AiMT

Advances in Military Technology
Vol. 14, No. 2 **(2019)**, pp. 263-277
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01248

Cyber Security Challenges in Future Military Battlefield Information Networks

M. Ďulík* and M. Ďulík jr.

Armed Forces Academy of General Milan Rastislav Štefánik, Slovak Republic

The manuscript was received on 21 February 2019 and was accepted after revision for publication on 1 September 2019.

Abstract:

This paper explains the evolution of technology from obsolete military battlefield networks towards the global military battlefield information network from information and cyber security point of view. The authors focus on the threat of the communication medium which is mainly used in military battlefield information networks – the wireless channel, which is the basis of different mobile wireless systems. This paper deals with complex threats to military cyberspace, in which primarily wireless channels may be easily available by the enemy. Employed subnetworks may have different properties. A unifying extended layered model is presented in the article, which in addition to ISO/OSI model spreads cyber threat to geographic and social spheres. The article also shortly illustrates the development of electronic military warfare towards cyber military warfare.

Keywords:

cybersecurity, cyberspace, cyber warfare, electronic warfare, radio networks, security

1. Introduction

The role of communication networks in military operations keeps on growing in importance, with mission areas such as covert special operations, time-critical targeting, command and control and logistics, and all of them heavily rely on networks and network applications. While networks bring the promise of increased flexibility and efficiency for defense organizations, they also present a myriad of new challenges arising from unique operating conditions and environments and the need for a high level of network security. The rapidly increasing dependence on networks requires the clear understanding of these challenges, as well as robust infrastructure which is secure from current and future cyber threats.

* *Corresponding author: Department of Informatics, Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 06 Liptovský Mikuláš 6, Slovak Republic.*
Phone: +421 960 42 30 34, E-mail: miroslav.dulik@aos.sk

For communication, the tactical environment is the most challenging. Fig. 1 presents some fundamental characteristics of obsolete military tactical networks which consist of nodes and communication links connecting them. It is essential to notice that the performance of these nodes and links is not as high as the performance of commercial or fixed networks. On the tactical level, basic communication infrastructure is based on combat network radios, mobile nodes (typically protocol – Transmission Control Protocol/Internet Protocol – TCP/IP) and long-haul Radio Relays (RRL). Bandwidth capacity is relatively low, if compared to commercial wireless technologies. Also, there are some specific military requirements which are not as important in the commercial systems. In this paper, the attention is paid to the part of the global military network deployed at the battlefield.

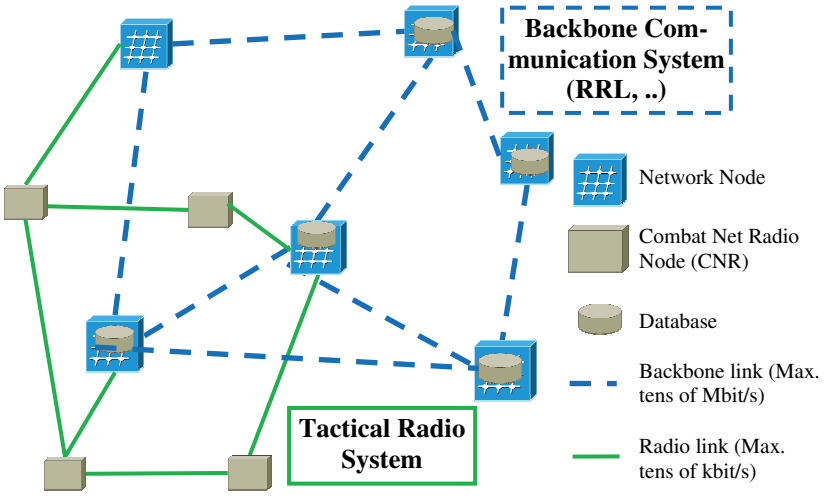


Fig. 1 Architecture of obsolete military tactical networks

Security architectures and controls of obsolete military networks were not designed to face the new threats (for example cyber attacks, remote access to databases ...). Traditionally, the military networks were isolated from other networks, and the access to them was very limited both in terms of geographical areas and the number of authorized users. The main threats were in physical area and obsolete enemy's Electronic Warfare (EW), Fig. 2. In the older systems, security control is often implemented after the network and new service deployment causing potential vulnerabilities and threats.

The development in information and communication technologies and systems toward information sharing near real time leads to the evolution of new doctrines. Military communications and networking are basic stones of Network Centric Warfare (NCW) doctrine [1], which can be summarized in four tenets [2]:

- a robustly networked force improves information sharing,
- information sharing enhances the quality of information and shared situational awareness,
- shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command,
- these, in turn, dramatically increase mission effectiveness.

