



# SPCSJ

**SCIENTIFIC AND PRACTICAL  
CYBER SECURITY JOURNAL**

**VOL8 No4**

NOVEMBER 2024

**SPECIAL ISSUE**

This issue was supported by Shota Rustaveli National  
Science Foundation of Georgia (SRNSFG) - CG-24-220

**ISSN 2587-4667**

## SOFTWARE AND HARDWARE IMPLEMENTATION OF THE AL04.2 ENCRYPTION ALGORITHM FOR SECURING HF RADIO COMMUNICATIONS

<sup>1</sup>N.A. Kapalova, <sup>1</sup>D.S. Dyusenbayev, <sup>3</sup>A.A. Nekrasov A.A., <sup>1,2</sup>O.A. Lizunov O.A.

<sup>1</sup>Institute of Information and Computational Technologies, Committee of Science, Ministry of Science and  
Higher Education of the Republic of Kazakhstan, Almaty, Kazakhstan

<sup>2</sup>Institute of Automation and Information Technologies, Satbayev University,  
Almaty, Kazakhstan

<sup>3</sup>Special Design and Technology Bureau 'Granit' LLP, Almaty, Kazakhstan  
e-mail: Kapalova@ipic.kz, dimash\_dds@mail.ru, nec@granit.kz, o.lizunov@bk.ru

**ABSTRACT:** This article explores the development of a High-Frequency (HF) encryptor aimed at securing voice communications in the HF band. The encryptor is designed as an intermediary device positioned between the handset and the radio station, ensuring compatibility with existing systems while addressing concerns over data security. Unlike foreign-made radio equipment that may contain backdoors or lack transparency in their cryptographic systems, the HF encryptor employs a domestically developed solution that is fully compliant with information security standards. Its software is built using the AL04.2 block encryption algorithm, implemented in the high-level programming language C++ to ensure robust cryptographic protection. The design emphasizes repairability, timely updates, and certification transparency, meeting both hardware and software requirements for secure communication. Additionally, this development demonstrates significant progress toward eliminating dependence on foreign cryptographic systems by creating a reliable domestic alternative that offers enhanced protection, efficiency, and adaptability for modern HF radio communications.

**KEYWORDS:** *HF band, radio communication, cryptographic information protection facility, integrated development environment.*

### INTRODUCTION

One of the key areas in the use of Cryptographic Information Protection Facilities (CIPFs) is ensuring the security of communication over radio channels. Foreign manufacturers of radio equipment typically do not provide documentation on the cryptographic systems and encryption algorithms used in their products, citing intellectual property protection and similar reasons. As a result, there is a possibility that foreign-made radio equipment may contain hardware or software backdoors that could weaken their built-in protection mechanisms. Another issue is the compatibility of various radio stations.

Given these challenges, the most appropriate solution is to develop a domestic CIPF that meets information security requirements and is fully transparent for certification, both in hardware and software. This will ensure high repairability, timely updates, and confidence in the declared cryptographic strength of the implemented encryption algorithm.

As part of a grant-funded project, research teams from the Information Security Laboratory at the Institute of Information and Computational Technologies under the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (RK MSHE ICT LIS) and the Special Design and Technology Bureau "GRANIT" have been working on the development of a domestic CIPF, which is now in the final stages.

At this point, two identical HF encryptors have been developed. The HF encryptor is designed to convert voice signals into digital format for subsequent transmission over an HF radio channel in a half-duplex mode.

Technical Specifications of the HF Encryptor:

1. Modulation method – OFDM.
2. Frequency range – 300 to 2500 Hz.

3. Frequency grid step – 62.5 Hz.
4. Transmission rate – 20 ms (50 baud).
5. Guard interval – 4 ms.
6. Channel transmission speed – 3600 bps.
7. Power supply voltage – 12 V DC.
8. Power consumption – no more than 200 mA.
9. Voice sampling rate – 8 kHz.
10. Voice transmission speed – 2400 baud.
11. Connection establishment time – no more than 1 second.
12. Dimensions – 140x210x70 mm.

Thus, based on the above, the development of a domestic CIPF, designed to protect information during HF radio communications, which will be housed in a separate unit and placed between the radio and the handset, is both relevant and important.

## **LITERATURE REVIEW**

Radio communication is one of the most critical forms of communication, and in some cases, the only means to ensure the command and control of forces and resources assigned to carry out combat tasks, as well as during the imposition of a state of emergency or the occurrence of emergencies. The loss of communication results in a loss of command and control.

High-frequency (HF) radio communication is one of the primary communication methods intended for use in regional and national radio networks. During special periods and wartime, HF radio networks become the main form of communication. Due to the ability of shortwaves to efficiently reflect off the ionosphere, radio communication over long distances with low transmitter power is possible (Stupnitsky M. M., 2018, p. 49).

The advantages of HF radio communication include (Romanyuk V.A. 2019):

1. The ability to establish communication over long distances (up to transcontinental).
2. Lower equipment cost compared to other types of communication providing the same range.
3. High mobility.

The disadvantages of the HF band include:

1. Difficulty in miniaturizing radio stations.
2. Large antenna sizes (tens of meters).
3. Low interference immunity.

To this day, the task of ensuring a secure and rapid communication channel in the face of potential adversarial electronic warfare remains one of the most pressing issues. Since the radio channel is inherently open, communications transmitted over it can be intercepted by both military forces and amateur radio operators. Therefore, the issue of ensuring the protection of information transmitted via radio channels is particularly critical, as adversaries may use intercepted open information for various purposes, including destabilizing the situation in society.

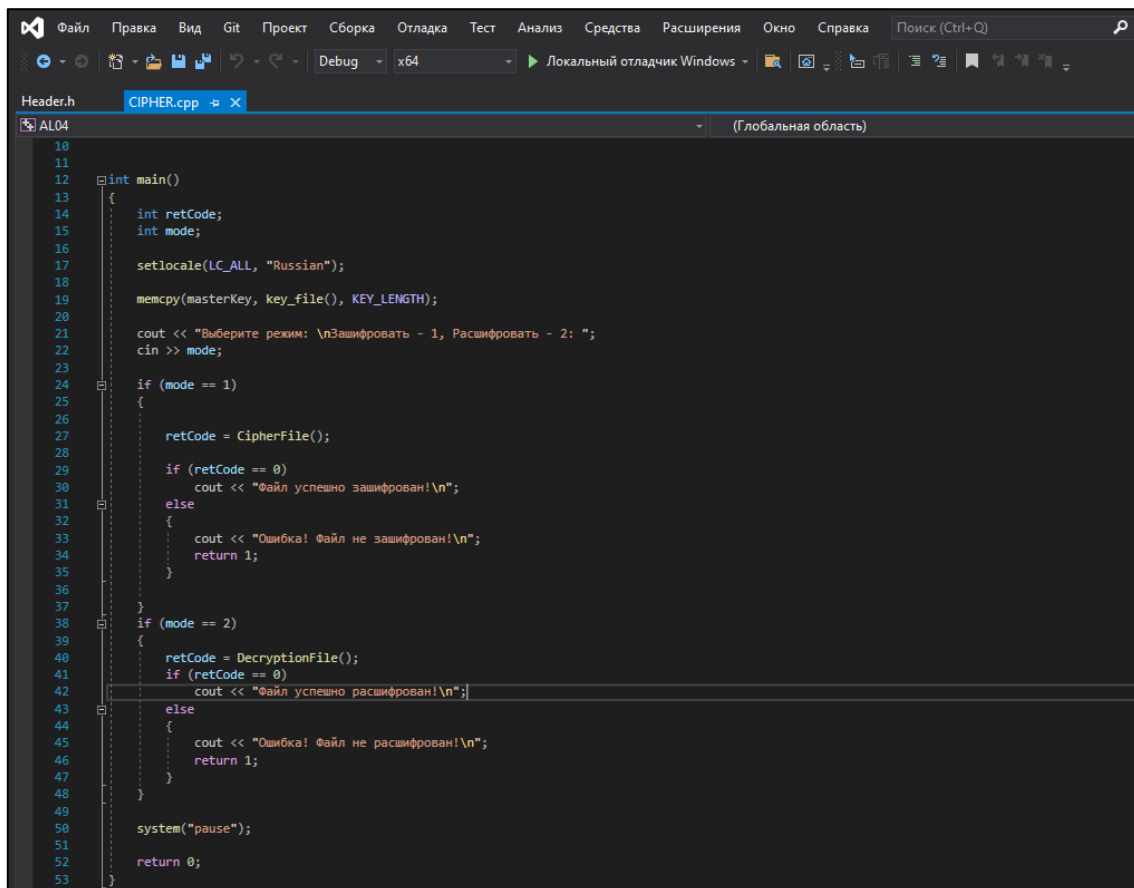
Various manufacturers on the market offer radio communication systems with built-in voice information protection capabilities. One such company is the Israeli firm Elbit Systems, formerly Tadiran Ltd, which produces digital radio communication systems like "Tadiran." In these systems, radio channel protection is ensured through the use of a voice scrambling device (VSD) integrated into the hardware of the radio station (Elbit Systems, n.d.). Another well-known provider of radio communication systems is the Australian company Barrett Communications, which manufactures both digital and analog communication systems. An example is the Barrett PRC-2090 radio, which offers extensive functionality and provides reliable and secure communication using DES encryption with a 56-bit key and AES encryption with a 256-bit key (Radio.com.kz, n.d.). In Russia, one of the largest enterprises developing and manufacturing communication systems with cryptographic protection is the Penza Scientific Research Electrotechnical Institute (PNETI). An example of its products is the "Ramzai" crypto-protected radio modem, which is designed for the cryptographic protection of confidential voice

information and its transmission via HF and VHF radio channels in simplex/duplex mode for both stationary and mobile radio communication systems. The cryptographic algorithm used is GOST 28147-89 in stream cipher mode, with key lengths ranging from 40 to 256 bits (BNTI, n.d.).

This overview of radio communication systems demonstrates that a wide variety of such devices are available on the market, with different implementations of voice information protection algorithms and varying levels of cryptographic security.

## RESEARCH RESULTS

The AL04.2 encryption algorithm was implemented in the Microsoft Visual Studio Community 2019 integrated development environment using the high-level C++ programming language. A fragment of the source code for the AL04.2 encryption algorithm in Microsoft Visual Studio Community 2019 is shown in Figure 1.



```
Header.h CIPHER.cpp
AL04 (Глобальная область)
10
11
12 int main()
13 {
14     int retCode;
15     int mode;
16
17     setlocale(LC_ALL, "Russian");
18
19     memcry(masterKey, key_file(), KEY_LENGTH);
20
21     cout << "Выберите режим: \n1-Зашифровать - 1, Расшифровать - 2: ";
22     cin >> mode;
23
24     if (mode == 1)
25     {
26         retCode = CipherFile();
27
28         if (retCode == 0)
29             cout << "Файл успешно зашифрован!\n";
30         else
31         {
32             cout << "Ошибка! Файл не зашифрован!\n";
33             return 1;
34         }
35     }
36
37     if (mode == 2)
38     {
39         retCode = DecryptionFile();
40         if (retCode == 0)
41             cout << "Файл успешно расшифрован!\n";
42         else
43         {
44             cout << "Ошибка! Файл не расшифрован!\n";
45             return 1;
46         }
47     }
48
49     system("pause");
50
51     return 0;
52
53 }
```

*Figure 1. A fragment of the source code of the AL04.2 encryption algorithm in Microsoft Visual Studio Community 2019*

To generate the files used for the microcontroller firmware upgrade in the HF encryptor, the IAR Embedded Workbench integrated development environment was employed. A fragment of the source code of the AL04.2 encryption algorithm in IAR Embedded Workbench is shown in Figure 2.

To create the firmware file for the OFDM modem, the integrated application development environment Code Composer Studio was utilized, as illustrated in Figure 3.

The microcontroller in the HF encryptor was flashed using the AVR Atmel programmer and the AVR Studio integrated development environment. After upgrading the microcontroller firmware in both HF encryptors, the correct operation of encryption and decryption was verified, where one device served as the transmitter of voice information (shown at the top) and the other as the receiver (shown at the bottom) (see Figure 4).

