On Network Functions Virtualization and Hybrid Circuit-Packet Switching

Manfred Sneps-Sneppe
Ventspils University of Applied Sciences
Ventspils, Latvia
manfreds.sneps@gmail.com

***Abstract*—A main goal of the paper is to discuss the world telecommunications strategy in transition to the IP world. Particularly, we analyze the network functions virtualization and network slicing from the viewpoint of shifting from circuit switching to packet switching in telecommunications. As a case, we are passing through three generations of American military communications: (1) The implementation of signaling protocol SS7 and Advanced Intelligent Network, (2) Transformation from SS7 to IP protocol and, finally, (3) The extremely ambitious cyber security issues. In Conclusion, we consider one hybrid circuit-packet proposal for Defense Red Switched Network and ask the crucial question, relating the Defense Information System Network transition to IP world: is it possible at all?**

I. INTRODUCTION

Network functions virtualization (NFV) is a network architecture concept that uses the IT technologies to virtualize network node functions into building blocks and to create communication services. A virtualized network function may consist of one or more virtual machines running different software and processes, on top of standard high-volume servers, instead of having custom hardware appliances for each network function. NFV include virtual session border controller, virtualized load balancers, firewalls, intrusion detection devices and WAN accelerators. Network slicing is a specific form of virtualization that allows multiple logical networks to run on top of a shared physical network infrastructure. The intent of network slicing is to be able to partition the physical network at an end-to-end level to allow optimum grouping of traffic, isolation from other tenants, and configuring of resources at a macro level. Fig. 1 shows the main idea of 5G architecture - network slicing. There are three traffic flows: Mobile Broadband (MBB) - very high throughput, MTC – large connection density, URLLC - ultra-low latency. Different services are served through different network slices.

A main goal of the paper is to discuss the world telecommunications strategy in transition to the IP world. We consider the challenges of the shifting from circuit switching to packet switching in the coming era of VNF. As a case, we are considering American military communications passed three generations of transformation: from signaling SS7 and intelligent networks to IP protocol and, finally, to the extremely ambitious plans of cyber security of networks. Note that DISN (Defense Information System Network) is one of the largest the most openly documented company. We have been discussed some shortcomings on the way of the DISN digital transformation and the network slicing role in this process. In our previous papers [2, 3], we have made already attempt to touch the DISA networks modernization issues. Here we continue the idea in the context of NFV initiative.

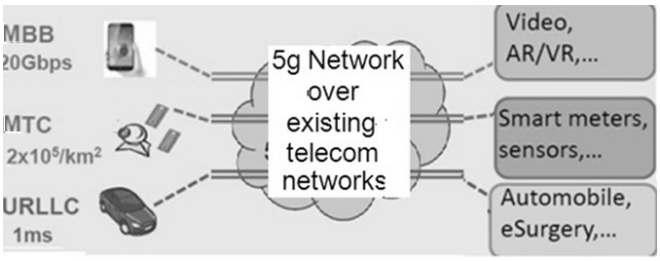

Fig.1.The modified idea of 5G architecture: network slicing [1]

The rest of the paper is the following. In Section II, we discuss the NFV basics. Then we are passing through three generations of DISN: implementation of signaling SS7 and Advanced Intelligent Network (Section III), transformation to IP protocol (Sections IV and V) and, finally, the extremely ambitious plans of cyber security (Section VI). In Conclusion (Section VII), we consider one hybrid circuit-packet proposal for DRSN and ask the crucial question – the DISA transition to IP world: is it possible at all?

II. NFV BASICS

The 5G System architecture consists of the following three types of equipment (Fig. 2):

1) six common network functions (NF) in multiple slices:

- Network Slice Selection Function (NSSF)
- Unified Data Management (UDM)
- Network Exposure Function (NEF)
- Network Repository Function (NRF)
– Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)

2) five slice specific NFs (each slice contains all these NFs):

- Policy Control Function (PCF)
- Application Function (AF)
- Session Management Function (SMF)

ISSN 2305-7254

- User Plane Function (UPF)

- (Radio) Access Network ((R)AN)

3) two separate components:

- User Equipment (UE)

- Data Network (DN), e.g. operator services, Internet access or 3rd party services, including the existing telecom networks.

