Netheads vs Bellheads – an Unceasing Scramble

Manfred Sneps-Sneppe

***Abstract*— The confrontation of these two technologies - packet-switching and circuit-switching – has a long history, and it seems to be incessant. It had started with Asynchronous Transfer Mode technology in the 1990s. The breakup of the Bell System marked a key loss in Bellheads camp but not defeat. The confrontation is going on in areas of telecommunication switches and emergency services. Starting in the late 2010s, AT&T is replacing older 4ESS switches with N4E-N1B switches developed by Nokia Bell Labs. Only in 2017, AT&T has been selected by the First Responder Network Authority to build and manage the first broadband network dedicated to America's police, firefighters, and emergency medical services. The most acute struggle unfolded in the area of defense information systems. According to a recent GAO report (in 2018), the U.S. weapons systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities. The move to the IP world is slow: there is too much risk of losing control over defense forces. Till now the Defense Red Switch Network (DRSN) uses 40 years old ISDN technology. The reason for this is unsolved cyber security issues.**

I. Introduction

The slogan "Netheads vs Bellheads" was coined in 1996 by Steve Steinberg [1] reporting the debate around Asynchronous Transfer Mode (ATM) technology. This was a war between packet-switching fans and circuit-switching fans. Bellheads are the original telephone people. These are engineers and managers who grew up in the Ma Bella era and continue to follow the Bell System practices. They believe in problem solving with reliable hardware methods and strict quality control. They believe that ATMs have been an elegant solution for the 21st century. Opposed to the Bellheads are the Netheads, young people who are combining computers to create a worldwide Internet. These engineers see the telecommunications industry as one more relic that will be overturned by the digital computing process.

The basics of ATM are not, in themselves, terribly revolutionary. The core techniques were developed independently in CNET (France Telecom's research lab) and Bell Labs in the 1970s. The main idea was to design a universal architecture that could transport data as well as voice at high speeds and that would make the most efficient use of the network's resources. The telecom establishment - the Bellheads - are solidly behind ATM. In fact, most of the major carriers are building ATM networks capable of carrying voice, data, and video.

Still, many IP proponents - the Netheads-say IP switching is the way to go. The biggest Nethead complaint about ATM is its transmission overhead. ATM partitions traffic into 53-byte cells, each of which contains a 5-byte header. That translates to an overhead of about 10 percent. But the "cell tax" is even higher, for instance, 64-byte Ethernet packets-a common packet size in LAN communications-require two ATM cells for transmission, with the second cell going more than half empty. In this case, the cell tax is close to 40 percent.

Now - 25 years after the battle for ATM, it is the right time to recall the history of the decline of America's telecom industry during this long period [2]. Then, the Netheads took over the Bellheads and this victory, probably, was frightful for America's telecom industry.

As America transitions to 5G wireless networks, the U.S. community sees the Chinese telecom giant Huawei as a systemic security risk. There is still deep concern that eventually Huawei will dominate global markets, displacing the other major 5G providers, Europe's Ericsson and Nokia (Fig. 1). One shall ask why there is no American telecom equipment company. After all, in the 1970s the two largest telecom equipment manufacturers were U.S. companies: Western Electric and ITT. Even in the late 1990s, the two largest were still based in North America: Lucent and Nortel (headquartered in Canada). By 2008, however, Nortel was bankrupt, and Lucent was sold off to Alcatel, a French company, which was later bought by Finland's Nokia.

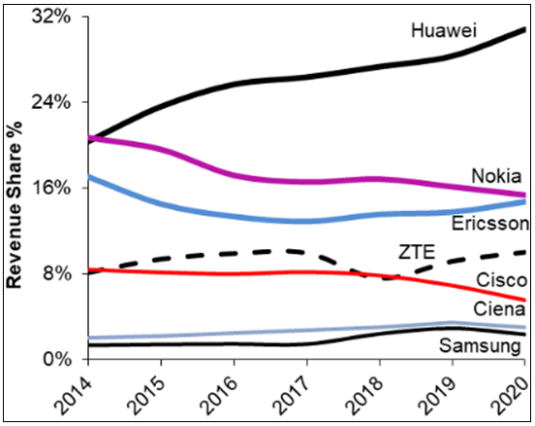

Fig. 1: Total Telecom Equipment Market 2020 [3]

The author of [2] in conclusion states: *"It is probably too late to resurrect an American equipment industry. But, it is possible that so-called software-defined networks will be transformative and shift innovation from hardware, where China leads, to software, where the U.S. is competitive."* Below we discuss some US telecom failures due to software issues basically. We should justly say the hope regarding the

US competitiveness in the software area seems a bit too optimistic.

II. The breakup of the Bell System – a key loss in Bellheads camp

What happened in the US? The industrial growth depends on technological advancement. Much has been written about Bell Labs as the world's most successful industrial laboratory [2]. From its founding in 1925 to its divesture in 1995, it averaged one patent per day, and by 1995 it was averaging three patents per day. It was responsible for some of the most important inventions of the twentieth century, including cellular technology, digital switches, fiber optics, lasers, the transistor, solar cells, satellite communication, undersea cables, and the UNIX operating system. Nine Nobel Prizes have been awarded for work completed at Bell Laboratories.

Recall some of Bell Labs' achievements in the telecom area.

1/1A Electronic Switching Systems. The Number One Electronic Switching System (1ESS) was the first large-scale stored program control (SPC) telephone exchange in the Bell System. It was manufactured by Western Electric and was first placed into service in May 1965. The switching fabric was composed of a reed relay. The #1ESS switching system generally serves between 10,000 and 65,000 lines. The #1ESS was updated in 1976 with the introduction of the 1A processor and beyond was known as the #1AESS switch. It was in service from 1976 to 2017 – for more than 40 years (!).

In the 1990s, the #1AESS was augmented in many central offices with the more powerful computer. This allowed for connection to Signalling System Seven (SS7) networks[1].

ISDN. Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the digitalized circuits of the public switched telephone network. Work on the standard began in 1980 at Bell Labs and was formally standardized in 1988.

The entry level interface to ISDN is the Basic Rate Interface (BRI), a 128 kbit/s service delivered over a pair of standard telephone copper wires. The 144 kbit/s overall payload rate is divided into two 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel or data channel). This is sometimes referred to as 2B+D. BRI-ISDN is very popular in Europe

The other ISDN access available is the Primary Rate Interface (PRI), which is carried over E-carrier (E1) with 32 channels in most other countries. Each channel provides transmission at a 64 kbit/s data rate. With the E1 carrier, the available channels are divided into 30 bearers (*B*) channels, one data (*D*) channel, and one timing and alarm channel. This scheme is often referred to as 30B+2D.

