
HÍRVILLÁM

**A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa**

SIGNAL Badge

**Professional journal of Signal Department
at the University of Public Service**

2021

**Proceedings of the
International
Scientific Conference
on Military
Information Security**





13th May 2021

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem, Híradó Tanszék
tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement
at the University of Public Service

Budapest, 2021



HÍRVALÓBÁDGE

Editor in Chief
Dr. Fekete Károly

*The Organising Committee of the
Conference and the Editorial Board*

Chairman of the Board
Dr. habil. Kerti András

Co-ordinating Editor
Dr. Tóth András

Members

Dr. habil. Farkas Tibor
Dr. Horváth Zoltán László
Dr. Jobbágy Szabolcs
Kralovánszky Kristóf
Dr. Magyar Sándor
Megyeri Lajos
Dr. Nyikes Zoltán
Prof. Dr. Rajnai Zoltán
Szatmári Balázs
Szűcs Attila

HU ISSN 2061-9499

.....
*University of Public Service
Signal Department
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15*

*International Scientific Conference on Military Information Security
2021*

Table of contents

Greetings	8
Conference Program	9
László BAKOS: Opening remarks	10
Sándor MAGYAR: HTE Information Security Department and its role	11
Tibor FARKAS: New National Officer Training System in the Faculty of Military Sciences and Officer Training: Infocommunication course	20
Zoltán RAJNAI: Cyber coordination of government level	26
Zoltán NYIKES: Security Awareness Increasing for Virus Attack Defence	33
Károly Imre FEKETE: A brief glance at Quantum Cryptography and Military Infocommunications	44
Balázs SZATMÁRI: Counter-UAV solutions	57
Kristóf KRALOVÁNSZKY: You can't protect what you can't see -- Cybersecurity challenges of critical and vulnerable infrastructures	73
Lajos MEGYERI: Biometric identification for security purposes	79
András TÓTH: Information security issues in IoT solutions	88
Attila SZÚCS: Security issues in distance education	95
Zoltán HORVÁTH: Information security of the radio networks, presentation of the possibilities of digital radios	102

Greetings

Welcome Dear Colleague, Dear Reader!

On 21 January 2021, the Department of Intelligence hosted the International Scientific Conference on Military Information Security. The main objective of the conference was to provide a professional, scientific forum for the presentation of research results, dissemination of knowledge and networking. A total of 11 researchers presented their research results, and the reviews have been published in this professional journal with the authors' contributions, covering areas that have a fundamental impact on information security in today's military environment.

In this publication, the Editorial Board has collected the abstracts of the presentations, which it is very pleasing to make available to the readers.

Budapest, 13th May 2021

Dr. Fekete Károly
Editor in Chief

Conference Program

International Scientific Conference on Military Information Security

Conference Program

13th May 2021

	Time	Presenter	Title of presentation
1	Section chairman: Dr. Károly Imre Fekete Lieutenant Colonel, PhD, Associate Professor Please click here to join the conference		
	10:00-10:15	László Bakos Colonel, Deputy Chief of HDFC CIS & CIS Security Directorate	Opening Remarks
	10:15-10:30	Dr. Sándor Magyar Colonel, PhD, Assistant Professor	HTE Information Security Department and its role
	10:30-10:45	Dr. habil Tibor Farkas Major, PhD, Associate Professor	New National Officer Training System in the Faculty of Military Sciences and Officer Training: Infocommunication course
Coffee break			
2	Section chairman: Dr. Sándor Magyar Colonel, PhD		
	11:00-11:15	Prof. Dr. Zoltán Rajnai Cyber Coordinator for Hungary	Cyber coordination of government level
	11:15-11:30	Dr. Zoltán Nyikes, PhD, Invited Speaker, Associate Professor of Milton Friedman University	Security Awareness Increasing for Virus Attack Defence
	11:30-11:45	Dr. Károly Imre Fekete Lieutenant Colonel, PhD, Associate Professor	A brief glance at Quantum Cryptography and Military Infocommunications
Lunch break			
3	Section chairman: Dr. András Tóth Major, PhD, Associate Professor		
	12:45-13:00	Balázs Szatmári Captain, Instructor	Counter-UAV solutions
	13:00- 13:15	Kristóf Kralovánszky, Assistant Professor	You can't protect what you can't see - - Cybersecurity challenges of critical and vulnerable infrastructures
	13:15-13:30	Lajos Megyeri Lieutenant Colonel, Assistant Professor	Biometric identification for security purposes
Coffee break			
4	Section chairman: Dr. Szabolcs Jobbágy Major, PhD, Assistant Professor		
	13:45-14:00	Dr. András Tóth Major, PhD, Associate Professor	Information security issues in IoT solutions
	14:00-14:15	Attila Szűcs Lieutenant Colonel, Assistant Professor	Security issues in distance education
	14:15-14:30	Dr. Zoltán Horváth Lieutenant Colonel, PhD, Assistant Professor	Information security of the radio networks, presentation of the possibilities of digital radios
5	14:30-14:35	Dr. Károly Imre Fekete Lieutenant Colonel, PhD, Associate Professor	Closing Remarks

László BAKOS¹: Opening remarks

First of all, allow me to thank you for registering and attending this event. Unusually, today's conference, considering the pandemic situation, will be conducted online.

Nowadays, the use of computer systems, smart devices connecting to the internet has become a part of our work and our private life. The safe use of these tools cannot be without adequate information security.

The information security is an area that requires continuous development, while new challenges are putting our existing information systems and their security to the test.

In addition, the epidemic situation of the past year poses new types of challenges for information security experts.

As a result of recently introduced regulations, online school education has become part of everyday life for families. A significant proportion of workers switched to working from home, not only the civilian but the military personnel too.

Various smart applications for managing our life are spreading. Online banking and payment methods are becoming more and more integrated into our everyday lives.

At the same time, the spread of malicious viruses, which are being used by cybercriminals to exploit the vulnerabilities of our systems and the credibility of users, are gaining ground.

Using command control and communication systems during the land and air operations planning and executing information security must be given a special attention. During the processing and storage of data, we must pay attention to the implementation of both electronic and physical security at the appropriate level.

Government IT systems are increasingly being targeted by hacker attacks. The protection of governmental and military infocommunication systems nowadays is a priority task of the information security experts.

I hope our event today will enrich them all with useful knowledge. With these thoughts, I open today's conference.

¹ Deputy Chief of HDFC CIS & CIS Security Directorate

**Sándor MAGYAR²: HTE Information Security Department
and its role**

Correferatum

On 15 September 2017, students graduating the Electronic Information Security Manager postgraduate specialist training course at the National University of Public Service in 2016/17 established a professional community, called Electronic Information Security Managers Smart Club (EIVOK). The Club, as the alumni community of training, held forums in every two months. The need for professional forums has increased with the growing number of the community. In 2018, it was decided that the Club join the Scientific Association for Infocommunications as its Information Security Department – EIVOK. The core values of EIVOK are professionalism, simplicity, immediacy, independence, sharing of knowledge and experience. Knowledge sharing in this area is extremely important. As more than 200 people have already joined a mailing list, the sharing of information within the community has become extremely effective. One of the strategic goals is bring information security leaders closer and provide an opportunity for collaboration, to which nearly 20 organized forums have so far effectively contributed.

² Assistant Professor of University of Public Service

eivok

SCIENTIFIC ASSOCIATION FOR
INFOCOMMUNICATIONS,
INFORMATION SECURITY
DEPARTMENT

HTE Information Security Department and its role

Sándor MAGYAR

International Scientific Conference on Military Information Security - 2021

eivok

SCIENTIFIC ASSOCIATION FOR
INFOCOMMUNICATIONS,
INFORMATION SECURITY
DEPARTMENT

“Coming together is a beginning. Keeping
together is progress. Working together is
success.”

Henry Ford



Scientific Association for Infocommunications

- ▶ Founded in 1949;
- ▶ Members are voluntary and autonomous professionals working in the fields of telecommunications, broadcasting, electronics, information and media technologies in Hungary.



Electronic Information Security Manager

Act L. of 2013

- Higher education and professional qualifications required or;
- 5 years of professional experience in the field.

26/2013. (X. 21.) KIM Decree

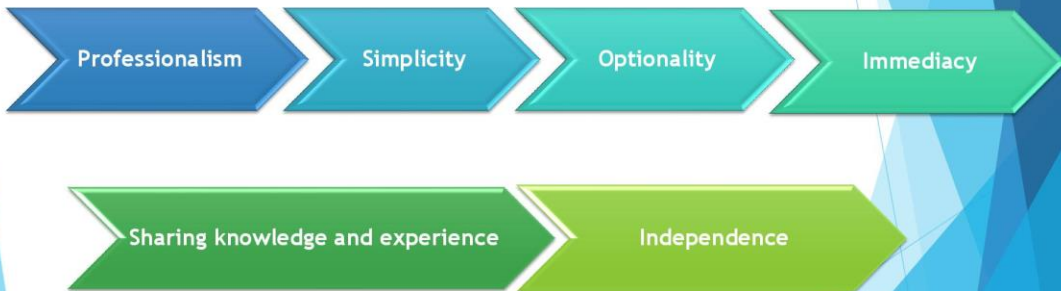
- Training are provided by the National University of Public Service or;
- CISA, CISM, CRISC, CISSP.

HISTORY of EIVOK

- ▶ On **15 September 2017**, students graduating the *Electronic Information Security Manager postgraduate specialist training course* at the National University of Public Service in 2016/17 established a professional community called Electronic Information Security Managers Smart Club (EIVOK).
- ▶ The Scientific Association for Infocommunications, Information Security Department – EIVOK was established on **28 May, 2018**.



Default values



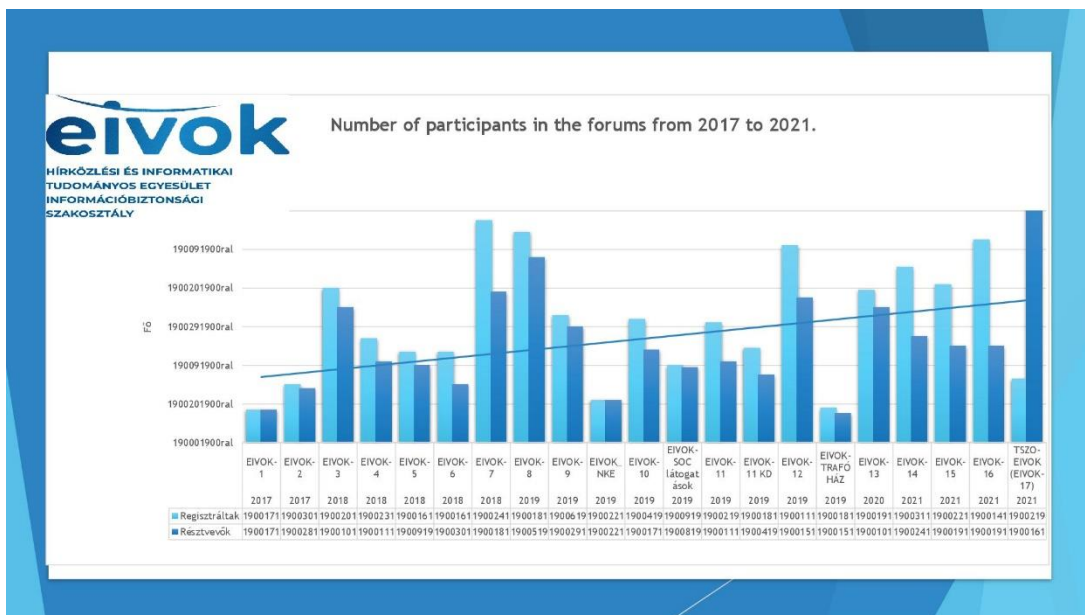
Strategic goals

- ▶ To bring closer the graduates and information security leaders.
- ▶ Provide personal contact opportunities between Electronic Information Security Managers.
- ▶ Provide members with useful information, ideas, suggestions, and solutions to gain a competitive edge in successfully solving future challenges.
- ▶ It organizes professional meetings and discussions (average every two months).
- ▶ It collects, organizes, coordinates electronic and printed professional materials, analyzes and studies.
- ▶ It involves additional information security professionals in the joint work.
- ▶ Organizing professional sections at HTE conferences.

Professional Events

- ▶ 1. OLÁH István György; NAGY Gábor; BÚS Nikolett Katalin,
- ▶ 2. KRASZNAY Csaba; MAGYAR Sándor; LEITOLD Ferenc,
- ▶ 3. RAJNAI Zoltán; NAGY Sándor; OLÁH István György,
- ▶ 4. MUHA Lajos; BARACSI Katalin; ROMASOVSKAI Attila,
- ▶ 5. KOVÁCS Zoltán; SIK Zoltán Nándor; NÉMETH Imre
- ▶ 6. KOVÁCS László; ERDŐSI Péter Máté; Bubán Márton
- ▶ 7. VERECKEZI Béla; KELETI Arthur; SCHEIDLER Balázs; TARJÁN Gábor
- ▶ 8. TÖRÖK Szilárd; MARSII Tamás; MAGYAR Sándor
- ▶ 9. BODÓ Attila Pál; KRASZNAY Csaba; Szűcs Judit
- ▶ 10. DEVECZ Miklós; HÁMOR Endre; BEDERNA Zsolt
- ▶ 11. BUTTYÁN Levente; BÁNYÁSZ Péter; OLÁH István György; TARJÁN Gábor
- ▶ EIVOK conference: BÚS Nikolett Katalin; LENCSE S Gábor ; BUBÁN Márton;
- ▶ NAGY Sándor; OLÁH István György
- ▶ 12. ZALA Mihály; ZBOZNOVITS Csaba; VÁCZI Dániel
- ▶ 13. KRASZNAY Csaba; BÍRÓ Péter; BÓDI Antal
- ▶ 14. SZÁSZ Péter
- ▶ 15. KRASZNAY Csaba; TÓTH Rebeka; KATONA Gergő
- ▶ 16. MÁTYÁS Gyula; SCHULCZ Norbert
- ▶ TSZO/EIVOK 17.: KISS Tamás; KUTAS Péter; BACSÁRDI László; KOVÁCS Benedek

<https://www.hte.hu/informaciobiztonsagi-szakosztaly-eivok>





Want to know more about us?

Visit our website:

<https://www.hte.hu/en/informaciobiz tonsagi-szakosztaly-eivok>

Read our latest report, which you can find here :

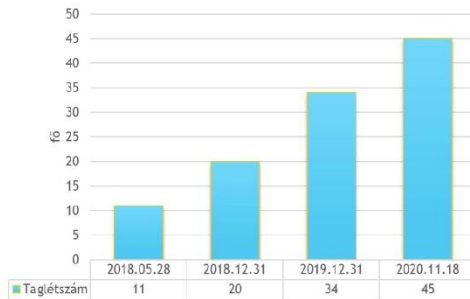
https://www.hte.hu/documents/10180/4569849/Besz%C3%A1mol%C3%B3_2019_HTE_inform%C3%A1ci%C3%B3biztons%C3%A1gi_Szakoszt%C3%A1ly_EIVOK.pdf



Do you want to join us?