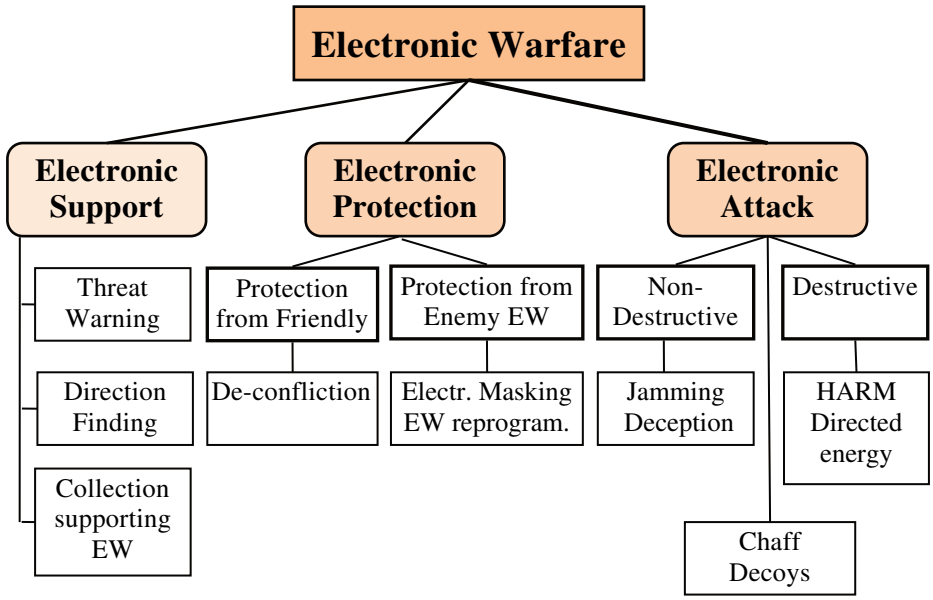


Fig. 2 Three subdivisions of classical electronic warfare [3]

Building a "hardened internet" for military purposes is essential for the realization of the military's NCW vision, which focuses on providing right person with the right information at the right time, at and beyond the battlefield. Some great challenges stand before modern military networks, because they have characteristics that transcend the current state of the art in networking today. The main problems result from the dynamics of military information flow, on top of an underlying infrastructure that is relatively unreliable and time-varying in both location and topology. Problem solution of "hardened internet" nowadays assumed creation of one complex network built from subnetworks – CYBERSPACE.

2. Military Information Networks Evolution towards Global Cyberspace Domain

To properly understand the term cyberspace, it is necessary to put it in the context. From a military perspective, cyberspace is a relatively recent addition to the four traditional operational domains of air, land, maritime and space – Fig. 3. An additional domain that cuts across all of these is the ElectroMagnetic Spectrum (EMS).

The complex of global interconnection between sources, communication and users creates a domain, often named as Cyberspace, which is a real, physical domain. It comprises of electronic and networked systems that use electromagnetic energy for connection. Cyberspace exists across the other domains (air, land, sea, and space), connecting these physical domains with the cognitive processes which use the data that is stored, modified, or exchanged.

Cyberspace is entirely man-made virtual environment and that is why it exists only thanks to persisting and continuous attention and maintenance. Cyberspace takes the

form of a global computer network located not only on land, but also across the air, sea and space. Cyberspace is a system of systems – cyberspace domain, in military it is a "domain of operations" as well [5].

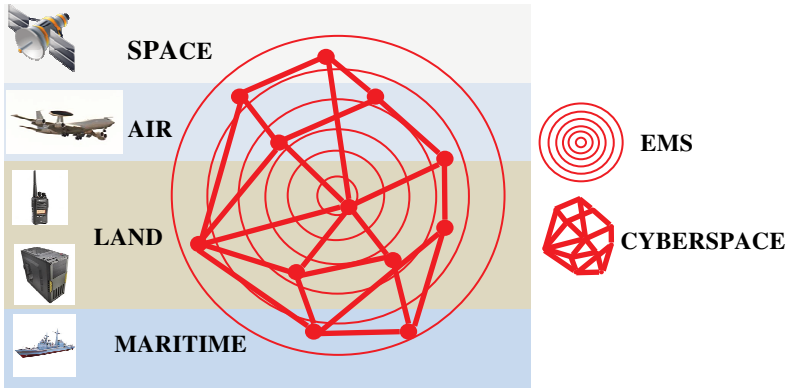


Fig. 3 Six operational domains of complex future battlefield [4]

Fig. 4 illustrates a perspective information service structure which gives a simplified view of numerous services that impact network communication. Nevertheless, this is just a very small portion of all available protocols and applications in use. It is important to realize that the military networks use several protocols which are also implemented in commercial networks (e.g. Internet). Each of these services could create cyber security issues because they are capable of being abused by potential adversaries.