One of ISDNs' successful use-cases was in the videoconference field. The H.320 standard for audio coding and video coding was designed with ISDN in mind, and more specifically its 64 kbit/s basic data rate.

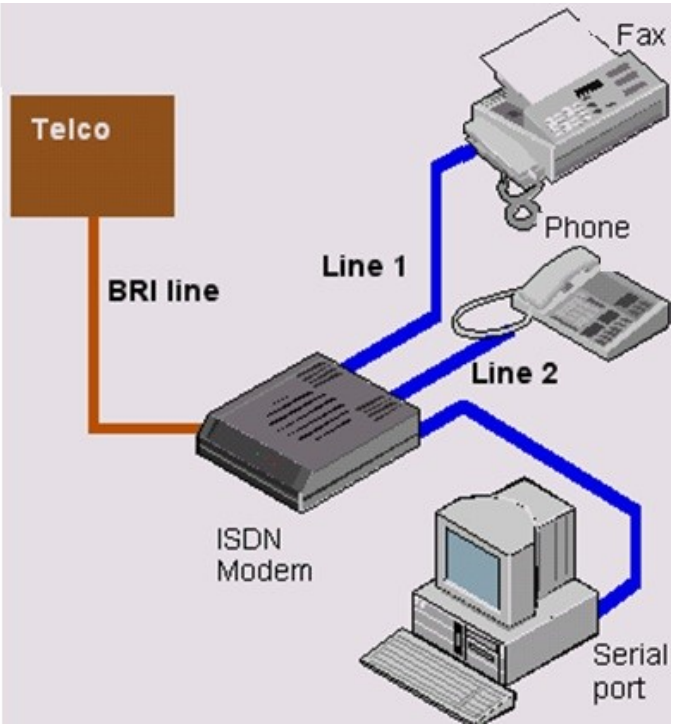

Fig. 2: The typical ISDN use

Signaling System 7. Signalling System No. 7 (SS7) is a set of telephony signaling protocols developed in 1975, which is used to set up and tear down telephone calls in most parts of the worldwide public switched telephone network (PSTN). The protocol also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other services. The protocol was introduced in the Bell System in the 1970s for signaling between No. 4ESS and No. 4A crossbar toll offices. SS7 is a signaling system that separates the content of telephone calls from the information used to set up the call (signaling information).

An SS7 network is composed of service switching points (SSPs), signaling transfer points (STPs), and service control points (SCPs). The SSP gathers the analog signaling information from the local line in the network (endpoint) and converts the information into an SS7 message. These messages are transferred into the SS7 network to STPs that transfer the packet closer to its destination. When special processing of the message is required (e.g., 800 calls), the STP routes the message to an SCP. The SCP is a database that can use the incoming message to determine other numbers and features that are associated with this particular call. This is so-called advanced intelligent network (AIN) architecture.

[1] Let us recall a tip from the USSR telecom industry. The toll exchange Kvartz has been prototyping after No1 ESS and produced in 44 installations (a production set down after the breakup of the USSR).

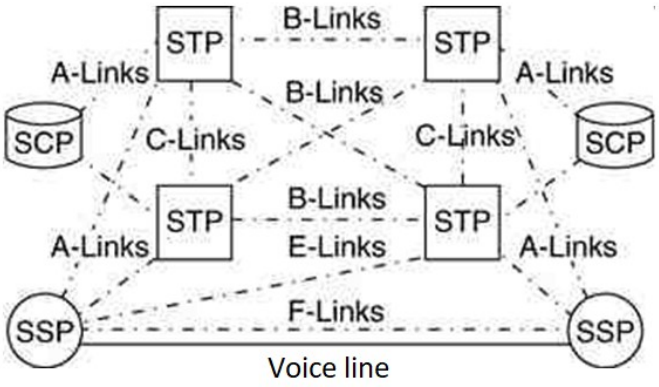

Fig. 3: SS7 Diagram

Figure 3 shows the basic structure of the SS7 control signaling system. There are multiple redundant links between switches, switching points, and network databases to help ensure the reliability of the telephone network. The links between points in the SS7 system have different functions and message structures. Access links (A-links) are used for access control between EOs and SCPs. Bridge links (B-links), cross-links (C-links), and diagonal links (D-links) interconnect STPs. Extended links (E-links) are optionally used to provide backup connections from an EO to the SS7 network. Fully associated links (F-links) share (associate with) the connection between EOs.

4ESS. The No. 4 Electronic Switching System is a telephone electronic switching system that was the first digital electronic toll switch introduced by Western Electric for long-distance switching. It was introduced in 1976, to replace the 4A crossbar switch.

Previous tandem switching systems, primarily the No. 4 Crossbar switch, used analog voice signaling. The decision to switch to a digital voice format (Pulse Code Modulation, PCM) was controversial at the time, both from a technical and economic viewpoint. At the peak of the product's lifetime in 1999, AT&T employed 145 4ESS switches in its long-haul network, and several were owned by various Regional Bell Operating Companies (RBOCs). Over 140 4ESS switches remained in service in the United States in 2007.

Nokia Bell Labs (from 2007). The Nokia N4E-N1B (New 4ESS) is the ATCA-based next-generation toll switch for AT&T. Starting in the late 2010s and continuing in the early 2020s, AT&T is replacing older 4ESS switches with N4E-N1B switches and is also adding new N4E-N1B switches in places where there was no 4ESS previously.

III. On Emergency Services: A Thorns Road to the IP World

From 9-1-1 to NG9-1-1. In traditional emergency calls 9-1-1 environment (Fig. 4), the public can primarily make only emergency voice calls and Teletype calls (by deaf or hearing-impaired persons). Only minimal data has been delivered with these calls, such as automatic number identification, subscriber name, and Automatic Location Identification, when available.

The move to the Next Generation 9-1-1 started in 1999 by Public Law 106-81 [5]. According to the USDOT views [6], the NG9 1 1 System is an evolutionary transition to enable the general public to make a 9 1 1 "call" from any wired, wireless, or Internet Protocol (IP)-based device, and allow the emergency services community to take advantage of Enhanced 9 1 1 (E9 1 1) for mobile users. By enabling the public to access 9 1 1 service through virtually any communications device, the NG9 1 1 System provides a more direct ability to request help or share critical data with emergency services providers from any location. In addition, call takers at the Public Safety Answering Points (PSAP) will be able to transfer emergency calls to another PSAP and forward the location and other critical data, such as text messages, images, and video with the call (Fig. 5). Up to now, unfortunately, the 911 system is built on an infrastructure of analog technology.

