sciendo

LATVIAN JOURNAL OF PHYSICS
AND TECHNICAL SCIENCES
2020, N 1-2

DOI: 10.2478/lpts-2020-0007

# INFORMATION SYSTEM CYBER THREATS AND TELECOMMUNICATIONS ENGINEERING COURSES

M. Sneps-Sneppe[1]*, D. Namiot[2]**, R. Pauliks[1]***

[1] Ventspils International Radio Astronomy Centre,
Ventspils University of Applied Sciences,
101 Inzenieru Str., Ventspils, LV-3601, LATVIA
*e-mail: manfredss@venta.lv
***e-mail: romass@venta.lv

[2] Faculty of Computational Mathematics and Cybernetics,
Lomonosov Moscow State University,
1 Leninskiye Gory, Moscow, 119991 RUSSIA
**e-mail: dnamiot@gmail.com

The article discusses the issue of training of telecommunications engineers. The architecture of telecommunications solutions is changing very quickly. Obviously, training programmes must also change. Cybersecurity issues are one of the main drivers of change in telecommunications solutions and, therefore, training programmes. They have become the main issues in all processes related to digital transformation. At the same time, it is clear that the development of education in telecommunications clearly lags behind modern requirements. Such issues come to the fore in relation to the development of digital economy programmes. Cyber security issues for military telecommunications solutions are discussed separately.

***Keywords:*** cybersecurity, education, telecom

## 1. INTRODUCTION

Several trends have shaped the telecommunications industry over the past few years. Most prominent examples, such as Software Defined Networks (SDN), Network Function Virtualization (NFV), Artificial Intelligence (AI), Internet of Things (IoT), and mobile technology 5G, show a growing number of connected devices and the increasing importance of the software. The knowledge of these trends is expected from graduates of telecommunications study programmes.

The paper is initiated by the approach to telecommunications engineer education developed at the University of Applied Sciences, FH Campus Wien [1]. In [1], the new study degree programme "Computer Science and Digital Communications" (hereinafter Vienna Programme) is offered. During the first three semesters, students obtain a solid basis in mathematics, programming and communication networks as well as fundamentals in telecommunications, security and software engineering. Four free elective modules in 4th and 5th semesters are introduced, namely:

- Micro-Controller for low-level programming skills;
- Software Systems for high-level programming and AI skills;
- Modern Networks for telecommunications and IoT skills;
- IT-Security for cryptography and cybersecurity skills.

The aim of the present study is to evaluate whether education changes proposed by the Vienna Programme are reasonable and justified. In the study, we focus on Information System issues. The rest of the paper is organised as follows. In Section 2, we discuss telecom fraud and telecom architectures. In Section 3, we target military communications. Section 4 is devoted to conclusions.

## 2. EVOLUTION OF TELECOM FRAUD

Cybersecurity and Telecommunications generally go hand in hand. Many of the targets of cybercrime are focused around the telecoms industry. As advanced technology changes the way telecoms companies run business, cybersecurity also needs to increase [2].

Understanding of the current threat landscape in the field of telecommunications can help reduce the impact of crime like telecom fraud and prepare us for future threats in the age of the IoT. The annual cost of telecommunications subscription fraud is estimated up to more than US$12 billion, while others foresee the actual losses to be far greater, between 3 percent and 10 percent of the operators' gross revenues [3].

**Circuit Switching.** The older type of telecom network design is circuit-switched technology, which is similar to the one that was once used by human switchboard operators. These switchboard operators would verbally ask who the call was for and manually plug cables into a switchboard to establish the connection (the circuit). Eventually, the human switchboard operators were replaced by automated machines, but the technology design was effectively unchanged for a hundred years (Fig. 1). A very common vulnerability in these networks was that the switchboard operators would listen to the conversations of all the most interesting people in the city [4].