Szakosztály tagok száma (fő)

Number of EIVOK community members



9/15/2017 17 people

1/15/2021 206 people

Admission to HTE's Information Security Department

<https://www.hte.hu/tagsag-belepes>

eivok

SCIENTIFIC ASSOCIATION FOR
INFOCOMMUNICATIONS,
INFORMATION SECURITY
DEPARTMENT

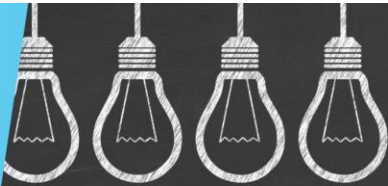
Our contacts:

Mailing list: eivok@lev-lista.hu

E-mail: eivok@hte.hu

Website: www.hte.hu

www.hte.hu/informaciobiztonsagj-szakosztaly-eivok



“None of us is as smart as all of us.”


Ken Blanchard.

Thank you for your
attention!

**Tibor FARKAS³: New National Officer Training System in the
Faculty of Military Sciences and Officer Training:
Infocommunication course**

Correferatum

In this presentation, the authors present the background and main steps of transforming national officer training. In addition to general skills and requirements, the lecture focuses on infocommunication officer training. It presents the tasks of the Hungarian Defence Forces Command and the Faculty of Military Science and Officer Training in connection with the transformation. The transformation is still ongoing, and some elements are not yet finalised; therefore, the presentation will focus on the general areas and the main orientations.

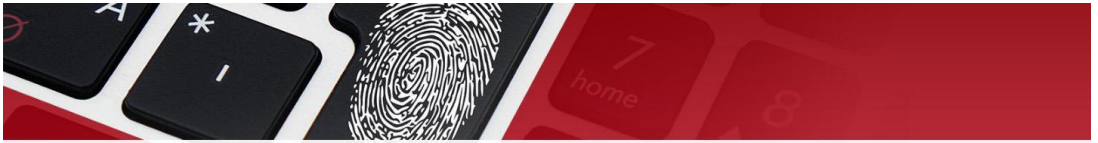


**New National Officer Training
System at the Faculty of Military
Sciences and Officer Training**

Military Cyber BSc

International Scientific Conference on Military
Information Security
13. May 2021.

³ Associate Professor of University of Public Service



- **BG. László KOVÁCS**
 - Inspector of the Hungarian Defence Forces Command Cyber Inspectorate (CI)
 - Professor
 - EW Department/FMSOT
 - former program leader (Military ICT and EW BSc)
 - kovacs.laszlo@uni-nke.hu
- **MAJ. Tibor FARKAS**
 - associate professor
 - CIS Department/FMSOT
 - program leader (Military ICT and EW BSc)
 - farkas.tibor@uni-nke.hu

Introduction

- Degree programs
- The higher education system at Military Faculty
- The need of the new system
- The new training system- overview
- The cyber BSc
- Questions to be answered

UPS structure



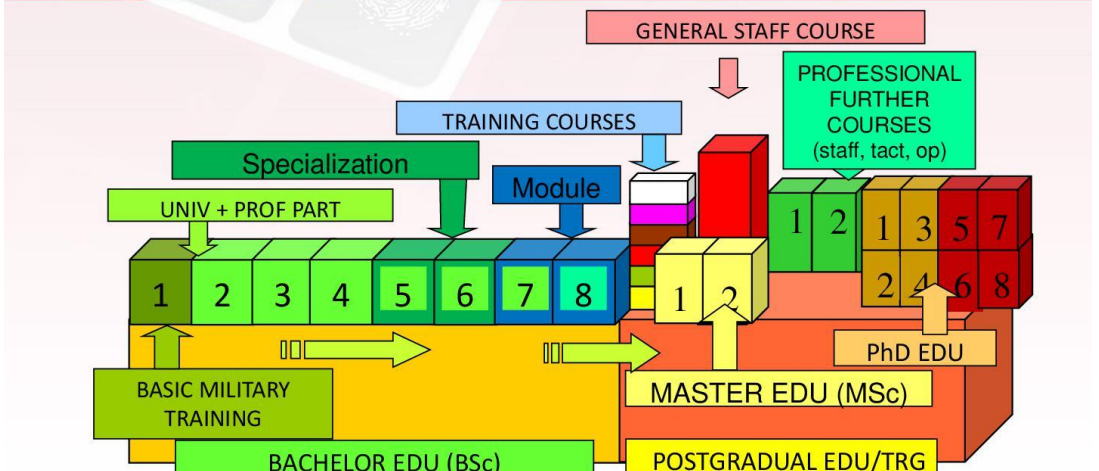
Degree programs



The aim of this program is to educate and to train officers capable of understanding, maintaining, and managing military systems and devices and also to introduce new technologies.

Specialisations: military informatics; signal intelligence and electronic warfare; signal (telecommunication, **information security** modules)

The higher education system at Military Faculty



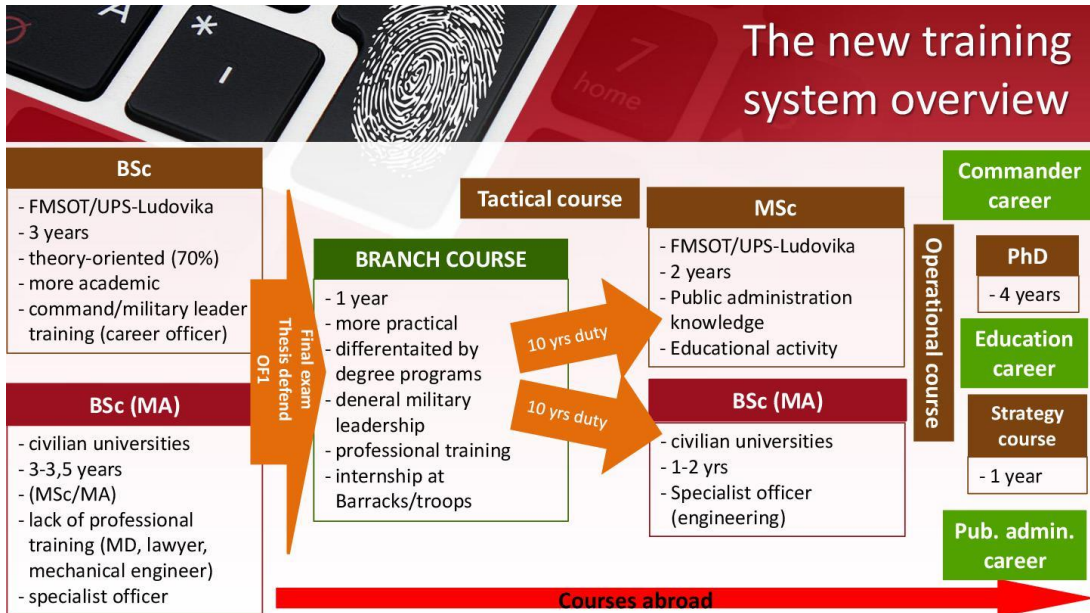
The need of new system

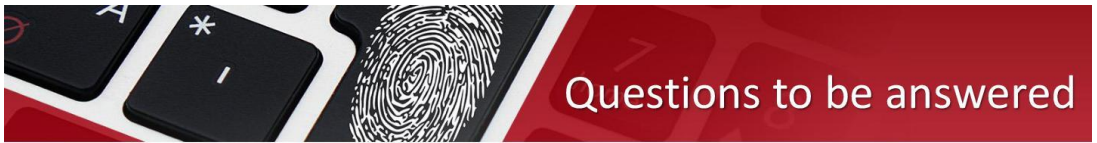
INFLUENCING FACTORS

- Impact of generational characteristics
- The evolution of warfare and technology
- The basic mission of the Defence Forces, a new concept
- The basic mission of the Defence Forces - new concept
- ZRÍNYI 2026 Defence and Military Development Programme
- Harmonisation of officer and NCO training

New capabilities and requirements







Questions to be answered

- 8 semester lectures to 6
- 240 credits to 180 credits
- ballance between the academic & branch part
- more complex knowledge
- continuous cooperation (Departments/CI/J6/J2)
- ballance between military leadership & prof. knowledge
- Lieutenant who able to lead a platoon!
 - Military leader
 - Spec. officer
- „Think out of the box!“



Military Cyber BSC

Thank you for your
attention!



Zoltán RAJNAI⁴: Cyber coordination of government level

Correferatum

In modern democracies the digital revolution has been stretching to all aspects of life which generates significant dependency. Nowadays members of the society are less viable if they do not use e-mail addresses, bank accounts and cards, or some sort of positioning system. The role and significance of digital infrastructures is undisputed, they became unquestionable components of transparent state functions, economic prosperity and successful scientific research.

On the one hand, modern information society considers information and communications technologies the engine of societal evolution. On the other hand, the challenges of dependency, the dynamics of development and the rate of penetration involve serious threats.

In the presentation I would like to speak about some questions about the hungarian aspects of national cyber security.

⁴ Professor of Óbuda University, Cyber Coordinator for Hungary

Cybercoordination on Government level in Hungary

Prof. Dr. Zoltan RAJNAI
National cybercoordinator



International Scientific Conference on Military
Information Security, Budapest

1. Cybersecurity laws,
and organisation
2. CECS Platform
3. EU and NATO
recommendations
4. Objectives and
identification of
priorities
5. Specified measures
and fields of action

Cybercoordination on government level in Hungary



Hungarian situation in cybersecurity 2013-

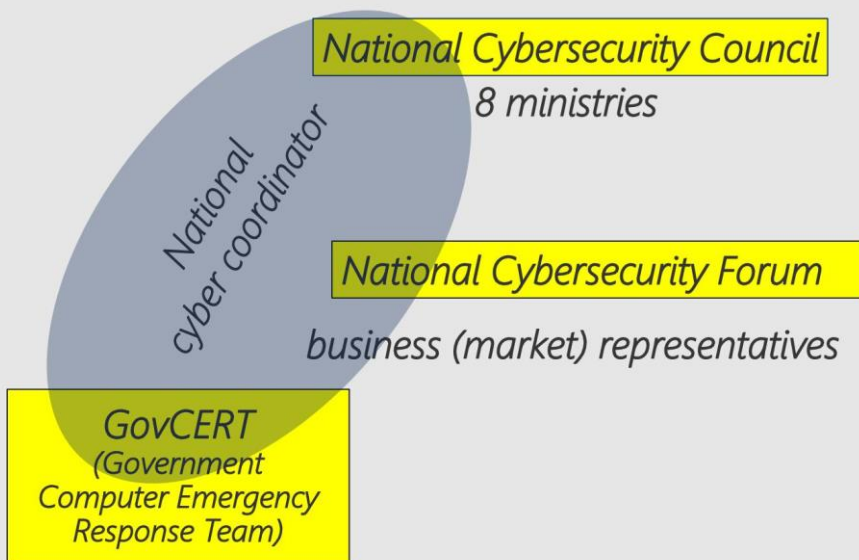
National cybersecurity strategy



Law on information security for government networks

Foundation for the Hungarian approach on cybersecurity

Cybersecurity's actors



2. Central European Cybersecurity Platform - CECSP

2013 – Austria +V4 countries

aims:

- to enable the information,
- best practices,
- lesson learned and know-how sharing about cyber threats and potential or successfully carried out cyber-attacks

common trainings, education, exercises and research and development coordination

3. EU, NATO, GFCE recommendations

ENISA: Practical Guide on the Development and Execution of National Cybersecurity Strategies

NATO: Cooperative Cyber Defence Centre of Excellence

Global Forum on Cyber Expertise

5. Measures and fields of action

Czech strategy the measures and goals are presented together, several measures from awareness-raising to the development of the legislative framework

Austria sets out measures in the field of process management, co-operation among governmental, economic and societal actors, critical infrastructure protection, awareness-raising, research and development and international co-operation

Slovak: covers a wide range of measures together with objectives, under the strategic priorities paragraph, including the protection of human rights and freedoms, awareness-raising, as well as national and international co-operation

Polish strategy is the only one where the authors draw attention to prioritizing the most important measures. Each task is preceded by a risk assessment. The next measures in order are connected to the security of government administration portals, the regulatory environment and organizational actions. Education, training and awareness-raising.

Hungary already possesses most tools required for its strategic goals regarding both competences and the potential resources.

CECSP member states have to walk different paths to reach the common goals.

Conclusion

- *ENISA: "Good Practice Guide on Vulnerability disclosure"*
- *International co-operation, best practices:*
 - Visegrad countries group + Austria (V4+A)*
 - Central European Cyber Security Platform (CECSP)*
 - Global Forum on Cyber Expertise (GFCE)*
 - Contractual Public Private Partnership (cPPP)*

NEW Cybersecurity strategy - 2018

2016 June: NIS Directives

2018 December: Last deadline for new
cybersecurity strategy

2018 December 28: NEW Cybersecurity strategy

Thank you!

Zoltán NYIKES⁵: Security Awareness Increasing for Virus Attack Defence

Correferatum

The user anti-virus lack and data backup lack in case of the user groups show a strong relationship with each other, which means that the users don't use these two applications on average in the same proportion. In the case of the users who haven't informatics knowledge up the virus attacks number, up the anti-virus lack and the data backup lack are high level. For the digital systems, the lower level rated users are risks based on the numbers of the occurred virus attacks. For all user groups is necessary the continuous and repeated safety awareness training to reach and retain high-level safety.



The poster features a dark blue background with a molecular structure pattern. At the top, there are two circular logos: the University of Public Security (UNISZ) and the University of Public Administration (UNI-NKE). To the right of the logos, the text reads: "International Scientific Conference on Military Information Security" and "May 13th 2021, Budapest, Hungary". The main title "SECURITY AWARENESS INCREASING FOR VIRUS ATTACK DEFENSE" is written in large, bold, yellow capital letters. Below the title, the author's name and affiliation are listed: "MAJ. DR. ZOLTÁN NYIKES (PHD) ASSOCIATE PROFESSOR" and "nyikes.zoltan@uni-nke.hu". A small green square is located in the top right corner of the poster.

⁵ Associate Professor of Milton Friedman University

Maj. Dr. Zoltán Nyikes (Ph.D., OF-3)



HDFC CIS & CIS Security Directorate

CIS Security Branch

CIS Security Officer

Milton Friedman University, Hungary

Department of Methodology and Informatics

Associate Professor



University of Public Service, Hungary
Faculty of Military Science and Officer Training
Department of Informatics

Lecturer



Doctor of Military Engineering (Ph.D.)

Dipl. Safety & Security Engineer (MSc)

IT Engineer (BSc)

Intorduction

The user is the "**weakest link**", his identification is necessary for the risk assessment of information systems according to **digital competence** and **security awareness** .

Assessment of digital competence

- ▶ A questionnaire was created to identify and classify users.
- ▶ A total of 1,274 questionnaires were completed, of which 1,195 completed the online questionnaire and 79 on paper.
- ▶ The questionnaire was compiled from six group of questions.



The question groups

General questions;

User habits and tools;

Questions about digital competence and security awareness;

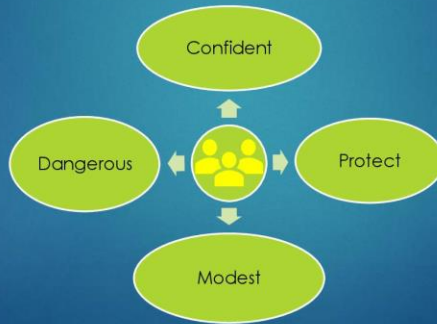
Cyberbullying;

Protect against malicious code;

Protecting data assets.