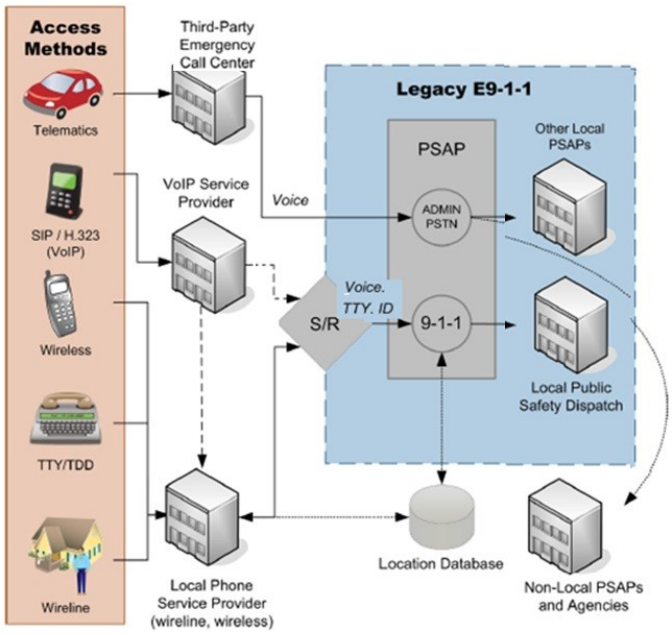

Fig. 4: Call Flow and Elements in Today's 9-1-1 [4]

The worries to implement the NG-911 initiative. Some 20 years were lost without any success in the NG-911 initiative. Why? In 2014, the Federal Communications Commission issued the Order [7] to kick-start the process for a diverse set of experiments and data collection initiatives to evaluate, how customers are affected by the historic technology transitions – from a network based on time-division multiplexed (TDM) circuit-switched voice services running on copper loops to an all-IP network.

Worthy to note, that the First Responders are extremely conservative people. About 30 years ago, the telecommunications industry rolled out Signaling System 7 (SS7) technology. In-band MF signaling was replaced with out-of-band signaling controlled by a computer database. However, the transition from multi-frequency (MF) signaling to SS7 signaling did not always flow easily. In the early 1990s, there was a spate of SS7 outages that cascaded throughout large portions of the country.

Due to SS7 failures, customers were without service for long periods of time; communities were isolated; airplane control system was put at risk, and public safety agencies were often inaccessible to citizens unless the 911 emergency calling services remained on MF signaling. E.g., in Maryland alone, some 5 million people were without telephone service for an entire day (June 26, 1991) because of an SS7 failure. The January 1990 AT&T outage resulted in more "than 65 million blocked call attempts". The Pacific Bell and Bell Atlantic SS7 failures together accounted for more than 30 million blocked call attempts. The FCC categorized these incidents as "catastrophic".

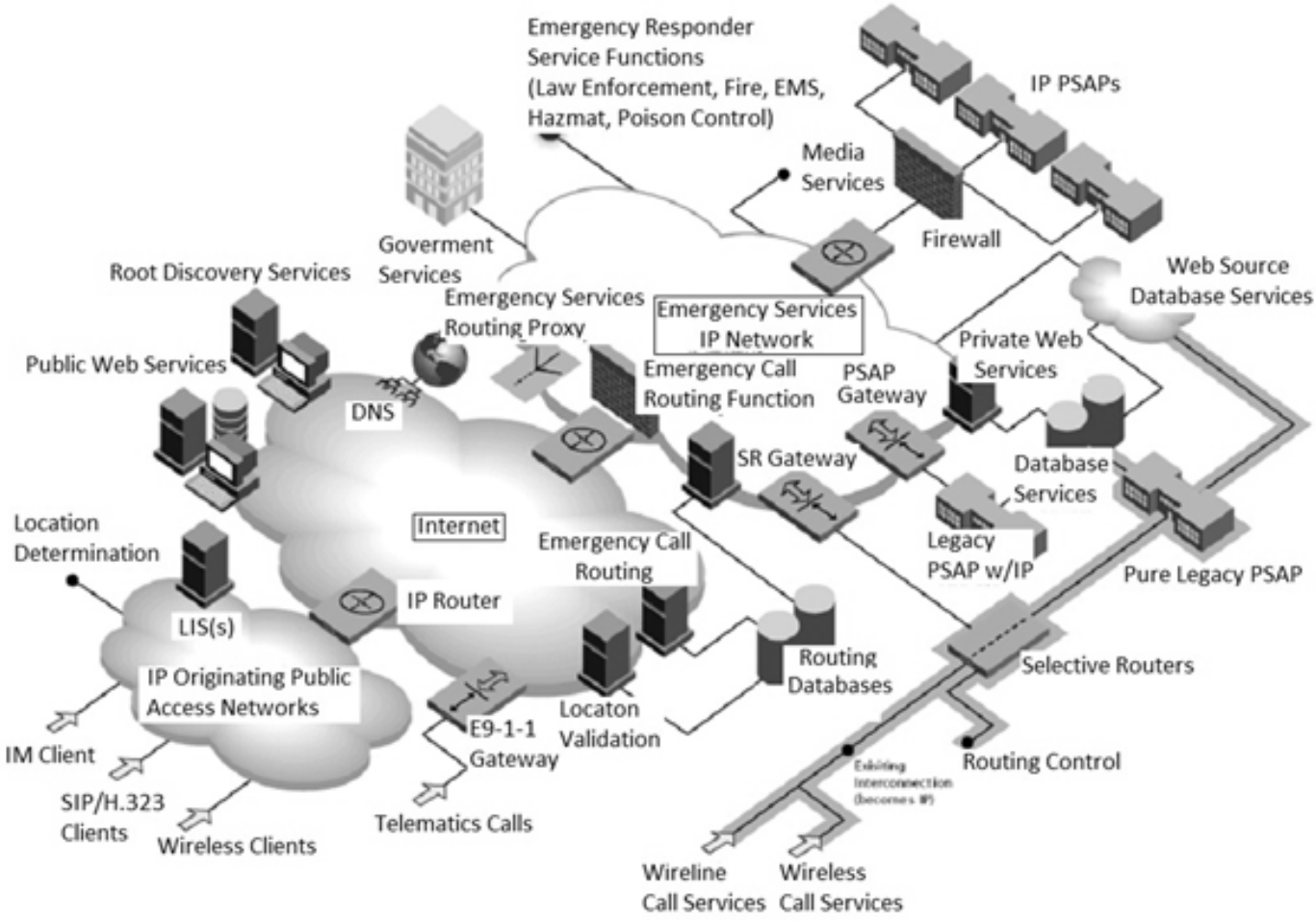

Fig. 5: NG9-1-1 Model [4]

Because of the risk to public safety posed by SS7 failures, the Industry generally left the 911 emergency calling network on the less-efficient MF signaling protocol or, if already converted, returned to MF signaling. Point out once more, SS7 is in service for as long as 30 years but not for emergency calls.