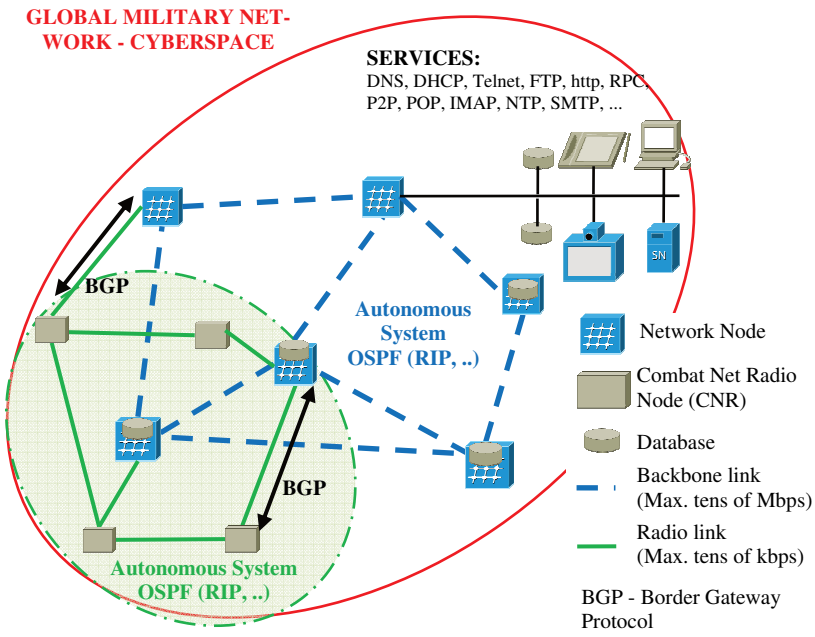


Fig. 4 Example of perspective global military network based on different systems

The main difference between obsolete networks and the global military network (Cyberspace) consists in the military cyber attacks scope. The full connectivity enables to spread attacks theoretically through the entire cyberspace (Fig. 5).

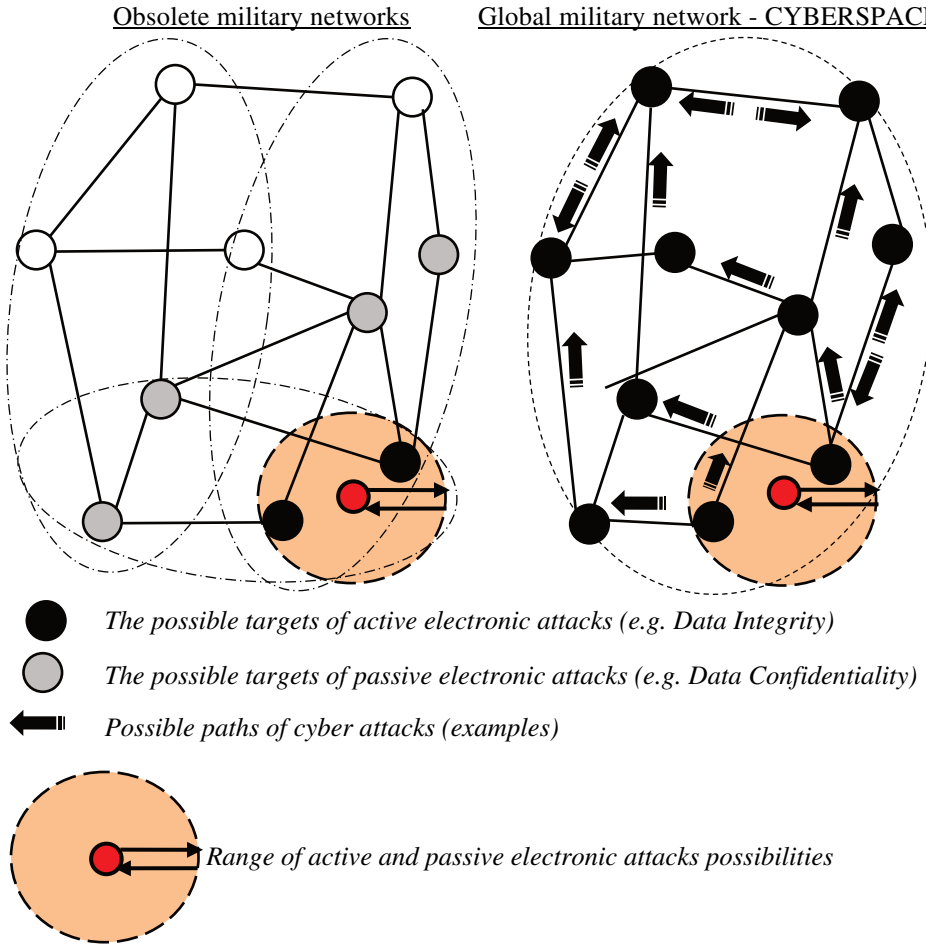


Fig. 5 Difference between attacks scope in obsolete military networks and in emerging global military network

Cyber threats are not only subject to the military Command and Control (C2) systems, but also to all military systems that include software and hardware. Overall military capabilities with technical systems of systems form a complex ICT (Information and Communication Technology) infrastructure with embedded Commercial Off-The-Shelf (COTS), military and civilian technologies. Managing cyber security in this challenging environment requires an architectural level design.

Fig. 6 shows the basic steps of cyberattack which is conditioned by acquisition of control technology (warfare) system after retrieving information gradually from Information and Communication Technology (ICT) assets and Information and Communication Systems (ICS) assets.