Digital competence assessment criteria

- ▶ 4 user groups have been defined based on the questionnaire evaluation.



The „Protect” user

- ▶ This category includes novice users who are also a source of danger, but because they are presumably aware of their own abilities (education and their own level of competence are almost the same), they use the Internet more cautiously.



The "Dangerous" user

- ▶ This category includes amateurs who could be a potential threat. This category is usually used to select "shadow IT" for companies.



The "Modest" user

- ▶ This category includes semi-professional users who have an IT degree/course but consider their abilities to be low (educational attainment and self-assessment are at the same level).

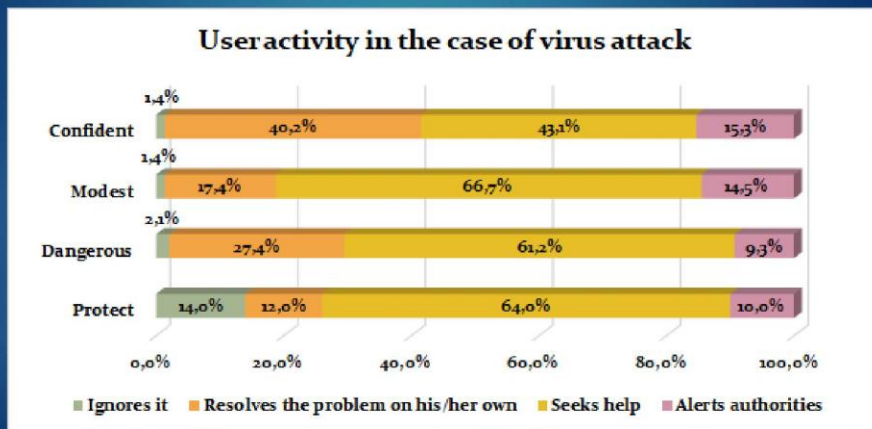


The „Confident“ user

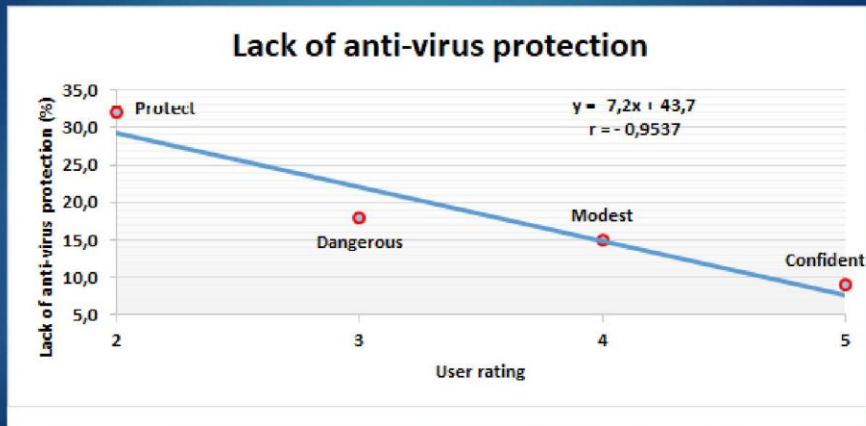
- ▶ This category includes professional users with IT qualifications/courses and who claim to be digitally competent and security conscious.



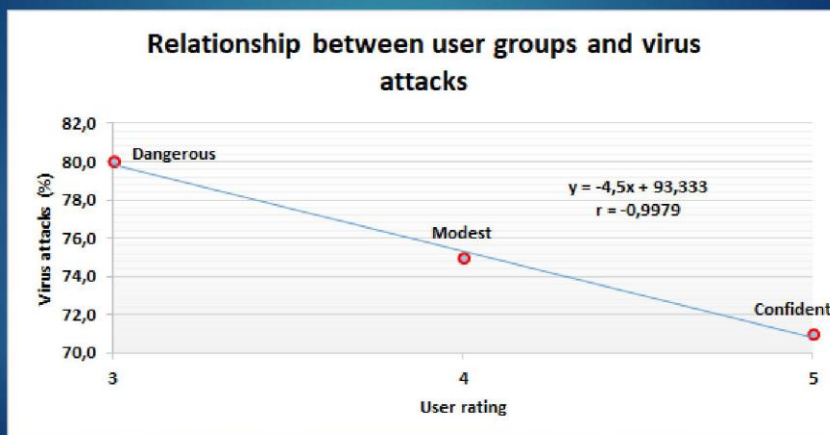
Virus attacks



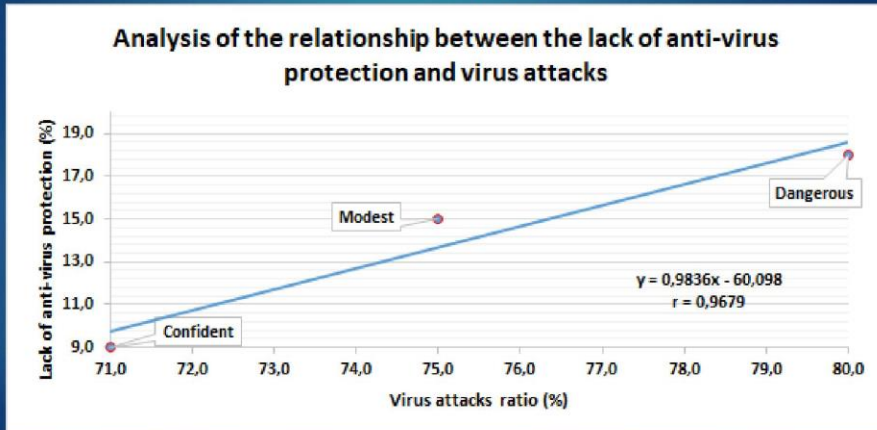
Connection between user classification and antivirus protection



Connection between user classification and virus attacks



Connection between virus attacks and lack of antivirus applications

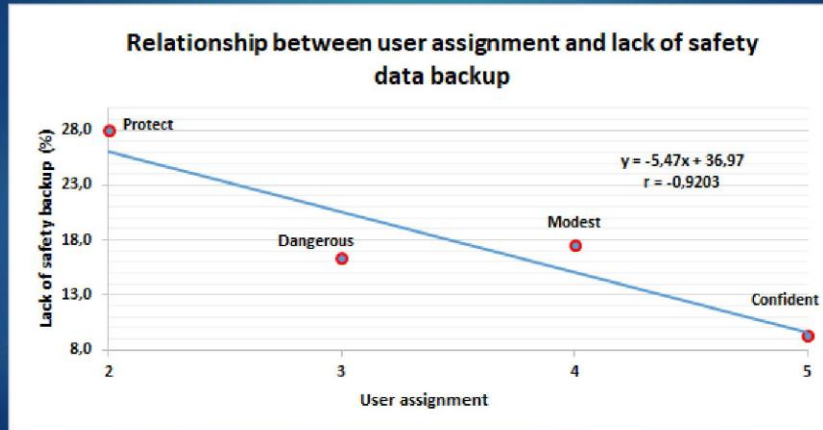


Partial conclusion

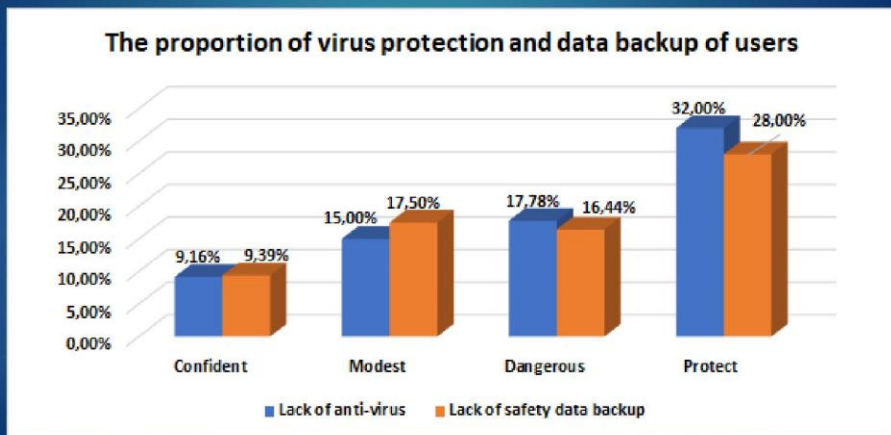


- The results show that if the user does not use virus protection, they will be attacked by a virus.

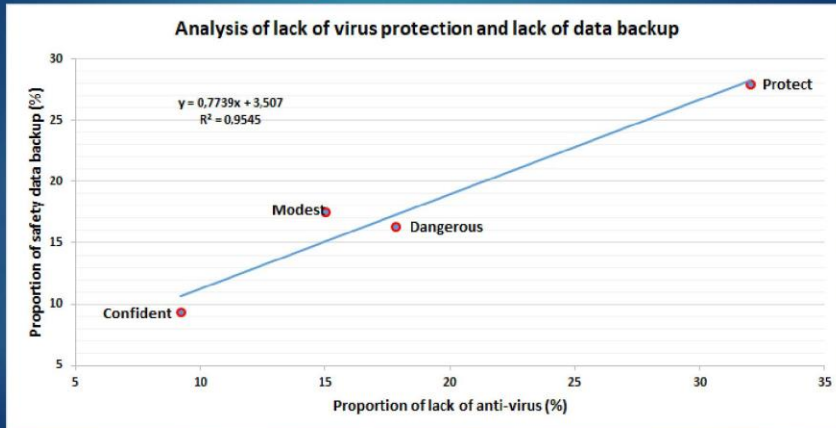
Correlation between user classification and security data backup



Users testing antivirus and data backup habits



Relation between users' antivirus and data saving habits



Summary

- ▶ Users with a higher level of IT knowledge will have greater backup and virus protection.
- ▶ Those who did not study IT do not use a backup or antivirus in a higher percentage.
- ▶ There are more ransomware attacks than those who have not learned computer science.
- ▶ Reducing this risk can greatly improve the CIS security of individuals and companies.

The image is a composite of two parts. The top part is a presentation slide with a dark blue background and light blue diagonal lines. It features several logos: the University of Public Service (Ludovika) logo on the left, the Hungarian Coat of Arms in the center, and the National Defense University (MF) logo on the right. A gold banner at the top right contains the text: "International Scientific Conference on Military Information Security May 13th 2021, Budapest, Hungary". Below the logos, the text "Thank you for your attention." is written in white, followed by the email address "nyikes.zoltan@uni-nke.hu" in green.

The bottom part is a Windows desktop with a red ransomware message. The message reads: "YOU ARE HACKED", "ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!", "IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!", "CONTACT US: no-reply@gmail.com", and "BUT! YOU CAN RESTORE YOUR DATA WITHOUT OUR DECRYPTOR !-:))))))". The desktop background is red. On the left side, there are icons for Firefox, This PC, and a Text folder. On the right side, there are icons for process64, pestudio, Downloads, CCleaner, Revo Uninstall..., Malwareby, Kaspersky internet..., and Recycle Bin. The taskbar at the bottom shows the Windows Start button, task view, and several application icons. The system tray on the right shows the date and time: "ENG 21:28 7/25/2018".

**Károly Imre FEKETE⁶: A brief glance at Quantum
Cryptography and Military Infocommunications**

Correferatum

Infocommunication is essential for current and future military operations. In order to achieve and maintain information supremacy, and from the level of each-fighter to the highest level of military leadership, it is important to ensure robust and secure infocommunications. Today's active components of military systems simply can't handle the immense extremely large amount of data and speed necessary for commanders and soldiers to gain a clear picture of their surroundings and the ability to use that information. The specific problem is that the building blocks of traditional infocommunication systems are based on the building blocks of classical physics and traditional military communication possibilities are developing up year after year, but they have reached their limits in terms of internal quality. But it is easy to see that we cannot make a conventional transistor of 1 or 2 atoms because the physical laws, defining atomic, subatomic and elementary particles quite different than macroscopic physical laws.

Few studies have prospectively examined that, although quantum mechanics and quantum technologies such as quantum computers, communications and cryptography are quite difficult to understand and often contradict ordinary physics, they can still offer unique advantages in some areas such as "superposition", "entanglement", "observation" and "quantum parallelism". The members of the elementary particle family are well introduced in 2021, and the overwhelming majority of our perceptible world is built from these and their interactions. Unfortunately, not all of these are suitable for direct use in the creation of quantum technologies, for now. For example, quarks cannot exist on their own, or the gravitational interaction boson (Higgs boson) is extremely weak, or the range of the strong interaction (Strong force) is very short.

As a hypothesis we can state that, such quantum physics systems as consisting mainly of light waves / photons or electrons or

⁶ Associate Professor of University of Public Service

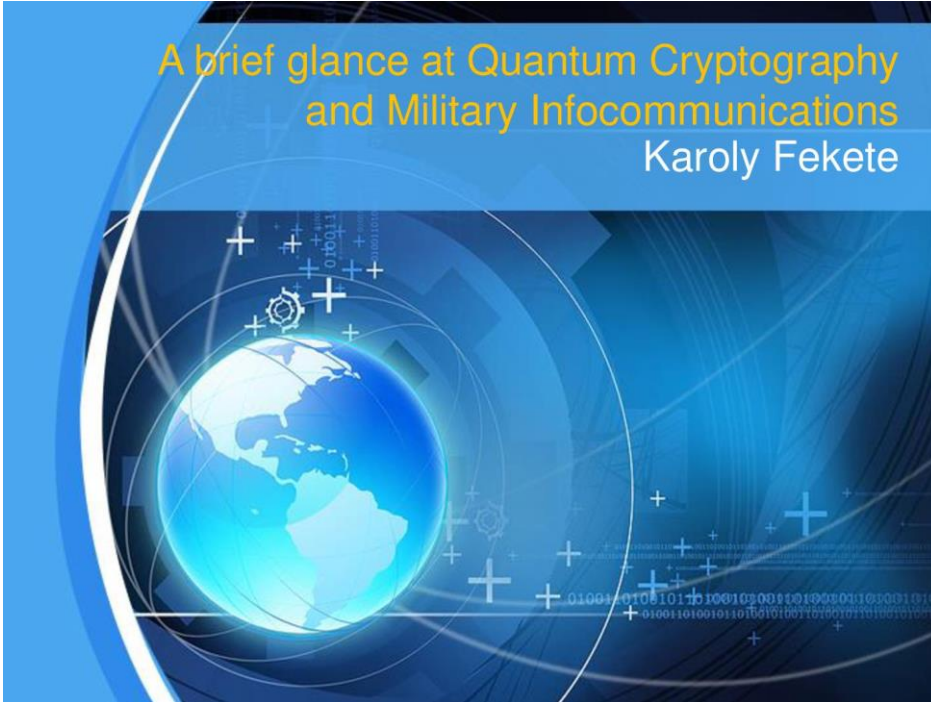
subatomic particles and containing 3 quarks (e.g., protons) are relatively manageable and could be useful in military infocommunications and information security practices.

The results of this approach we may tell that entangled photons can be transmitted about a hundred kilometers through optical fibers before the signal becomes too weak to detect reliably. They can travel much farther through free space, approx. 1200 km nowadays. Quantum entanglement also offers a physical guarantee of security because it allows detection of eavesdropping. That enables secure distribution of a quantum key, which recipients could use to securely encrypt and decrypt a message.