On the complexity of emergency network software. It is time to keep in mind that, honestly speaking, the emergency network transition to the IP world is rather sophisticated. Name, for example, Telcordia Emergency Services Demo (now Telcordia is a subsidiary of Ericsson). The five companies were involved, as shown in Fig. 6 [8]:

- Telcordia implemented: OMA LOCSIP Technical Specification (Location Client, Location Server, Resource List Server); OMA Presence SIMPLE V2 Specification (Presence Source, Watcher, Presence Server, Resource List Server); GSMA Rich Communication Suite
- FOKUS implemented: 3GPP IMS Emergency Services Specification (3GPP TS 23.267)
- BBN implemented: IETF HELD Specification (HELD Client and HELD Location Information Server (LIS))
- Columbia University: IETF LoST Specification
- MAXWell Lab: WiMAX (IEEE 802.16e Specification)

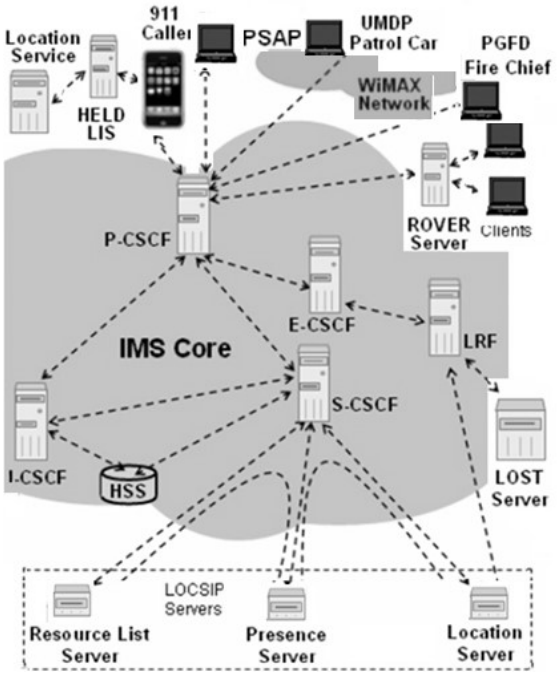

Fig. 6: Telcordia Emergency Services Demo [8]

What is FirstNet? FirstNet was born out of 9/11, namely, FirstNet is an initiative driven by US authorities with a history dating back to the 9/11 terrorist attack in 2001. The First Responder Network Authority (FirstNet) is an independent authority within the U.S. Department of Commerce. The organization's mission is to develop, build and operate a nationwide, broadband network for first responders. In 2012, Congress signed a bill into law that created the FirstNet organization and provided initial funding to build the FirstNet network.

In 2017, a negative article on FirstNet appeared in the *Atlantic*, "The $47 Billion Network. That is Already Obsolete" [9]. According to the U.S. Government Accountability Office, estimates of FirstNet cost range from $12 billion to $47 billion. The article noted the progress in FirstNet as well as in NG9-1-1 development is extremely slow.

To put an end to decades-long interoperability and communications debates and to help keep communities and emergency responders safe, the principle solution was done: FirstNet will use a nationwide 700 MHz spectrum [10]. Public safety broadband (BB) is ranging from 758 MHz to 768 MHz and 788 MHz to 798 MHz. The Narrowband (NB) spectrum is represented by blocks ranging from 769 MHz to 775 MHz and 799 MHz to 805 MHz. This part of the 700 MHz public safety band is available for local public safety entities for voice communication. The law, that established FirstNet, specified the network should be based on LTE technical requirements, at least (Fig. 7).

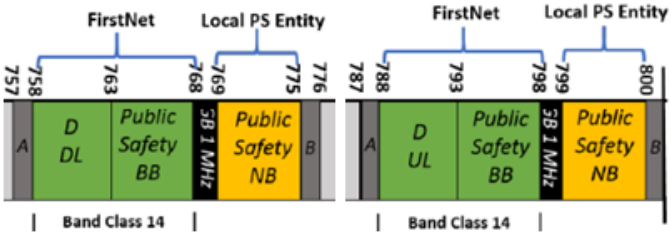

Fig. 7: FirstNet nationwide 700 MHz spectrum (Band Class 14) [10]

FirstNet is responsible for building the enhanced packet core network, a key component for ensuring users have a single nationwide interoperable platform [10]. Essentially, the core serves as a giant umbrella covering all of the United States. The core is connected to radio access networks in each state via the backhaul layer of the network. Initial modeling has shown that tens of thousands of radio base stations are needed to cover at least 99% of the population and the national highway system. Everything from smartphones to laptops, tablets, dongles, and a wide variety of specialty devices will be developed for FirstNet users (Fig. 9). Devices will also have to be secure. Transport Backhaul links carry user traffic, such as voice, data, and video, and signaling from the radio base stations to the core network (Fig. 8).

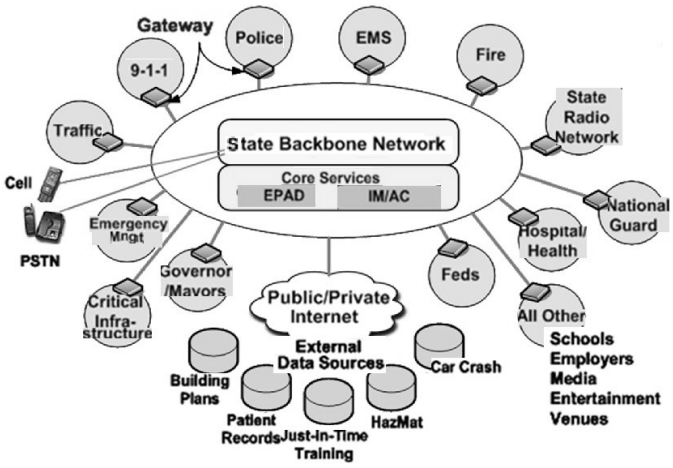

Fig. 8: NG9-1-1 model architecture for a State [10]

AT&T deal. In 2017 [11], AT&T has been selected by the First Responder Network Authority (FirstNet) to build and manage the first broadband network dedicated to America's police, firefighters, and emergency medical services (EMS). The FirstNet network will cover all 50 states, 5 U.S. territories, and the District of Columbia, including rural communities and tribal lands in those states and territories. This is a much-needed investment in America's communications infrastructure to support millions of first responders and public safety personnel nationwide who protect and serve more than 320 million people across the U.S.