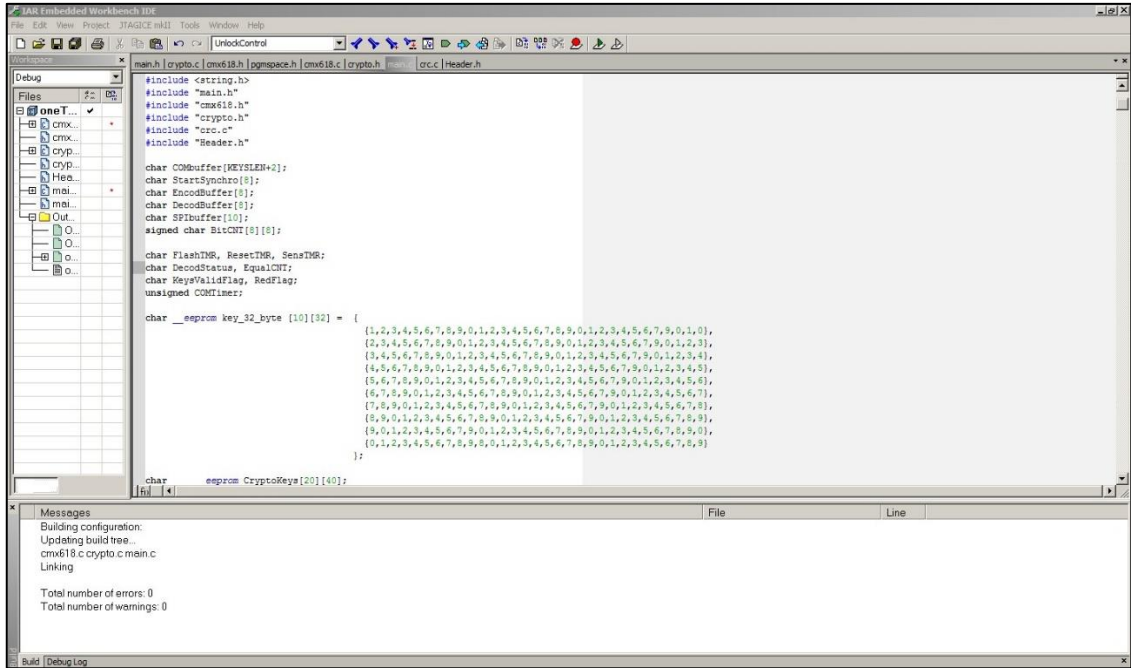


Figure 2. Fragment of the AL04.2 encryption algorithm source code in IAR Embedded Workbench

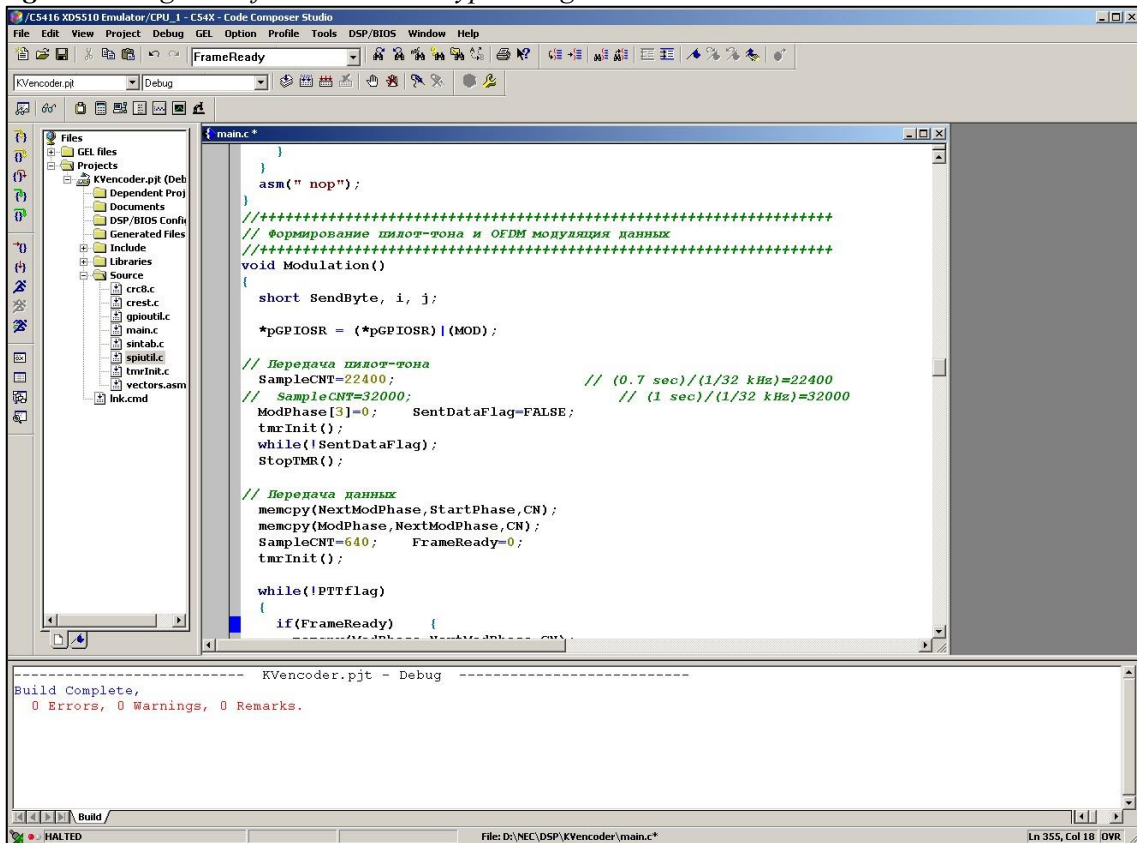
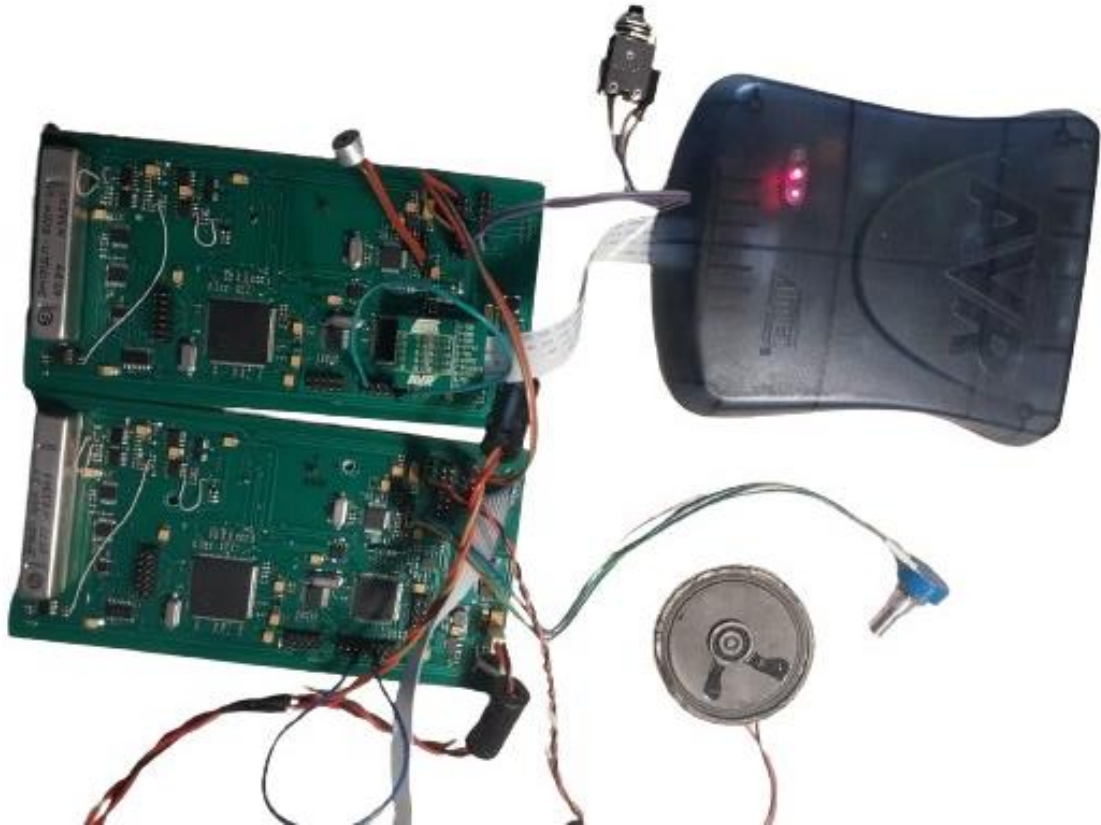


Figure 3. Fragment of the encoder source code in Code Composer Studio



*Figure 4. Testing the operation of two HF encryptors*

The HF encryptor operates in two modes:

- Unencrypted mode;
- Encrypted mode.

In the encrypted mode, the HF encryptor provides the following functions:

1. In the reception mode:

The analog signal received from the radio station is converted into digital form, the digital data stream is decrypted using the AL04.2 encryption algorithm with the application of loaded encryption keys, and the signal is converted back into analog form, and then transmitted to the handset.

2. In the transmission mode:

The analog signal received from the handset is converted into digital form, the digital data stream is encrypted using the AL04.2 encryption algorithm with the application of loaded encryption keys, and the signal is converted back into analog form, and then transmitted to the radio station.

In the unencrypted mode, the device relays the signal from the handset to the microphone input of the radio station and the audio signal from the radio station to the handset, acting as a relay for audio signals. In this case, the operation with the radio station is fully in accordance with the radio station's operating manual.

In the encrypted mode, the encryption of the digital data stream in the HF encryptor is carried out using one of the keys selected by the "key selection" switch.

Functionally, the HF encryptor consists of a vocoder and an OFDM modem. Connection to different types of radio stations is made via the headset jack using appropriate adapters. In the transmission mode, the signal coming from the microphone of the handset enters the input of the vocoder chip, where it is converted to digital form, compressed using the RALCWI algorithm, sent to the controller, encrypted by the AL04.2 algorithm, and then transmitted to the modem. In the modem, the data is modulated using the OFDM method and transmitted via the radio station over the air. In the reception mode, the signal received from the radio station enters the modem, is demodulated, and sent to the controller for decryption. Once restored, the digital data is transferred to the vocoder chip, converted into an analog

signal, and output to the loudspeaker. Switching between reception and transmission modes is controlled by the Push-to-talk (PTT) signal.

The OFDM modem consists of an analog-to-digital converter (ADC), a digital-to-analog converter (DAC), a digital signal processor (DSP), automatic gain control (AGC) circuits, and an automatic frequency control (AFC) system. The modem operates in two modes: modulation and demodulation. Mode switching is controlled by the PTT signal from the vocoder's control unit.

In the modulation mode, the DSP receives data blocks consisting of six bytes from the AVR control microcontroller at 20 ms intervals. The received data is modulated using the OFDM method, converted to analog form by the DAC, and transmitted to the microphone input of the radio station.

Each of the 36 carrier frequencies is modulated using the DQPSK method. The most significant bit of the data is transmitted on the lowest tone frequency. A symbol consists of 9 bytes: 6 data bytes, 1 checksum byte, and 2 error correction code bytes. The CRC8 checksum is used as the error detection mechanism. The Hamming code is used as the error correction code. To reduce cross-distortion, the initial phases of all carrier frequencies are shifted. The initial phase shift is calculated using Newman's formula. The signal is generated programmatically in the DSP. The total output signal with a clock rate of 64 kHz is sent to a 16-bit DAC for conversion to analog form.

In the demodulation mode, an analog signal with an amplitude ranging from 0.1V to 1.2V is received from the radio station's output and sent to the input of the 16-bit ADC, where it is converted into digital form. The sampling rate of the input signal is 32 kHz. The input signal in digital form from the ADC is sent to the DSP memory buffer, where it is processed every 2 ms. A 1024-point Fast Fourier Transform (FFT) is used to extract the instantaneous amplitude and phase of the input signal. Synchronization is achieved using the matching method based on data obtained from two consecutive processing cycles. The demodulated 20 ms interval is transmitted in digital form to the control microcontroller for decryption and conversion into voice.

The front side of the HF encryptor, displaying the control elements, is shown in Figure 5.



Figure 5. Front side of the HF encryptor

Key loading into the HF encryptor is performed through an 8-pin connector, as shown in Figure 6.



*Figure 6. Key loading into the HF encryptor is performed through an 8-pin connector*

The final stage of testing the operation of the two created HF encryptors is to verify their functionality using a radio station. The selected radio equipment for testing the operation of the HF encryptors is the PT-100C transistor HF transceiver, shown in Figure 7.



*Figure 7. PT-100C transistor HF transceiver*

Note: The PT-100C transistor HF transceiver (RTSV n.d.) is a next-generation transceiver designed for operation in the HF frequency range as part of radio centers, including automated communication systems. The device is software-configurable.



Key Technical Specifications of the PT-100C:

- Control: Local or remote via the front panel using RS-232C, RS-485, and Ethernet interfaces.
- Types of Transmission and Reception: J3E, H3E, R3E, A1A, G1B, F1B, J7B, J2D.
- Operating Frequency Range: 1.5-30 MHz.
- Number of Programmable Frequencies: 1000.
- Sensitivity for Signal Reception: In J3E mode (at a signal-to-noise ratio of 10 dB) – not worse than 0.97  $\mu$ V, and in F1B mode – not worse than 0.6  $\mu$ V.
- Re-tuning Time for Programmable Frequencies: No more than 50 ms.

Thus, the work carried out on the development of the AL04.2 encryption algorithm, the creation of two HF encryptors, the programming of the encryption algorithm into the microcontroller, and the testing of the HF encryptors functioning directly connected without using radio stations has shown promising results. The final stage of testing the HF encryptors using the PT-100C transistor HF transceiver will be conducted in the near future.

## CONCLUSION

Thus, as a result of the conducted research, the AL04.2 encryption algorithm has been developed, files for programming the microcontroller have been prepared, two identical HF encryptors have been created, and the correctness of the AL04.2 encryption algorithm's operation in the HF encryptor has been verified during the transmission and reception of voice information directly without the use of radio stations. In the future, it is planned to test the operation of the HF encryptor with the PT-100C transistor HF transceiver.

## ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220. The research work was carried out as part of the grant funding project AP14870419 "Development of a cryptographic information protection facility for securing communications in HF radio communication."

## REFERENCES

Stupnitsky, M. M., & Luchin, D. V. (2018). The Potential of HF Radio Communication – for Creating a Digital Ecosystem in Russia. *Electrosvyaz*, 5, pp. 49–54.

Romaniuk, V. A. (2019). *Analog Devices of Transceivers*. Moscow: Solon-Press.

Elbit Systems. n.d. "Communication Systems." Accessed September 24, 2024. <https://elbitsystems.com/products/communication-systems/>

Radio.com.kz. n.d. "Barrett PRC-2090 Radio Station." Accessed September 24, 2024. [https://www.radio.com.kz/products/radiostantsii/radiostantsiya\\_barrett\\_prc\\_2090/](https://www.radio.com.kz/products/radiostantsii/radiostantsiya_barrett_prc_2090/)

BNTI. n.d. "Crypto-Protected Radio Modem 'Ramzai'." Accessed September 24, 2024. <http://www.bnti.ru/des.asp?itm=3334&tbl=04.03.07.03.&p=1>

RTSV. n.d. " Transistor HF Transceiver PT-10." Accessed September 24, 2024. <https://rtsv.kz/tproduct/519993351-130304709401-tranzistornii-kv-priemperedatchik-pt-10>.

## STATISTICAL ANALYSIS OF THE HAS03 HASH FUNCTION BASED ON THE SPONGE STRUCTURE

<sup>1</sup>K.T. Algazy, <sup>1</sup>K.S. Sakan, <sup>1</sup>D.S. Dyusenbayev

e-mail: kunbolat@mail.ru, kairat\_sks@mail.ru, dimash\_dds@mail.ru

<sup>1</sup>Institute of Information and Computing Technologies, Almaty, Kazakhstan

**ABSTRACT.** This work focuses on the statistical analysis of the HAS03 hash function, which is based on the Sponge structure. The algorithm involves defining a fixed-length internal state and includes the absorption and squeezing phases. The paper presents the results of statistical testing of the cryptographic hash function. The analysis was performed using the software implementation of the statistical test suite recommended by the U.S. National Institute of Standards and Technology (NIST). Additionally, one of the key requirements for cryptographic hash algorithms is the presence of the avalanche effect. The results of the analysis confirm that the sequences produced by this hashing algorithm fully meet the criteria for the avalanche effect and exhibit a high level of statistical security.