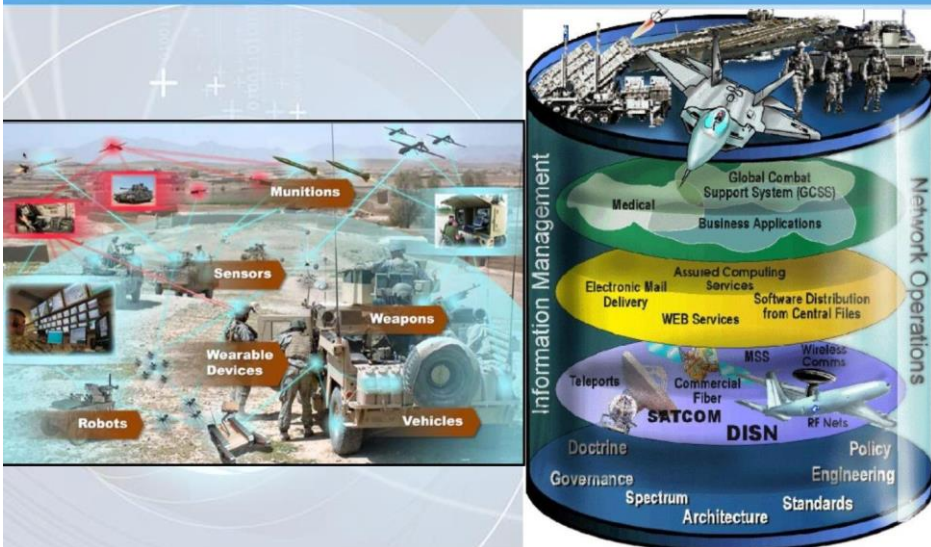
So quantum parallelism allows a single quantum computer to do the work of a distributed military infocommunication system of classical computers, enabling better brute force attacks on cryptographic systems by using this technique along with efficient quantum algorithms, and quantum computational power scales exponentially with the number of qubits added to the system and encoding qubits as entangled photons would allow sharing their states to distribute quantum-computing tasks between locations. Consequently quantum entanglement also offers a physical guarantee of military security because it allows detection of eavesdropping and that enables secure distribution of a quantum key, which recipients could use to securely encrypt and decrypt a message.

A brief glance at Quantum Cryptography and Military Infocommunications

Karoly Fekete

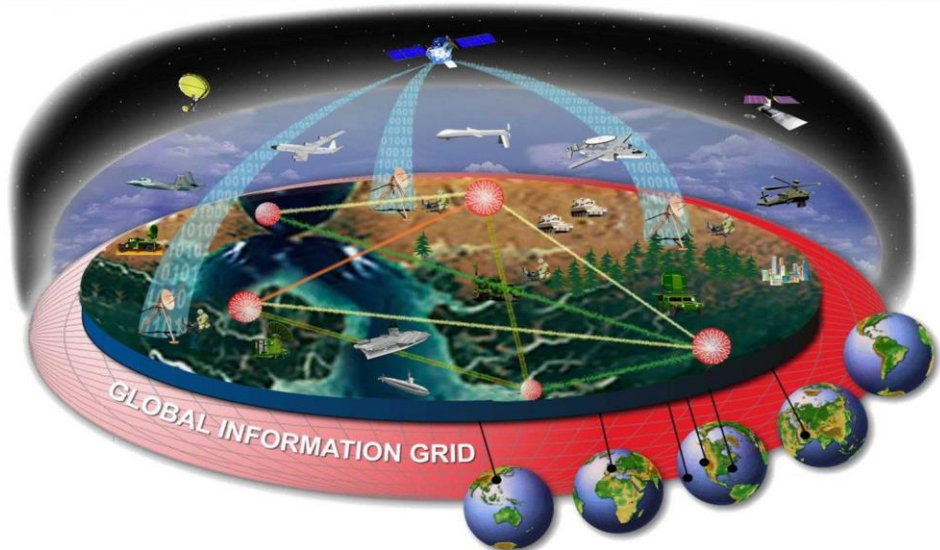


Large amount of data





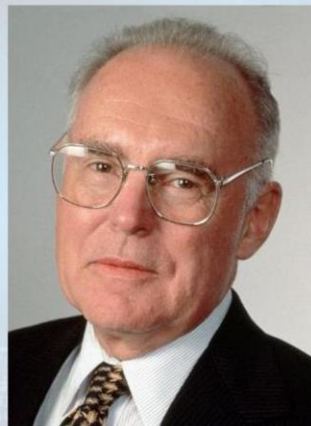
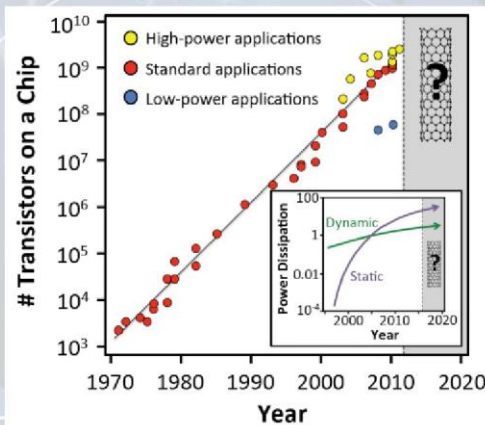
Global information grid