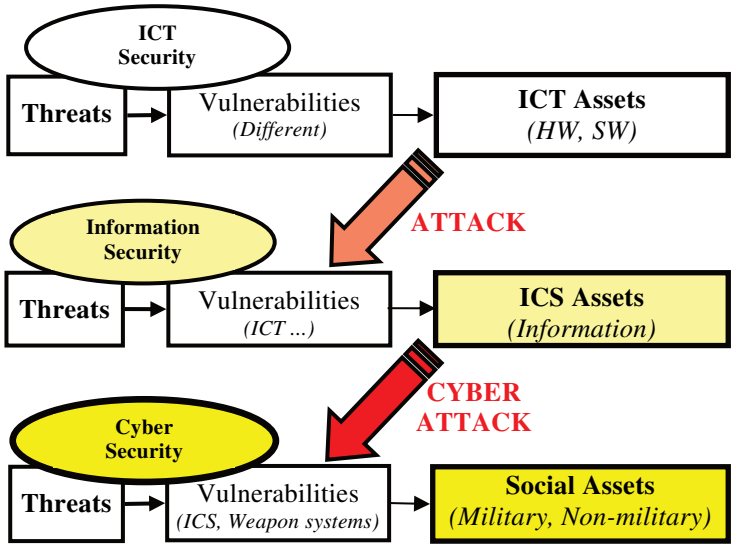


Fig. 6 Possible basic attack steps in cyberspace [6]

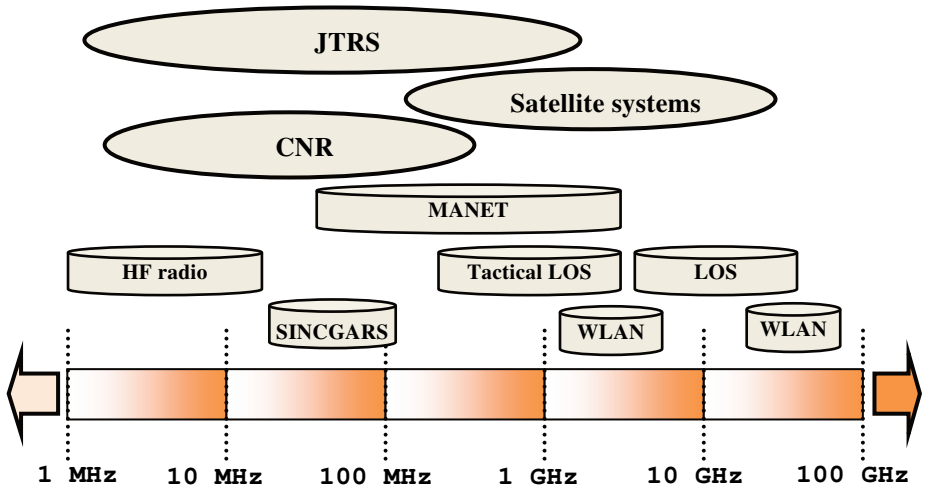
3. Cyber Threats in the Military Battlefield Information Networks

The emerging global military network (Cyberspace) consists of many different and often overlapping networks, as well as the nodes (any device or logical element with IPv4, IPv6 address or other analogous identifier) in these networks, and the system data (such as routing tables) that support them. Although not all nodes and networks are globally connected or accessible, cyberspace continues to become increasingly interconnected. Networks can be intentionally isolated or subdivided into enclaves using access control, encryption, disparate protocols, or physical separation. With the exception of physical separation, none of these approaches eliminate underlying physical connectivity; instead, they limit the access.

Tactical networks are crucial for modern mobile military communications. The mobility requirement excludes the possibility to use stationary communication infrastructure. Standard sources of communication channels (metallic, coaxial and fibre cables, Public Switched Telephone Network – PSTN) are not appropriate; therefore, different types of radio networks with miscellaneous properties and possibilities have been developed. Fig. 7 shows some examples of wireless military systems spreading over frequency bands. The different kinds of radio networks are heterogeneous from many points of view.

The basic differences in military environment ICS are based on specific military forces tasks – combat action. The basic differences are:

- massive wireless communication utilization,
- heterogeneous infrastructure and communication links,
- relatively low degree of infrastructure redundancy,
- high degree of command and control processes dependence on continuous communication and information exchange mainly in real time,
- professional attackers,
- no legal enemies' barriers (Physical destruction, Use of physical cruelty ...).



CNR *- Combat Net Radio*
HF *- High Frequency*
JTRS *- Joint Tactical Radio System*
LOS *- Line of Sight (Radio Relay)*
MANET *- A Mobile Ad hoc NETtwork*
SINCGARS *- Single Channel Ground and Airborne Radio System*
WLAN *- Wireless Local Area Network*

Fig. 7 Review of basic wireless military systems through frequency band

In advanced ICS, different security technologies are used to protect networks and handle traffic. The basic technologies are equivalent both in wired and wireless networks, but in wireless networks it is necessary to ensure security in EMS environment as well.