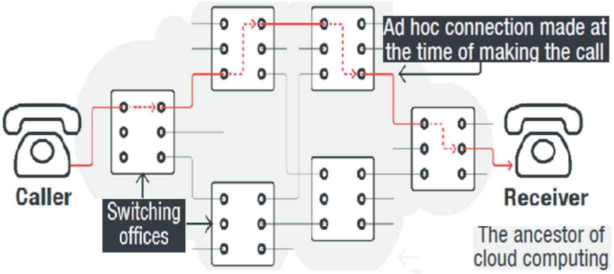
Ad hoc connection made at the time of making the call
Caller
Switching offices
Receiver
The ancestor of cloud computing

*Fig. 1.* Switch paths establishing voice circuits to carry voice calls in a circuit-switched network [4].

**The Hardware Defined Network – Packet Switching.** When the resource constraints and scalability limitations of circuit-switched networks became obvious, the emerging "new" information technology and circuit miniaturization became very attractive. Many carriers are on track to become content delivery networks (voice and video), replacing most methods people use to consume media content (Fig. 2).

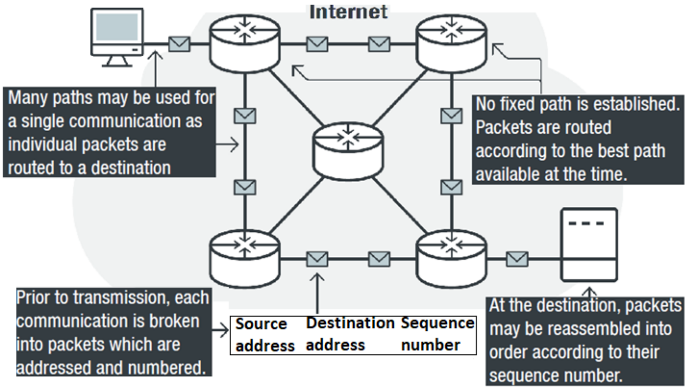
Internet
Many paths may be used for a single communication as individual packets are routed to a destination
No fixed path is established. Packets are routed according to the best path available at the time.
Prior to transmission, each communication is broken into packets which are addressed and numbered.
Source address
Destination address
Sequence number
At the destination, packets may be reassembled into order according to their sequence number.

*Fig. 2.* Internet equipment responsible for establishing voice circuits to carry voice calls [4].

Packet-switched networks combine many of the vulnerabilities and risks in circuit-switched networks (e.g., wiretap, roaming frauds, SIM card supply chain issues, etc.) with "traditional" IT security risks (e.g., hackers, spies, viruses, worms, etc.). The primary approach of protecting these networks comes from an unscalable kind of network isolation in which every carrier attempts to replicate the IT security means.

**The Software-Defined Network.** The newer types of telecom automation require advanced management techniques called cloud orchestration or orchestrators, which include Software-Defined Network and Network Function Virtualization. These orchestrators handle the various hybrid circuit-like, packet-like networks called network slices. Such type of network architecture is extremely sophisticated. Note that each User Equipment has up to eight channels having different QoS features (up to eight QoS Flows) that transmit these flows through up to eight slices. The 5G architecture expects the underlying networks and base stations to ensure the required QoS characteristics (such as packet delay, packet loss) without specifying how (at least, by now).

Since these networks inherit the vulnerabilities of both circuit-switched and packet-switched networks, the result is that the effects of old risks will be amplified due to the automation of their delivery media (the carrier amplifies the effect of the attack), or new hybrid attacks will become available (telecom fraud viruses and worms).

**Fraud Case 1: International Revenue Share Fraud.** IRSF is a general term for a number of frauds. Generically, the frauds in this group are characterised by the involvement of three parties:

- One victim from whom fraudulent billing or criminal revenue is taken through a variety of methods, and two sets of criminals;

- Being the “grey or white” money laundering function group for stolen billing or revenue;
- Being a “black” function driving the hacking originating the fraud (Fig. 3).

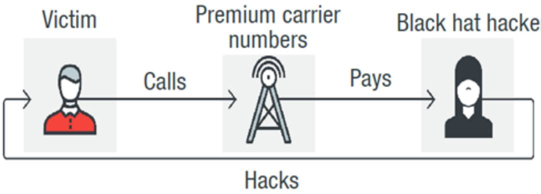

*Fig. 3.* The simplest IRSF scheme [4].