Now (as of October 2021) [12], more than 18,500 public safety agencies and organizations, accounting for more than 2.8 million connections nationwide, are on FirstNet, built with AT&T. AT&T has surpassed 95% of our nationwide Band 14 coverage target with the FirstNet Authority. There are now 315+ FirstNet Ready devices and more than 180 apps in the FirstNet App Catalog, which includes a carefully curated category of safety and wellness apps to further support the mental and physical health of first responders. AT&T's FirstNet project is now well ahead of schedule. But, keep in mind, that it is yet a starting step of AT&T's FirstNet project.

On the cybersecurity of NG9-1-1 calls. We are looking now to AT&T future success. FirstNet, built with AT&T, is one extremely huge project. It is comparable to the biggest military projects and, at least, not less important from point of cybersecurity. Let us take a case in parallel.

Despite being at the forefront of technology, according to a recent GAO report [13], the United States weapons systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities. The federal information security (i.e. cybersecurity) needs to improve *"the abilities to detect, respond to, and mitigate cyber incidents",* increase its cyber workforce and increase cybersecurity training efforts. How to say for sure that all vulnerabilities are detected and removed?

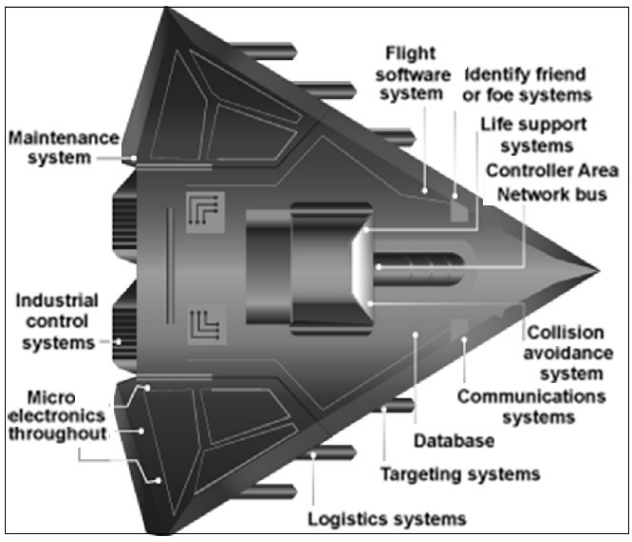

Fig. 9: Embedded software and information technology systems are pervasive in weapon systems (represented via fictitious weapon systems for classification reasons) [13]

DoD weapon systems are more software dependent and more networked than ever before (Fig. 9). From ships to aircrafts, the weapons made available to the DoD are becoming more technologically advanced and use more software and less hardware to control everything from navigation to weapons systems. 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 [14]. This software is developed by hundreds of suppliers. How to check them for cybersecurity? The same is true for the FirstNet system.

IV. On DoD obsolete information networks

AT&T against DoD. According to the AT&T experts' view [15], the Department of Defense (DoD) today still has analog, fixed, premises-based, time-division multiplexing (TDM), and even asynchronous transfer mode (ATM) infrastructure that drains billions of dollars in legacy operations and maintenance expenses from the DoD's annual budget, while unnecessarily exposing the DoD to cybersecurity risks. This aging network architecture is based on point-to-point circuits that require constant hardware maintenance and upgrades.

The current situation is partially a result of defense contracting, not network providers. The roughly 15,000 separate networks that comprise the DoD's network were built by hundreds of different companies that are not in the business of networking. Why should the DoD outsource the operation of networks to contractors whose networks are then managed by AT&T? "*The existing TDM environment is 30 years behind current commercial technologies*", - such is the harsh rebuke of AT&T [1].

US Army Regulator fights for IP technology. A similar kind of harsh sentence of the DoD's activities flows from the Army Regulation document [16] 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. All these services will use IP technology. Name a 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.

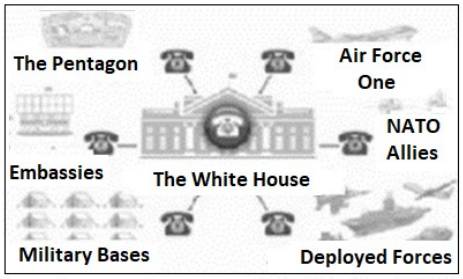

Fig. 10: Scheme of the government network DRSN and "Red phone" [16]

Why is the move to the IP world so slow? Obviously, there is too much risk of losing control over defense forces, much worse than losing a doctor's call. The claims for Internet Protocol architecture seem as of Don Quixote fighting with a windmill. No reason to be surprised that the Defense Red Switch Network (DRSN) uses 40 years old ISDN technology. It looks like some kind of birthmark in the IP environment. DRSN is a dedicated telephone network, which provides global secure communication services for the command and control structure of the United States Armed Forces as well as NATO forces (Fig. 10). The network is maintained by DISA and is secured for communications up to the level of Top-Secret SCI.

"Red Phone" (Secure Terminal Equipment, STE) connects to the network via an 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).

STE sets communicate with systems that use the Secure Communications Interoperability Protocol (SCIP). SCIP is a US standard for secure voice and data communication. It is for circuit-switched one-to-one connections, not packet-switched networks. SCIP was designed by the Department of Defense in cooperation with the U.S. National Security Agency. There are several components to the SCIP standard: key management, voice compression, encryption, and a signalling plan for voice, data, and multimedia applications.

"Joint Vision 2010" plan. In 1996, General Shalikashvili as the Chairman of the Joint Chiefs of Staff approved "Joint Vision 2010" - a strategic development plan for US military departments for 15-year period. "Joint Vision 2010" was focused on achieving dominance across the range of military operations through the application of new operational concepts [17]. Unfortunately, "Joint Vision 2010" met harsh criticism from the US General Accounting Office side just in 1998 [18]. 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.*"

In reality, at that time many shortcomings of military information networks had been revealed. First of all, this was the low level of integration of many hundreds of networks included in DISN, which significantly limits interaction within a single network and hampers effective unified management of all its resources. Under conditions of technological uncertainty, 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 "old" developments of BellLabs, namely, on the telephone signaling protocol SS7 and the Advanced Intelligent Network (AIN). Note that SS7 protocols had been developed at BellLabs since 1975 and in 1981 were defined as ITU standards.

The details we found in one paper from Lockheed Martin Missiles & Space [19] – the well-known Defense contractor. The Advanced Intelligent Network (AIN) was originally designed as a critical tool to offer sophisticated services such as expert operator assistance and directory assistance. Fig. 11 shows the AIN components that operate in the worldwide telecommunication network, as well as how they are deployed in the SS7 backbone: (1) the space Wide Area Network (WAN), (2) circuit switched voice network, and (3) the packet switched terrestrial WAN. The AIN components include the Service Creation Environment (SCE), Service Management System (SMS), Service Control Point (SCP), Service Switching Point (SSP), Intelligent Peripheral (IP), Adjunct, and the Network Access Point (NAP).