Basic areas of security measurement in wireless networks are:

- usage of the modern cryptology means for data confidentiality,
- the security protocols used in networks and applications for authentication and authorization,
- manipulation with transmitted radio signal with the goal to hide communication, or, alternatively, to decrease possibility of attack by jamming or eavesdropping. For example Frequency Hopping (FH), Direct Sequence (DS) modulation, smart adaptive antennas etc.

These measures have strengths and weaknesses, and it is important to keep them reliable and effective. In case of cyberspace, it is not possible to divide networks on less or more important from the point of view of security level, so is necessary to keep the whole cyberspace (all networks) on the same required level of security.

In the following part of the paper, the main attention is paid to the problems based on wireless communication, mainly composing battlefield military networks.

The concerns of wireless security, in terms of threats and countermeasures, are similar to those found in a wired environment, such as an Ethernet Local Area Network (LAN) or a wired wide-area network. The security requirements in wireless environment are the same, such as access control, accountability, authentication, availability, communication security, confidentiality, integrity etc. [7].

However, some of the security threats are unique to the wireless environment. The most significant source of risk in wireless networks is the underlying communication medium. Specific features of wireless radio systems and some factors typical of mobile environment are introduced in short description in Tab. 1.

Tab. 1 Specific features of military wireless radio systems [8]

Segment	Problems
Channel	Wireless networking typically involves broadcast communication, which is far more susceptible to eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols. Wireless channels between nodes may spread through enemy's area.
Nodes	Military nodes may be compromised and destroyed by various types of strong, concentrated electromagnetic signals.
Mobility	Wireless devices are, in principal and usually in practice, far more portable and mobile than wired devices. This mobility results in a number of risks.
Resources	Some wireless devices, such as smartphones and tablets, personal/manpack/vehicle radio station have sophisticated operating systems, but limited memory and processing resources to counter threats, including denial of service and malware.
Accessibility	Some wireless devices, such as personal/handheld radio, sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks or equipment abuse.

Emerging of Software Defined Radio (SDR) technology [9] allows radios to operate with multiple waveforms to provide a wide range of capabilities depending on frequency, waveforms characteristics, and bandwidth. That variability allows forming flexible wireless networks based on different platforms with all advantages and disadvantages, depending on demands and circumstances.

While the benefits of commercial convergence to IP networks are strong motivators for adoption by military networks, IP also has some undesirable characteristics that require attention, especially in terms of security (IPSec and key management) and a somewhat excessive frame structure that results in high overhead on bandwidth-constrained links. This latter characteristic is especially troublesome in the High Frequency (HF) radio band, which still heavily relies on the military for a variety of tactical communication needs.

4. Cyber Warfare and Attacks in Cyberspace

Military networks operate under extreme circumstances. Networks are deployed in harsh environments, where temperature, weather and other factors set high requirements for functioning. For wireless communication, the movement of troops brings a challenge with the mobility of the networks. In addition, the military networks are located in a hostile environment, where an active adversary is always present. Hence,

for network availability and usability, it is important that the networks are well secured against external and internal attacks.

In terms of classification, it is generally possible to divide attacks on battlefield cyberspace by different criteria, for example:

- threat source – Inside, Outside, Combination,
- security objectives – Confidentiality, Integrity, Availability...,
- operational impact – Misuse of resources, Installed Malware, DoS Attacks…,
- information impact – Distort, Disrupt, Destruct …,
- attack targets – Warfare, Operation system, Network, User, Application...,
- attacks on ISO/OSI layers – Physical, Data Link, Network….

Standard electronic warfare (Fig. 2) was not built to face the new threats (for example cyber attacks, remote access to databases...). In the past, the main attacks used to be in the physical area. However, the new cyber warfare needs to be able to face more sophisticated security challenges, especially in digital environment [10]. Fig. 8 shows the layered model of cyber warfare (CW), which extends the possibilities of electronic attack weapons by cyber operations facilities in digital environment. This part (Digital Environment) of modern cyber warfare is similar to those in wired networks.

