular, characterizes the set of requirements for potential JRSS developers, named in the invitations to work for Leidos. The requirement list includes work experience of 12–14 years and knowledge of at least two or more products from ArcSight, TippingPoint, Sourcefire, Argus, Bro, Fidelis XPS, and other companies. In reality, it is extremely hard work to combine all these software complexes for cyber defense. The more, these high-level software developers should work in top-secret environment.

It turned out that the project has a significant critical flaw: JRSS equipment is too S-L-O-W, the time for information stream processing is too long. It sounds like a sentence on the fate of the JRSS project [19]. Despite of that, the JRSS is going on.

5.3 Could Leidos cope with GSM-O II?

On October 2018, the Defense Information Systems Agency has released a final solicitation for the potential 10-year 6.52 billion dollars project Global Solutions Management-Operations (GSM-O II). The contract winner is Leidos. GSM-O II is a single award contract designed to provide a full global operations and sustainment solution to support DODIN/DISN [20].

The key GSM-O II attributes include the cybersecurity defense of the DISA enterprise infrastructure and Joint Regional Security Stacks aids in the support to enhance the mission (?).

Now we are looking for Leidos success (or failure). It is yet unclear and 10-year period, of course, is a rather long time. Could Leidos cope with GSM-O II?

6. On JEDI cloud strategy and artificial intelligence initiative

The Defense Department's never initiative concerns the cloud strategy. The foundation of cloud initiative is the general-purpose Joint Enterprise Defense Infrastructure (JEDI) [21]. The strategy emphasizes a cloud hierarchy at DOD, with JEDI on top. Many fit-for-purpose military clouds, which include MilCloud 2.0 run by DISA, will be secondary to the JEDI general-purpose cloud.

On April 10, 2019, the Department of Defense confirms that Amazon and Microsoft are the cloud contract winners. The competitors Oracle and IBM are officially out of the race for a key 10 billion dollars defense cloud contract.

Could be the JEDI Cloud Strategy successful? A key technological difficulty for the JEDI project is interoperability of clouds (**Figure 11**). The Pentagon's JEDI cloud strategy leaves a series of unanswered questions that could be reasons for disasters in the future [22].

For internal interoperability, the strategy lays out the correct goal, common data and application standards. There are the 500+ clouds already used within the Pentagon. They have own data formats. Now they need to migrate and interoperate onto the unique JEDI platform.

The next unanswered question regards the JEDI cloud's external interoperability. It concerns a future conflict situation. Would America's allies need to use the same cloud provider (e.g., Microsoft) and the same data-formatting practices as the DoD? The strategy does not discuss these long-term issues.

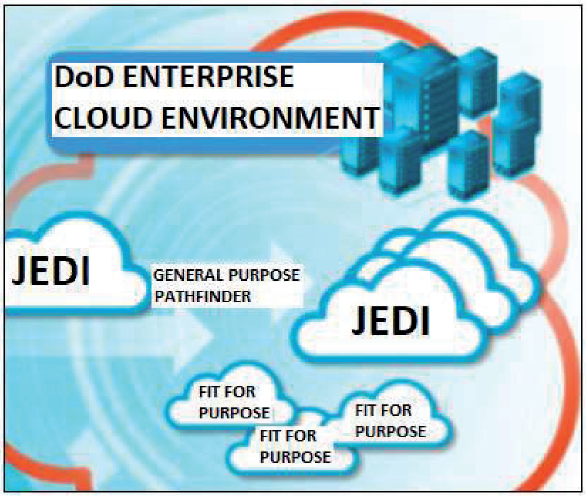

Figure 11.
DoD pathfinder to hybrid cloud environments [21].

The cloud strategy has started in 2015 by establishing the Defense Innovation Unit (DIU). This DoD organization has founded to help the US military make easier and faster use of innovative commercial technologies. The organization has headquartered in Silicon Valley (California) with offices in Boston, Austin, and some more. The next step – the establishing of Joint Artificial Intelligence Center as a focal point of the DoD Artificial Intelligence Strategy [23].