**Fraud Case 2: Intermarket/Interconnect Bypass Fraud.** SIM boxes are devices capable of using many SIMs at once. A SIM box can be used for making calls, originating data, or sending SMS (Fig. 4). When used to perform a criminal activity, this device and its management are controlled by the criminal and it passes only the information the criminal intends. According to a rough estimate, fraudsters can easily generate over US$100 per modem in a SIM box, and since one SIM box can contain 30 to 60 modems, this adds up to a US$6,000 revenue loss per day or over US$2 million per year.

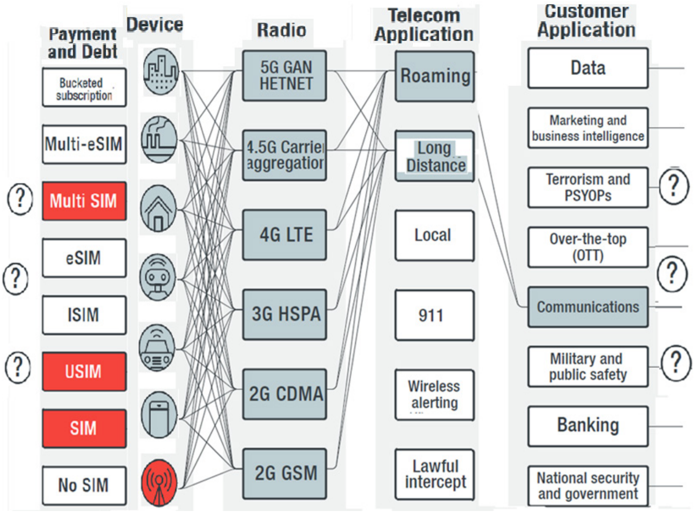

*Fig. 4.* Intermarket/interconnect bypass fraud threat model:
combined network model showing both ends of the telecom delivery “pipe”
at far-left and far-right ends of the diagram, each represented as ? sign [4].

In conclusion, on the one hand, the current trend indicates larger and more scalable attacks; on the other, additional motivators drawing attention to this class of attack are the very lucrative employment opportunities for individuals with security/hacking/fraud skills. At the time of writing [4], a senior individual might be offered US$250,000 and additionally US$150,000 in bonuses and equity, for a total of US$400,000 in salary. In Europe, a consultant might be offered 2,000 euros daily.

## 3. CYBERSECURITY IN MILITARY COMMUNICATIONS

The telecom modernisation process of the Department of Defence (DoD) through three generations:

- The implementation of signalling protocol SS7 and Advanced Intelligent Network;
- Transformation from SS7 to IP protocol;
- The extremely ambitious cybersecurity issues. During this process, the cyber vulnerabilities are increasing.

All these digital transformations asked for more and more skilled professionals in both telecommunications and software.

**DoD cyber threats.** According to a recent Government Accounting Office (GAO) report [6], the United States weapon systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities, and the federal information security needs to improve "the abilities to detect, respond to, and mitigate cyber incidents", increase its cyber workforce and cybersecurity training efforts. How to say for sure that all vulnerabilities are detected and removed?

DoD weapon systems are more software dependent and more networked than ever before (Fig. 5). From ships to aircraft, the weapons are becoming more technologically advanced and use more software and less hardware to control everything from navigation to weapon systems. The F-35 Lighting II software (aircraft) contains eight million lines of code and controls everything from flight controls to radar functionality, communications, and weapon deployment.

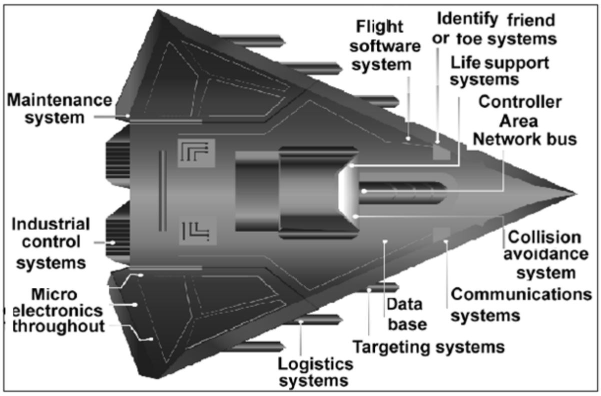
Flight software system
Identify friend or foe systems
Life support systems
Controller Area Network bus
Maintenance system
Industrial control systems
Micro electronics throughout
Collision avoidance system
Communications systems
Data base
Targeting systems
Logistics systems

*Fig. 5.* Embedded software and information technology systems in weapon systems (represented via fictitious weapon system for classification reasons) [6].