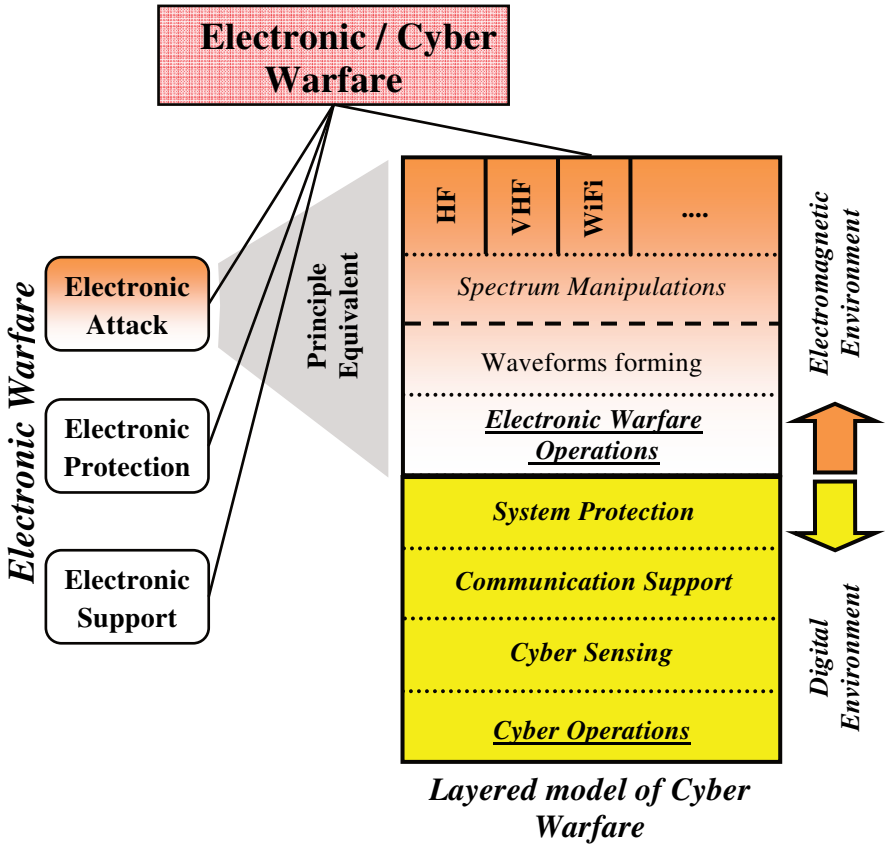


Fig. 8 Model of cyber warfare compared to classical electronic warfare

In the context of electronic warfare and wireless networks, it is essential to mention an enormous progress in software-defined radio area and to offer tremendous potential for encouraging cyber – electronic warfare collaboration. SDR concept is emerging as a potential pragmatic solution: it aims to build flexible radio systems, which are multi-service, multi-standard, multiband, re-configurable and re-programmable by software [11]. All possible tasks (full-band recognition, waveform change …) are possible to carry out in a very short time period (near real time).

SDR and Cognitive radio (CR) [12] technology implement radio functionalities, as modulation/demodulation, signal generation, signal processing and signal coding in software instead of hardware, as it is the case in conventional radio systems. The software implementation provides a higher degree of flexibility, re-configurability and many other benefits including the capability to modify the transmission parameters or communication protocols. These technological options are ideal for cyber warfare design, both for attacks and defense.

Events in cyberspace occur at high speed and therefore traditional responses may not be sufficient to protect critical infrastructure and services. Although risks in cyberspace can be managed in several ways, they do not often match this complex and dynamic environment. Increasing dependence on cyberspace brings not only new benefits but also new threats. Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and military information, disrupting critical operations, and imposing serious threats on the battlefield. On principle, it is possible to divide the attacks by its complexity (Tab. 2).

Tab. 2 Levels of cyber attacks complexity (The table does not include the level of military threat, damages or actual loss)

Simple Target Attack	**Group Target Attack**	**Complex Attack**		
Attack on element of system	Attack on subsystem Attack on group of elements	Hidden Attack	Active Stealth Attack	Active Destroying Attack
Sensors, Drones, Unmanned vehicle, Autonomous warfare systems	*Warfare system*	*Attacks on battlefield warfare and ICS systems*		

Today's military networks are more and more based on obsolete commercial technologies and protocols. Military-specific technology is costly, and it requires special knowledge of maintenance and configuration. However, in a situation where commercial technologies do not fulfil the high-level military specifications, some modifications and development of commercial products are conducted. Thus, commercial hardware, applications and protocols are widely used from the strategic to even the tactical level of military networking. Based on these facts, it can be assumed that the basic attacks scenarios may be the same as in commercial and public TCP/IP networks.

For classification of information security, the traditional layered ISO/OSI model and TCP/IP model are usually employed. For cyber security description, it is more

proper to use layered model published in [13]. Fig. 9 summarizes classic attacks and cyber attacks [14, 15], structured by network layers. The brief description of some of them is in Tab. 3; however, a detailed description is out of scope of this paper.

<table>
<tr><th colspan="2">Network layer</th><th>Classic Attack</th><th>Attacks in Cyber Age</th></tr>
<tr><td colspan="2">Geographic sphere</td><td>Physical attacks
(Mainly destroying)</td><td>Physical attacks
(Equipment abuse)
Enemy subject forged</td></tr>
<tr><td>Physical</td><td rowspan="5">Layers of Network Models ISO/OSI, TCP/IP sphere</td><td>Jamming
Eavesdropping</td><td>ICS Connections and Intrusion</td></tr>
<tr><td>Link</td><td colspan="2">Disruption of MAC table, Traffic analysis, Resource consumption</td></tr>
<tr><td>Network</td><td colspan="2">Flooding, Location disclosure, Sybil, Selective forwarding, Wormhole, Blackhole, Sinkhole, Rushing</td></tr>
<tr><td>Transport</td><td colspan="2">SYN flooding, Session control</td></tr>
<tr><td>Application</td><td>Repudiation, Virus and Worm</td><td>Resource misusage</td></tr>
<tr><td>Person
Organization
Government</td><td rowspan="2">Social sphere</td><td rowspan="2"></td><td rowspan="2">Access rights seizure
Data (Information) access – Read, Write, Change, Erase
Access and takeover of HW and SW
Takeover ICS processes
Takeover warfare systems control
False objects and subjects creation</td></tr>
<tr><td>Person
Unit
ICS
Weapons systems</td></tr>
</table>