Taking into account the potential magnitude of Artificial Intelligence's impact on the whole of society, and the urgency of this emerging technology international race, President Trump signed the executive order "Maintaining American Leadership in Artificial Intelligence" on February 11, 2019. That document has launched the American AI Initiative. This was immediately followed by the release of DoD's first-ever AI strategy [24].

Artificial intelligence - this is really one great idea, if it happens be successful. Could it have more success than JRSS initiative?

7. Conclusion: do not touch what works

US Army Regulator fights for IP technology but, honesty speaking, unsuccessfully. The Army regulator recognizes in 2017 [25] that there is 'old' equipment on the network: time-division multiplex equipment, integrated services digital networking, channel switching video telecommunication services. According to the document [25], all these services will use IP technology, at least, in the nearest future. As an example, name the instructive claim regarding DRSN:

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.

In conditions of cyberwar, no reason to be surprised that the Defense Red Switch Network (DRSN) will use 40 years old ISDN technology for long time yet, 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 both the United States Armed Forces and the NATO Allies (**Figure 12**). The network has maintained by DISA and has secured for communications up to the level of Top Secret.

"Red Phone" (Secure Terminal Equipment, STE) uses ISDN line for connections to the network. "Red Phone" operates at a speed of 128 kbps. There is the slot at the

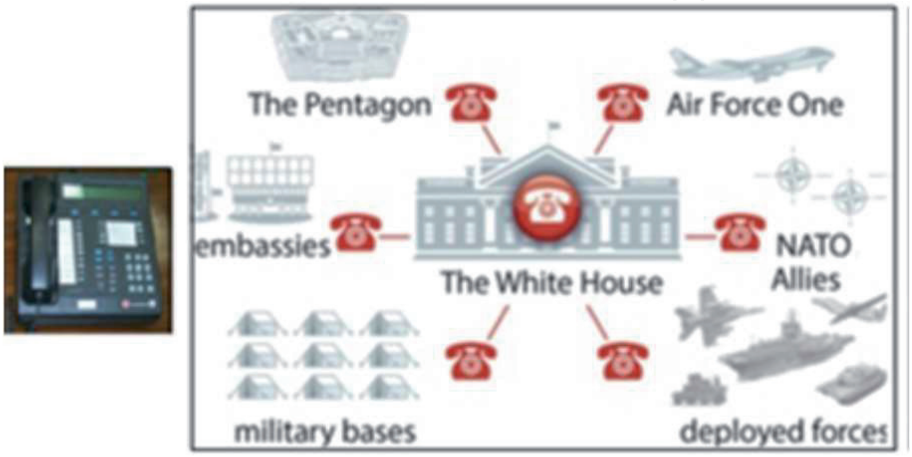

Figure 12.
Secure terminal equipment; note slot in front for crypto PC card (left). The DRSN architecture (right) [25].

bottom right serving for a crypto-card and four buttons at the top - to select the priority of communications. The STE is the primary device for enabling security. It may be used for secure voice, data, video, or facsimile services.

As we have mentioned above citing the AT&T view [1], the DoD today still has analog, fixed, premises-based, time-division multiplexing and seems could remain for unpredictable period according to the well-known software developers slogan: “Don’t touch what works”. In conditions of cyberwar, the very transition to internet technologies in telecommunications seems doubtful. Thus, we conclude that the long-term channel-packet coexistence seems inevitable, especially in the face of growing cyber threats.