**DoD modernisation program.** Under the pressure of the industry, the DoD is trying to introduce the latest achievements [7], namely, Software Defined Network and Network Function Virtualisation (Fig. 6), which, honestly speaking, increase cyber threats as any new technology added.

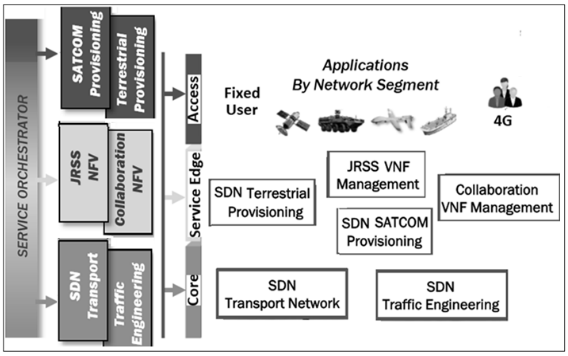

*Fig. 6.* The latest DISN architecture (the excerpt from slide 8 [7]).

The newly released cloud strategy of the Defence Department positions the general-purpose Joint Enterprise Defence Infrastructure (JEDI) cloud initiative as the foundation [8]. The strategy emphasises a cloud hierarchy at DoD, with JEDI on top. Fit-for-purpose clouds, which include MilCloud 2.0 run by the Defence Information Services Agency (DISA), will be secondary to the commercially run JEDI general-purpose cloud.

JEDI is not  the first one into cloud computing. The Pentagon already is a multi-cloud environment. There are some 500 clouds in operation across DoD various offices, agencies and departments. Some of these are quite long and involve expenditures of billions of dollars. One of the largest is the milCloud managed by the DISA.

On 25 October 2019, the Pentagon awarded Microsoft a $10 billion cloud computing contract for 10 years bidding for the huge project JEDI, pitted leading tech titans Microsoft, Amazon, Oracle and IBM against one another. A key technological difficulty for the JEDI project is interoperability of clouds (Fig. 7). The interoperability of a technology (getting different parts to function in combination) can be divided into three main categories: internal, external, and iterative. Unfortunately, in each category, the Pentagon's JEDI cloud strategy leaves a series of unanswered questions that could spell disaster in the future [9].

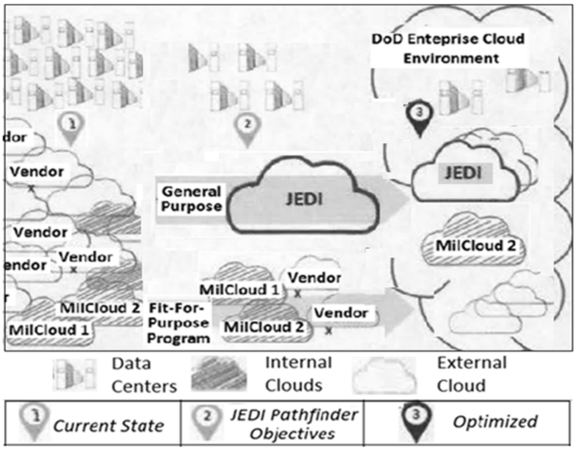

*Fig. 7.* DoD pathfinder to hybrid cloud environments and multiple vendors [10].

The Defence Innovation Unit (DIU) is a DoD organisation launched in 2015. The Joint Artificial Intelligence Centre is a focal point of the DoD AI Strategy [10]. The DoD has created this DoD Cloud Strategy to align with larger DoD cyber strategy, strengthening the security and resilience of the networks and systems that contribute to the Department's military advantage. Underscoring the potential magnitude of AI impact on the whole of society, and the urgency of this emerging technology race in the world, President Trump signed the executive order "Maintaining American Leadership in Artificial Intelligence" on 11 February 2019, launching the American AI Initiative. This was immediately followed by the release of DoD's first-ever AI strategy [11].