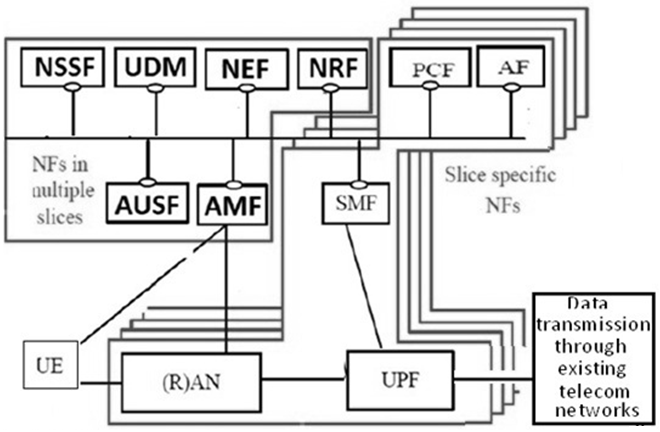

Fig. 2. 5G functional architecture: non-roaming case [4]

Network slicing is based on QoS Flows (Fig. 3). The 5G QoS model supports:

(1) QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and

(2) QoS Flows that do not require guaranteed flow bit rate (Non-GBR QoS Flows).

The QoS Flow is the finest granularity of QoS differentiation in the PDU Session (PDU - Protocol Data Unit). A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System (5QI). User Plane traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment (e.g. scheduling, admission threshold).

Table 1. Mapping of 5QI values to QoS Characteristics (Extract of Table 5.7.4-1 from TS 23.501 [4])

5QI value	Resource Type	Packet Delay	Packet Error Rate	Example Services
B	Delay Critical GBR	5 ms	10-5	Remote control
1	GBR	100 ms	10-2	Conversational Voice
2	GBR	150 ms	10-3	Conversational Video
65	GBR	75 ms	10-2	Mission Critical Push To Talk Voice
5	Non-GBR	100 ms	10-6	IMS Signaling
	Non-GBR	300 ms	10-6	Video TCP-based

Note that each User Equipment UE has up to eight channels having different QoS features (up to eight QoS Flows). The 5G architecture expects the underlying networks and base stations to ensure the required QoS characteristics (such as packet delay, packet loss) without specifying how (at least, by now).

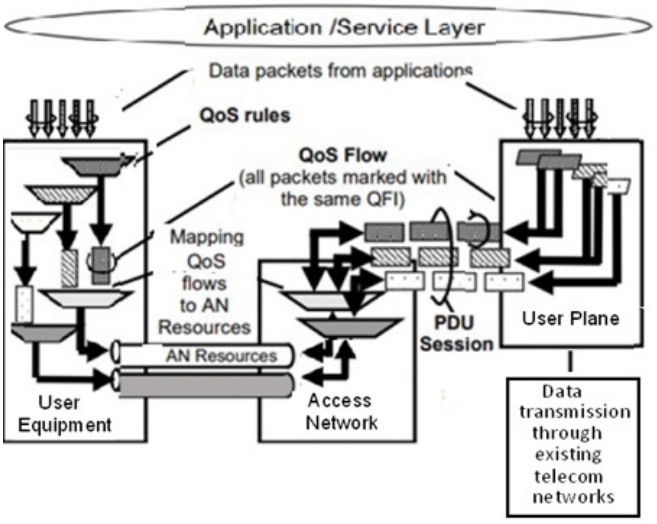

Fig. 3 The principle for classification and User Plane marking for QoS Flows and mapping to AN Resources

On 5G standards. The first phase of 5G specifications in Release-15 will be completed by April 2019 to accommodate the early commercial deployment. The second phase in Release-16 is due to be completed by April 2020. In IP networks, QoS mechanisms such as DiffServ exist for QoS Differentiation, but these are not widely used end-to-end in public networks.