Abbreviations

AI	artificial intelligence
AIN	advanced intelligent network
AS-SIP	assured services session initiation protocol
CS	capability set
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
GAO	Government Accounting Office
IP	internet protocol
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
MG	media gateway
MGC	media gateway control
NIPRNet	non-classified internet protocol router network
RFC	request for comments
SIP	session initiation protocol
SIPRNet	secret internet protocol router network
SS7	signaling system protocol #7
SSA	single security architecture
UC	unified capabilities
TDM	time division multiplexing

Author details

Manfred Sneps-Sneppe
Ventspils International Radio-astronomy Centre, Ventspils University of Applied Sciences, Ventspils, Latvia

*Address all correspondence to: manfreds.sneps@gmail.com

References

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

[2] 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. United States Government Accountability Office. October 2018

[3] Osborn Ch. Defense Information Systems Network (DISN). An Essential Weapon for the Nation's Defense. Infrastructure Directorate. 16 May 2018. [Internet]. Available from: http://www.disa.mil› Symposium/ [Accessed: 2020-10-14]

[4] Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. 30 May 1995. [Internet]. Available from: http://waffenexporte.de/NRANEU/others/jp-doctrine/jp6_0(95).pdf/ [Accessed: 2020-10-14]

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

[6] Chao W. W. Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters. In: Proceedings of MILICOM, 1999. IEEE.

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

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

[9] U.S. Army Unified Capabilities (UC) Reference Architecture (RA). Version 1.0. 11 October 2013.

[10] U.S. Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP). Errata-1, July 2013 [Internet]. Available from: http://www.defense.gov/news/newsarticle.aspx?id=122949/ [Accessed: 2020-10-14]

[11] U.S. Department of Defense. Unified Capabilities Master Plan (UC MP), October 2011.

[12] U.S. Department of Defense. Information Enterprise Architecture Unified Capabilities. Reference Architecture. Version 1.0 January 2013

[13] Metz D. Joint Information Environment Single Security Architecture (JIE SSA). DISA. 12 May 2014. [Internet]. Available from: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ [Accessed: 2020-10-14]

[14] JRSS Deployments [Internet]. Available from: https://c.ymcdn.com/sites/alamoace.site-ym.com/resource/resmgr/2017_ace/2017_speakers/2017_AACE_Keynote_Presentations/doc_keynote_Yee.pdf / [Accessed: 2020-10-14]

[15] DoD Instruction 8010.01. Department of Defense Information Network (DODIN) Transport. September 10, 2018. [Internet]. Available from: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ [Accessed: 2020-10-14]

[16] Corrin A. Leidos-Lockheed merger changes the face of federal IT. Federal Times. February 5, 2016. [Internet]. Available from: https://www.federaltimes.com/it-networks/2016/02/05/

leidos-lockheed-merger-changes-the-face-of-federal-it/

[17] Cyberscoop. Available from: https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/ [Accessed: 2020-10-14]

[18] Williams L.C. DOD CIO: JRSS set for 2019 completion. Mar 05, 2018. Available from: https://fcw.com/articles/2018/03/05/jrss-completionmiller. aspx/ [Accessed: 2020-10-14]

[19] Williams L. C. Is it time to rethink JRSS? Feb 01, 2019. Available from: https://defensesystems.com/articles/2019/02/01/jrss-pause-report-williams.aspx/ [Accessed: 2020-10-14]

[20] Edwards J. DISA Issues Final RFP for $6.5B GSM-O IT Telecom Support Recomplete Contract. October 16, 2018. Available from: https://www.govconwire.com/2018/10/disa-issues-final-rfp-for-6-5b-gsm-o-it-telecom-support-recompete-contract/ [Accessed: 2020-10-14]

[21] Williams L. C. DOD cloud strategy puts JEDI at the center. Feb 05, 2019. Available from: https://defensesystems.com/articles/2019/02/06/dod-cloud-strategy.aspx/ [Accessed: 2020-10-14]

[22] Keelan F. The Pentagon's JEDI cloud strategy is ambitious, but can it work? March 21 2019. Available from: https://www.c4isrnet.com/opinion/2019/03/21/the-pentagons-jedi-cloud-strategy-is-ambitious-but-can-it-work/ [Accessed: 2020-10-14]

[23] Department of Defense. DoD Cloud Strategy Readiness for Artificial Intelligence (Al). December 2018.

[24] U.S. Department of Defense. Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity, February 12, 2019. Available from: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf/ [Accessed: 2020-10-14]

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