**Some Criticism against Software-Defined Networking [12].** SDN does not solve any practical problems. All it does is taking the control plane of the network and centralising it. Due to redundancy, you cannot really just centralise it, you have to have multiple redundant control planes. This adds complexity. Controllers now have to control elements, implying a new control interface. This is more complex. Controllers are a security risk. The communication between the controller and element is a security risk. SDN causes every network operator become also a systems integrator: they now have to find a controller, controller software, and elements that interoperate. There is more complexity and much more work at a time when most enterprises would like to simplify their network operations and outsource them.

**Some Criticism against Artificial Intelligence.** Paper [13] presents a literature review of Machine Learning (ML) and Deep Learning (DL) methods for network security. The paper, which has mostly focused on the past three years, introduces the latest applications of ML and DL in the field of intrusion detection. Unfortunately, the most effective method of intrusion detection has not yet been established. Each approach to implementing an intrusion detection system has its own advantages and disadvantages. Thus, it is difficult to choose a particular method to implement an intrusion detection system over the others.

Datasets for network intrusion detection are very important for training and testing systems. The ML and DL methods do not work without representative data, and obtaining such a dataset is difficult and time-consuming. However, there are many problems with the existing public dataset, such as uneven data, outdated content and the like. These problems have largely limited the development of research in this area.

As AI programs become more sophisticated, the security measures designed to deal with them will also become more complex. AI is making the telecoms industry more efficient, but it comes at a cost of security.

**DRSN are still ISDN based.** No reason to be surprised that due to cyber threats the Defence Red Switch Network (DRSN) uses a 40 year-old ISDN technology. DRSN is a dedicated telephone network, which provides global secure communication services for the command and control structure of the United States Armed Forces (Fig. 8). The network is maintained by DISA and is secured for communications up to the level of Top Secret.

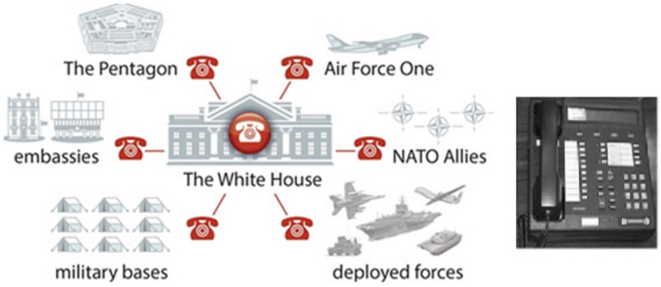

*Fig. 8.* Scheme of the government network DRSN and “Red phone”.

## 4. CONCLUSIONS: WHAT TO TEACH TELECOMMUNICATIONS ENGINEERS?

When multibillion-dollar losses of fraud due to the vulnerabilities of 5G are coming, the need to work together for the benefit of all will have never been greater.

The main goal of the paper is to look for new university courses with regard to the digital economy [14]. The national programme “Digital Economy of the Russian Federation” names the main end-to-end digital technologies: Big Data; neurotechnologies and artificial intelligence; quantum technologies; industrial internet; robotics and sensory; wireless communication; technologies of the virtual and complemented realities and few others. Now it is time to revise our previous course list [15]. The same relates to cyber-security issues [16].

According to the latest Pentagon activities, the key attention in the field of Information Systems has been devoted to Cloud Strategy and Artificial intelligence. This Pentagon’s new strategy has been developed after the serious critics of the current state recovered by GAO inspections. Due to the mentioned SDN and NFV criticism, it is reasonable to develop new education courses aimed at telecommunications engineers with the strong component of system approach, which gives the common view regarding all these latest technologies at the same time keeping in mind cyber security issues.