The current state of DISN. To illustrate the current DISN architecture we refer to the certification of Avaya S8300D by DISA Joint Interoperability Test Command in 2012 [20]. The tested Avaya S8300D is a Private Branch Exchange (PBX). Its Media Server provides a Voice over Internet Protocol (VoIP)-based integrated voice mail messaging capability for up to 450 light-duty users. The DISN architecture is a two-level network hierarchy consisting of (1) DISN backbone switches MFS and (2) Service/Agency installation switches. The DISN architecture; therefore, consists of several categories of switches including PBXs (Fig. 12). Here MFS – MultiFunctional Switch stands for channel switching electronic exchange.

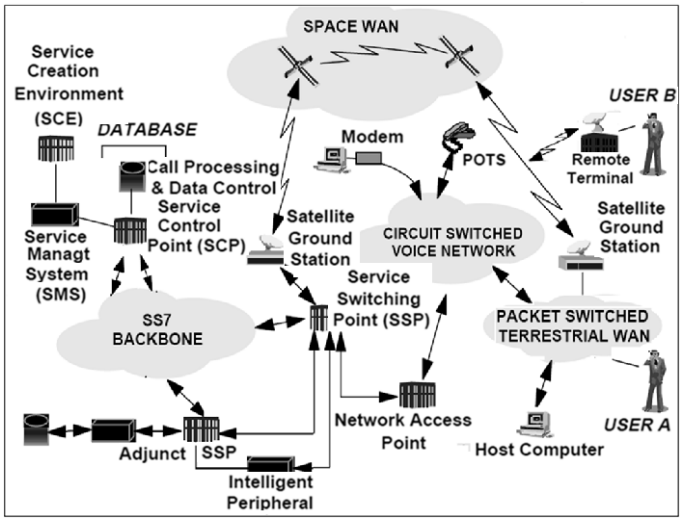

Fig. 11: AIN Service Architecture [19]

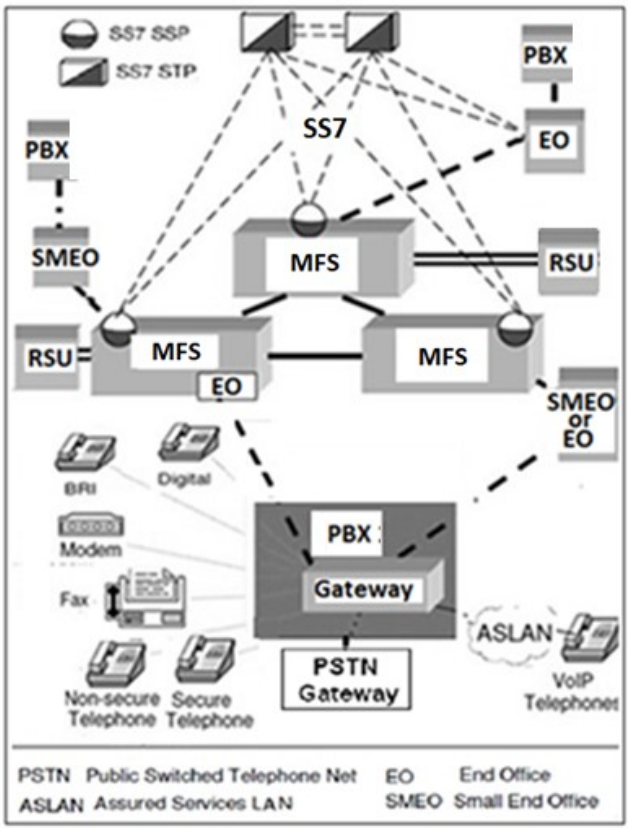

Fig. 12: The simplified DISN view [20]

It is still difficult to predict the time, during which the DISN network will finally switch off from the path initialized by General Shalikashvili and his program Joint Vision 2010.

V. CYBERSECURITY - ACHILLES' HEEL OF THE PENTAGON

Joint Vision 2020 plan: an unpredictable delay. Just a few years later as "Joint Vision 2010" had been introduced, namely, in 2007 a new Pentagon strategy "Joint Vision 2020" appeared. Pentagon published a fundamental program [21], in which we find the most important point: DISN must be built on basis of IP protocol (Fig. 13). AS-SIP protocol should be the only means of communication between the transport layer and applications [22]. It is an extremely hard challenge. Like with any military communications system, security is of the highest importance. The architecture needs to be able to handle all types of classified and unclassified data.

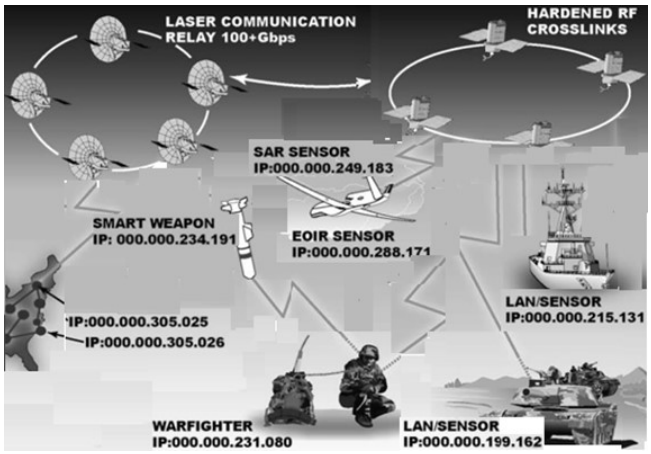

Fig. 13: Joint Vision 2020: Each warfare object has own IP address

The target architecture of the future DISN network contains two levels: Tier 0 and Tier 1 (Fig. 14). 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. 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.

The most important step for DISN modernization is the replacing of channel switching Multifunctional Switches MFS (i.e. electronic exchanges) by packet switching tools - Multifunctional SoftSwiches (Fig. 15). 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 SS7 and SIP. The Service Control Function plays the leading role here. SCF is cooperating with as many as 19 servers and using a plenty of protocols: SOAP, HTTP, LDAP, SQL, RADIUS, DIAMETER, etc. This new 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.