The Internet Engineering Task Force (IETF) has started to examine how the underlying IP network will implement network slices. Protocols like DiffServ and VPN support network slicing like features. The IETF is still debating which protocols, existing or new, will be developed for network slicing [5]. By August 2018, the IETF had eleven active Internet-Drafts [6] examining issues surrounding network slicing. Several of these documents describe “enhanced VPNs” (or VPN+) that comprises an approach to achieve network slices.

III. DISN JOINT VISION 2010: SS7 AND AIN

Up to now, the main military communications networks of the Pentagon are circuit-switched networks:

(1) DSN - Defense Switched Network,

(2) DRSN (Defense Red Switched Network) - for the top secret government communications,

(3) DVS - video conferencing network (DISN VIDEO).

Two highly important message transmission networks are working over TCP/IP protocols:

(4) SIPRNet (Secret Internet Protocol Router Network) - to transmit sensitive information,

(6) NIPRNet (Non-classified Internet Protocol Router Network) is a network used to exchange unclassified but important service information between "internal" users.

In this article, we use the novel open DISA (Defense Information Systems Agency) documents, particularly: Department of Defense (DoD) Information Enterprise Architecture [7, 8], 916-page document describing DoD Unified Capabilities (UC) Requirements [9], 295-page description of the UC framework for the army [10].

Let's give a short historical insight on telecommunication evolution using the Defense Information Systems Network (DISN) as a case. The 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.

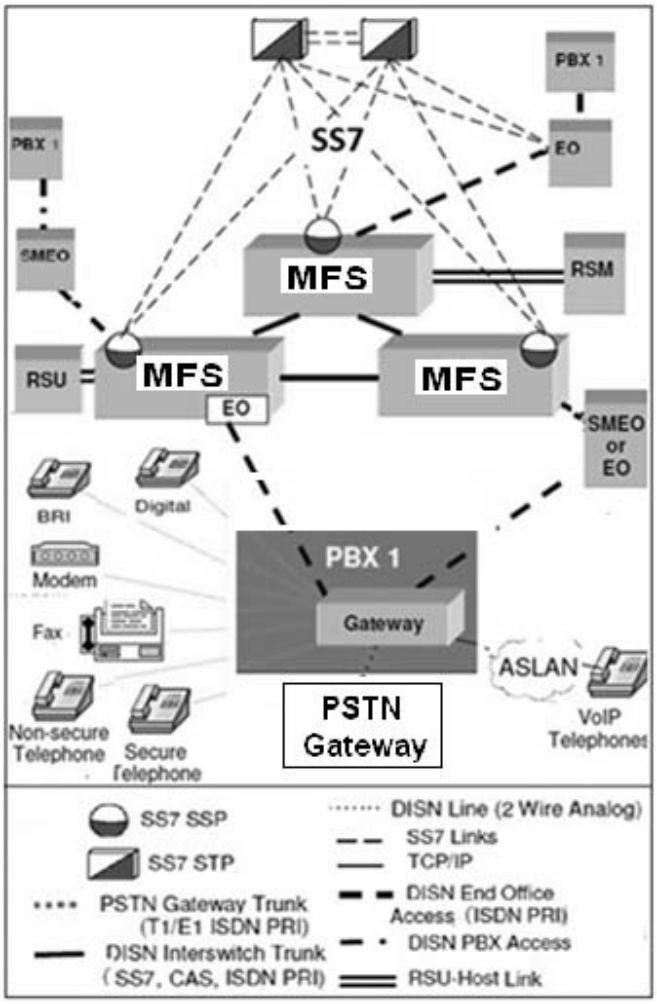

Fig. 4. The simplified DISN view (Avaya PBX1 testing) [12

In 1996, DISA approved "Joint Vision 2010" - a strategic development plan for US military departments for a 15-year period. DISA 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 "old" developments of Bell Labs, namely, on the telephone signaling protocol SS7 and on the Advanced Intelligent Network (AIN) [11]. SS7 protocols have been developed at Bell Labs since 1975 and in 1981 were defined as ITU standards. (Note, that the Bell System was dismembered in 1983.)