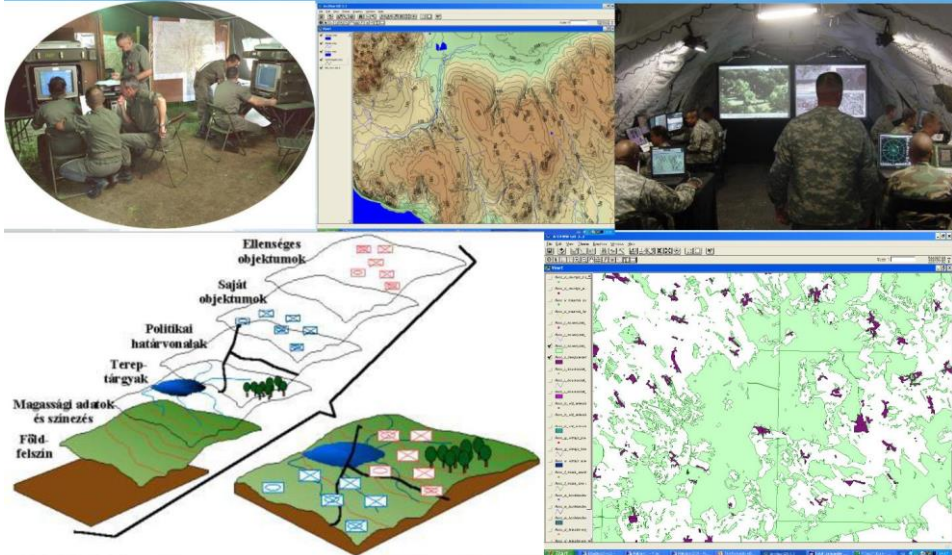
Physical mediums



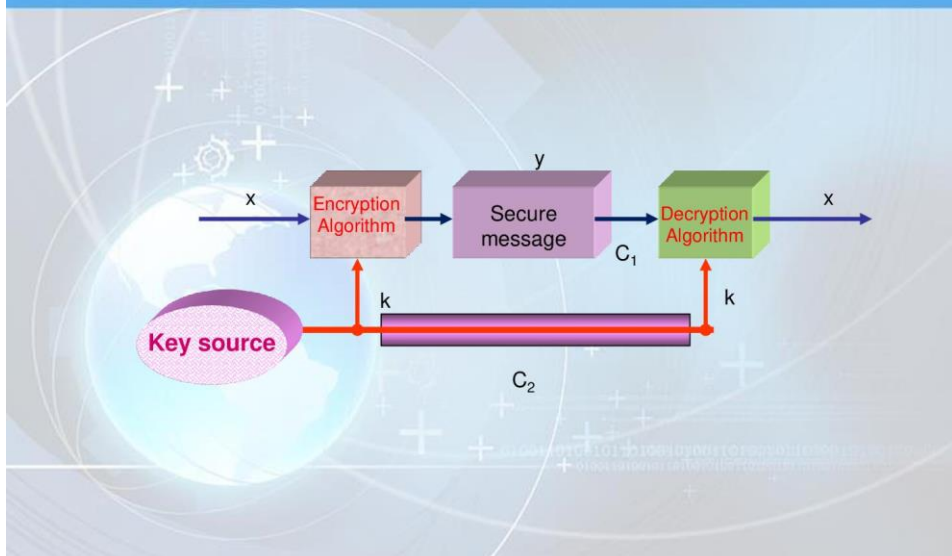
Computing Power



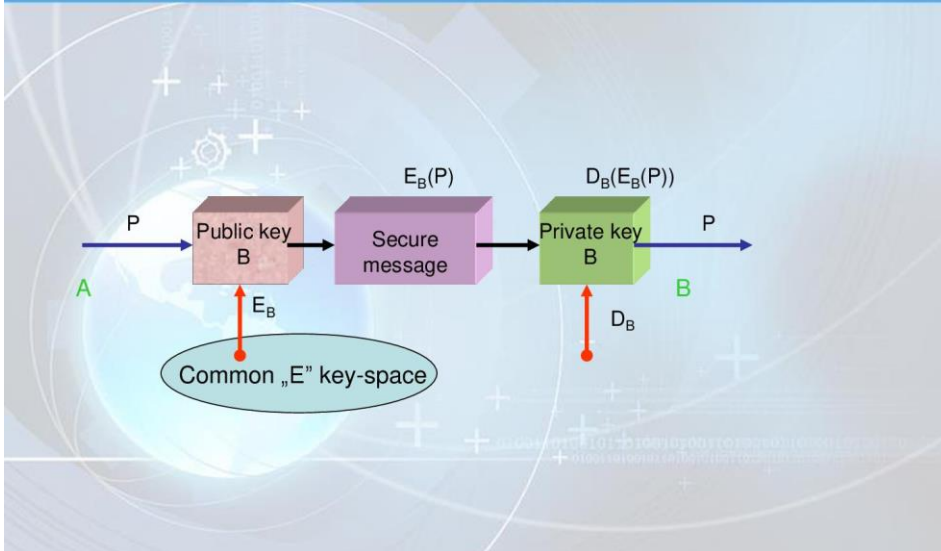
Different Layers of Global Overview



Symmetric-Key Cryptography



Asymmetric (Public) -Key Cryptography

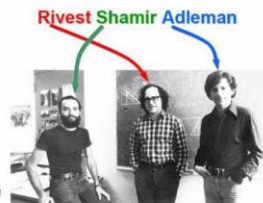


$$f(x) = x^e \pmod{m}$$

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAgb5XVQ+X4+Hvj0kcevRH3avsY2wMctUY6XWKOuiOawoSpBPFs653ndqK6+U
6VSqsjs+b1f9+wBFFP9lGgNhb1M7QWYX+4tu28ibtZCLkoMr+emaTOZqdSr0QbfbD206glvTj01
srW50RZ7HkPuzfjrdEdBykxQx/CnfV1pAf18UKXq16d2RE2S3zFS6HE3lgDuBjGrK4MpzIorb05X
BVM3zqWZ2ZyXzSBd019Hke/OPw+jStxz2eWKAatWprw11CoiT5OwI0iF4qrWkTGMyBe1FfjtYXVb
3Dv91forRkD9rNhl9Yryf0/VDZMcsr7p09BD7YxqN81uVHXcd/10QIDAQABAoIBACLBew9iQfoV
yCrGFxDmrVqSvUojjppTOG8JOB10hdyVNAxjyov9jOT/cD2Lp4Rp3eAo5qyAfduDwYlnoz2eMiEk
Mvw7h3oLP8x9yKeQve14i/WENKHX5L0gRjiUcc+URaZ8KIj475aX/9L3BrwwoP2eBfKDuG2V913
pi27I2oYrvH8QkbHLesLY0Pn3Eh/huBTdQtdG1GpqjR2329xMUxwmmM9VQFUnrQ9TKGbpUmJtGcx
oE006TaU01FnWQ8rAhAgyzJRvhPplgZK3bvicyjZ2otEXuUL9+76RW0KE91/ZRO4m8A1AIOED1/cN
Hf17k3VD3281wnMR0Ngk/utD4eEGYEA0HmoVKRZbo73TWuvG08iiYlq+3BvYnyNk6qBv671OEOu
6uig6jJNzZBctj2GJUnloZhcS2Pm21zXrgo8Rn744ZN9QBHLrS4Ztg49BA7h1Lg1Cc67/i1FFKPF
6n6tDoae19oz2Y24Wln7hbZJet6YraWgTD4gIp81oU60gTisoS0CgYEAn1M7W/BzXbQFoppChMNO
Vss0094WqYbcrxheI2ulsYsRwRtjiUDNow+BWJISz19R1BCqJU3ottt9LN0xibdBwmmDskCUT
IuFwcbQ1E9VgMeRzA7o2Uth/5bkdlJ1hLLErE8b60ex1IxPerVb0o/sKoshRpLpxElmz9JmwpbUC
gYEAatGzF2VNP rXZ+Q3vx1XG8k0nh0/CwBy2EPgtwNYPm6KXzKYzhTy7wFFtesb43beg/dHZXUkwI
yTvCaFclYxS0T14H9T4xhUB3YUQ2Qa4PhCann1USBvH8z05Jvjv7ERnz0Owwg7V9UHAJC3qFDO3
8XkjbVLLHwvBqg2H6v8A5UCgYEA1s1B/vovVpV2So/1KajW9oILO/EvBBDJkTmrKIEN/MIfaao
r4WS7/t37ADy+1KT2H8ISHoOWII1oewm1wxf177q+V3aep4D1daVH4UZ8r5fNrYAKpzkwh1n9X
1Zt1ORcMTfdLkPkum7B56GjYfe1snLz8Qe3Sf11FLh+aS0CgYBEGko6b+FQDmuJnIN7CzhC2nLn
7TAImjB+TmCNPRTmbozZCOUy7To6Tv5whjRPUGloob0P1RZg6rsiE/Wtx+gjjchOj0BnFnGKPO/JD
oCv8LEX/982tB0dwFmRvJdtVd0R1B481HmMePwaE+13Vg5X2Syr5GSPuqeFwEzkXe==
-----END RSA PRIVATE KEY-----

```



Can someone work backwards with a 2048 bit public key to decrypt a cyphertext?

2048 bit → 617 digit

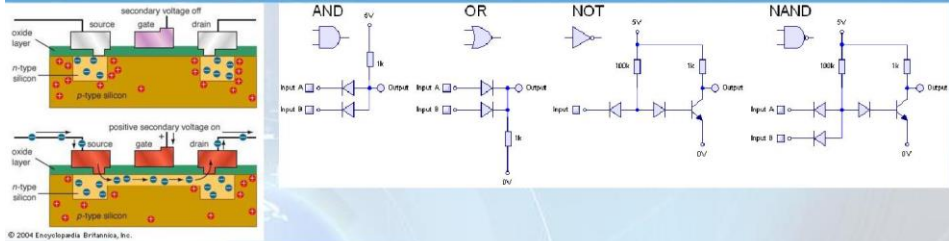
Desktop computer:

470,000 times the age of the universe *

* Age of the universe ~ 13.8 billion years

Application of relative primes, mod (m), Fermat theorem, Euclidean algorithm and congruence !!!

Classic Computer



secondary voltage off

secondary voltage on

oxide layer, source, gate, drain, n-type silicon, p-type silicon

AND, OR, NOT, NAND

Input A, Input B, Output, 5V, 0V, 1k, 10k

© 2004 Encyclopædia Britannica, Inc.

Figure 1. Truth tables

x	y	x ∧ y
0	0	0
0	1	0
1	0	0
1	1	1

Figure 2. Logic gates

Figure 3. De Morgan equivalents

Figure 4. Venn diagrams

Converting the text "hope" into binary

Characters:	h	o	p	e
ASCII Values:	104	111	112	101
Binary Values:	01101000	01101111	01110000	01100101
Bits:	8	8	8	8

Classical and Quantum Physics

Classical physics

- 10K BC? - 1900
- Describes the macroscopic world



- Deterministic
- Intuitive

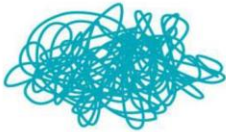
Quantum physics

- 1900 - ?
- Description of the microscopic world

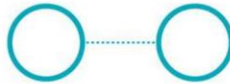


- Probabilistic
- Central role of the observer
- Not very intuitive

Strange principles of Quantum Physics



SUPERPOSITION



ENTANGLEMENT



OBSERVATION

Standard Model of Elementary Particles

	three generations of matter (fermions)			interactions / force carriers (bosons)	
	I	II	III		
mass	$\approx 2.2 \text{ MeV}/c^2$	$\approx 1.28 \text{ GeV}/c^2$	$\approx 173.1 \text{ GeV}/c^2$	0	$\approx 124.9 / \text{GeV}/c^2$
charge	$2/3$	$2/3$	$2/3$	0	0
spin	$1/2$	$1/2$	$1/2$	1	0
	u up	c charm	t top	g gluon	H higgs
	d down	s strange	b bottom	γ photon	
	e electron	μ muon	τ tau	Z Z boson	
	ν_e electron neutrino	ν_μ muon neutrino	ν_τ tau neutrino	W W boson	
	$\approx 0.511 \text{ MeV}/c^2$	$\approx 105.66 \text{ MeV}/c^2$	$\approx 1.7768 \text{ GeV}/c^2$	$\approx 81.19 \text{ GeV}/c^2$	
	-1	-1	-1	0	
	$1/2$	$1/2$	$1/2$	1	
	$< 1.0 \text{ eV}/c^2$	$< 0.17 \text{ MeV}/c^2$	$< 18.2 \text{ MeV}/c^2$	$\approx 80.39 \text{ GeV}/c^2$	
	0	0	0	≈ 1	
	$1/2$	$1/2$	$1/2$	1	

QUARKS (left side of the table)

LEPTONS (left side of the table)

GAUGE BOSONS VECTOR BOSONS (bottom right of the table)

SCALAR BOSONS (right side of the table)

Digital Bit vs. Qubit

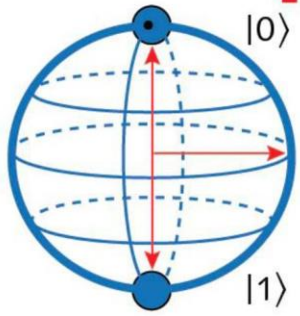
Digital bit in one of two states

○ 0

● 1

Can be either 0 or 1

Qubit superposition of two states



$|0\rangle$

$|1\rangle$

$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Superposition of states can be anywhere on sphere

CLASSIC COMPUTER

2 bit:

Operation is repeated separately for each combinations of 0 and 1

00
10
01
11

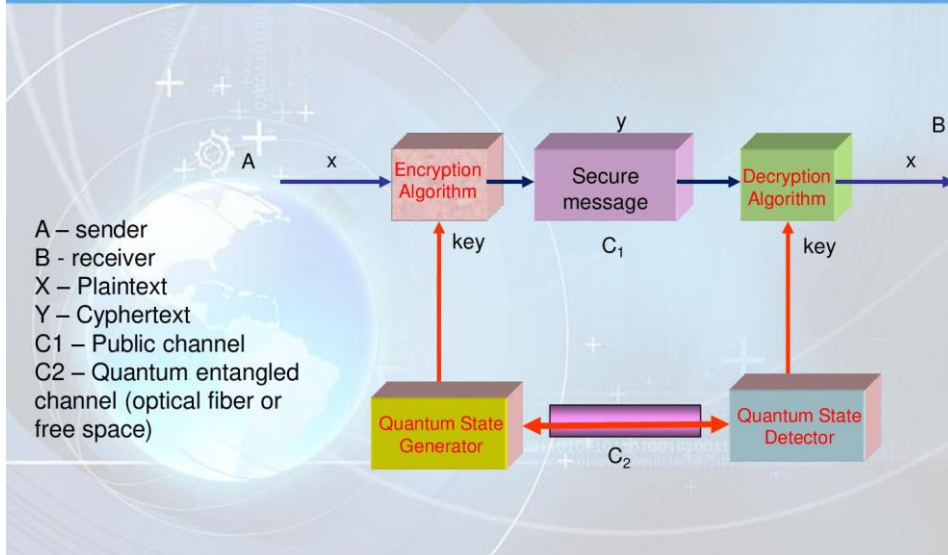
QUANTUM COMPUTER

2 qubit:

Operation is performed only once for all combinations of 0 and 1



Quantum Cryptography



Cracking the key (RSA-2048)