**KEYWORDS:** *hash function, sponge, NIST test suite, cryptographic avalanche effect.*

### INTRODUCTION

Hashing emerged in the early days of computer science and was initially used for efficient data retrieval. Over time, its applications have significantly expanded, especially in the field of cryptography, where hashing has become a fundamental component for ensuring data integrity and security in the digital age. A hash function is a mathematical algorithm that transforms an input message into a fixed-size string, typically in the form of a hash value. This transformation is deterministic, ensuring that a given input message consistently produces the same hash output, and it is one-way, preventing the original input from being derived from the hash value (Fashim P., 2021).

The primary purpose of hashing is information verification. This task is critical in numerous scenarios: from password verification on websites to complex computations in blockchain technology. Since a hash represents a unique code for a specific data set, it can be used to determine whether the information matches the expected value. Consequently, programs can store hashes instead of the original data for comparison purposes. This approach is particularly useful for protecting confidential information and conserving storage space. For example, instead of storing passwords on a server, their hashes are stored; antivirus programs keep hashes of viruses in their databases rather than the actual virus samples; digital signatures use hashes for verification; cryptocurrency transaction information is stored as hashes.

Other, less common uses of hashing include searching for duplicates in large datasets, generating identifiers (IDs), and constructing special data structures. An example of such a structure is a hash table, where an element's identifier is its hash, which also determines the element's position in the table.

There are numerous methods for generating hashes. These can include formulas based on multiplication, division, and other mathematical operations, as well as algorithms of varying complexity (Chiambarasan N.R., 2021). However, if a hash is used for data protection, its function must be cryptographic, possessing certain properties.

The operation of a cryptographic hash function typically involves several stages. Data is divided into parts and passed through a compression function, which reduces the information to a smaller number of bits. Such a function must be cryptographically secure, meaning its output must be practically impossible to forge. The main properties of cryptographic hash functions include irreversibility, determinism, uniqueness, and diversity (Peiser S.C., 2020).

## LITERATURE REVIEW

In the article (Rasool M., 2020), a novel approach is presented to address current security issues by using a generalized Collatz process to create a chaos-based hash function. By leveraging the unpredictable behavior of the Collatz sequence, the proposed hash function enhances ergodicity and entropy properties, making it highly suitable for cryptographic applications.

Hash functions are extensively used in measuring high-speed network traffic. In the work (Ying Hu, 2020), the authors introduce a practical development of hash functions for IPv6 measurement. This development is based on an entropic analysis of IPv6 network data and an automated multi-objective genetic programming (GP) method. Three fitness functions are used as optimization goals: active flow estimation, uniformity, and the avalanche effect, with active flow estimation being the primary objective for this specific measurement task.

Recent attacks on modern hash functions have raised doubts about the adequacy of standard hash function construction principles. The paper (Regenscheid A., 2007) examines a multiplication-based hash function construction in the group of  $2 \times 2$  matrices over a finite field, proposed by Zemor and Tillich.

A hash chain is constructed by repeatedly hashing the initial value. The study (Lee D., 2007) investigates the complexity of compromising the security properties of hash functions through hash chain attacks using probabilistic algorithms. It is demonstrated that each hash function has a vulnerability index that measures its inherent susceptibility to hash chain attacks.

SHA-256 is a secure cryptographic hash function. Its output should not exhibit any detectable properties. The paper (Bouam M., 2021) describes three-bit strings whose hashes by SHA-256 are nonetheless correlated in a non-trivial way: the first half of their hashes XORs to zero. These were found using a brute force method without exploiting any cryptographic weaknesses in the hash function itself.

The works (Luo P., 2016) focus on the differential error analysis of the SHA-3 algorithm family, specifically the SHA3-224 and SHA3-256 algorithms. The authors developed an error injection model and enhanced the realism of the attack for various SHA-3 implementation architectures. Later, the authors extended the application of this developed approach to an attack based on error injection.

## RESEARCH METHODOLOGY

A one-way function is a fundamental concept in cryptography and plays a crucial role in ensuring the security of hash functions. A one-way function is a function that is easy to compute in one direction but extremely difficult to invert without specific information. In the context of hash functions, this property ensures that hashing data can be done quickly and efficiently, but it is impossible to recover the original data from its hash (Levin A., 2003).

Let's provide a formal definition of a hash function. Let  $\{0, 1\}^m$  be the set of all binary strings of length  $m$ , and  $\{0, 1\}^*$  be the set of all finite-length binary strings. Then, a hash function  $h$  is a transformation of the form  $h : \{0, 1\}^* \rightarrow \{0, 1\}^m$ , where  $m$  is the length of the hash output.

There are various approaches to constructing cryptographic hash functions today. Among these, the sponge construction is a versatile cryptographic primitive used to create hash functions. The main idea behind it is the flexibility, security, and efficiency of the construction, making it suitable for various cryptographic tasks (Beirendonck M., 2019).

The sponge construction is characterized by two parameters:

- Absorption rate ( $r$ ): The part of the state that is updated with each block of input data.
- Capacity ( $c$ ): The part of the state that remains unchanged for each block of input data. The total length of the sponge state is  $b=r+c$ .

The avalanche effect is a key property of cryptographic algorithms that characterizes their resistance to analysis and cracking. This property denotes that a slight change in the input data (e.g., changing one bit) should cause significant changes in the output data, affecting a large number of bits. For hash functions, the avalanche effect plays a critically important role. Changing one bit in the original message results in a drastically different hash. This property ensures that two similar messages will have

completely different hashes, making it difficult to predict or match the original message from its hash (Upadhyay D., 2022).

The avalanche effect parameter is an important indicator of the quality of cryptographic algorithms. Its use allows evaluating and comparing the robustness of various algorithms against cryptanalysis, thereby providing a high degree of data protection. The avalanche effect parameter is defined by the following formula:  $\varepsilon_i = |2k_i - 1|$ , where  $i$  is the number of the changed bit in the input sequence,  $k_i$  is the probability of changing half of the bits in the output sequence when changing the  $i$ th in the input, and  $\varepsilon_i$  is the avalanche parameter. The ideal value for cryptographic hash algorithms is 0.5, indicating that, on average, changing one bit of input data alters half of the output bits.

## RESULTS AND DISCUSSION

### Development of a hashing algorithm

The hashing algorithm runs over a working range of 1024 bit (that is, the size of the internal state is 1024 bits). The original plaintext is divided into blocks of 512 bits. If the total plaintext length is not a multiple of 512, i.e. the length of the last block is less than 512 bits, then it is padded. As a complement, a bit sequence is used, the first and last positions of which are ones, and all the other positions are filled with zeros. The algorithm is based on sponge construction, the general scheme of which is shown in Figure 1. The internal state is divided into two parts. The developed algorithm uses an internal state consisting of two 512-bit parts A and V.

At the stage of absorbing, a consecutive plaintext block  $A_i$  is combined with both parts of the internal state of the algorithm using the XOR operation and written instead of the first part, and the second part remains unchanged:  $A'_i = A_i \oplus A_{i-1} \oplus V_i$ ,  $V'_i = V_{i-1}$ ,  $i = \overline{0, n-1}$ . As the initial internal state, one can choose a sequence consisting only of zeros (in the general case, it is possible to choose any fixed sequence) with a length of 1024 bit. Using the function  $f$ , we transform the data obtained as a result of these operations. After all the plaintext blocks have been processed, we move on to the squeezing stage. At this stage, the input to the function  $f$  is the internal state  $A_{n-1} \parallel V_{n-1}$  and the first 64 bits of the output are chosen as the hash value. This is repeated until a hash value of the required length is obtained. That is, to get a 256- or 512-bit hash value, one need to repeat this procedure 4 or 8 times, respectively.

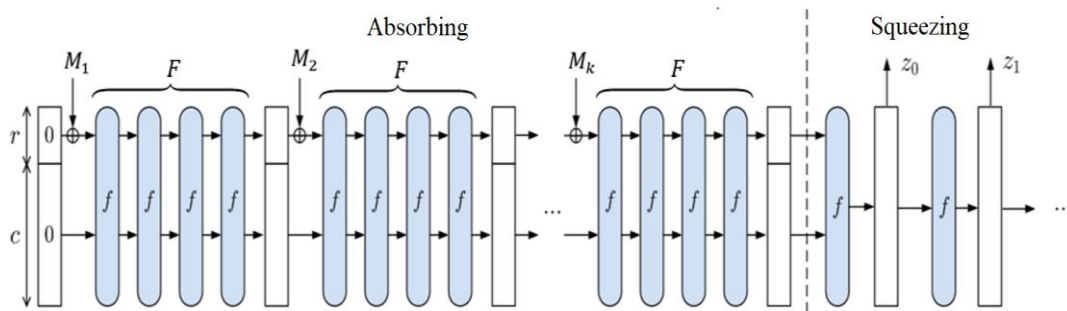


Figure 1. Sponge construction scheme

Function  $f$ . The structure of the internal state used by the function  $f$  is a  $4 \times 4$  square matrix whose elements are 64-bit words (see Fig.2).  $W_i, C_i$   $i = \overline{0, 7}$  are 64-bit words,  $W_i$  are plaintext data ( $A_j$  in the general scheme of the algorithm),  $C_i$  is the second part involved in the transformation ( $V_j$  in the general scheme).

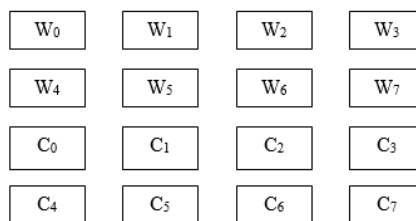


Figure2. The structure of the internal state used by the function  $f$

The function  $f$  consists of transformations  $X, S, R$  and  $P$ , where  $X$  is performed twice. Let's describe each of these transformations.

X-transformation performs the addition of the corresponding elements of the first and second columns of the matrix using the xor operation and places the result in the first column, i.e.  $W'_0 = W_0 \oplus W_1$ ,  $W'_4 = W_4 \oplus W_5$ ,  $C'_0 = C_0 \oplus C_1$ ,  $C'_4 = C_4 \oplus C_5$ . The same transformation is used to get the elements of the second and third columns:  $W'_1 = W_1 \oplus W_2$ ,  $W'_5 = W_5 \oplus W_6$ ,  $C'_1 = C_1 \oplus C_2$ ,  $C'_5 = C_5 \oplus C_6$ ,  $W'_2 = W_2 \oplus W_3$ ,  $W'_6 = W_6 \oplus W_7$ ,  $C'_2 = C_2 \oplus C_3$ ,  $C'_6 = C_6 \oplus C_7$ . The fourth column does not change. S-transformation. Each of the values  $W_i, C_i$   $i = \overline{0,7}$  consists of 8 bytes, and their total number is 16. Then the total number of bytes processed by the function  $f$  is 128. As a result of the transformation  $S$ , these 128 bytes will be replaced by other bytes using S-box, i.e.  $S: \{0, 1\}^{1024} \rightarrow \{0, 1\}^{1024}$ .

After the S-transformation, the X-transformation is performed on the first and fourth columns, and the result is written as the new elements of the fourth column:  $W''_3 = S(W'_0) \oplus S(W'_3)$ ,  $W''_7 = S(W'_4) \oplus S(W'_7)$ ,  $C''_3 = S(C'_0) \oplus S(C'_3)$ ,  $C''_7 = S(C'_4) \oplus S(C'_7)$ .

R-transformation. Let's denote each of the 16 internal state words as  $X_n$ ,  $n = \overline{0,15}$ . Then, for  $n = \overline{0,1,2,3}$ , the  $SHRL(X_n)$  operation is performed, and in other cases, the  $ROTRL(X_n)$  operation is performed. Here  $SHRL(X_n)$  is a logical shift operation of the 64-bit argument by  $n + 3$  bits to the right if  $n$  is even and to the left if  $n$  is odd. Similarly,  $ROTRL(X_n)$  is an operation to rotate a 64-bit argument  $n + 3$  to the right if  $n$  is even, and to the left if  $n$  is odd.

P-transformation. The main purpose of the transformation is to mix the input elements. Each byte of the input sequence is moved to a different location in a specific order (Table 1).

**Table 1 - Permutation table for P-transformation.**

<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>
0	16	32	48	64	80	96	112	1	17	33	49	65	81	97	113
<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>	<b>20</b>	<b>21</b>	<b>22</b>	<b>23</b>	<b>24</b>	<b>25</b>	<b>26</b>	<b>27</b>	<b>28</b>	<b>29</b>	<b>30</b>	<b>31</b>
2	18	34	50	66	82	98	114	3	19	35	51	67	83	99	115
<b>32</b>	<b>33</b>	<b>34</b>	<b>35</b>	<b>36</b>	<b>37</b>	<b>38</b>	<b>39</b>	<b>40</b>	<b>41</b>	<b>42</b>	<b>43</b>	<b>44</b>	<b>45</b>	<b>46</b>	<b>47</b>
4	20	36	52	68	84	100	116	5	21	37	53	69	85	101	117
<b>48</b>	<b>49</b>	<b>50</b>	<b>51</b>	<b>52</b>	<b>53</b>	<b>54</b>	<b>55</b>	<b>56</b>	<b>57</b>	<b>58</b>	<b>59</b>	<b>60</b>	<b>61</b>	<b>62</b>	<b>63</b>
6	22	38	54	70	86	102	118	7	23	39	55	71	87	103	119
<b>64</b>	<b>65</b>	<b>66</b>	<b>67</b>	<b>68</b>	<b>69</b>	<b>70</b>	<b>71</b>	<b>72</b>	<b>73</b>	<b>74</b>	<b>75</b>	<b>76</b>	<b>77</b>	<b>78</b>	<b>79</b>
8	24	40	56	72	88	104	120	9	25	41	57	73	89	105	121
<b>80</b>	<b>81</b>	<b>82</b>	<b>83</b>	<b>84</b>	<b>85</b>	<b>86</b>	<b>87</b>	<b>88</b>	<b>89</b>	<b>90</b>	<b>91</b>	<b>92</b>	<b>93</b>	<b>94</b>	<b>95</b>
10	26	42	58	74	90	106	122	11	27	43	59	75	91	107	123
<b>96</b>	<b>97</b>	<b>98</b>	<b>99</b>	<b>100</b>	<b>101</b>	<b>102</b>	<b>103</b>	<b>104</b>	<b>105</b>	<b>106</b>	<b>107</b>	<b>108</b>	<b>109</b>	<b>110</b>	<b>111</b>
12	28	44	60	76	92	108	124	13	29	45	61	77	93	109	125
<b>112</b>	<b>113</b>	<b>114</b>	<b>115</b>	<b>116</b>	<b>117</b>	<b>118</b>	<b>119</b>	<b>120</b>	<b>121</b>	<b>122</b>	<b>123</b>	<b>124</b>	<b>125</b>	<b>126</b>	<b>127</b>
14	30	46	62	78	94	110	126	15	31	47	63	79	95	111	127

The function  $f$  consists of repeating the above transformations 14 times, except that the R-transformation is not performed in the last round.