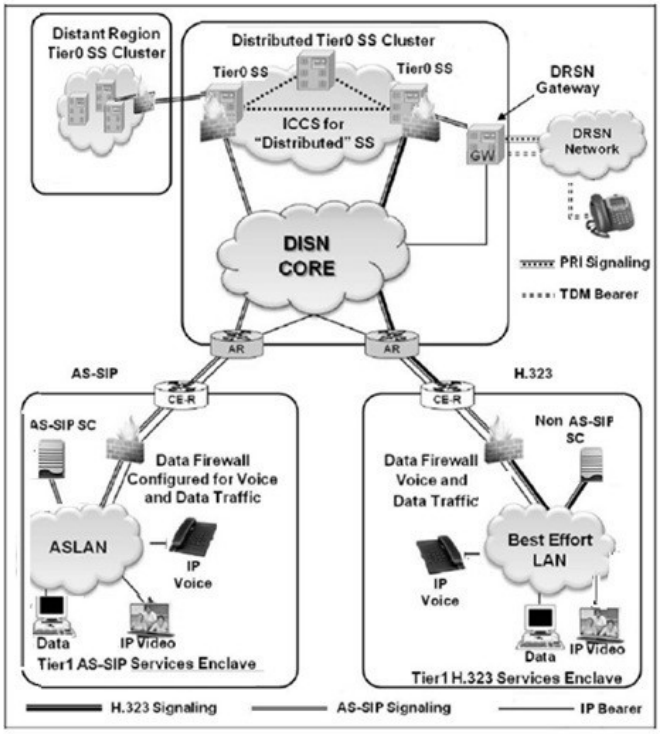

Fig. 14: The target architecture of DISN [22]

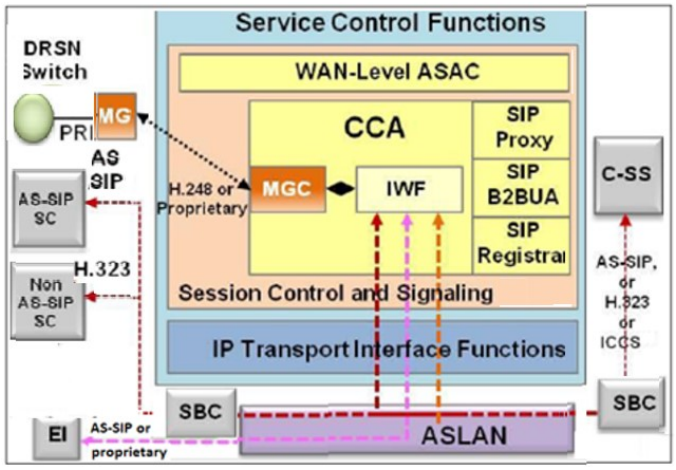

Fig. 15: Reference model for Multifunction SoftSwitch (MFSS) [23]

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 rather cumbersome [22]. The ordinary SIP uses only 11 other RFC standards while AS-SIP has support up to 200 RFCs.

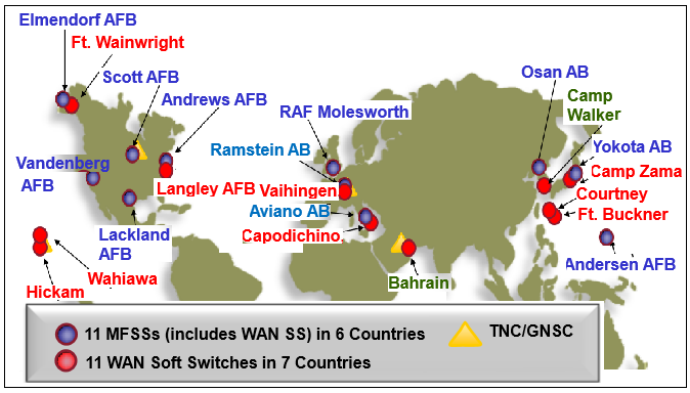

Fig. 16: CISCO plans to install 22 Softswitches [24].

CISCO has installed 22 major softswitches all around the NATO world (Fig. 16). By now, we have no information on whether any single packet switching MFSS is in operation and successfully replaced a channel switching MFS.

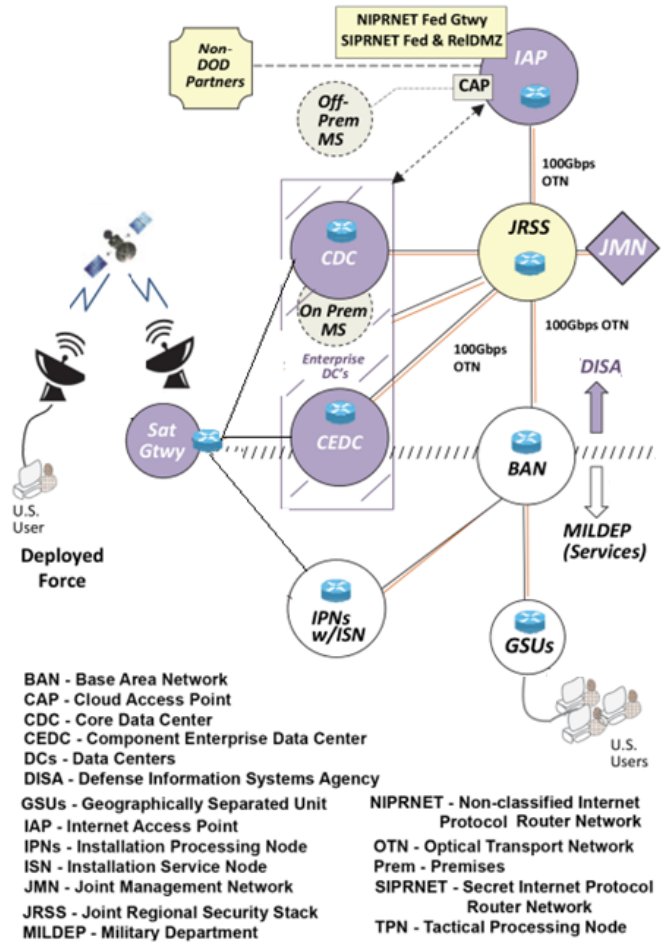

Fig. 17: JIE topology [25]

Joint Regional Security Stacks: a total failure. In October 2010, the U.S. 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. One of Cyber Command's key tasks is Joint Information Environment (JIE) [25]. The very concept of the Joint Information Environment is extremely complex (Fig. 17), and the requirements of cybersecurity make it even more difficult. The essence of the JIE concept is to create a common military infrastructure, and provide corporate services on unified security architecture. Joint regional security stacks (JRSS) are the main components of the JIE environment that provide a unified approach to the structure of cybersecurity and the protection of 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 host of other network security capabilities. 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 and activated 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 work include the installation of 23 JRSS stacks on the NIPRNet service network and 25 JRSS stacks on the secret SIPRNet network (Fig. 18). As of 10 Oct 2018, 5 NIPR sites were installed, 3 of them activated; 19 SIPR sites installed. By 2019, it was planned to transfer cybersecurity programs to these stacks, which are now deployed in more than 400 locations [26].