```
-----BEGIN RSA PRIVATE KEY-----
•
• MIIePAlBAAKCAQEAqb9XVQ+X4+Hvj0kcgEvRH3avSY2wMctUY6XWKou1OawoSpBPFs653ndqK6+U
• 6Vsqjs+blf9+wBFPvPg1GgNhbIM7QWYX+4tuZ8ibtZCLk0Mr+smaTOZqDsr0QbfbdB206glvTj0i
• srW50RZ7HkPuzfjxdEdBykxQx/Cnfv1pAf18UkXq16d2RE2S3zFS6HE31gDuBjGrK4MpzIOrb05X
• BVDM3zqRwJ2ZyXzSbd019Hke/OPw+jSrxZeWkAtWprw11CoiT5OwI0iF4qrWkTGMyBe1FFjtYXVb
• 3Dv91forRkD8fNhsYryf0/yDZMcsr7p08BD7yXqhN81uVHXKcd/10QIDAQAABAoIBACLBsw9iQfoV
• yCrGfXDMrvqsvJojppQIOG8J0b10hdyVNaXjyov9jOT/cD2Lp4Rp3eAo5qyAfdUDWY1noz2eMiEk
• Mvw7h3oLP8x9yKeQVeI4i/WENKHx5LOgRjiUcr+URaZ8KIj475aX/9L3B rwwzoP2sBfKDuG2V913
• piZ7I2oYrvH8QkbH1ssLY0Pn3Eh/huBTdQtdGIGPqjR2329xMUxwmmM9VQFUNq9TKGpbUmJtGrx
• oE006TaU01FnWQ8rAhAgyzJrvhPplg2K3bvcyJj2otEXuuL9+76RWOKE91/ZRO4m0A1AIOED1/rN
• Hf17k3VD3Z8IwnMR0Ngk/utD4sECgYEA0HmoVKRZbo73TWuvG08iiYlq+3BvYnyNk6qBv6710EOu
• 6uig6jJNzBctj2GJUn1oZhcS2Pm2IzXrgo8Rn744Zn9QBHLrS4Ztg4sBA7h1Lg1Cc67/i1FFKfF
• 6nGtDoae19oz2YZ4Wln7hbZJet6YraWgTD4gIp81oU60gTis0CgYEAn1M7w/HzXbQFoPpCHMNO
• Vss0094WqYbcrxheI2ulsYsRwRtjiUDNow+BJWISz19R1BCqCJU3ottt89LN0xibdBwmmDSKcUT
• IuPwcbQ1EyVgMerA27o2Urh/5bkdlJIhLLErE8b60ex1IxRerVb0o/sKoshRpLpxElmzsJmmpbUC
• gYEAtGzF2VNPrrxz+Q3vx1XG8kOnh0/CwBY2EPgtwNYPm6KXzKYzhTy7wFPtesb43beg/dHZXUkwI
• ytvCAfclYx0T14H9T4xhxUB3YUQ2Qa4PhCannlUSBvH8z05Jv7w7Ernz00wwg7V9UHAJC3qfD03
• 8XkjbVLLHwubVqq2H6v8A5UCgYEA1s1B/voYvpVZSo/1KaJWsOIL0/EvBBDJKtXmrKIEN/MIfaao
• R4WS7/t37ADY+1KT2H8ISHoOWIIiOoewmIwxcfl77Q+V3aep4D1daVH4UZHr5fNrYAKpzkwlin9X
• 1ztlorcMTfDlkPkum7B5GJcyfelnLz8Qe3Sf11FLh+aSo0CgYBEGko6b+fqDmuJnIn7CzhC2nln
• 7TAlmjB+TmCNZPRTmbz2C0Uy7To6Tv5wHjRPUG1oObOPiRZg6rsiE/Wtx+gjchOj0BnPnGKP0/JD
• oHcv8LEX/982tBodw6FmRvJdtvd0R1B481hMrMePwaE+13Vg9X2SYr5GSPuqeFwfzKXeA==
• -----END RSA PRIVATE KEY-----
```

Can a 2048-bit quantum computer break it the RSA-2048 encryption key?

NOT YET.

References

- Niels M. P. Neumann, Maran P. P. van Heesch, Patrick de Graaf: Quantum Communication for Military Applications, International Conference on Military Communication and Information Systems, ICMCIS 2021, 4-5 May 2021, Virtual edition, Cornell University;
- Jeffrey D. Morris, Ph.D.: Implications of Quantum Information Processing On Military Operations, DEPARTMENT OF THE ARMY UNITED STATE MILITARY ACADEMY, ARMY CYBER INSTITUTE, West Point, New York ;
- C. E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal 28(4), pp. 656-715. 1949., http://dm.ing.unibs.it/giuzzi/corsi/Support/papers-cryptography/Communication_Theory_of_Secrecy_Systems.pdf.
- Bernhardt, Chris: Quantum Computing for Everyone, The MIT Press, Cambridge, Massachusetts, London, England, 2019, ISBN 9780262039253;
- Yacine Merdjemak: Cybersecurity in a post-quantum world, Homeland Defense & Security Education Summit, March 23-24, 2017, George Mason University, Arlington, VA;

References

- Seiki Akama: Elements of Quantum Computing: History, Theories and Engineering Applications, Springer International Publishing Switzerland 2015, ISBN 978-3-319-08283-7, DOI 10.1007/978-3-319-08284-4;
- International Institute for Strategic Studies: Quantum computing and defence, The Military Balance 2019, February 2019, pp: 18-20;
- Jeff Hecht: Quantum science: The quest for quantum information technology expands, LaserFocusWorld, Jul 14th, 2020, ISSN 1043-8092;
- Sanjeev Naguleswaran: A New Paradigm for Secure Military Communications: Quantum Information Processing; Defence Systems Innovation Centre (DSIC), c/o CDCIN, The University of Adelaide, Adelaide, Australia, January 2010.

**A brief glance at Quantum Cryptography
and Military Infocommunications**

Karoly Fekete



**Thank you very much for
attention!**

Balázs SZATMÁRI⁷: Counter-UAV solutions

Correferatum

The growth of C-UAV (Counter-Unmanned Aerial Vehicle) technology is directly related to the mounting concerns about the threat UAVs pose in both civilian and wartime environment. The FAA predicts there will be between 1.3 million and 1.7 million hobby drones in the U.S. by 2023. The last 10 years a lot of incidents happened connected with UAVs.

Counter UAV system usually consist of a detections systems (radar, and acoustic, radio frequency (RF) emission and electro-optical (EO) sensing), an electronic defences (command link jamming and appropriation, and Global Navigation Satellite System (GNSS) jamming and spoofing), and kinetic defences (shooting down UAVs and net capture using interceptor UAVs).

In my presentation you can find few C-UAV solutions which are working in reality.

⁷ Instructor of University of Public Service


NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTSZTKÉPZŐ KAR
ELEKTRONIKAI HADVISELÉS TANSZÉK



Conter-UAV Solutions

**NO DRONE
ZONE**



Cpt. SZATMÁRI Balázs
Tel.: 29-217
+36309811851
szatmari.balazs.gabor@uni-nke.hu


NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTSZTKÉPZŐ KAR

Schedule

- UAV,
- Drone,
- UAS,
- Why we use UAVs?,
- Why the UAVs threat us?,
- How can we protect us from a UAV attack?
- C-UAV solution,
- Questions.



What is UAV?

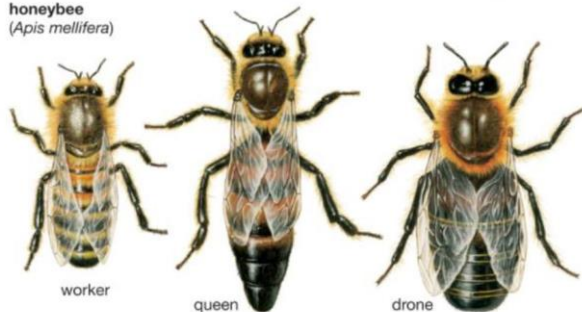
- UA – Unmanned Aircraft,
- UAV – Unmanned Aerial Vehicle,
- UAVS - Unmanned Aerial Vehicle System,
- UAS - Unmanned Aerial System,
- RPV – Remotely Piloted Vehicle,
- RPAS - Remotely piloted aircraft systems,
- UCAV – Unmanned Combat Aerial Vehicle,
- RC – Radio Control (Airplanes)



What is drone?



honeybee
(*Apis mellifera*)




© 2012 Encyclopædia Britannica, Inc.

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZAKÉPZŐ KAR

What is UAS consist of?

- Unmanned aircraft,
- Ground Control station,
- Communication channel,
- GNSS,
- Operator.

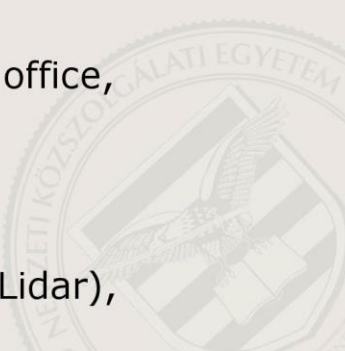


The diagram illustrates the components of a UAS system. At the top left, a satellite is shown with signal waves. A yellow lightning bolt labeled 'Data Link' connects the satellite to an unmanned aircraft in the center. Below the aircraft, a ground control station (GCS) is depicted, consisting of a laptop and other equipment. To the right of the GCS, an operator in a uniform is shown standing next to a handheld remote control device. The background features a faint watermark of the National Defense University logo.

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZAKÉPZŐ KAR

Why we use UAV?

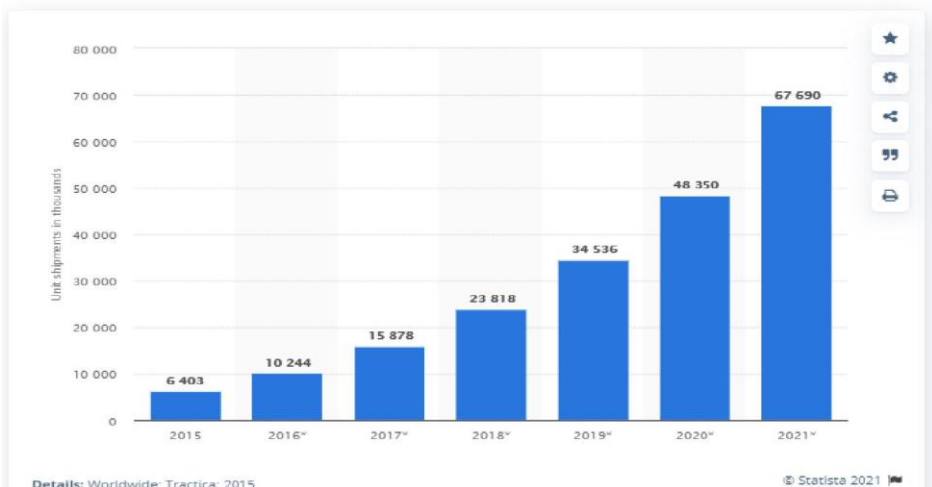
- Transporting goods (Amazon, pizza, icecream),
- Health care (medicine, emergency blood transport, defibrillator),
- Lifeguard,
- Military, police, fireman, tax office,
- Just for fun,
- Agricultural,
- 3D modelling,
- Archaeological excavations (Lidar),



The background of this slide features a large, faint watermark of the National Defense University logo, which includes a shield with a cross and a crown on top.



Global unit shipments of consumer drones from 2015 to 2021
(in 1,000s)



Why the UAVs threat us?

- Japan Prime Minister Office Tokio (2015),
- White House incident (2015),
- Serbia – Albania football match (2014),
- F91 Dudelange – FK Qarabag football match (2019),
- Venezuela President Attack (2018),
- German Luna incident in Kabul (2009),
- Angela Merkel (2013),
- Queen Elizabeth (2017),
- ISIS propaganda video, bombing,

Why the UAVs threat us?

- Russian Military Base Syria (2018),
- Prison,
- Gatwick Airport (2018),
- Smugling,
- Oil processing facilities in Saud Arabia (2019),
- Erbil International Airport (2021).

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KAR

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KAR

Japan Prime Minister Office Tokio (2015)



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KAR

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KAR

White House Washington (2015)

SMALL DRONE CRASHES NEAR WHITE HOUSE



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZAKÉPZŐ KAR

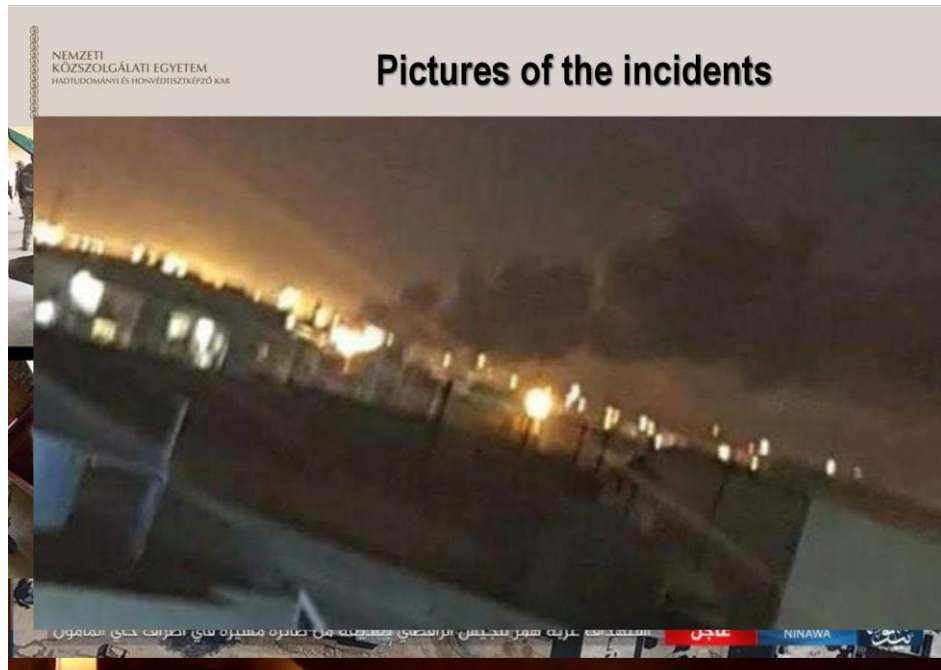
President of Venezuela Caracas (2018)



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZAKÉPZŐ KAR

Kabul 2009





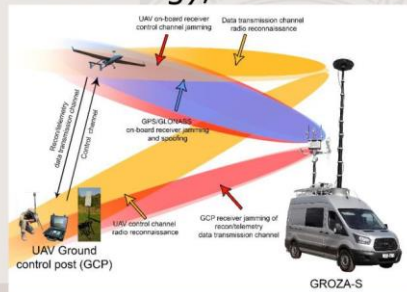
NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKÉZŐ KAR

How can we protect us from a UAV attack?

- With law?
- With Air Defence?
- With gun? <https://www.youtube.com/watch?v=rGLxKXtkHpY>
- With run?
- With a bird?
- With a net?
- With an another drone?
- With a CUAV system?

What we should do?

- Detect:
 - Visible light;
 - Sound waves;
 - Infra;
 - With radar;
 - Electronic warfare (DF-direction finding);



The spectrum of the C-UAC activities

- Kinetic spectrum:
 - Gun???, Special C-UAV gun,
 - Birds of prey,
 - Net.
- Electromagnetic spectrum:
 - Jamming the control frequencies,
 - Jamming the GNSS frequencies,
 - Spoofing the GNSS,
 - Directed energy weapons,
 - Hacking, take control.



Dropster Net gun



Skywall

Open Works Engineering (UK)

Use compressed air
Smart projectile
Weight: 12kg
Laser rangefinder
Range 10-100m
Max UAV speed: 15m/s



Drone Buster

Radio Hill (USA)

Jamming the control and GNSS frequencies

3 hours continuous jamming

Weight: 2kg

Range: 3x the distance
between the UAV and GCS



Drone Rannger

Van Cleve and Associates (USA), MGT EUROPE (UK), VTE (ITA)

360° Scan by radar

Range: ~ 2km

Visible light, infrared

Jamming the control frequencies

Jamming GNSS signal



NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KARR

Mesmer

Department 13(USA)

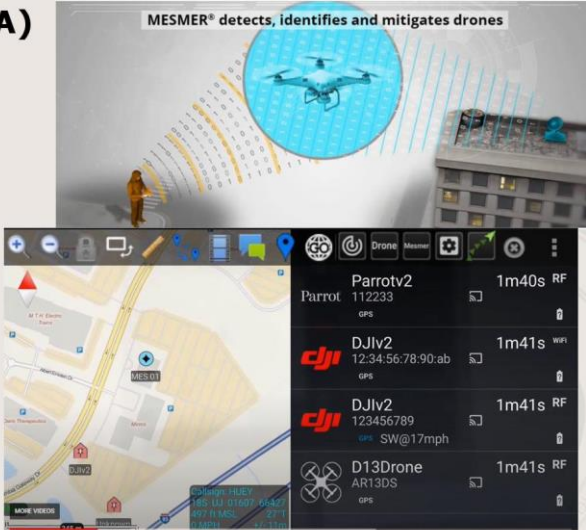
Detect, identifies
and mitigates UAV,

Non kinetic,

Non jamming,

Range: 4km,
Take control th UAV.


MESMER® detects, identifies and mitigates drones



Drone Model	Altitude	Speed
Parrotv2	1m40s	RF
DJiV2	1m41s	WiFi
DJiV2	1m41s	RF
D13Drone	1m41s	RF

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTSZÉKFEJZŐ KARR

Dutch Company is training eagles



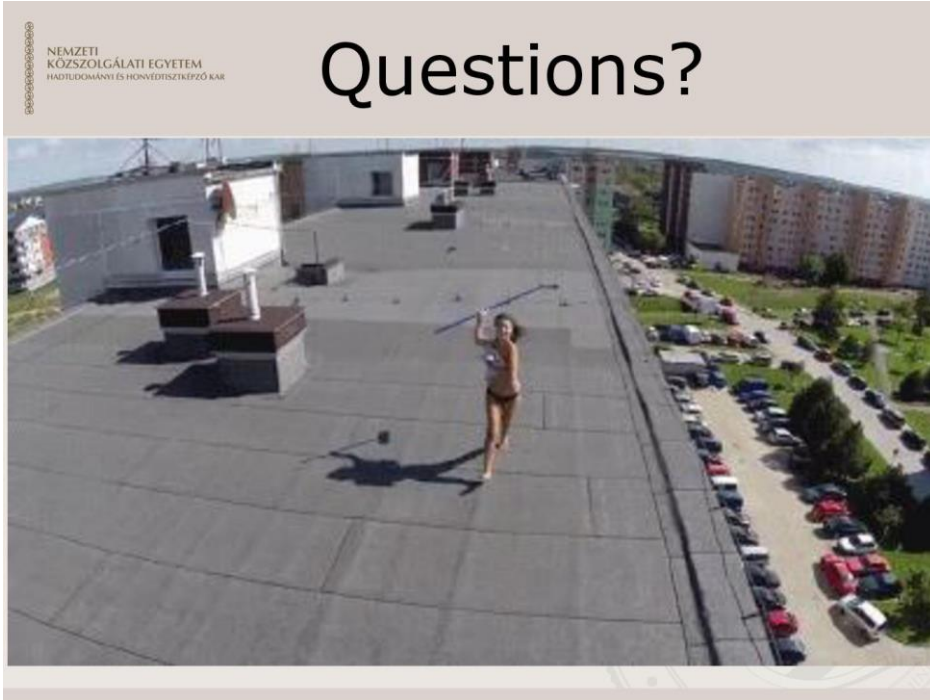
Raytheon

szabadszolgálat

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDELTECHNOLÓGIAI KAR

Conclusion, future questions

- You can only think in system !!!,
- False alarms, lack of detection -> Is the device reliable?,
- Filter out our own drones, don't attack it,
- Safe delivery of the "captured" drone,
- Smart UAVs,
- UAV swarm,
- Use UAV to fight against UAV.



Kristóf KRALOVÁNSZKY⁸: You can't protect what you can't see -- Cybersecurity challenges of critical and vulnerable infrastructures

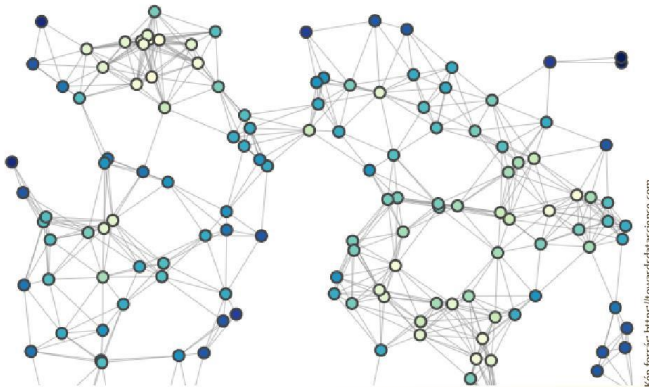
Correferatum

We need to know exactly what the infrastructure to be protected consists of. However, this is far from exhaustive in the physical components of infrastructures. Perhaps even more important is the identification of interdependencies, which is at the same time an extremely complex process and increasingly challenging to complete. Significant risks need to be identified in the old-fashioned way – no question about that. Certain other groups of risks need to be ruled out quite simply, which can be achieved by eliminating specific vulnerabilities. However – to eliminate such vulnerabilities – it is necessary to identify those that usually occur using defensive techniques.

The exponential increase in the complexity of systems and the highly dynamic changes of threats do not leave enough time for a defensive approach, so offensive protection is increasingly unavoidable, which – in this case – is the batch elimination of partially unidentified vulnerabilities.

The presentation aims to show the details and justification of this new approach.

⁸ Assistant Professor of University of Public Service



You can't protect what you can't see

Cybersecurity challenges of critical and vulnerable infrastructures

Kristóf Kralovánszky, jr. assistant professor – NUPS Department of Electronic Warfare

13 May, 2021.

Problem #1

Number of critical
infrastructure in practice



Number of critical
infrastructure by law

Already a huge gap