Let's show the results of the transformations used in the function  $f$  using a simple example. Let  $M$  be a binary sequence 512 bits long, consisting only of zeros. Processing begins with the absorption stage.

## STUDY RESULTS

One of the universal attacks carried out on all cryptographic algorithms is exhaustive search or brute-force attack. If the hash value of the message  $M_1$  is  $H(M_1)$ , then the attacker needs to find a message

$M_2$  that satisfies  $H(M_1) = H(M_2)$ . If the length of the resulting hash is  $n$ , then the complexity of this method is  $O(2^n)$ . Usually, when developing algorithms, special attention is paid to this condition and the algorithm is constructed in such a way that the required level of security is ensured. In the HAS03 algorithm, the length of the resulting hash value is 256 and 512 bits, so using the brute force method is inefficient.

Another universally valid attack technique used for hash functions is the "birthday paradox". This cryptographic analysis method estimates how many messages need to be examined to detect a collision with a probability greater than 0.5. To find a collision, one needs to generate two sets, each containing  $2^{n/2}$  messages and calculate their hash values. According to the birthday paradox, among them there are messages with the same hash values with a probability of more than 0.5. However, this method requires a large amount of memory. Even if the hash length is 256, modern computers will not be able to implement this method. To find a collision of the second kind, it is necessary to make calculations in the amount of at least  $2^{128}$ .

The avalanche effect is one of the mandatory properties of cryptographic algorithms. A small change in the input of block ciphers and cryptographic hash functions should significantly change the output value (for example, change half of the output bits).

To check the avalanche effect of the constructed hashing algorithm, consider the above example, i.e. as the source text, we choose a binary sequence consisting only of zeros (Zima V.M., 2000). By inverting one of the zero bits in each position of this sequence, we will get a new 512-bit text. The probability of changing  $k_i$ ,  $i = 0,511$ , is calculated, where  $k_i$  is the probability that the  $i$ th bit in the output value will change if the  $i$ th element of the input value is inverted from the original output value (see Fig.3).

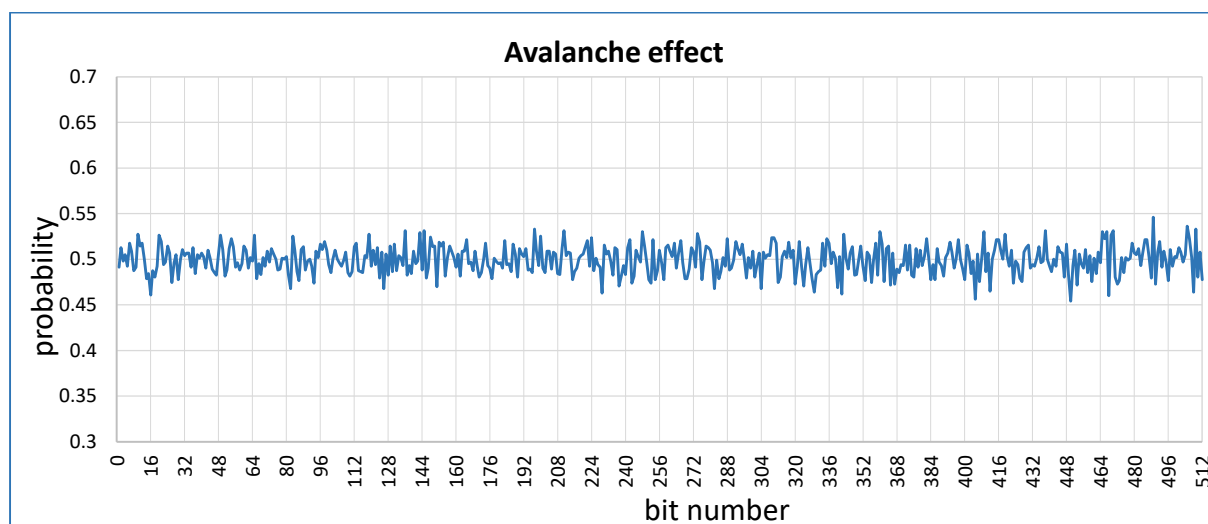


Figure 3. Avalanche effect of the 6th round

The closer the value of each  $k_i$  is to 0.5, the better the avalanche effect. Figure 4 shows a diagram of the improvement in the avalanche effect from round to round. In the sixth round, the algorithm shows a good result.

### Evaluation of the statistical properties of hash values

For any hash value  $h(M)$  of a hashing algorithm, one of the essential conditions is the presence of properties of pseudorandom sequences.

Therefore, an evaluation of the HAS03 hashing algorithm was conducted using a set of statistical tests from the National Institute of Standards and Technology (NIST). The purpose of the testing is to determine the degree of deviation of the sequence of hash values from truly random sequences.

Each test in the NIST suite evaluates randomness according to specific criteria by calculating the p-value. Small p-values indicate that if the null hypothesis  $H_0$  is true, the probability of obtaining the same or more extreme test statistics is very low. If the test yields a p-value  $p > \alpha = 0,01$ , it means that the examined sequence is random with a confidence level of 99%. Here,  $p \in [0,1]$  and  $\alpha$  is the significance level, i.e., the probability of rejecting the null hypothesis  $H_0$ .

The statistical tests using the NIST suite were conducted as follows. A random \*.zip file of size 31,250 KB was selected for testing. According to the HAS03 algorithm description, each consecutive 64-byte block of the hashed message is processed, and the resulting 64-byte hash value is sequentially written to a new file. In our case, 500,000 hash values were obtained from 500,000 message blocks. The output file with the \*.hash extension was split into 100 files, each 3,125 KB in size. These files were then tested using the NIST statistical test suite.

Figure 4 presents the results of the pseudo-randomness analysis of the hash value sequences generated by the HAS03 algorithm using NIST tests. Two significance levels,  $\alpha$ , were considered, and the number of successfully passed NIST tests is shown.

The experiment results indicated that all tests were passed successfully. According to NIST recommendations, a test is considered successful if at least 96 out of 100 sequences pass.

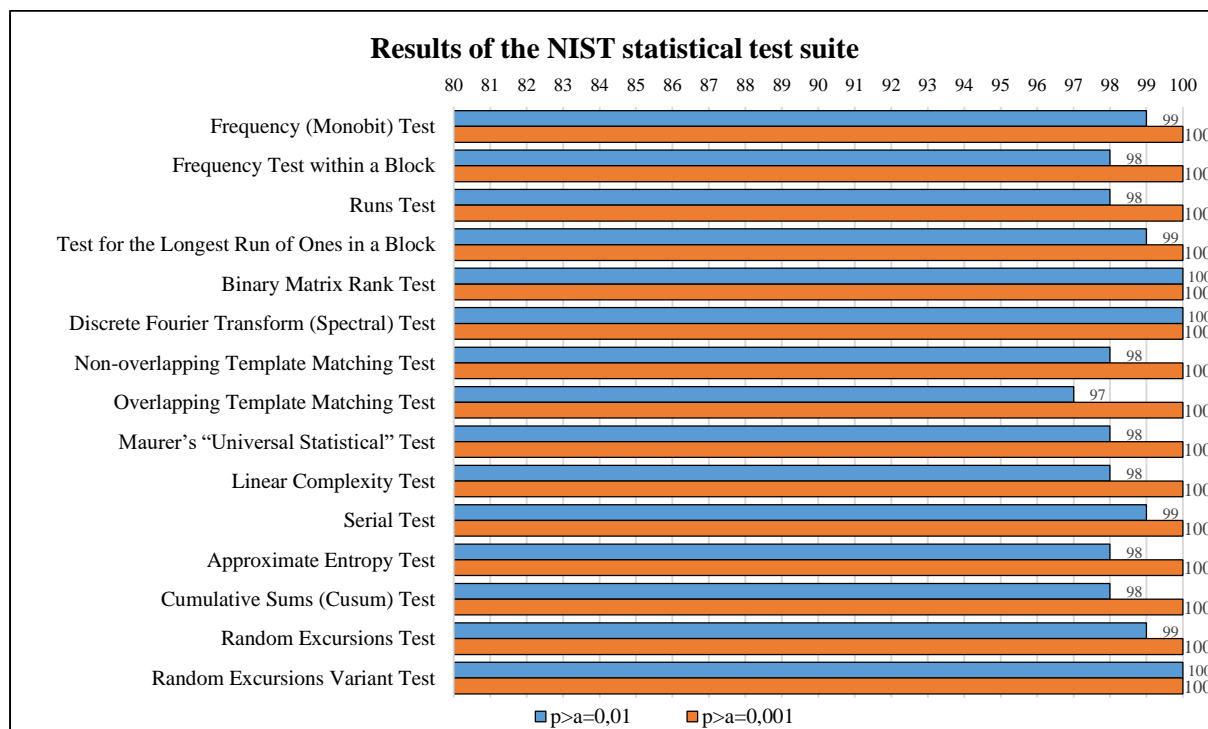


Figure 4. NIST statistical test results

## CONCLUSIONS

This article provides a brief overview of research on the development and analysis of cryptographic hash functions, as well as a study of the current state of security and known structures of these functions. The developed hashing algorithm, HAS03, is based on the sponge construction and transforms plaintext of arbitrary length, divided into 512-bit (64-byte) blocks, into a hash value of either 256 or 512 bits. Research has been conducted to confirm the cryptographic properties of the developed algorithm, including evaluations of the avalanche effect of the HAS03 hashing algorithm. The algorithm demonstrates a significant avalanche effect after just the 6th round of hashing. For experimental rigor, the avalanche criterion was applied to the analysis after the 8th, 10th, 12th, and 14th rounds of hashing, confirming the necessary degree of avalanche effect propagation in the HAS03 algorithm.

Additionally, the NIST testing results showed no deviations in the sequences generated by the HAS03 hashing algorithm. Therefore, it can be concluded that this algorithm provides a high level of statistical security.

A promising direction for future research is a comprehensive study of the HAS03 hashing algorithm in terms of its efficiency and security, specifically the search for collisions and preimages using cryptanalysis methods. This will help identify its vulnerabilities and develop corresponding protective measures.

## ACKNOWLEDGMENTS

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

The research work was funded by the Ministry of Science and Higher Education of Kazakhstan and carried out within the framework of the project AP14870719 “Development and study of post-quantum cryptography algorithms based on hash functions” at the Institute of Information and Computational Technologies.

## REFERENCES

Farshim, Pooya, and Stefano Tessaro. "Password Hashing and Preprocessing." In *Advances in Cryptology – EUROCRYPT 2021*, edited by Anne Canteaut and François-Xavier Standaert, vol. 12697 of *Lecture Notes in Computer Science*. Cham: Springer, 2021.

Chilambarasan, N. R., and A. Kangaiammal. "Matyas–Meyer–Oseas Skein Cryptographic Hash Blockchain-Based Secure Access Control for E-Learning in Cloud." In *Inventive Systems and Control*, edited by V. Suma, J. I. Z.

Chen, Zubair Baig, and Hui Wang, vol. 204 of *Lecture Notes in Networks and Systems*. Singapore: Springer, 2021. [https://doi.org/10.1007/978-981-16-1395-1\\_65](https://doi.org/10.1007/978-981-16-1395-1_65).

Peiser, S. C., L. Friberg, and R. Scandariato. "JavaScript Malware Detection Using Locality Sensitive Hashing." In *ICT Systems Security and Privacy Protection*, edited by Marko Hölbl, Kai Rannenberg, and Tomaz Welzer, vol. 580 of *IFIP Advances in Information and Communication Technology*. Cham: Springer, 2020. [https://doi.org/10.1007/978-3-030-58201-2\\_10](https://doi.org/10.1007/978-3-030-58201-2_10).

Rasool, M., and S. B. Belhaouari. "From Collatz Conjecture to Chaos and Hash Function." *Chaos, Solitons & Fractals* 176 (2023): 114103. <https://doi.org/10.1016/j.chaos.2023.114103>.

Hu, Ying, Guang Cheng, Yongning Tang, and Feng Wang. "A Practical Design of Hash Functions for IPv6 Using Multi-Objective Genetic Programming." *Computer Communications* 162 (2020): 160–68. <https://doi.org/10.1016/j.comcom.2020.08.013>.

Regenscheid, Andrew. "An Algebraic Hash Function Based on SL<sub>2</sub>." 2007. <https://doi.org/10.31274/rtd-180813-15958>.

Lee, D. "Hash Function Vulnerability Index and Hash Chain Attacks." In *2007 3rd IEEE Workshop on Secure Network Protocols*, 1–6. Beijing, China: IEEE, 2007. <https://doi.org/10.1109/NPSEC.2007.4371616>.

Bouam, M., Christophe Bouillaguet, C. Delaplace, and C. Nous. "Computational Records with Aging Hardware: Controlling Half the Output of SHA-256." *Parallel Computing* 106 (2021): 102804. <https://doi.org/10.1016/j.parco.2021.102804>.

Luo, P., Y. Fei, L. Zhang, and A. A. Ding. "Differential Fault Analysis of SHA3-224 and SHA3-256." In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 4–15. IEEE, 2016. <https://doi.org/10.1109/FDTC.2016.17>.