The SS7 network is, figuratively speaking, the nervous system of DISN up to resent time (see the upper part of Fig. 4) [12]. The SS7 network is connecting the channel mode MFS (MultiFunctional Switches). That is, within the DISN network, the connections are established by means of SS7 signaling and, in the periphery, devices of any type are used (Fig. 5).

As Fig. 5 shows, the DISN devices are using different protocols: 4-wire (4W); classified LAN (ASLAN); ISDN BRI; Internet telephony (VoIP); Video-conferencing (VTC); proprietary protocols. Despite the fact that all new terminal equipment what appears is largely of IP type, SS7 network nevertheless retains its central place. From this, we make an important conclusion: the presence of the SS7 network does not prevent the transition to IP protocols, but rather the opposite - it facilitates the transition to packet switching, makes it step by step.

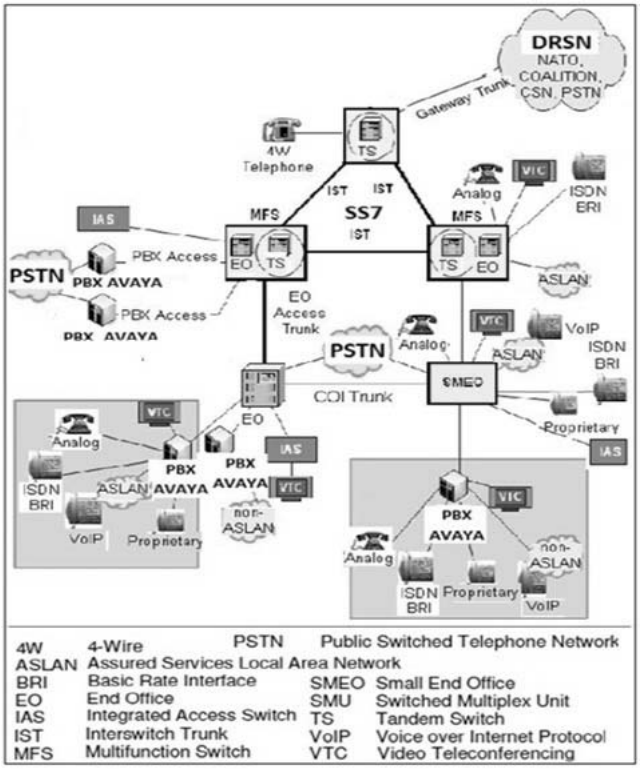

Fig. 5. The current DISN state in more detail [12]

Shortcoming Nr.1. DISA has facing many shortcomings during the transition to IP world. From the very beginning of Joint Vision 2010 program, Lockheed Martin was responsible for the AIN. The emergence of new military equipment and new services requires the continuous improvement of AIN. This is evidenced by the invitation to work in Lockheed

Martin (Fig.6). In the long list of vacancies, the first place takes the search for analysts of multifunctional information systems for DISA. From the applicants are required skills to develop new services for AIN and docking the AIN network with equipment from CISCO, Juniper, etc. Veterans with 28 years experience were invited also. Young professionals who grew up in a web programming environment seem unable to support and develop existing AIN networks built on circuit switching technology.

Industry Job Title	Mult Functional Information Systems Analyst
Job Description	Provides engineering and technical expertise on all issues relating to the specified telecommunications networks/information systems within the DISN. Applies specialized knowledge of military unique features, specifically built into the network and its subtending hardware and software, to ensure appropriate support to the warfighter's requirements. Implements or extends advanced intelligent network features into the network/system.
Basic Qualifications	Requires expertise in one or more of the following devices/vendors: CISCO, Juniper, Promina, Safenet, Ciena, Sycamore, or Ericsson.
Security Clearance	Top Secret

Fig. 6. Systems Analyst Lockheed Martin jobs available (in 1998)

VI. Joint Vision 2020: Transition to IP Protocol

Only four years have passed since the "Joint Vision 2010" plan was launched, as lobbyists of Internet technologies persuaded the Pentagon leadership in updating the weapons program, and a document "Joint Vision 2020" appeared. In 2007, Pentagon published a fundamental program [13], in which we find three main points:

- First, to build a single Global Information Grid (GIG),
- Second, the network should be focused on network-centric war concept,
- Third, and most important, GIG must be built on the basis of IP protocol as the only means of communication between the transport layer and applications.