between the numbers

Vulnerable: critical in
practice,
not just by law

Lot of vulnerabilities
invisible to the law

Problem #2

Increased exposure to
critical infrastructure
by magnitudes



Society's increased
exposure to cyber

Take cyber out from the
equation



Exposure increase is not
that significant



The real problem we have to
deal with is: **cyber**



Problem #3

- Cyber is not an issue - nor is a difficulty
- **Cyber is a fully functional domain**
- In current state sponsored operations it is the most widely used domain
- The reasons are easy – and make cyber the ideal domain:
 - Cheap
 - Accessible from anywhere
 - Operations can mostly stay in the grey zone
 - Successful operations really hurt



Problem #4

- As societies develop we are more and more reliant on *supporting infrastructure*.
- In a modern society these supporting infrastructures became vital
- This is how the two supercritical infrastructures were born: power (electricity) and telecommunications
- They don't work without each other
- No other critical infrastructure works without them



Problem #5

We look at the entire infrastructure and see that it is critical, but we don't see what really makes them critical.



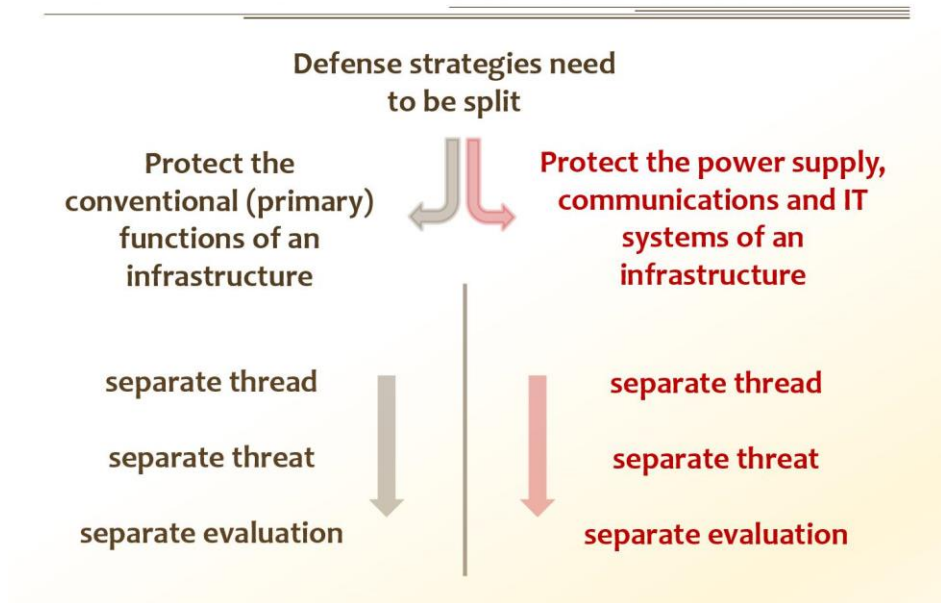
What we don't (want to) see
we cannot protect



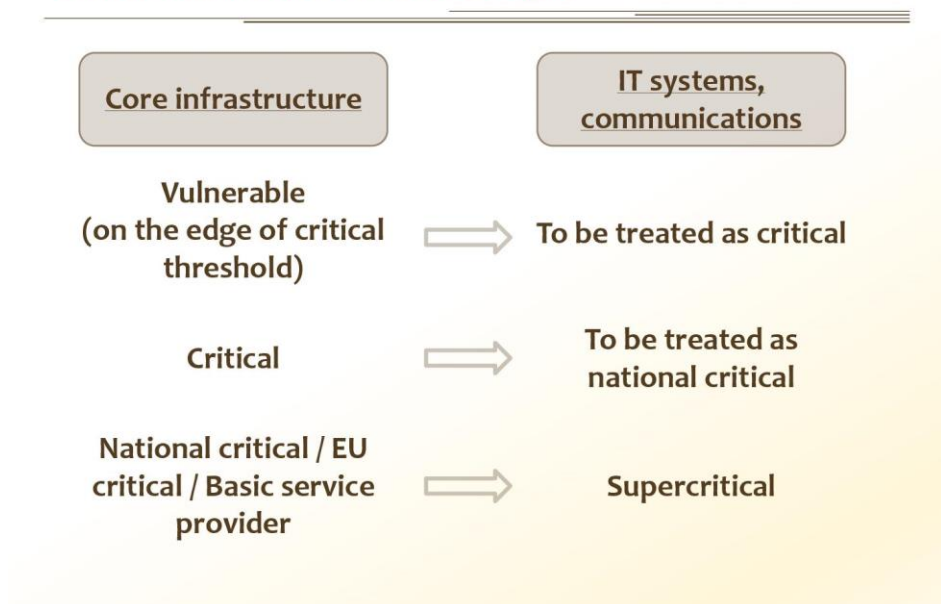
This is what makes and
leaves us vulnerable



A possible way forward



Other fields that need to be split



Further requirements

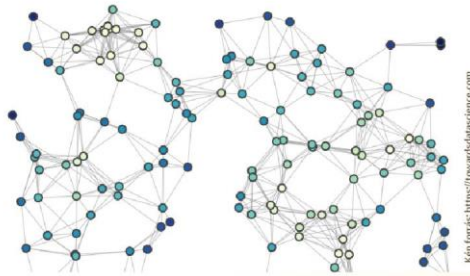
- Separate, simple, clean legislation for different levels of critical infrastructures.
- Simple, detailed requirements for IT systems in critical infrastructures – divided into levels with clear, specific thresholds.

without these

Insufficient protection will further increase overall vulnerabilities.

and the risk:

What we cannot see, we cannot protect!



Thank you!

**Lajos MEGYERI⁹: Biometric identification for security
purposes**

Correferatum

This publication presents the possibilities of biometric identification, a significant part of it. The sub-area selected from a wide range of handling of special personal data is evolving dynamically. This publication examines the possibilities of facial recognition, including special cases of application.

With the development of the system of technical tools, the legislators try to develop the legal background of the field in accordance with the current situation and to amend it if necessary. In the publication, I also touch on the current situation of this, I also analyze the advantages and possible disadvantages of the framework created by the legislation.



Biometric identification for
security purposes

University of Public Service

Faculty of Military Science and Officer Training

Signal Department

Megyeri Lajos Lt.col.

Zrínyi kampusz A building. 808

Tel.: 29-361

e-mail: megyeri.lajos@uni-nke.hu

⁹ Assistant Professor of University of Public Service



Content

- History
- Technical requirements
- Structures of System
- Software
- Legislation
- Results



History

- Biometric identification is the same age as humanity.
- Among people who know each other closely, facial recognition was crucial.
- One consequence of the scientific revolutions was a more accurate knowledge of the human body.
- New means of identification, fingerprinting, appeared in law enforcement.





Face recognition

- Of course, there are other unique personality traits that can be identified in the human body, such as fingerprints, iris recordings, voice recognition, digitization of palm veins, and behavioral measurements. Why face recognition?
- Facial biometrics remain the preferred biometric reference. This is because an installed system can quickly and accurately identify individuals without physical interaction.



Purpose

- Person authentication, Biometric data protection, access to services (mobile unlocking) Increasing physical security.
- Person identification: Screening of criminals, terrorist suspects, detection on a fixed image, tracking a person's movement in space.



Technology: (Person identification)



- Face recognition systems are basically made up of four parts:
- Camera - resolution, volume
- Data transmission channel - continuous, secure data transmissionprocessing
- Software - fast, error-free operation
- Storage unit - adequate capacity, CIA principle

Camera



- The algorithm used by the software running in the system depends on the quality of the image required for successful recognition, but a certain minimum must be met in order for the algorithm to be able to efficiently process the received image information signals.
- The resolution and sensitivity of the camera determine its usability. In general, the required minimum image resolution of 5 Mp and the resolution of the optics mounted on the camera cannot be worse. The degree of sensitivity required depends on the place of use, as well as the natural and artificial lighting there. The mounted positioning, height and angle of the camera are also important.



Technology: (Person authentication)

- **Two-dimensional face recognition:** Your phone's camera takes a photo of the face from multiple angles and then stores certain geometric proportions of the mouth and face into a digital sequence. The degree of security is technology dependent.
- **3D Face Detection:** Uses an extra sensor, such as infrared recording. Security level is higher. According to Apple, Touch ID (i.e. fingerprint unlock) has a 1: 50,000 chance of accidentally opening the phone when using an unauthorized finger. Face ID (face recognition unlock) has a significantly lower ratio of 1: 1,000,000 - (except for identical twins) So their 3D face recognition function is many times more secure than fingerprint readers.

Data transmission channel



- If the camera and data processing location are different.
- Bandwidth should be sufficient.
- It can be metal based, traditional systems, optical cable for modern systems, wireless network.
- Ensuring confidentiality, integrity and availability requires technical design and the application of different rules for each system.





Processing software

- In 2014, Facebook announced its DeepFace program, which can determine with 97.25% accuracy whether two photographed faces belong to the same person. When you take the same test, people answer correctly in 97.53% of cases, which is only 0.28% better than the Facebook program.
- Clearview AI combines photos from millions of websites in a database of more than three billion photos, seven times the size of the U.S. Federal Bureau of Investigation.
- (Defense: The user can apply a filter that modifies certain pixels in the image before it goes to the web. These changes are invisible to the human eye, but are very confusing to facial recognition algorithms.)



Processing software

- In 2015, FaceNet achieved a new record accuracy with 99.63% match accuracy.
- Online operation:Thales 'facial recognition software (LFIS) solution achieved excellent results with a 99.44% face capture rate in less than 5 seconds.





Legal situation

- Storing image information is the source of most legal problems.

Prohibitions:

- Concerns from civil rights defenders have increased. In the U.S., San Francisco voted to ban facial recognition on May 6, 2019. It was then followed in Boston, Oakland, San Diego, California, and Portland. Federal legislation has not yet been enacted.
- In Europe, the GDPR regulates the processing of biometric data (General Data Protection Regulation).
- In Hungary, the basic legislation is Regulation 2016/679 of the European Parliament and of the Council (eu), which entered into force on 27 April 2016, with a grace period of 2 years.) And which became known as the GDPR. According to the law, a digital signal sequence made of a human face is considered personal data.



Newest issue : COVID 19

- Mandatory wearing of masks makes facial recognition difficult.
- Thales, NEC, and EDGENeural.ai, are shaping their algorithms to improve the face recognition accuracy of masked individuals.
- After September 11, 2001, the U.S. increased biometric identification upon entry. This can also mean iris, DNA, vein scans.
- In high-security locations, it may also be mandatory to remove the mask for a few moments.



Newest issue: COVID 19

- In July 2020, the National Institute of Standards and Technology (NIST) report following a series of experiments using pre-COVID-19 algorithms to assess the ability of existing biometric systems to cope when faces are partially obscured.
- It uses a combination of facial and iris recognition technologies in its Bio-IDiom system. Even with mask wearers, we can achieve approximately 99% recognition accuracy with the technology.



Summary

- Face recognition is of great importance primarily in the fight against crime
- Proper design and consistent compliance can reduce citizens' concerns about restrictions on their freedom.
- Masking the face, of course, makes accurate identification difficult, but where resources allow, an effective protection system can be established and operated.

Sources:

- Otti Csaba Arcfelismerő rendszerek gyakorlati problémái Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar otti.csaba@bgtk.uni-obuda
- <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition>
- <https://broutonlab.com/blog/how-facial-recognition-works-with-face-masks>



Thank you for your attention!

Don't worry if the presentation was short.

The coffee break will be longer :))

András TÓTH¹⁰: Information security issues in IoT solutions

Correferatum

This presentation gives the results of the first step of a longer research project. The main topic of the fundamental research is the cloud-based cyber defence possibilities for IoT devices funded by the Hungarian Academy of Sciences and the Ministry of Innovation and Technology.

In this presentation, the presenter shows the results of his examination of the vulnerabilities and threats of IoTs today. He was looking for the answer to the following two questions:

- What are the main vulnerabilities and threats in IoT solutions?
- How are these risks related to each other?

To answer the research questions and get the best results, a literature review and keyword analysis were used to identify the most common keywords for IoT vulnerabilities. For this, the Scopus database was used to analyse the most relevant works to the topic. After identifying keywords, the occurrence of each keyword in the documents was examined, based on which the 25 most common issues were identified that could affect IoT devices and systems.

Finally, the VOSviewer software was used to perform a comparative analysis illustrating the connexions of each keyword concerning the relevant literature.

After deeper examination, the most common security issues were identified, and the conclusion was drawn that there are strong links between them.

¹⁰ Associate Professor of University of Public Service



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA

FACULTY OF MILITARY SCIENCE
AND OFFICER TRAINING
PRO PATRIA AD MORTEM!



International Scientific Conference on Military Information Security

13th May 2021

Information security issues in IoT solutions

Andras TOTH

University of Public Service



„Supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-20-5-NKE-5 New National Excellence Program of the Ministry of Innovation and Technology from the source of the National Research, Development and Innovation Fund.”



Objectives

- I Research purpose, motivation
- II Methodology
- III Research
- IV Results
- V Conclusions

I. Research purpose, motivation