Levin, L. A. "The Tale of One-Way Functions." *Problems of Information Transmission* 39, no. 1 (2003): 92–103. <https://doi.org/10.1023/A:1023634616182>.

Beirendonck, M., L. Trudeau, P. Giard, and A. Balatsoukas-Stimming. "A Lyra2 FPGA Core for Lyra2REv2-Based Cryptocurrencies." In *IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–5. Sapporo, Japan: IEEE, 2019. <https://doi.org/10.1109/ISCAS.2019.8702498>.

Upadhyay, D., N. Gaikwad, M. Zaman, and S. Sampalli. "Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications." *IEEE Access* 10 (2022): 112472–86. <https://doi.org/10.1109/ACCESS.2022.3215778>.

Zima, V. M. *Security of Global Network Technologies*. BHV-Petersburg, 2000.

## REVIEW OF THE GRAPHS DIRECTED TO 2024

<sup>1</sup>Jerzy Dorobisz

<sup>1</sup>Institute of Information Technology and Cyber-security, Faculty of Cybernetics, WAT, 2 Gen. Sylwestra Kaliskiego St., 00-908 Warsaw  
email: jerzy.dorobisz@wat.edu.pl

**ABSTRACT.** A directed graph, also known as a sgraph or digraph, is a mathematical structure used to model relationships between objects in which the relationships have a specific direction. Unlike undirected graphs, where edges connect vertices without specifying the direction of flow, in directed graphs the edges, also called arcs, have arrows indicating the direction of flow. There are different types of directed graphs, e.g. acyclic graphs (DAG), strongly consistent graphs, Euler graphs. Many algorithms and techniques for analysing directed graphs used to solve different problems. Directed graphs are an important tool in computer science, mathematics, engineering, and play an important role in the field of cyber security, providing a valuable tool for modelling and analysing complex information systems and identifying potential threats.

**KEYWORDS:** Directed Path., Directed Cycle, Score Vector, Underlying Graph, Consecutive Vertex

### 1. INTRODUCTION

Directed graphs (digraphs) are graphs in which the edges have a specific direction. This means that an edge  $(u, v)$  leads from node  $u$  to node  $v$  and not necessarily from  $v$  to  $u$ . Directed graphs are widely used in various fields such as computer science, computer networks, graph theory and social network analysis. Edge Direction: Each edge has a specific direction, indicating which node it starts from and which node it ends at. Degree of Nodes: In directed graphs, we distinguish between the input degree (the number of edges entering a node) and the output degree (the number of edges leaving a node). Cycle: A directed graph can contain a cycle, i.e. a path that starts and ends at the same node, passing through other nodes according to the direction of the edges.

### 2. DIRECTED GRAPHS

Directed graphs are a fundamental data structure in computer science and mathematics, allowing complex relationships and interactions between different elements to be modelled. In this context, a directed graph is an abstract representation of directed connections between vertices, which enables the analysis and understanding of complex relationships found in various domains. An introduction to directed graphs is key to developing an understanding of their nature and potential applications.

Directed graphs find their application in a variety of fields, from computer science to the social sciences, offering a tool for modelling and analysing relationships and structures. One of the key aspects of directed graphs is their ability to represent and analyse social networks. In the context of social network analysis, the vertices of a graph represent social entities, such as people, organisations or places, and the edges reflect the relationships between them, such as friendship, cooperation or social group membership. In this way, directed graphs enable deep analysis of community structure, identification of key individuals and prediction of social trends<sup>1</sup>.

In the area of computer networks, directed graphs play a key role in routing problems. Each node of a graph can represent a router or network device, and the edges between them are the paths along which data is transmitted. The analysis of directed graphs in the context of routing allows efficient planning

---

<sup>1</sup> Schiff, K. (2011). An algorithm for determining multicommodity maximum flow in directed graphs. Logistics (2).

of communication routes in networks, minimising latency and optimising data flow. The introduction of directed graphs in this field enables network engineers to design efficient communication systems, which is crucial in today's globalised IT environment<sup>2</sup>.

In addition, directed graphs are used in dependency analysis in data science, project management, pattern recognition in big data, and recommendation systems. Their versatility makes them an invaluable tool in a variety of fields where it is important to understand the relationships between elements.

In summary, an introduction to directed graphs is a key step in understanding and use of this powerful data structure. Their importance in social network analysis, routing in computer networks and many other fields make them indispensable tools in today's world dominated by complex relationships and interactions. Unraveling the mysteries of directed graphs is becoming not only a fascinating mathematical subject, but also a key element in the advancement of applied science. Directed graphs are an important area of graph theory, and understanding them requires a sound knowledge of basic definitions and terminology. The following are key concepts related to vertices, edges, vertex degree, path and cycle in the context of directed graphs.

A vertex is a fundamental element in the structure of a directed graph. It is represented by a point in the graph that can be connected by an edge to other vertices. Vertices are abstract entities that represent different elements such as places, objects or social entities depending on the context of the application. An edge in a directed graph is a directed arrow connecting two vertices. Each edge has a specific direction, indicated by the arrow, and consists of two points: a source (the starting vertex) and a target (the ending vertex). Edges represent relationships, connections or dependencies between vertices<sup>3</sup>.

The vertex degree is the number of edges that enter or leave a given vertex. The degree of a vertex can be used to analyse the structure of a graph. Vertices with degree zero are isolated vertices, degree one indicates vertices that are the ends of edges, and degree greater than one indicates vertices that are connected to other vertices.

A path in a directed graph is a sequence of edges that connect vertices together. Unlike an undirected graph, in a directed graph a path has a direction, meaning that we move from the source to the destination, rather than both ways. Path analysis is crucial to understanding the relationships and connections between elements in a graph.

A cycle is a closed path in a directed graph in which the start and end vertices are the same. This means that we can return to the starting point by passing through a series of edges. Cycles are important in the analysis of directed graphs, especially in terms of identifying cyclic structures and their impact on the functioning of the systems represented by the graph<sup>4</sup>.

In understanding these basic definitions and terminology lies the key to effectively analysing and modelling the complex structures represented by directed graphs. With these concepts, we become able to explore relationships, identify patterns and understand data structure in the context of a variety of application domains.

The operation of graph traversal and the search for shortest paths in directed graphs are key elements in the analysis of the structure of these complex data structures. Graph traversal is the process of visiting vertices and edges in order to better understand the layout of a graph. There are several main methods of traversal, of which DFS (Depth-First Search) and BFS (Breadth-First Search) are the most important.

### **3. DFS**

DFS is based on deep exploration of the structure of a graph, starting from one vertex and following as far as possible along one branch before returning to the previous vertex. This approach is compared to exploring a maze, where we aim to explore one direction as much as possible before paying attention to other possibilities. BFS, on the other hand, explores the graph in layers, visiting all the neighbours

---

<sup>2</sup> Magiera, J. (1995). Graphs as metric spaces. *Prace Naukowe Akademii Ekonomicznej we Wrocławiu (696 Dydaktyka matematyki)*, 55-65.

<sup>3</sup> Wozniak, A. (2010). Graphs and networks in decision-making techniques. *Infrastructure and Ecology of Rural Areas*, (04).

<sup>4</sup> Kaminska, A. M. (2018). Application of graph structures for bibliometric and webometric analyses. *Models and methods. New Library. Services, Information Technology and Media*, 29(2), 47-63.

of a given vertex and then proceeding to the neighbours of those neighbours. This approach resembles a wave propagating from a source and allows us to explore neighbourhoods at different levels of distance<sup>5</sup>.

The search for shortest paths in directed graphs is a crucial operation, especially in the context of analysing the distance between two vertices. Dijkstra's algorithm is used to find shortest paths in a graph with non-negative edge weights. Starting from the source vertex, this algorithm iteratively visits the nearest vertices, updating the shortest distances. This is often used in packet routing in computer networks or route planning in logistic routing.

#### 4. BELLMAN-FORD ALGORITHM

The Bellman-Ford algorithm, on the other hand, allows the search for shortest paths in a graph with edges with possibly negative weights. This is a more flexible approach that also allows the detection of cycles with negative weights. Although less efficient than Dijkstra's algorithm, it is more versatile in handling different scenarios. In summary, graph traversal and shortest path search are key operations in directed graph analysis. The use of these methods is essential in fields ranging from computer science to logistics, where complex relationships and graph structures require efficient understanding and use<sup>6</sup>. In directed graphs, where edges reflect the relationships between elements, topological sorting emerges as a key tool for determining the order in which tasks are performed. This is particularly important in the context of tasks where there is a need to follow a hierarchy, and topological sorting ensures that no task is completed before the tasks on which it depends.

Topological sorting involves assigning ordinal numbers to vertices in such a way that each directed edge leads from a lower-numbered vertex to a higher-numbered vertex. In practice, this means arranging tasks in such a way that each task preceding another has a lower number, so that they can be performed in the correct order<sup>7</sup>.

Cycle analysis in directed graphs is becoming a key aspect, especially the context of detecting errors or conflicts in the data structure. Cycles, i.e. closed paths in a graph, can introduce ambiguities or lead to infinite loops, which is unacceptable in many application domains such as information systems or data analysis.

Spanning trees, on the other hand, are an important part of directed graph analysis. A spanning tree is a cycle free subgraph that spans all vertices of a graph. In the context of directed graphs, spanning trees are used to analyse hierarchy and structure, and to extract key relationships between elements. In practice, a spanning tree can represent a decision or logical structure, where vertices are decisions and edges are their consequences.

In summary, topological sorting, cycle analysis and spanning trees are important operations in directed graph analysis. They offer tools for the efficient organisation of tasks, the detection of potential errors and the analysis of structure and hierarchy in various application domains<sup>8</sup>.

#### 5. EMBEDDING

Embeddings of graphs is a modern approach to modelling graph structures that revolutionises the way vertex relationships in directed graphs are analysed. Under this technique, the vertices of a graph are mapped to a low-dimensional space and their structural features are preserved.

The main goal of graph embeddings is to effectively capture complex relationships between vertices, enabling more precise modelling and understanding of graph structure. In practice, graph embeddings find applications in a variety of fields, introducing new possibilities in data analysis and decision-making.

---

<sup>5</sup> Swierczek, A. (2007). From supply chains to supply networks. *Logistics*, 1, 74-77.

<sup>6</sup> Kawa, A. (2013). Analysis of enterprise networks using the SNA method. *Entrepreneurship and Management*, 14(13), 1.

<sup>7</sup> M. Cencelj, J. Dydak, A. Vavpetič, Z. Virk, A Combinatorial Approach to Coarse Geometry, arXiv:math.MG/0906.1372v1 (2009)

<sup>8</sup> G. Bell, A. Dranishnikov, Asymptotic Dimension in Będlewo, arXiv:math.GR/0507570v2 (2005)

The process of representing a graph using embeddings involves assigning a vector of real numbers to each vertex, so that the similarity between vertices in the original graph structure is represented as the proximity of the corresponding vectors in the embedding space. In practice, embeddings of graphs find application in various areas. In recommendation systems, graph embeddings enable the generation of precise recommendations, taking into account complex relationships between users or products. In social networks, graph embeddings make it possible to detect communities and group users based on their behavioural patterns. In time-sensitive graphs, embeddings enable the analysis of the evolution of relationships between vertices over time, which is crucial for understanding changes in the graph structure. In dynamic graphs, embeddings support the analysis of changes over time and allow better planning based on the dynamics of the graph structure<sup>9</sup>.

Graph representation using embeddings is an innovative approach that extends our capabilities in the analysis of graph structures. It has practical applications in a variety of fields, enabling more advanced data analysis and a better understanding of complex relationships in directed graphs.

Time-sensitive modelling of directed graphs is becoming a key area of in the analysis of temporal data and dynamic structures. Dynamic graphs, which reflect changes in graph structure over time, introduce new possibilities for studying the development of relationships between vertices. This approach is particularly useful in areas such as change analysis in social networks, prediction in communication networks or analysis of dynamics in biological systems<sup>10</sup>.

The analysis of changes in social networks is one of the key applications of dynamic graphs. With them, the evolution of user relationships over time can be monitored and analysed to understand changes in online communities or social platforms. Identifying trends and assessing the impact of specific events on community structure become possible with this advanced approach.

In the context of communication networks, dynamic graphs make it possible to model and forecasting changes in the communication infrastructure. It is a useful tool to support the optimisation of data routes and network load management. These activities are key to maintaining network performance in a dynamic environment where relationships and connections are constantly changing. In the field of biology, time-sensitive graphs are used to in the analysis of interactions between proteins or genes. They allow the modelling and understanding of dynamic processes in organisms, enabling a better understanding of changes in molecular interactions and the identification of temporal sequences of biological phenomena<sup>11</sup>.

The introduction of a temporal dimension to directed graph modelling is essential for a more realistic representation of the complex processes taking place in different fields. Time-sensitive graphs are a powerful tool in the analysis and prediction of dynamic processes that are central to evolving areas of science, technology and practice.

## **6. NEURAL NETWORKS OF GRAPHS (GNNS)**

Graph neural networks (GNNs) are an innovative approach that has gained considerable popularity in the field of machine learning. It is an advanced tool for learning the representation of the vertices of a graph, given their environment. The main goal of GNNs is to extract information from the relationships between vertices in a graph, which translates into a more complex analysis of the graph structure.

The applications of GNNs are broad, covering tasks such as vertex classification, edge prediction or analysis of overall graph structure. In practice, GNNs prove to be particularly effective in modelling directed graphs, where dependencies between vertices are crucial<sup>12</sup>.

---

<sup>9</sup> J. Roe, Lectures on Coarse Geometry, University Lecture Series, American Mathematical Society (2003), 12-14.

<sup>10</sup> R. Engelking, K. Sieklucki, Geometry and Topology. Part II: Topology, Państwowe Wydawnictwo Naukowe (1980), 22-26.

<sup>11</sup> A. Uzawa and T. Oshima. Polypeptide synthesis directed by dna as a messenger in cell-free polypeptide synthesis by extreme thermophiles. The Journal of Biochemistry, 131:849-853, 2002.

<sup>12</sup> K. Z. Y. Han, B. Ma. Spider: Software for protein identification from sequence tags with de novo sequencing error. Journal of Bioinformatics and Computational Biology, 3:697-716, 2005.