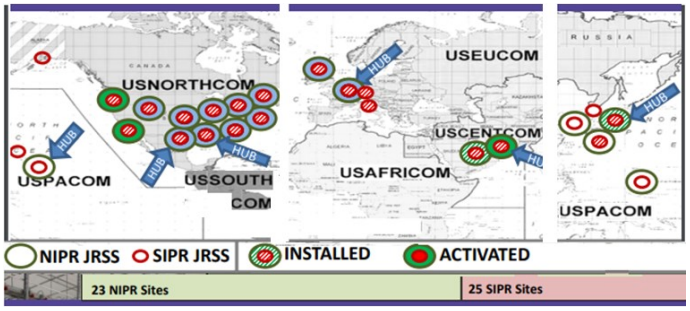

Fig. 18: JRSS current/planned deployments (2019)

During several last years, the GAO has been paying attention to Pentagon's budget, particularly to the JRSS budget. In July 2016, a report GAO-16-593 [27] required more control over the spending of funds for the creation of the Joint Information Environment of the Pentagon. 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. "

In 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. 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 [28]. Despite the GAO critics, DoD has continued the JRSS initiative.

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 (see Fig.21)? How to hire such high-level software developers and for work in a top-secret environment?

More importantly, is the project worth to be doing? The crucial JRSS failure is extremely important: JRSS is too S-L-O-W.

Finally, in November 2021, the Department of Defense chief information officer announced a sunset of the Joint Regional Security Stacks program [29]. Thus, Pentagon pauses the $2 billion cyber security project. As JRSS is phased out, DISA will begin phasing in Thunderdome, its approach and architecture for zero trust networking. This is a newer cybersecurity approach. Thus, the very JIE is under a cardinal revision now. Time will tell if the Thunderdome project and, in turn, the JIE program at all will be successful.

Now is the right time to recall the well-known software developer slogan: "Don't touch what works". The main DISA projects in the telecommunications field (MFSS, JRSS, JIE) have failed. Could software-oriented networks and cloud computing have more success? In conditions of cyberwar, the very transition to internet technologies in telecommunications seems doubtful.

VI. Conclusion

Unsolved cyber security issues may become packet-switching technology failure. Any critical infrastructure such as emergency services or defense weapon systems is becoming more technologically advanced and uses more software and less hardware to control everything. In conditions of cyberwar, the very transition to internet technologies in telecommunications seems doubtful. Could software-oriented networks and cloud computing have more success?

References

[1] Steve G. Steiberg Netheads vs Bellheads. Wired. 1996. https://www.wired.com/1996/10/atm-3/

[2] Robert D. Atkinson. Who Lost Lucent? The Decline of America's Telecom Equipment Industry. American Affairs. 2020. Vol IV, No3: 99-135
[3] Total Telecom Equipment Market 2020. https://www.delloro.com/key-takeaways-total-telecom-equipment-market-2020/
[4] Model State 911 Plan. U.S. Department of Transportation, National Highway Traffic Safety Administration. Version 1.0, February 2013.
[5] Wireless communications and public safety Act of 1999. Public law 106-81. October 26, 1999.
[6] Next Generation 9-1-1 (NG9-1-1) System Initiative. Concept of Operations. The U.S. Department of Transportation (USDOT). Washington D.C. April 6, 2007.
[7] Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report & Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13-5, FCC 14-5 (rel. Jan. 31, 2014).
[8] Mike Loushine et al, "Emergency Services Demo with Location-based Services, IMS, and WiMAX". Telcordia Applied Research, May 11, 2010.
[9] Web; https://www.theatlantic.com/magazine/archive/2016/09/the-47-billion-network-thats-already-obsolete/492764/ Retrieved: Mar, 2019
[10] Phillip Tracy, "Understanding FirstNet, the post-9/11 public safety initiative", August 31, 2016. Web: http://www.rcrwireless.com/20160831/fundamentals/firstnet-tag31-tag99/ Retrieved: Jan, 2022.
[11] AT&T Selected by FirstNet to Build and Manage America's First Nationwide Public Safety Broadband Network Dedicated to First Responders. March 30, 2017. Web: https://about.att.com/story/firstnet_selects_att_to_build_network_supporting_first_responders.html/ Retrieved: Jan, 2022.
[12] FirstNet Surpasses 2.8 Million Connections and Establishes Market Leadership with Law Enforcement. October 27, 2021. https://about.att.com/story/2021/momentous-public-safety-expansion.html
[13] 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.
[14] Ch. Osborn. "Defense Information Systems Network (DISN) An Essential Weapon for the Nation's Defense". 16 May 2018. Web: file:///G:/Pentagon-book+/Osborn_%20DISN%20An%20Essential%20Weapon2018.pdf/ Retrieved: Jan, 2022.
[15] The Defense Network of Tomorrow—Today. AT&T White paper. 2018
[16] Army Regulation 25–13 Information Management. Army Telecommunications and Unified Capabilities. Headquarters Department of the Army Washington, DC. 11 May 2017
[17] Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. 30 May 1995.
[18] Defense Networks. Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals. US General Accounting Office. GAO/AIMD-98-202. July 30, 1998
[19] William W. Chao. Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters, MILICOM, 1999. IEEE
[20] Special Interoperability Test Certification of Avaya S8300D with Gateway 450 (G450). Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), 17 Apr 2012
[21] Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Department of Defense. June 2007
[22] Department of Defense Assured Services (AS) Session Initiation Protocol (SIP). Errata-1, July 2013 http://www.defense.gov/news/newsarticle.aspx?id=122949
[23] U.S. Army Unified Capabilities (UC) Reference Architecture (RA). Version 1.0. 11 October 2013.
[24] Local Session Controller (LSC) Overview https://www.cisco.com/web/strategy/docs/gov/Cisco_LSC_Overview_Jan2011.pdf Retrieved: Jan, 2022.
[25] Joint Information Environment (JIE) https://www.dote.osd.mil/Portals/97/pub/reports/FY2019/dod/2019jie.pdf?ver=2020-01-30-115432-767
[26] JRSS Overview Joint Regional Security Stack https://events.afcea.org/TNAP18/Custom/Handout/Speaker0_Session6936_1.pdf
[27] GAO-16-593. Joint Information Environment: DOD Needs to Strengthen Governance and Management. Jul 14, 2016.
[28] 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, 2022.
[29] The Pentagon is moving away from the Joint Regional Security Stacks https://www.c4isrnet.com/it-networks/2021/11/01/the-pentagon-is-moving-away-from-the-joint-regional-security-stacks/

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