The most important step for DISN modernization is the replacing of channel switching MFS by packet switching routers - Multifunctional SoftSwiches (Fig. 7).

MFSS acts as a media gateway (MG) between TDM channels and IP channels. The media gateway is controlled by the MGC via H.248 protocol. The Signaling Gateway (SG) provides communication between CCS7 and SIP. The Service Control Function plays the leading role here. SCF is cooperating with as many as 19 servers and using a lot of protocols: SOAP, HTTP, LDAP, SQL, RADIUS, DIAMETER, etc.

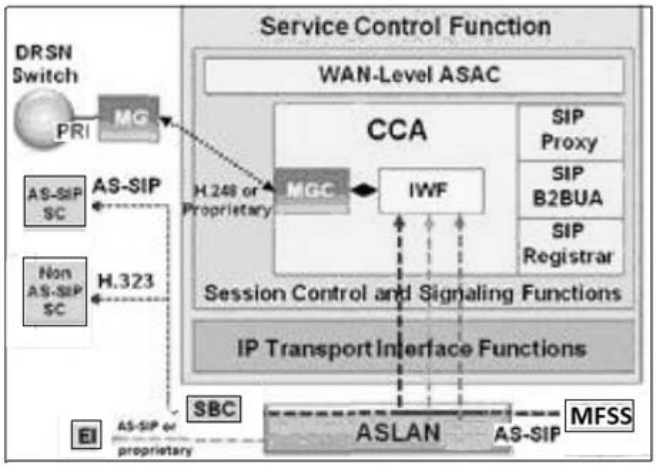

Fig. 7. Reference model for Multifunction SoftSwitch (MFSS) [10]

Take an attention to the AS-SIP protocol. The well-known SIP, as a signaling protocol, does not have the ability to break into ongoing calls, e.g. emergency calls, to support Multi-Level Precedence and Preemption (MLPP) calls. For these reasons, a new protocol - Assured Services SIP protocol was invented [14]. To implement Unified Capabilities requirements [10], AS-SIP got many features and had required support by up to 200 RFCs. The AS-SIP protocol turned out to be very cumbersome: the ordinary SIP uses only11 other RFC standards.

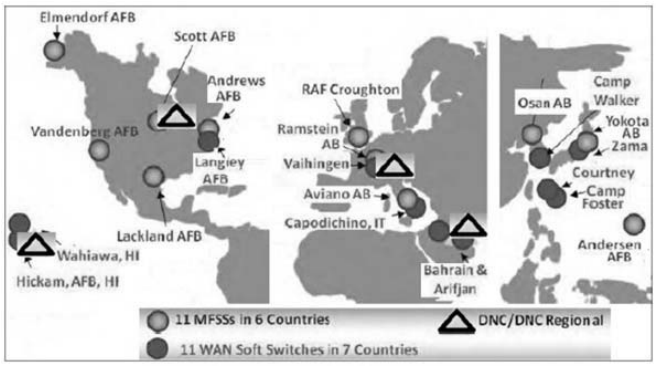

Fig. 8. CISCO has installed 22 major softswitches all around the NATO world [15]

CISCO - the largest contractor of the Pentagon – has installed 22 large softswitches at military bases around the world (Fig. 8). There are two types of top-level softswitches: WAN SS = Wide Area Network SoftSwitch, MFSS = MultiFunction SoftSwitch. Besides, there are also four Global Network Support Center (GNSC) - two in the US (at Scott Air Base and Hawaii), as well in Germany and Bahrain. This new UC architecture offers any soldier and army employee a rich set of communication tools: e-mail, chat, voice, video, search, and all this is available at a single user address and in a secure environment.