The process of learning the representation of vertices in GNNs involves iterative processing of information based on relationships with the environment. Each vertex updates its representation based on its neighbouring vertices, which allows the context and structure of the graph to be taken into account.

In vertex classification tasks, GNNs are used to assign labels or categories to individual graph elements based on their structure and relationships to other vertices. In edge prediction, GNNs can predict whether an edge will exist based on existing relationships between vertices. GNNs introduce an advanced approach to the analysis of graph structures, especially in the context of directed graphs, where the direction of relationships matters. They can effectively model relationships between vertices, which is crucial in situations where the analysis of dynamic relationships between elements is necessary to understand complex phenomena.

In summary, graph neural networks (GNNs) are an innovative tool in the field of machine learning that is revolutionising the way we analyse and model graphs, especially directed graphs. With the ability to learn vertex representations from their environment, GNNs are becoming a key component in the growing field of graph analysis and network structures<sup>13</sup>.

## **7. GRAPH MINING**

Graph mining, also known as graph mining, is an advanced technique that uses data mining algorithms to discover hidden patterns, relationships and structures in graphs. In the context of directed graphs, where relationships have a specific direction, graph mining becomes a powerful tool to identify key substructures, analyse cycles and trajectories of change over time.

Data mining in directed graphs opens up new possibilities for researchers and analysts, allowing a better understanding of complex relationships between vertices. In practice, graph mining is used to extract information about the structure of the data, which can include identifying important graph patterns or analysing dynamic changes over time.

Among the main applications of graph mining in directed graphs is the identification of key substructures that are frequently present in the network under analysis. In addition, the technique allows efficient detection of cycles, which is important in the analysis of dependencies between vertices and potential loop problems in the data structure. For time-sensitive graphs, graph mining can help identify trajectories of change over time, enabling an understanding of the evolution of the graph structure and analysis of dynamic relationships between elements<sup>14</sup>.

Graph mining algorithms, such as subgraph isomorphism or cycle detection algorithms, are used in practice to identify specific patterns, analyse data structure and extract information from complex relationships between directed graph elements.

In summary, directed graph mining provides an advanced tool to explore the structure and relationships between vertices. It acts as an effective tool for discovering hidden patterns, analysing relationships and understanding the evolution of data over time, making it a key component in the field of data analysis. Modern approaches and trends in graph modelling represent a fascinating research area that is rapidly evolving with advances in technology. Analysis of recent scientific publications and participation in conferences on directed graph modelling shed light on the innovations and directions that are shaping the future of this field<sup>15</sup>.

In recent years, there has been a noticeable increase in interest in techniques based on artificial intelligence, especially using graph neural networks (GNNs). Scientific publications often explore the capabilities of GNNs in analysing the structures of complex relationships between vertices in directed graphs. In addition, scientific conferences are an arena where experts present the latest developments,

---

<sup>13</sup> D. E. Knuth. *Art of Computer Programming, Volume 1: Fundamental Algorithms*. Addison-Wesley Professional, 3rd edition, Massachusetts, 1997, 23-27.

<sup>14</sup> D. J. M.R. Garey. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.

<sup>15</sup> M. G. C. Resende and C. C. Ribeiro. Greedy randomized adaptive search procedure. *Handbook of Metaheuristics*, pages 716-719, 2003.

showcasing a variety of GNN applications ranging from social network analysis to modelling temporal structures in graphs.

Nowadays, graph modelling also takes into account dynamic and evolutionary aspects. New approaches are focusing on the study of changes over time, which is applicable to the analysis of the dynamics of relationships between vertices. Techniques are being discovered to take into account temporal aspects in graph structure, which is becoming crucial in understanding processes across domains, from social networks to biological systems. Trends in directed graph modelling also focus on the development of graph mining techniques that enable the discovery of hidden patterns, relationships and substructures in the networks being analysed. Modern approaches emphasise the need to develop advanced algorithms that can effectively deal with increasingly complex data<sup>16</sup>.

In light of these cutting-edge directions, graph modelling is becoming not only a tool for analysing network structure, but also a dynamic area of research that is influencing the development of artificial intelligence and data science. Scientific publications and conferences play a key role in the propagation and exchange of these modern ideas, shaping the future of directed graph modelling. Modern approaches to graph modelling introduce innovative techniques that enable more precise analysis and understanding of network structures. Two of these advanced approaches are the representation of graphs using embeddings and the consideration of temporal aspects.

Graph representation using embeddings is a technique in which the vertices of a graph are mapped to a low-dimensional space while preserving their structural features. This approach enables the efficient analysis of complex relationships between vertices by representing the graph in a more comprehensible and compact way. In practice, graph embeddings find applications in various fields such as recommendation, social network analysis or prediction in communication networks.

The second modern approach is to include temporal aspects in graph modelling. This is important, especially in the context of analysing temporal data and dynamic structures. Graphs that incorporate temporal aspects allow the study of changes in graph structure over time, which is crucial for understanding the evolution of relationships between vertices. Examples of applications include the analysis of changes in social networks, prediction in communication networks or the study of dynamics in biological systems<sup>17</sup>.

These modern approaches to graph modelling open the door to more advanced analysis and applications in a variety of fields. They range from techniques that enable a better understanding of graph structure to those that allow tracking and predicting changes over time, which is important in a dynamic data analysis environment. Together, these techniques are key tools in the field of graph modelling, supporting the development of advanced network analysis methods. The analysis of social data up to 2023 includes extensive use of directed graph models. These models are a key technique in identifying central figures, social groups and relationships between users in social networks. They make it possible not only to study community structure, but also to predict potential influences and interactions within social networks<sup>18</sup>.

In the context of research, analysing community data using graph models enables a better understanding of online community dynamics. Researchers use these models to identify communication patterns, the role of key individuals in communities and to analyse changes in community structure over time. In marketing practice, in turn, the analysis of online community behaviour has become an integral part of communication and branding strategies.

The modelling of directed graphs in online community analytics also enables the personalisation of content, tailoring it to individual user preferences. This, in turn, influences the effectiveness of marketing campaigns, improving customer relationships and increasing community engagement around a brand.

Looking ahead to 2023, it is anticipated that directed graph models in social data analysis will continue to develop and improve. Technological advances will allow for even more sophisticated social

---

<sup>16</sup> Szestało, P. (2015). Exploring Hamiltonian graphs with the Python language, 18-26.

<sup>17</sup> Matuszak, M. (2011). Bayesian networks in adaptation and optimization of behavioral patterns. *Artificial Intelligence*, 7006, 204-215.

<sup>18</sup> Kucharski, P. (2018). Dynamical systems as limits of inverse sequences of graphs, 33-39.

relationship research, which will contribute to a more complete understanding of the structure of online communities and more effective use of this data for research and business purposes<sup>19</sup>.

Case studies using specific models in real projects up to 2023 provide fascinating insights into the practical use of graph analysis models. These use cases illustrate how different industries and fields use graph models to solve specific problems and optimise their processes. In the e-commerce sector, for example, analysing customer behaviour with directed graph models can lead to more personalised product recommendations, which in turn increases the chances of a purchase. A case study can illustrate how the application of a specific graph algorithm identified complex relationships between different products and resulted in improved conversion rates.

## **8. APPLICATION OF DIRECTED GRAPHS**

In the field of cyber security, case studies can demonstrate the effective use of directed graph models to detect anomalies in computer networks. Analysing a specific incident where graph algorithms helped to identify suspicious traffic patterns and respond quickly to potential threats can provide practical guidance for other companies<sup>20</sup>.

In research, a case study could focus on the use of directed graph models to analyse interactions in biological networks. An example project could show how the identification of key genes and relationships between them using directed graphs has contributed to a better understanding of biological mechanisms.

In logistics, the use of directed graph models to optimise delivery routes could be the subject of a case study. An example project could describe how a specific graph algorithm helped to minimise logistics costs, taking into account various parameters and constraints.

Looking ahead to 2023, the case studies provide a valuable tool for understanding the practical benefits and challenges of using directed graph models in various projects. These real-world examples inspire further research and improvement of graph analysis technologies, while providing practical knowledge for companies and organisations interested in using these techniques in their fields of operation<sup>21</sup>.

In the financial sector until 2023, directed graph models are applied in a variety of areas, as illustrated by the case studies. Analysing the relationships between different financial institutions is key to understanding market structure and risk assessment. Case studies can demonstrate how specific graph models support the identification of relationships between banks, investment funds or other entities, enabling better management of systemic risk and faster response to changes in financial markets. In addition, directed graph models can be used to effectively identify potential cases of fraud or abuse by analysing the complex relationships between different financial transactions and market participants<sup>22</sup>.

In the area of healthcare by 2023, innovative solutions based on directed graph models are changing the way we analyse the relationship between patients, doctors and medical data. Case studies can showcase the concrete implementation of these models in projects where the analysis of the graph structure based on medical data allowed the optimisation of diagnostic processes, treatment and led to the personalisation of healthcare. Example projects can show how graph models support doctors in identifying new disease relationships, which can contribute to faster diagnosis and more effective treatment<sup>23</sup>.

In both sectors, finance and healthcare, projections up to 2023 suggest further development and refinement of directed graph models, allowing for even more precise analysis, faster decision-making and effective management of complex relationships and data. The case studies provide a valuable tool

---

<sup>19</sup> Deptuła, A., Zawislak, S., & Partyka, M. A. (2017). Application of decision logic trees and dependency graphs in the analysis of automatic transmission boxes. Buses: technology, operation, transport systems, 18.

<sup>20</sup> Markowski, K. (2008). Existence and determination of positive realizations of linear univariate and multivariate systems (Doctoral dissertation, The Institute of Control and Industrial Electronics).

<sup>21</sup> Nowak, R., & Michalowski, A. (2011). Graphs and graph algorithms, 19-29.

<sup>22</sup> Barodzich, A. (2023). Latin squares and list coloring of graphs (Doctoral dissertation, Department of Algebra and Combinatorics), 44-48.

<sup>23</sup> Mieczkowska, D. (2017). Development and implementation of an algorithm for visualization of directed acyclic graphs in radial layout (Doctoral dissertation, Department of Physics of Complex Systems), 55-57.



for understanding the practical benefits of applying these models to real-world projects, while providing inspiration for further developments in this rapidly growing field. In public transport, applications of directed graph models are shown through case studies that focus on route optimisation, vehicle fleet management and planning for transport infrastructure expansion. Example projects can illustrate how specific graph algorithms support the planning of the most efficient routes for public transport modes, minimising passenger journey times and reducing operational costs. In addition, graph models can be used for optimised vehicle fleet management, monitoring their location in real time, resulting in improved efficiency and passenger service<sup>24</sup>. In the manufacturing industry, case studies illustrate how directed graph models are used to analyse the relationships between different elements of the production process. Examples of applications can include identification of key points in production, optimisation of material routing or maintenance planning. Graph models enable a better understanding of the structure of the production process, leading to more efficient production organisation, optimised inventory management and minimised downtime.

In the field of business decisions, case studies show how directed graph models support decision-making processes at different levels of management. Competitive analysis using directed graphs can help to identify the strengths and weaknesses of competitors, which in turn informs business development strategies. Customer relationship management can be optimised through graph analysis, enabling a better understanding of customer preferences and behaviour. In addition, supply chain optimisation using directed graph models allows for better logistics management, reduced delivery times and minimised operating costs<sup>25</sup>.

These case studies illustrate the versatility of the applications of directed graph models in different sectors, bringing benefits both in terms of operational efficiency and support for decision-making processes at different organisational levels.

In the field of education until 2023, directed graph models are applicable in a variety of contexts, as illustrated by the case studies. Project examples can focus on analysing knowledge structure, identifying key concepts and optimising learning pathways. The case studies can illustrate how graph models support teachers to better understand the relationships between different knowledge domains, enabling the adaptation of curricula to meet individual students' needs. In addition, graph analysis can help identify areas that need more attention in the teaching process and facilitate the monitoring of students' progress<sup>26</sup>.

In the context of open source and community projects until 2023, describing the activities of communities developing directed graph models is crucial. Case studies can show how different scientific, software or educational communities are using open directed graph projects for collaborative development and knowledge sharing. Examples of such projects could include developing new graph algorithms, creating programming libraries or organising educational events. Describing how these communities contribute to the development and dissemination of directed graph technology can inspire other groups and individuals, encouraging active participation in open source communities.

The challenges of modelling directed graphs up to 2023 are an area of intense interest, in view of the growing importance of these models in various fields. Current trends and technological advances also involve some challenges that may affect the development and successful application of directed graphs. The first of the important challenges is scalability. As the amount of available data grows and the complexity of analysing relationships in large networks increases, directed graph modelling must meet the needs of efficiently processing massive amounts of information. Efficient algorithms and optimisation techniques become crucial to maintain high performance while maintaining analysis accuracy<sup>27</sup>.

Another major challenge is to account for the dynamic nature of the data. Where relationships between vertices are constantly changing over time, modelling directed graphs needs to take these dynamics into account. The adaptability of models to changes in network structure becomes a key factor, especially in the context of analysing social data or predicting changes in communication networks.

---

<sup>24</sup> Salawa, D. (2020). Analysis of heuristic algorithms for the problem of the set of disjoint edges in directed graphs, 77-79.

<sup>25</sup> Krawczyk, A. (2016). Exploring Halina graphs with the Python language, 88-93.

<sup>26</sup> Zwiernik, P. On graphical modelling in the context of time series analysis, 91-94.

<sup>27</sup> Malinowski, Ł. (2014). Implementation of selected algorithms for weightless graphs in Python, 22-26.

In addition, the challenge is to develop more advanced methods for representing vertices in graphs. Traditional approaches to graph embeddings are being developed to better account for complex relationships between vertices. The use of technologies such as graph neural networks (GNNs) allows a more precise capture of the structure of directed graphs, but at the same time presents researchers with challenges related to the with the interpretability of these models<sup>28</sup>.

## **9. DATA SECURITY IN DIRECTED GRAPHS**

Data security in the context of directed graphs is another issue that requires attention. With the increasing use of graph models in the areas of finance, healthcare or transport, issues of data confidentiality and integrity are becoming a priority. Effective data protection mechanisms need to be developed, especially when these models are used to analyse sensitive information.