RQ1

What are the main vulnerabilities and threats in IoT solutions?

RQ2

How are these risks related to each other?

II. Methodology

- Literature review and keyword analysis with the objectives:
 - identification of keywords for IoT vulnerabilities (SCOPUS);
 - quantitative analysis based on keyword matches for different threats and vulnerabilities;
 - comprehensive analysis of keywords and topic (VOSviewer).

III/1. Research

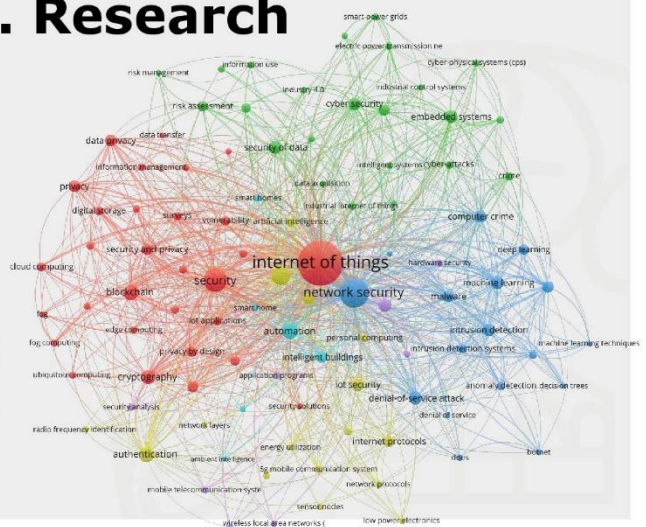
Data

- Research queries:
 - IoT AND vulnerabilities – 2161 results;
 - IoT AND vulnerabilities AND LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) – 1379 results.
- Type of documents:
 - Conference Proceeding – 594;
 - Journals – 565;
 - Books – 220.

III/2. Research

7687 Keywords –
Top 100 keyword network
6 different clusters

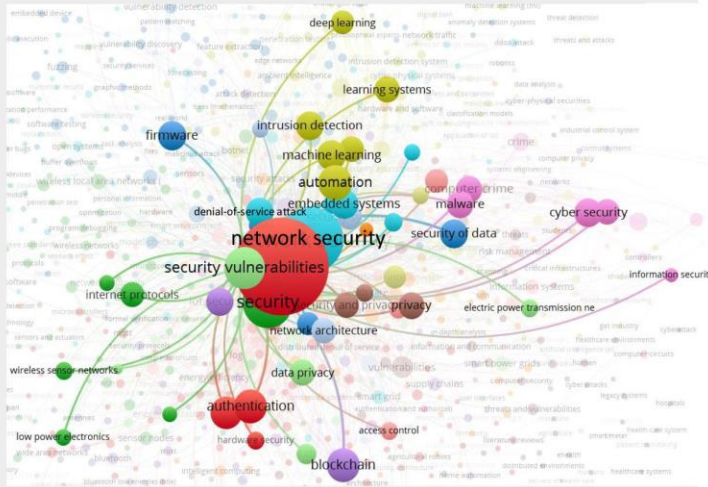
Cluster 1 (30 items)	Cluster 2 (23 items)	Cluster 3 (17 items)
access control	crime	anomaly detection
big data	cyber physical system	botnet
blockchain	cyber security	computer crime
cloud computing	cyber-attacks	ddos
cryptography	cyber-physical systems	decision trees
data privacy	cybersecurity	deep learning
data transfer	data acquisition	denial of service attack
decision making	electric power transmis	future research director
digital storage	embedded systems	intrusion detection
edge computing	industrial control system	intrusion detection syst
fog	industrial internet of thi	learning algorithms
fog computing	industry 4.0	learning systems
health care	information systems	machine learning techn
information manage	information use	malware
internet of things	intelligent systems	network security
iot applications	risk assessment	
privacy	risk management	
privacy by design	security mechanism	
security	security of data	
security and privacy	smart grid	
security challenges	smart power grids	
security issues	vulnerabilities	
security requirements	vulnerability assessment	
security solutions		
security systems		
security threats		
smart city		
surveys		
ubiquitous computing		
vulnerability		



III/3. Research

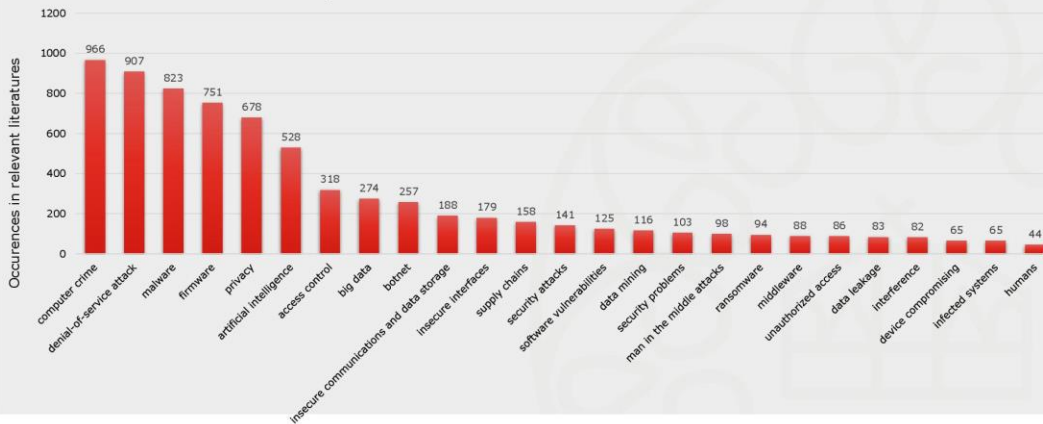
The main connections of security vulnerabilities

- DoS;
- Firmware;
- Malware;
- Privacy;
- Big data;
- Access control...



IV/1. Results

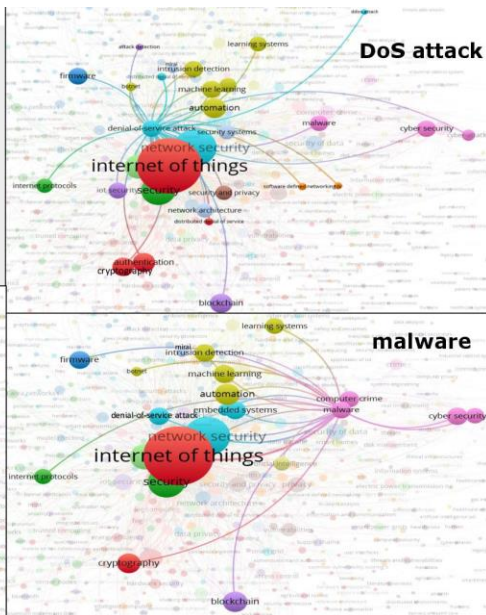
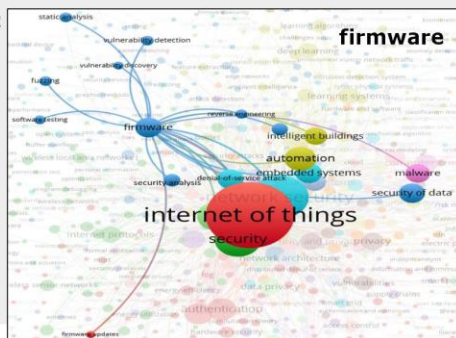
The top 25 IoT vulnerabilities and threats



IV/2. Results

The main connections of denial-of-service attack & malware & firmware

- firmware;
- malware;
- botnet;
- Mirai...



Conclusions



References

- K. Kandasamy et al., 'IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process', *Eurasip Journal on Information Security* 2020, no. 1 (2020), <https://doi.org/10.1186/s13635-020-00111-0>.
- S. Singh, K. Singh, and A. Saxena, 'Security Domain, Threats, Privacy Issues in the Internet of Things (IoT): A Survey', 2020, 287-94, <https://doi.org/10.1109/I-SMAC49090.2020.9243358>.
- A.K. Tyagi and D. Goyal, 'A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things', 2020, 386-94, <https://doi.org/10.1109/ICCES48766.2020.09137886>.
- X. Jiang, M. Lora, and S. Chattopadhyay, 'An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices', *ACM Transactions on Internet Technology* 20, no. 2 (2020), <https://doi.org/10.1145/3379542>.
- M. Yu et al., 'A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices', *Future Internet* 12, no. 2 (2020), <https://doi.org/10.3390/fi12020027>.
- F. Meneghello et al., 'IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices', *IEEE Internet of Things Journal* 6, no. 5 (2019): 8182-8201, <https://doi.org/10.1109/JIOT.2019.2935189>.



THANK YOU!

en.uni-nke.hu

Attila SZÚCS¹¹: Security issues in distance education

Correferatum

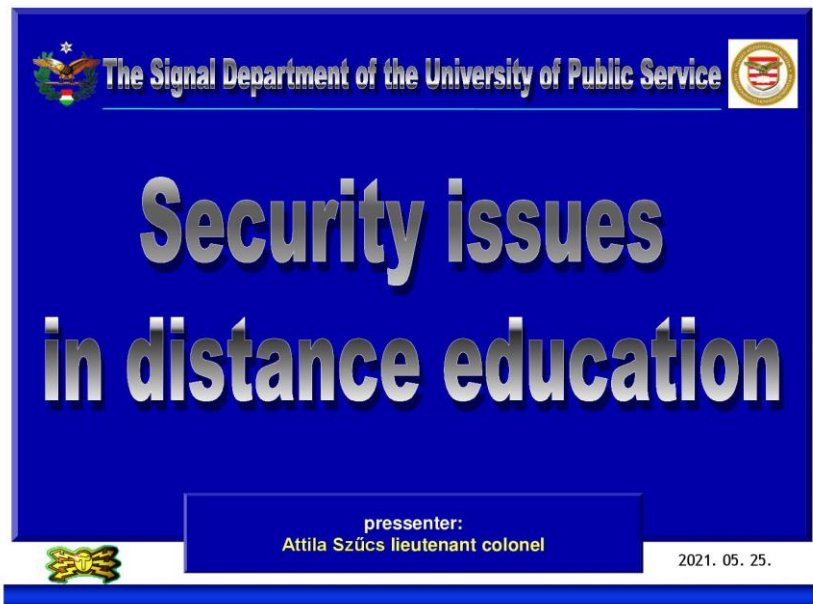
What is distance learning and what's the problem with it?

The problems occur in three areas:

First, the security of communication and information flow.
Transmission channel reliability.

The Information security in the classical sense, information protection. What we can share on online interfaces and what we can't. How can we easily make mistakes? How can we avoid this?

The third type of security issue is the checking. It is difficult to control how much of the student's own knowledge is what we see.



¹¹ Assistant Professor of University of Public Service

Initially

- ▶ At the end of the 19th century by mail.
- ▶ In the first half of the 20th century by the radio.
- ▶ In the last decades of 20th century the breakthrough came from computer networks.

Up to 2 years ago

- ▶ electronic distance education: in higher education and in specialized training centers
- ▶ Specially curricula, audit evaluation.
- ▶ Distance learning system for communication.
- ▶ appropriate security protocols.

And the COVID crisis began

- ▶ In higher education, there was something to reach for.
- ▶ There are well-established channels of communication (Neptun or MOODLE)
- ▶ Software application capability (teames, zoom, etc ...)

Security of transmission.

- ▶ The transmission channel reliability.
- ▶ Did they get the message? Did they read the message?
- ▶ Stable the network.
- ▶ Lack of feedback.

Information security in the classical sense, information protection.

- ▶ Classified or confidential cannot transferable!
- ▶ What about the abstracts and teaching aids prepared?
- ▶ The moodle cannot protecte in 100%
- ▶ The student downloads are uncontrollable!

The online lessons problematic.

- ▶ The providers cannot prevent malicious acces.
- ▶ The chat surface is preserved.
- ▶ The students recorded?

Information security in the checking.

- ▶ Tasks requested by e-mail.
- ▶ Well for a general topic ← → avoided for a sensitive topic.
- ▶ Sometimes the answer is problematic

Suggestion

We “proofread” each other

to spot problems that result from simple inattention.

The future: VPN and encrypted connections ?

Security issue in the checking

- ▶ How much of the student's own knowledge is what we see.
- ▶ In an oral hearing, you can use a "tool" or the help of a partner.
- ▶ The built-in test system of moodle can help.
- ▶ If someone use an aid → runs out of time.

Summary

- ▶ The technical side are outside of us.
- ▶ It is up to us to control the information transmitte. Help to each other.
- ▶ Realistically control the knowledge transferred.

Thank you for your kind attention.

Questions?

Zoltán HORVÁTH¹²: Information security of the radio networks, presentation of the possibilities of digital radios

Correferatum

The author aims to present the technical possibilities on the shortwave and in the lower band of the ultrashortwave of how to protect the information transmitted on the radio network and how to make it too difficult to locate the installed radios. Information security is a complex task. This affects the environmental, personal, and administrative areas and increases the security of information processed and transmitted electronically.

Comparing traditional analog and modern digital radios possibilities is not the same. How to increase the security of transmission paths and possibilities to encode and decode information. The radio channel is an open channel. Not only the recipient but also other stations can receive and interpret the transmitted signals. To prevention this, digital radios have many advantages over analog devices.

The analog radio systems use a selected frequency. It is received and demodulated in an analog manner. The modulation methods used mainly analog amplitude modulation and frequency modulation. Observing and listening to the radio channel is a simple task; the radio system can be easily detected and listened to. However, digital radios are microprocessor controlled. The technological level of our time makes it is possible. A requirement is that digital radios be able to work with traditional systems.

Interoperability digital signal processing has many possibilities, such as encoding-decoding, communication between radios, during which radios can identify each other, evaluate the quality of the radio channel, refine the system time.

By switching to digital signal processing at a fixed frequency, it is no longer possible to connect with traditional devices. Interception is not possible with a conventional reconnaissance device. On the other hand, its advantage is the ability to transfer data to establish a computer-to-computer connection.

¹² Assistant Professor of University of Public Service

One way of machine communication between radios is to identify the radios. This allows building a point-to-point connection within a network. Using several frequencies for some independent connection system can be established.

During frequency hopping, the hopping sequence is dependent on more parameters. It depends on the date and network ID. If these parameters do not match, the frequencies are changed in a different order.

The great advantage of this is that several hopping networks can be operated simultaneously in a given band, as the current transmission frequency will not be the same. This means that several networks can operate in the same band at the same time.

We can use it, for narrowband hopping (Its bandwidth requirement does not exceed the bandwidth requirement of a traditional AM channel.), for broadband hopping (In this case, the bandwidth demand can reach the order of 1 MHz.), and list hopping (in this case, only the preselected frequencies are used.).

There are several advantages to using it in the shortwave and the lower band of the ultrashortwave with digital signal processing in the future.



Information security of the radio networks, presentation of the possibilities of digital radios

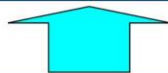


Horváth Zoltán László PhD
Professor assistant



Information Security

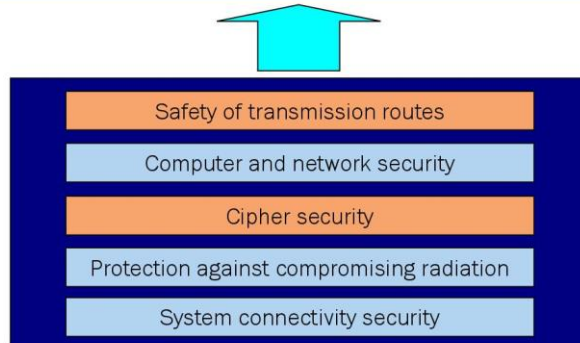
Protect information against unauthorised cognition, copying, transmission, modification or destruction that may occur intentionally or inadvertently.



Introduction

Electronic Information Security

Ensuring the Confidentiality, Integrity and Availability of electronic information.

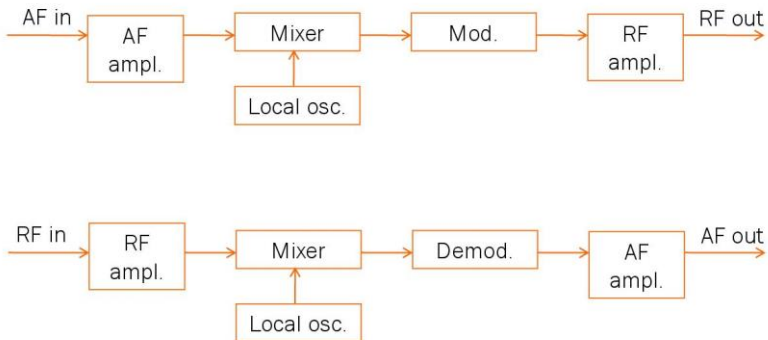


Safety of transmission

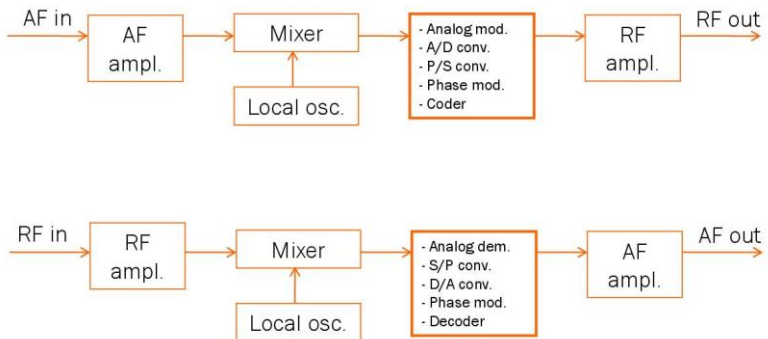




Analog radio structure



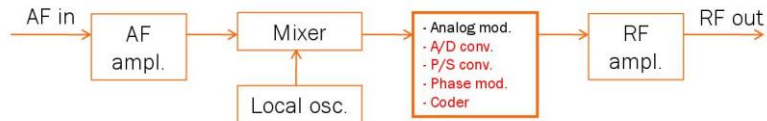
Digital radio structure



FIX frequency mode

Using voice-modems (digitization of sound)

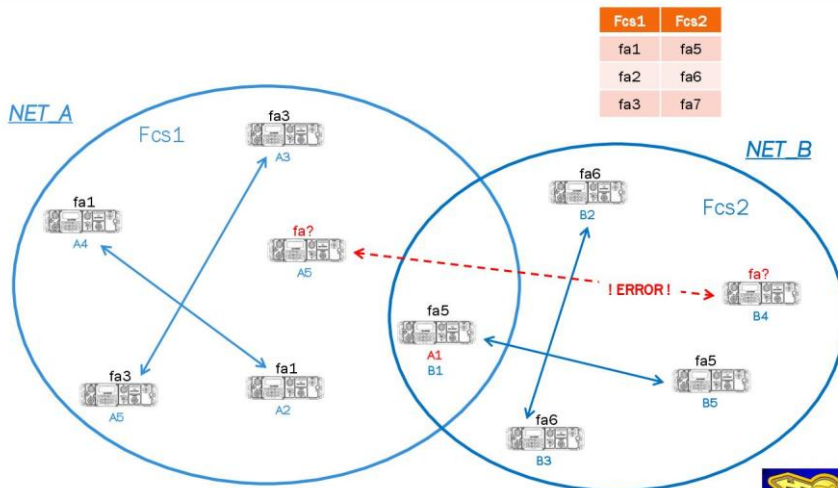
- o Voice modems provide digitization of the analog signal. Analog signals are emitted as digital phase modulated signals.



- o Contact is not possible with conventional devices.
- o With a conventional reconnaissance device, eavesdropping does not take place.



Automatic link establish





Frequency hopping



Joint applicability of bands

- The frequency hopping sequence is affected by several parameters
 - Date: year, month, day, hour, minute, second
 - Network ID
- If the parameters do not match for the different systems, the currently used frequency is not the same

Because of its:

More than one systems can operate in the same band without interfering with each other.



Frequency hopping



Narrow band frequency hopping

- Its bandwidth requirement is not greater than that of a conventional AM signal

Wide band frequency hopping

- The applied bandwidth may exceed 1 MHz.

Frequency hopping according to a list

- Use only predefined frequencies.





**THANK YOU FOR YOUR
ATTENTION**



Published by the Signal Department of the University of Public
Service

www.comconf.hu

HU ISSN 2061-9499

University of Public Service
Signal Department
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15