Shortcoming Nr.2. In June 2012, Lockheed Martin won the largest tender for managing the DISN network (Global Services Management-Operations, GSM-O). The essence of the GSM-O contract is the modernization of the management system for cybersecurity requirements. The cost of work is a

huge amount - 4.6 billion dollars for 7 years. The co-executors of the GSM-O contract are *AT&T, ACS, Serco, BAE Systems, Mantech* and a number of other enterprises.

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 - 8,100 computer systems in more than 460 locations in the world, which in turn are connected by 46,000 cables. The first deal was to upgrade the GIG management system. It was decided to consolidate the operating centers - from four to two): GIG network management centers are expanding at the air bases Scott (Illinois) and Hickam in Hawaii, but the centers in Bahrain and Germany are being closed.

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.

V. The target architecture of the DISN network

The target architecture of the future DISN network contains two levels: Tier 0 and Tier 1 (Fig. 9). The Tier 0 cluster is responsible for the invulnerability of the entire DISN network. It contains three Tier 0 softswitches connected by the ICCS (Intra-Cluster Communication Signaling) protocol, which automatically updates their databases.

A cluster is essentially one distributed softswitch. It is required that the delay in the exchange of database contents does not exceed 40 ms. Since the signal transmission takes 6 microseconds per 1 km, the distance between softswiches cannot exceed 6,600 km (1,860 miles). At the lower, second level of the DISN network, Tier 1, there are two types of local networks: a secure ASLAN using the AS-SIP protocol and a traditional LAN using the H.323 protocol (for video conferences). Thus, the secure hybrid network DISN provides voice and video over IP.

Shortcoming Nr.3. The DRSN (Defense Red Switch Network) network is a dedicated telephone network that provides control of the US Armed Forces (Fig. 10). DRSN is some kind of "birthmark" in the future AS-SIP environment.

"Red Phone" (Secure Terminal Equipment, STE) connects to the network via ISDN line and operates at a speed of 128 kbps. For data transfer and facsimile, an RS-232 port is built-in. Note the slot at the bottom right - for a crypto-card and four buttons at the top - to select the priority of communications.

VI. About cyber security

In October 2010, the US Army Cyber Command was set up. USCYBERCOM is now a part of the Strategic Command along with strategic nuclear forces, missile defense and space forces. This recognizes that cyberspace is the same field of military operations as land, sea and air. The US Cyber Command will also be oriented toward conducting offensive operations, and for this purpose a special unit of combat operations (Combat Mission) has been created.

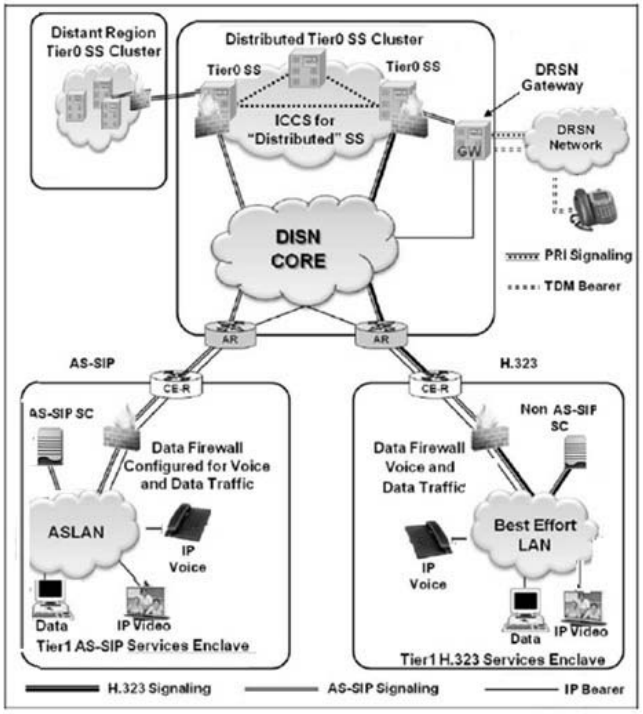

Fig. 9. The target architecture of DISN [10]

Fig. 10. Architecture of the government network DRSN and "Red phone"

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, and Joint regional security stacks (JRSS) are the main components of the JIE environment that provide a unified approach to the structure of cyber security and the protection of computers and networks in all military organizations.