## REFERENCES

1. Miladinovic, I., Schefer-Wenzl, S., & Hirner, H. (2019). Curriculum of a Telecommunications Study Program—A Matter of Trends? In *Proc. CONTEL2019. The 15th International Conference on Telecommunications*, 3–5 July 2019, Graz, Austria.
2. Global Telecom Crime Undermining Internet Security: Cyber-Telecom Crime Report. (21 March 2019). Available at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/global-telecom-crime-undermining-internet-security-cyber-telecom-crime-report
3. ThreatMetrix. (15 January 2019). *Telco Fraud: Why this Industry is Unique in the Cybercrime Landscape*. Available at https://www.threatmetrix.com/digital-identity-blog/cybercrime/telco-fraud-why-industry-unique-cybercrime-landscape/

4. Europol's European Cybercrime Centre. (21 March 2019). *Cyber-Telecom Crime Report 2019*. Available at https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019
5. ETSI TS 123 501 V15.2.0. (2018-06). *5G; System Architecture for the 5G System* (Release 15). Available at https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf
6. United States Government Accountability Office. (9 October 2018). *GAO-19-128. Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities. Report to the Committee on Armed Services*. Available at https://www.gao.gov/products/GAO-19-128
7. Osborn, Ch. (16 May 2018). *Defense Information Systems Network (DISN). An Essential Weapon for the Nation's Defense*. Available at file:///G:/Pentagon-book+/Osborn_%20DISN%20An%20Essential%20Weapon2018.pdf/
8. Williams, L.C. (5 February 2019). *DOD Cloud Strategy Puts JEDI at the Center*. Available at https://defensesystems.com/articles/2019/02/06/dod-cloud-strategy.aspx/
9. Keelan, T. (21 March 2019). *The Pentagon's JEDI Cloud Strategy is Ambitious, but Can it Work?*. Available at https://www.c4isrnet.com/opinion/2019/03/21/the-pentagons-jedi-cloud-strategy-is-ambitious-but-can-it-work/
10. Department of Defense. (December 2018). *DoD Cloud Strategy Readiness for Artificial Intelligence (Al)*.Available at https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF
11. U.S. Department of Defense. (12 February 2019). *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*. Available at https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF/
12. Li, T. (7 October 2015). *What are Some Criticisms, if any, against Software-Defined Networking?* Available at https://www.quora.com/What-are-some-criticisms-if-any-against-software-defined-networking
13. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., … & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, 35365–35381. DOI 10.1109/ACCESS.2018.2836950
14. Digital Economy of the Russian Federation. Order of the Government of the Russian Federation of 28 July 2017 No. 1632-p (Tsifrovaya ekonomika Rossiyskoy Federatsii. Rasporyazheniye Pravitel'stva RF ot 28.07.2017 N 1632-r). Available at http://ac.gov.ru/en/projects/014097.html
15. Namiot, D., & Sneps-Sneppe, M. (2017). On Internet of Things and Big Data in University Courses. *International Journal of Embedded and Real-Time Communication Systems*, *8* (1), 18–30.
16. Sneps-Sneppe, M., Sukhomlin, V., & Namiot, D. (2018). On Cyber-Security of Information Systems. In *Proc. Distributed Computer and Communication Networks. 21st International Conference, DCCN 2018* (pp. 201–211), 17–21 September 2018, Moscow, Russia.

# INFORMĀCIJAS SISTĒMU KIBERDROŠĪBA UN TELEKOMMUNIKĀCIJU INŽENIERU APMĀCĪBA

M. Šneps-Šneppe, D. Namiots, R. Pauliks

## Kopsavilkums

Rakstā apspriesti telekomunikāciju inženieru apmācības jautājumi. Telekomunikāciju risinājumu arhitektūra mainās ļoti ātri. Acīmredzot ir jāmaina arī apmācības programmas. Viens no galvenajiem pārmaiņu virzītājspēkiem telekomunikāciju risinājumos un apmācības programmās ir kiberdrošības jautājumi. Kiberdrošības jautājumi ir kļuvuši par galvenajiem jautājumiem visos procesos, kas saistīti ar digitālo pārveidi. Tajā pašā laikā ir skaidrs, ka izglītības attīstība telekomunikāciju jomā atpaliek no mūsdienu prasībām. Šie jautājumi izvirzās priekšplānā saistībā ar digitālās ekonomikas attīstību. Atsevišķi tiek apspriesti kiberdrošības jautājumi militāro telekomunikāciju jomā.

***Atslēgas vārdi:*** *izglītība, kiberdrošība, telekomunikācijas*