The future of directed graph modelling until 2023 will be shaped by the responses to these challenges. Innovations in algorithms, data processing technologies and the development of modern approaches, such as graph neural networks, will be key to the further development of this rapidly growing field. At the same time, the anticipated changes and advances provide motivation to continue research into directed graph modelling in order to exploit its potential even more effectively in different areas.

A review of anticipated developments in graph modelling up to 2023 sets out areas where significant progress and innovation is expected. The first key direction is the further improvement of graph analysis algorithms. Modern approaches such as the use of advanced machine learning techniques, including graph neural networks, are expected to enable more precise and efficient processing and analysis of large graph datasets. At the same time, the development of scalable algorithms will become crucial to deal with the increasing complexity of networks<sup>29</sup>.

Another direction is the evolution in the representation of graphs. New methods for graph embeddings will strive to represent even better the complex relationships between vertices, as well as to account for dynamic changes in network structure. Advances in this area have the potential to improve the effectiveness of graph models in applications ranging from community analysis to predicting changes in temporal networks.

The foreseeable direction of development also includes the development of new technologies and tools for graph visualisation. As the amount and complexity of graph data increases, visualisation tools need to evolve to provide users with more intuitive and efficient ways to analyse the structure of graphs.

In the context of the rapidly growing field of Graph Neural Networks (GNNs), it is anticipated that their application will expand to new areas and the models themselves will become more advanced. GNNs will be developed to deal with more complex graph structures, as well as to optimise their interpretability, allowing a better understanding of the decision-making processes undertaken by these models.

Finally, it is anticipated that graph modelling will become more accessible to a variety of disciplines, including non-computer scientists. Tools and platforms that enable graphs to be more easily created, managed and analysed will be key to expanding the applications of graph modelling in different areas of life.

These developments show that the future of graph modelling up to 2023 is dynamic and full of potential for further innovations that will impact a variety of fields, from data science to artificial intelligence<sup>30</sup>. With the growing influence of graph models in various fields, ethical issues are becoming central to the discussion on the collection, analysis and use of graph data until 2023. In this context, focused attention to ethics and responsibility becomes essential. Research on ethical frameworks and the development of responsible practices in graph modelling will become a key aspect guiding the development of the field.

---

<sup>28</sup> Augustyn, D. R., & Warchał, Ł. (2011). Application of Bayes networks in query selectivity estimation in the Oracle database server query optimizer. *Studia Informatica*, 32(1A), 94.

<sup>29</sup> MAGISTER, P. D. Implementation of a recursive self-associative network for encoding and classifying directed graphs with labelled vertices, 33-37.

<sup>30</sup> Schiff, K. (2011). An algorithm for determining multicommodity maximum flow in directed graphs. *Logistics*, (2).

Understanding the ethical challenges of graph data includes aspects such as privacy, confidentiality, fairness, transparency and honesty in analysis and interpretation of results. Defining ethical guidelines will aim to protect the rights of individuals, prevent abuse and ensure that the benefits of graph modelling are evenly distributed, respecting the principles of social justice.

Paradoxically, the development of interdisciplinarity in the field of graph modelling is one of the key solutions to ethical challenges. By integrating knowledge from the fields of mathematics, computer science, sociology, economics and biology, researchers can better understand the context in which graph data are collected and analysed. Collaboration between different disciplines will contribute to a more holistic view of the structures and relationships in different types of networks, which in turn will lead to more sustainable and ethical approaches to graph modelling. Anticipated developments in ethics and interdisciplinarity will guide the development of graph modelling towards more responsible, fair and sustainable practices. These trends reflect the understanding that developments in technology and data science must go hand in hand with moral considerations to achieve real benefit for society.

Global collaboration and the establishment of standards in the field of graph modelling are setting directions that play a key role in the further development of the field until 2023<sup>31</sup>.

International cooperation on graph data standards is becoming essential in the context of the increasing complexity of projects and organisations working with graph data. Developing global standards will allow for better interoperability between different projects, enabling more effective information sharing and collaboration on a global scale. Common graph modelling platforms, based on global standards, will help to improve the processes of graph data analysis and integration, both on a national and international level.

In the context of the development of the market for graph modelling tools and platforms, rapid growth and the emergence of new innovations are anticipated. New tools and platforms may emphasise ease of use, offering more intuitive interfaces, making graph modelling accessible to a wider range of users. Advanced visualisation features will be key to better understanding the structure of graphs, and integration with other analytical tools will enable more comprehensive data analysis.

Overall, these trends point to the need for collaboration and standardisation in graph modelling and the growing demand for modern tools to help effectively manage and analyse increasingly complex graph data structures<sup>32</sup>.

Increasing awareness of graph modelling is becoming a priority among professionals in various fields, and this issue will remain central to the development of the field until 2023. Educational programmes and training in graph modelling are essential for professionals across industries to more fully understand the potential and limitations of these advanced tools.

Education in graph modelling allows professionals not only to learn how to use specific tools, but also to understand the basic concepts, algorithms and practices associated with graph data. This, in turn, enables them to use graph modelling more effectively in their fields of work and also supports the development of new applications and solutions.

The parallel emerging field of graph analysis and processing at the edge (edge computing) is an innovative approach that has the potential to change the way we work with graph data. Analysing and processing graphs at the point of origin, i.e. at the edge, allows for more efficient data management and faster decision-making, eliminating the need to send huge amounts of data to central servers. This approach has the potential to revolutionise working with graph data, especially in the context of the Internet of Things (IoT) and applications requiring low latency and fast processing<sup>33</sup>. As a result, increased awareness among professionals and the development of graph processing technology at the edge will contribute to a more effective and comprehensive use of graph modelling in practice.

The evolution of directed graph structures is an important area of review until 2023, covering the dynamic development of the field in the context of changing technologies and new types of data. With advances in technology and the emergence of increasingly diverse data, directed graph structures are evolving, with implications for methods of modelling and analysis.

---

<sup>31</sup> Wait, M. (2012). An application for visualising different types of graphs, 45-49.

<sup>32</sup> Wozniak, M. Directed versions of the 1-2-3 and 1-2 hypotheses. combinatorics and cryptography, 56-59.

<sup>33</sup> Hajder, M., Nycz, M., & Różycki, P. (2014). Analysis of functional and operational characteristics of hierarchical communication networks, 52-61.

Developments in technology are introducing new challenges and opportunities in directed graph modelling, and one of the key trends is the use of artificial intelligence. The growing interest in AI is opening up new horizons in directed graph analysis and modelling. Machine learning algorithms, especially those based on advanced neural networks, are becoming an integral part of the analysis, prediction and generation of graph structures. Artificial intelligence can effectively support pattern identification, analysis of complex relationships and automation of information extraction processes from graph data.

As AI-based models become more sophisticated, their ability to adapt to evolving directed graph structures increases. Machine learning algorithms, including those using deep neural networks, can dynamically adapt to changes in the structure of the data, enabling more accurate predictions, identification of relevant patterns and more efficient analysis of directed graphs.

As a result, a 2023 review focused on the evolution of directed graph structures and the growing use of artificial intelligence in their modelling will identify key trends and innovations shaping the field in the coming years<sup>34</sup>.

In the context of the 2023 review, an important aspect is to highlight the growing role of directed graphs in the field of scientific research. With advances in technology and the increasing availability of data, directed graph models are becoming an indispensable tool in life science fields.

Scientific research in biology, chemistry and physics often requires complex analysis of the relationships and interactions between different elements. Directed graphs excel at modelling these complex structures, allowing scientists to identify new relationships and patterns that can lead to breakthroughs. In molecular biology, for example, directed graphs can represent interactions between proteins or genes to aid understanding of biological functions.

Paradoxically, as the amount of available data increases, so do the challenges of processing large graph data. The 2023 review should emphasise tools and techniques for efficient processing, analysis and visualisation of large directed graphs. Advanced algorithms and tools for processing large amounts of graph data are crucial for researchers, enabling them to efficiently extract information and understand relationships in complex systems.

As a result, the development and growing application of directed graphs in scientific research are important directions that will contribute to advances in many scientific fields, while at the same time requiring effective data processing tools to maximise the potential of the available information<sup>35</sup>.

In Poland, the developed academic and research sector opens up prospects for applications of directed graphs in various fields. In the field of scientific research, especially in biology, chemistry and computer science, directed graph models are becoming an invaluable tool for analysing the relationships between different elements.

In the field of biology, directed graphs can be used to represent interactions between different proteins or genes. This allows for a better understanding of complex biological mechanisms and the discovery of new relationships. In chemistry, directed graphs can represent molecular structures, which is important for analysing chemical reactions and identifying the properties of substances.

In the industrial sector, in both manufacturing and services, directed graphs are becoming a tool for process optimisation. In supply chain analysis, these models help to manage the relationships between different logistical elements, which contributes to more efficient operations. Furthermore, analysing the organisational structure of companies using directed graphs enables a better understanding of the relationships between different organisational units.

In the field of education, Polish universities and research institutes use directed graphs to analyse the structure of knowledge. They can be used to identify key concepts in a given field of study, which supports the learning process. Optimising learning paths with directed graphs allows the curriculum to be adapted to the needs of students, facilitating the acquisition of knowledge.

In this way, directed graphs represent an important tool for researchers, industry and academia in Poland, enabling more sophisticated and effective analyses of complex relationships and structures<sup>36</sup>.

---

<sup>34</sup> Holowinski, G., & Malecki, K. (2023). Graph cellular automaton with variable relational cellular neighborhoods-assumptions for implementation in FPGA. *Measurement Automation Control*, 57(8), 861-863.

<sup>35</sup> Hare, K. (2019). Estimating eigenvalues using directed graphs.

<sup>36</sup> Hajder, M., & Kolbusz, J. (2014). Minimizing the memory complexity of graph models of technical objects.

In the context of technological innovation, Poland, being a developing technology market, finds a number of opportunities for the use of directed graphs in innovative high-tech projects. Directed graphs are a powerful tool in the field of data analysis, which can lead to innovative solutions in various sectors. In the technology sector, directed graph models can be used to analyse the relationships between different technologies, system components or software architectures. This allows for more effective project planning, identification of potential areas of optimisation and adaptation to a dynamically changing technological environment.

Public administration in Poland can also benefit from the potential of directed graphs. Analysis of the structure of relationships between different administrative units can help to streamline administrative operations, optimise processes and identify areas for improvement. Directed graphs can also be used to analyse the relationships between different public projects, which contributes to effective resource management and resource allocation<sup>37</sup>.

Poland can also actively participate in open source projects and scientific communities related to directed graphs. Cooperation with international research and business teams allows for the exchange of experience, development of innovative solutions and joint contribution to the development of directed graph technology on a global scale.

In this way, Poland can play an active role in the global technological ecosystem, using the potential of graphs directed to the creation of innovative solutions, both at the technological and administrative level.

The overview of graphs directed to 2023 presented here provides a comprehensive analysis of the area, showing both the basic issues and modern trends as well as the future of the field.

The paper begins with an introduction to directed graphs as data structures, highlighting their importance in various fields such as social network analysis or routing in computer networks.

It then focuses on basic definitions and terminology related to directed graphs, explaining the essence of vertices, edges, vertex degree, paths and cycles. Basic operations on directed graphs are also presented, such as graph traversal, finding shortest paths, topological sorting, cycle analysis and spanning trees<sup>38</sup>.

Another area of analysis is the practical applications of directed graphs, including social data analysis, network behaviour prediction, recommendations, route optimisation in public transport, management in the manufacturing industry or business decision support. Case studies from various sectors such as finance, healthcare or education are also presented, showing specific projects using directed graphs.

In the context of modern approaches to graph modelling, techniques such as graph embeddings, consideration of temporal aspects and the use of Graph Neural Networks (GNNs) are discussed. A review of research and conferences provides a glimpse into the latest trends and innovations in the field, as well as open source projects and community collaborations.

The challenges of the directed graph model are then analysed, both ethical and technological, including the development of the tool market, education or graph analysis at the edge. Predictions for the future of the field are also presented, including the evolution of graph structures, the use of artificial intelligence and the role of directed graphs in scientific research<sup>39</sup>.

The work also takes into account the Polish perspective, showing the potential of directed graphs in research, the industrial sector, education, technological innovation, public administration and cooperation with the scientific and business community.

In summary, this review offers a comprehensive understanding of directed graphs, demonstrating their key role in data analysis, the various applications and trends that are shaping the field. The work sheds light on current and future challenges, as well as on the potential for development, highlighting the importance of ethics, education and international cooperation.

---

<sup>37</sup> Czarnowska, M., & Migawa, K. (2013). Identification of the operation process of means of transport in the road transport system. *Advances in Mechanical Engineering*, (1), 18-27.

<sup>38</sup> Wisniewska, M., & Wisniewski, R. (2010). Application of hypergraph coloring in the process of parallel decomposition of concurrent automata. *Methods of Applied Computer Science*, 23, 151-157.

<sup>39</sup> Laszkiewicz, B., & Sobczak, T. (2022). Analysis and implementation of path finding algorithms for use in browser games. *Scientific Bulletin of the Wrocław College of Applied Informatics. Computer Science*, 9(1).