JRSS equipment, in fact, are IP-routers with a complex set of cyber protection software. The typical physical NIPR JRSS stack is comprised of as many as 20 racks (!). Currently, JRSS stacks are installed for the NIPRNet. It is planned also to install the stacks for the SIPRNet. The first JRSS stack was installed and successfully operated at the military base of San Antonio, Texas. In 2014, 11 JRSS stacks were 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 (Fig. 11). By 2019, it is planned to transfer to these stacks cyber security programs, which are now deployed in more than 400 locations [17].

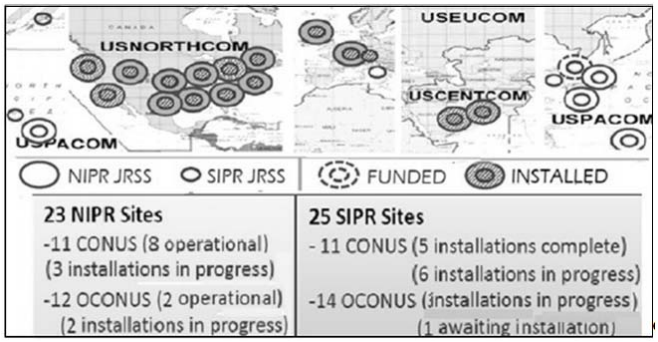

Fig. 11. JRSS Current and Planned Deployments: CONUS = the 48 CONtiguous States and the District of Columbia, OCONUS = Outside Continental United States [17]

During several last years, the Government Accounting Office (GAO) has paying an attention to Pentagon's budget, particularly to JRSS budget. The JRSS's 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". The Pentagon, which started spending on the JRSS in fiscal year 2013, estimates it will have spent over $900 million by the end of the current fiscal year 2016; and will spend approximately $1.6 billion more in fiscal years 2017 through 2021 [18].

Despite the GAO critics, DoD continues the JRSS initiative: it is more than halfway complete. 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 is slated to be completed by the end of 2019 [19].

Shortcoming Nr.4. Under the pressure of GAO critics, in January 2018, the Pentagon's chief weapons tester said the Department of Defense should stop deploying its new network security platform, known as Joint Regional Security Stacks. Why? 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 [20].

Could the Pentagon's grandiose plans be fulfilled? 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 of cyber defense. How to combine them?

"Until DOD determines how it will document the costs of its JIE effort and officials and congressional committees are provided accurate information about expected costs, they are limited in their ability to provide oversight for performance and make effective resource decisions," the audit concludes.

VII. Discussion on DISA transition to IP world: is it possible at all?

Our goal concerns telecom network evolution. Many shortcomings on DISA move from TDM to IP world mentioned above raise doubts about the feasibility of this ambitious project at all. Moreover, honesty speaking, hopes for success of 5G technology and network functions virtualization as well as network slicing for military communications are until also very illusory. Therefore, it seems reasonable to make a compromise, namely, to look for some hybrid circuit-packet switching solution.

The most important shortcoming among above mentioned is a channel switching mode for Defense Red Switched Network. Recall that DRSN is used for the top secret government communications and each "Red" phone has own crypto-card ensuring top-level security.

Fig. 12 shows such a compromise solution. On basis of the existing VPN (virtual private network) approach, two VPNs could be built: VPN SS7 and VPN TDM flow. These two VPNs are able to fulfill the DRSN requirements for transmission of voice, data and pictures, not hoping for an unclear future of AS-SIP signaling and for unified security architecture success, and the more – taking in the mind the scandalous history with JRSS "racks".