Fig. 9 Extended layered TCP/IP model cyber security threats examples [14, 15]

5. Findings and Recommendations

In the previous part, we mentioned several types of attacks according to the layer. Here is a short overview of the most widely spread attacks:

- physical layer – Sniffing, Jamming, Physical destroying, Device tampering,
- link layer – Disruption of MAC table, Traffic analysis, Resource consumption,
- network layer – Flooding, Location disclosure, Sybil, Selective forwarding, Wormhole, Blackhole, Sinkhole, Rushing,
- transport layer – SYN flooding, Session control.

In this section, the most frequent weaknesses and vulnerabilities are discussed. To avoid common attacks on network infrastructure, it is advised to follow these recommendations to assure the defined security level. There are the basic vulnerabilities and weaknesses in future military battlefield information networks:

- physical attack on ICS devices and personnel – not only computer and network devices are subject to physical attack. ICS personnel can also be a target – obtaining access credentials from a person can facilitate access for an attacker. In addition, the risk of revealing is quite minimal, as the administrator usually neglects this possibility,

Tab. 3 Brief description of presented security threats

Attack type	Description
Blackhole	The compromised node refuses to participate in the routing process by dropping all packets received.
Flooding	Overwhelms victim's limited resources memory, processing or bandwidth.
Location disclosure	Location of the certain nodes and the topology of the network are revealed mainly through traffic analysis techniques.
Repudiation	Denial of participation in communications.
Rushing	A fast side-channel is created between two attackers which act as effective DoS attack.
Selective forwarding	The compromised node forwards only selected packets while dropping the other ones coming from certain nodes.
Session control	The attacker spoofs the IP address of a node and then continues to communicate with other nodes.
Sibyl	Multiple attacker personalities are created throughout the network.
Sinkhole	The route is tampered by an attacker in order to effectively attack.
SYN flooding	The adversary creates many uncompleted TCP connections to a victim node.
Wormhole	Packets at one location in the network are tunnelled to another location. It implies the cooperation of two adversaries.

- COTS based software – the main part of ICT uses civil technologies. To accomplish some kind of a simple attack on infrastructure scenario we do not assume any special devices or software. In order to perform traffic analysis (Physical and Link layer) it is necessary just to sniff the traffic flow. After gaining some useful information (usernames, passwords, keys), the attacker can obtain the access either to particular devices or to all infrastructure. For example, if attacker obtains the access to a router in a network, he can modify routing tables and make data flow through his device,
- weak passwords – this is probably the most frequent vulnerability. Users usually have default, poor or weak passwords, which are easy to be cracked (dictionary attack, brute-force, etc.). Some administrators (users) even store them in unencrypted form. After deploying a new device system, the administrator has to define some criterions to avoid weak passwords (minimal length of password, using numbers, lower case and upper case characters etc.),
- privileged access – the problem in this case is using standard user credentials with granted administrative privileges. Standard user should be limited to defined operations with limited access to resources and data. Another issue is that the administrator uses identical passwords across multiple servers and devices

to simplify access to huge number of devices. In addition, each device should have a limited group of privileged administrators and its own password to manage it,

- access control – to ease the implementation and deployment of software products, the administrators usually allow access using unsecure protocols (e.g. HTTP instead of HTTPS, FTP instead of FTPS etc.). Moreover, the administrators do not block network services exposed to the Internet allowing the attacker to gain the access into internal network,
- network monitoring – from the side of the standard user, it is necessary to limit removable devices, which are prone to carry malicious and harmful software. Without up-to-date firewall and antivirus software, this is the way how to easily obtain access into internal network even if some specific kind of firewall is deployed on the gateway,
- dominating wireless networks:
  - wireless technology is easy to implement and use. However, without proper configuration (e.g. defining access lists, using strong encryption) this technology is very dangerous and prone to be misused. Data transferred between access point and client without encryption can be either sniffed or even intercepted (and modified). Therefore strong encryption and strict access policy is required,
  - since the wireless environment offers quite trivial passive and active attack (e.g. passive attack = sniffing, active attack = jamming), it is vital to take special measures to avoid data tampering. The most deployed methods are FH, DS, directional antennas, adaptive transmitter power adjusting and their hybrid implementation,
- workstations, servers and network devices configuration – in case of a huge numbers of workstations and servers it is quite challenging to keep them up-to-date. Unpatched tools and software, misconfigured services and servers and unauthorized access due to weak passwords are an ideal way how to intrude any network. To increase security, the user policy must be defined and strictly followed. On top of that, data must be stored on a secure storage limiting access just for authorized users – without exception,
- the basic networks devices are prone to these attacks:
  - switches – depending on the scenario, the switch can be configured according to traffic analysis based on source/destination address, ingress/egress port or other criteria. However, if the attacker gains an access to the switch, they can tamper and analyse the traffic entering and leaving the device, analysing every frame (packet) including header and payload,
  - routers – the router is usually configured to route packets to another network – connected directly to this device or via neighbouring gateways. In case of attack, enemy can provide network devices with forged routes in order to redirect packets. Packets are usually redirected to the attacker's device to analyse its payload (Sinkload attack). In other scenarios, the attacker discards packets in order to deny some service (Blackhole). In these scenarios, no special abilities are required. In the past, the network protocols were designed to be reliable but not secure. Over the time, some safety mechanisms were added to some network

protocols. However, many protocols still have security vulnerabilities if they are not properly configured and secured. To give an example, we mention ICMP, BGP, OSPF or RIP routing protocols which are prone to be misused if the administrator neglects basic security measures,