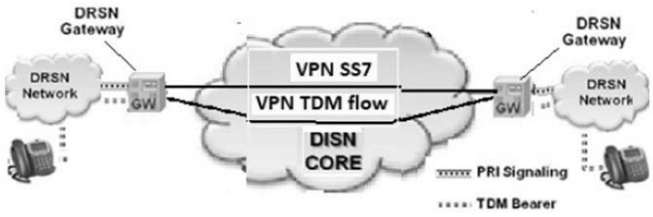

Fig. 12. A hybrid circuit-packet switching solution for DRSN

Summing up, the most fundamental question about the ubiquitous DISN transition to IP technology arises. Many DISA shortcomings leads to the following: the future of the very transition to IP technology everywhere in the world is unclear.

Acknowledgment

We would like to thank anonymous reviewers. Their critical remarks, we hope, help to make the paper much more understandable for young people generation being far from circuit switching era.

References

[1] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, T. Miyazawa, "Consideration on Automation of 5G Network Slicing with Machine Learning", *In Proc. ITU Kaleidoscope 2018: Machine learning for a 5G future*. Santa Fe, Argentina, 26-28 November 2018.

[2] Manfred Sneps-Sneppe, "On telecommunications evolution: Pentagon case and some challenges", *In Proc. 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. 6-8 Nov. 2017. Munich, Germany.

[3] Manfred Sneps-Sneppe, Dmitry Namiot, "Time to Rethink the Power of Packet Switching". *In Proc 23d Open Association FRUCT Conference,* 14-16 Nov. 2018, Bologna, Italy.

[4] *ETSI TS 123 501 V15.2.0 (2018-06) 5G; System Architecture for the 5G System (Release 15)*.
[5] D. King, "Network slicing at the IETF", August 23, 2018. Web: https://metro-haul.eu/2018/08/23/network-slicing-at-the-ietf/ Retrieved: Jan, 2019.
[6] Web: https://datatracker.ietf.org/doc/search?name=slic&activedrafts=on & Retrieved: Jan, 2019.
[7] *Department of Defense Information Enterprise Architecture (IEA)*, Vol. I & II, Version 2.0, July 2012.
[8] *Department of Defense Information Enterprise Architecture Unified Capabilities Reference Architecture.* Version 1.0, January 2013.
[9] *Department of Defense Unified Capabilities Requirements (UCR 2013)*, January 2013.
[10] U*.S. Army Unified Capabilities (UC) Reference Architecture (RA).* Version 1.0. 11 October 2013.
[11] B.T. Bennet, "Information Dissemination Management. Advanced intelligent Network services for department of Defense", *in Proc. MILCOM,* 1999.
[12] *Special Interoperability Test Certification of Avaya S8300D. DISA Joint Interoperability Test Command (JTE),* 17 April 2012.
[13] *Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Department of Defense,* June 2007.
[14] *Department of Defense Assured Services (AS) Session Initiation Protocol (SIP).* Jan 2013; Errata-1, July 2013 Web: http://www.defense.gov/news/newsarticle.aspx?id=122949 Retrieved: Jan, 2019.
[15] Cisco Communication Strategy. Web: https://www.cisco.com/web/strategy/docs/gov/Cisco_LSC_Overview_Jan2011.pdf Retrieved: Jan, 2019.
[16] Web: https://c.ymcdn.com/sites/alamoace.siteym.com/resource/resmgr/2017_ace/2017_speakers/2017_AACE_Keynote_Presentations/doc_keynote_Yee.pdf Retrieved: Jan, 2019.
[17] Web: https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/ Retrieved: Jan, 2019
[18] L.C. Williams, "DOD CIO: JRSS set for 2019 completion". Mar 05, 2018 Web: https://fcw.com/articles/2018/03/05/jrss-completionmiller. aspx Retrieved: Jan, 2019.
[19] M. Gruss, "The debate about whether DISA's new security system is ready for primetime", Febr 7, 2018 Web: https://www.c4isrnet.com/show-reporter/afceawest/2018/02/08/the-debate-about-whether-disas-new-securitysystem-is-ready-for-primetime/ Retrieved: Jan, 2019.