- complex type of infrastructure – any network without properly configured network monitoring is considered insecure. All activities must be monitored, logged and stored for the case of security breach. After performing a detailed analysis of a security breach, it is possible to draw a conclusion. In order to secure the topology, it is also recommended to limit the access just for allowed devices and to deny the unauthorized access for both wired and wireless devices.

6. Conclusion

Security in military cyberspace is a critical issue. Cyberspace has become a place with growing importance. The increasing usage of cyberspace means that its disruption can affect armed forces' ability to operate effectively during a crisis.

Complex cyberspace and CW support may require a scheme to show integration and synchronization requirements and task relationships. This includes a discussion of the overall cyberspace and CW concept of operations, required support, and specific cooperation.

Because most battlefield communication uses wireless technologies, new challenges and issues for military communications networks appear:

- cognitive networks and intelligent radio utilization,
- type of the overall cyber security architecture,
- functional properties of the architecture,
- security functions and control of the infrastructure, service and application layers.

References

[1] ALBERTS, D.S., GARSTKA, J.J. and STEIN, F.P. *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP publication series, USA, 2000. 25 p. ISBN 978-1-57906-019-0.

[2] KÄRKKÄINEN, A. *Cyber Security Architecture for Military Networks Using Cognitive Network Approach* [PhD Thesis]. Helsinki: National Defence University, 2015. 94 p.

[3] *Cyber Electromagnetic Activities* [on-line]. Field Manual 3-38. Headquarters, Department of the Army, Washington, USA, 2014. 96 p. [cited 2018-01-12]. Available from: https://fas.org/irp/doddir/army/fm3-38.pdf.

[4] CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations [on-line]. Mountain View, California, 2016. 48 p. [cited 2018-01-08]. Available from: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf.

[5] *NATO Recognises Cyberspace as a 'Domain of Operations'* [on-line]. NATO Warsaw Summit held on 8-9 July 2016. [cited 2018-01-11]. Available from: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit.

[6] SOLMS, R. and NIEKERK, J. From Information Security to Cyber Security. *Computers & Security,* 2013, vol. 38, p. 97-102. DOI 10.1016/j.cose.2013.04.004.

[7] ISO/IEC 27033-3:2015, *Reference network scenarios – Risks, design techniques and control issues.*

[8] STALLINGS, W. and BROWN, L. *Computer Security. Principles and Practice*. New Jersey: Pearson Education, 2015. 848 p. ISBN 978-0-13-377392-7.

[9] SAARELAINEN, T. Towards Tactical Military Software Defined Radio (SDR). In *Proceedings of the Eighth International Conference on Sensor Technologies and Applications*. 2014. p. 96-106. ISBN 978-1-61208-374-2.

[10] DAVIES, M. Science and Technology to Understand and Counter Threat Using Electronic Means [on-line]. *DST Partnerships Week 2016,* 2016. [cited 2018-01-10] Available from: https://www.dst.defence.gov.au/sites/default/files/events/documents/CEWD%20Presentation.pdf.

[11] PLESSIS, W.P. du. Software-Defined Radio (SDR) as a Mechanism for Exploring Cyber-Electronic Warfare (EW) Collaboration. In *Proceedings of the 13th Information Security for South Africa Conference (ISSA).* Johannesburg: IEEE, 2014. DOI 10.1109/ISSA.2014.6950516.

[12] *It's all SDR-related: Understanding Adaptive Radio, Cognitive Radio, and Intelligent Radio* [on-line]. Nutaq Innovation [cited 2018-02-05]. Available from: https://www.nutaq.com/its-all-sdr-related-understanding-adaptive-radio-cognitive-radio-and-intelligent-radio.

[13] RILEY, S. "Cyber Terrain": A Model for Increased Understanding of Cyber Activity [on-line]. October 2014. [cited 2018-08-02]. Available from: http://cyber-analysis.blogspot.sk/.

[14] ZUBAIRI, J.A. and MAHBOOB, A. *Cyber Security Standards, Practices and Industrial Applications. Systems and Methodologies*. Pennsylvania: Hershey, 2012. 336 p. DOI 10.4018/978-1-60960-851-4.

[15] ZAVIDNIAK, M.P. Operational Military Perspective in Cyber Security *IEEE Technology Summit* [on-line]. May 2008. [cited 2018-01-15]. Available from https://slideplayer.com/slide/6216812.