## Bibliography

1. Augustyn, D. R., & Warchał, Ł. (2011). *Application of Bayes networks in query selectivity estimation in the Oracle database server query optimizer*. *Studia Informatica*, 32(1A), 94.
2. Barodzich, A. (2023). *Latin squares and list coloring of graphs (Doctoral dissertation, Department of Algebra and Combinatorics)*.
3. Czarnowska, M., & Migawa, K. (2013). *Identification of the operation process of means of transport in the road transport system*. *Advances in Mechanical Engineering*, (1), 18-27.
4. Wait, M. (2012). An application for visualising different types of graphs.
5. D. E. Knuth. *Art of Computer Programming, Volume 1: Fundamental Algorithms*. Addison-Wesley Professional, 3rd edition, Massachusetts, 1997.
6. D. J. M.R. Garey. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.
7. Deptuła, A., Zawisłak, S., & Partyka, M. A. (2017). *Application of decision logic trees and dependency graphs in the analysis of automatic transmission boxes*. *Buses: technology, operation, transport systems*, 18.
8. G. Bell, A. Dranishnikov, Asymtotic Dimension in Będlewo, arXiv:math.GR/0507570v2 (2005)
9. Hajder, M., & Kolbusz, J. (2014). *Minimizing the memory complexity of graph models of technical objects*.
10. Holowinski, G., & Malecki, K. (2023). *Graph cellular automaton with variable relational cell neighborhoods-assumptions for implementation in FPGA*. *Measurement Automation Control*, 57(8), 861-863.
11. J. Roe, *Lectures on Coarse Geometry*, University Lecture Series, *American Mathematical Society* (2003)
12. K. Z. Y. Han, B. Ma. *Spider: Software for protein identification from sequence tags with de novo sequencing error*. *Journal of Bioinformatics and Computational Biology*, 3:697-716, 2005.
13. Kaminska, A. M. (2018). *Application of graph structures for bibliometric and webometric analyses*. *Models and methods*. *New Library. Services, Information Technology and Media*, 29(2), 47-63.
14. Kawa, A. (2013). *Analysis of enterprise networks using the SNA method*. *Entrepreneurship and Management*, 14(13), 1.
15. Krawczyk, A. (2016). *Exploring Halina graphs with the Python language*.
16. Kucharski, P. (2018). *Dynamical systems as limits of inverse sequences of graphs*.
17. Laszkiewicz, B., & Sobczak, T. (2022). *Analysis and implementation of path finding algorithms for use in browser games*. *Scientific Bulletin of the Wrocław College of Applied Informatics. Computer Science*, 9(1).
18. M. Cencelj, J. Dydak, A. Vavpetič, Z. Virk, *A Combinatorial Approach to Coarse Geometry*, arXiv:math.MG/0906.1372v1 (2009)
19. M. G. C. Resende and C. C. Ribeiro. *Greedy randomized adaptive search procedures*. *Handbook of Metaheuristics*, pages 716-719, 2003.
20. Magiera, J. (1995). *Graphs as metric spaces*. *Scientific Works of the Wrocław University of Economics*, (696 Didaktyka), 55-65.
21. MAGISTER, P. D. *Implementation of a recursive self-associative network for encoding and classifying directed graphs with labelled vertices*.
22. Malinowski, Ł. (2014). *Implementation of selected algorithms for weightless graphs in Python*.

23. Markowski, K. (2008). *Existence and determination of positive realizations of linear univariate and multivariate systems* (Doctoral dissertation, The Institute of Control and Industrial Electronics).
24. Matuszak, M. (2011). *Bayesian networks in adaptation and optimization of behavioral patterns. Artificial Intelligence*, 7006, 204-215.
25. Mieczkowska, D. (2017). *Development and implementation of an algorithm for visualization of directed acyclic graphs in radial layout* (Doctoral dissertation, Department of Physics of Complex Systems).
26. Nowak, R., & Michalowski, A. (2011). *Graphs and graph algorithms*.
27. R. Engelking, K. Sieklucki, *Geometry and Topology*. Part II: Topology, PWN (1980)
28. Salawa, D. (2020). *Analysis of heuristic algorithms for the problem of the set of decimating edges in directed graphs*.
29. Schiff, K. (2011). *An algorithm for determining multi-commodity maximum flow in directed graphs. Logistics*, (2).
30. Schiff, K. (2011). *An algorithm for determining multi-commodity maximum flow in directed graphs. Logistics*, (2).
31. Szestało, P. (2015). *Exploring Hamiltonian graphs with the Python language*.
32. Swierczek, A. (2007). *From supply chains to supply networks. Logistics*, 1, 74-77
33. Uzawa and T. Oshima. *Polypeptide synthesis directed by dna as a messenger in cell-free polypeptide synthesis by extreme thermophiles*. The Journal of Biochemistry, 131:849-853, 2002.
34. Wisniewska, M., & Wisniewski, R. (2010). *Application of hypergraph coloring in the process of parallel decomposition of concurrent automata*. Methods of Applied Computer Science, 23, 151-157.
35. Wozniak, A. (2010). *Graphs and networks in decision-making techniques. Infrastructure and Ecology of Rural Areas*, (04).
36. Wozniak, M. *Directed versions of the 1-2-3 and 1-2 hypotheses. combinatorics and cryptography*.
37. Hare, K. (2019). *Estimating eigenvalues using directed graphs*.
38. Zwiernik, P. *On graphical modelling in the context of time series analysis*.

## სატელეკომუნიკაციო ქსელებში ინფორმაციის უსაფრთხოების დარღვევის გამომწვევი მიზეზები და ინფორმაციის დაცვის მეთოდები

ელვირა ბჟინავა<sup>1</sup>, სალომე მახარაძე<sup>2</sup>, მანანა გოგბერაშვილი<sup>3</sup>  
<sup>1,2,3</sup>ციფრული სატელეკომუნიკაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი  
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

### CAUSES OF INFORMATION SECURITY BREACHES IN THE TELECOMMUNICATION NETWORKS AND METHODS OF PROTECTING INFORMATION

Elvira Bzhinava<sup>1</sup>, Salome Makharadze<sup>2</sup>, Manana Gogberashvili<sup>3</sup>  
<sup>1,2,3</sup>Department of Digital Telecommunication Technologies, Georgian Technical University  
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

**რეზიუმე.** ადამიანების საქმიანობის ყველა სფეროს ციფრულ ფორმატში გადასვლამ, კაცობრიობას მოუტანა დიდი მიღწევები, გაამარტივა კომუნიკაცია და გაზარდა ბიზნეს პროცესების ეფექტურობა. დადებით ასპექტებთან ერთად მნიშვნელოვნად გაიზარდა კონფიდენციალურობაზე მოთხოვნა. მონაცემების უმეტესობა ინახება ციფრული ფორმით, რაც უბიძგებს თავდასხმელებს ინფორმაციის მოპარვის ახალი გზების ძიებაზე. ბიზნესის სფერო და ფიზიკური პირები ყოველწლიურად აწყდებიან კიბერსაფრთხეებს, რომელთა მთავარი მიზანია ზიანი მიაყენოს ელექტრონულ კომპიუტერულ სისტემებსა და ქსელებს, ასევე ინფორმაცია უნებართვოდ მიითვისონ. ინფორმაციის დაცვის საშუალებების ტექნოლოგიურმა განვითარებამ დღეისათვის მიაღწია იმ დონეს, როდესაც პირველ პოზიციებზე უკვე წამოწეულია მათი გამოყენების აუცილებლობა. განსხვავებული კიბერშეტევები, ერთის მხრივ მოითხოვს განსხვავებულ ტექნოლოგიურ გადაწყვეტილებებს, მეორეს მხრივ დაცვის კომპლექსური სისტემის შექმნას, კომპლექსში გამოყენებული დაცვის საშუალებების მინიმალური რაოდენობის შერჩევის საფუძველზე, რაც ხარჯების შესაბამისად, ოპტიმიზაციის პროცესის განხორციელების ექვივალენტურია. სამუშაოს მიზანია, ინფორმაციის უსაფრთხოების უზრუნველსაყოფად განისაზღვროს შესაბამისი კონკრეტული მიზეზები, გაანალიზდეს შედეგები და შეირჩეს დაცვის საშუალებები. მეთოდოლოგია: კვლევაში გამოყენებულია თვისობრივი კვლევის მიდგომები, რაც გულისხმობს ვრცელი ლიტერატურის თეორიულ მიმოხილვასა და ანალიზს. დასკვნები შედგენილია მთავრობის ანგარიშებიდან და რეცენზირებადი ჟურნალებიდან. გაანალიზებულია უსაფრთხოების გამოკვლევის მეთოდები და ტექნიკური საშუალებები, ასევე მომავალი პერსპექტივები და მათემატიკური გაანგარიშების აუცილებლობა.

**საკვანძო სიტყვები:** ციფრული, უსაფრთხოება, ინფორმაციული, ანტივირუსი, მომხმარებელი, ინტერნეტ ქსელი, ჰაკინგი, ფიშინგი.

**ABSTRACT:** The transition of all spheres of human activity to digital format has brought great achievements to humanity, simplified communication and increased the efficiency of business processes. Along with the positive aspects, the demand for privacy has increased significantly. Most data is stored in digital form, which pushes attackers to look for new ways to steal information. Businesses and individuals face meet cyber threats every year, the main goal of which is to damage



electronic computer systems and networks, also to misappropriate information without authorization. The technological development of information protection tools has now reached a level where the necessity of their use has already been put at the forefront. Different cyberattacks, on the one hand, require different technological solutions, on the other hand, the creation of a complex protection system based on the selection of the minimum number of protection means used in the complex, which is equivalent to implementing an optimization process in accordance with costs. The goal of the work is to identify relevant specific reasons, analyze the results, and select protection measures to ensure information security. Methodology: the study uses qualitative research approaches, which involves a theoretical review and analysis of extensive literature. The conclusion are compiled from government reports and peer-reviewed journals. Are analyzed methods and technical means of security research, also future prospects and the need for mathematical calculations.

**KEYWORDS:** Digital, Security, Information, Antivirus, User, Internet network, Hacking, Phishing.

**1. შესავალი.** ინფორმაციული სისტემების ფუნქციონირების ეფექტურობის დარღვევა, ანუ ინფორმაციული სისტემების ქმედითუნარიანობის დარღვევა, შეიძლება ხდებოდეს ინფორმაციის დამახინჯების ან ბლოკირების გამო, რაც განსაკუთრებულად აქტუალური პრობლემაა რეალური დროის ინფორმაციის დაცვის ინტეგრირებული სისტემებისთვის. ტექნოლოგიური თვალსაზრისით პრობლემა, რომ არ მოხდეს, ინფორმაციის გაჟონვის სახით საჭიროა ორგანიზაციული და ტექნიკური ღონისძიებების გატარება, აუცილებელია მომხმარებელთა აუტენტიფიკაცია და ავტორიზაცია სათანადო დონეზე, კავშირგაბმულობის არხებში შიფრაციის განხორციელება, პერსონალურ მონაცემებთან ხელმისაწვდომობის შეფასება და სატელეკომუნიკაციო არხებში მონაცემების გადაცემის მთლიანობის დაცვა. ამასთანავე, გასათვალისწინებელია, რომ დაცული ინფორმაცია ლოკალურ ქსელში შეიძლება მომხმარებელისათვის პრაქტიკულად მიუწვდომელი გახადოს. მაგრამ, ინტერნეტის ქსელში ეს შეუძლებელია, ვინაიდან ინფორმაციული საზოგადოებისათვის ასეთი ღონისძიება მიუღებელია. ჩვენ ვცხოვრობთ ღია ინფორმაციულ სამყაროში, სადაც სახელმწიფო ორგანოების მოღვაწეობის შესახებაც კი მონაცემები უნდა იყოს მაქსიმალურად ღია [2].

**2. ინფორმაციის გაჟონვა.** როცა დასრულდება ინფორმაციული საზოგადოების კონცეფციის რეალიზება, ელექტრონული მთავრობის, სახელმწიფო მომსახურების უზრუნველყოფა ინტერნეტით და ა.შ. შეიქმნება „ღია გასაღებების“ ინფრაქტრუქტურა. მაგრამ, ამ შემთხვევაშიც წარმოიქმნება ქსელური უსაფრთხოების პრობლემა. „ღია გასაღებების“ ინფრასტრუქტურაც დაუცველი აღმოჩნდება შემოტევებისაგან, ვინაიდან მისი საქსელო კომპონენტები გაფანტულია ღია ქსელებში. გასათვალისწინებელია, რომ ინფორმაციის მისაღებად, ნებისმიერ შემთხვევაში აუცილებელია მიერთების ქსელის არსებობა, შესაბამისად ინფორმაციული უსაფრთხოების საკითხის გადასაწყვეტად, საჭიროა შესაბამისი რესურსებით სატელეკომუნიკაციო სივრცის უზრუნველყოფა[7].

ყველა კომპანიას, მიუხედავად მისი ინდუსტრიისა და განვითარების მასშტაბისა, აქვს ამა თუ იმ სახის კონფიდენციალური ინფორმაცია (პირადი და კომერციული ინფორმაცია, ინტელექტუალური საკუთრება და ა.შ.). ნებისმიერი ორგანიზაციისთვის სავალდებულო მოთხოვნაა ასეთი აქტივების დაცვა გარე და შიდა თავდამსხმელებისგან. მაგრამ ხშირად არის პრობლემები, რომლებიც დაკავშირებულია იმასთან, რომ კომპანიები ყოველთვის ვერ აცნობიერებენ გარკვეული მონაცემების მნიშვნელობას და არ აქცევენ საკმარის ყურადღებას მათ დაცულობას. შედეგად, კონფიდენციალური ინფორმაცია შეიძლება იყოს რისკის ქვეშ და კომპანიამ შეიძლება სერიოზული ზიანი მიიღოს. სტატიაში მოცემულია რა

პრობლემების წინაშე დგანან კომპანიები, რა საფრთხეს წარმოადგენს უსაფრთხოების არასრულყოფილი სისტემები და თანამშრომლებზე კონტროლის ნაკლებობა. ასევე განხილულია სისუსტეების აღმოფხვრისა და რისკების მინიმიზაციის მეთოდები. ორგანიზაციულად მნიშვნელოვანი მონაცემები არის ინფორმაცია, რომელიც საჭიროა ბიზნეს მიზნებისა და ამოცანების მისაღწევად და სტრატეგიული გადაწყვეტილებების მისაღებად. ეს შეიძლება იყოს მონაცემები კლიენტების, გაყიდვების, ფინანსური მაჩვენებლების, წარმოების პროცესების, კონკურენტების და ა.შ. ეს მონაცემები უნდა იყოს ზუსტი, განახლებული და სანდო, რათა ორგანიზაციამ შეძლოს ეფექტური ფუნქციონირება და დაეხმაროს მას განვითარებაში.

კორპორატიული ინფორმაციის შენახვისა და დამუშავების ორგანიზებაში არაადეკვატურობამ შეიძლება გამოიწვიოს გაჟონვა. გარკვეულმასის სისუსტეებმა განსაკუთრებით ხშირად შეიძლება გამოიწვიოს შემდეგი სახის ინციდენტები:

- მონაცემთა დაცვის არაადეკვატური შიდა სისტემა, მოძველებული ხელსაწყოების ან პროგრამული უზრუნველყოფის გამოყენება დაუდასტურებელი ეფექტურობით.
- თანამშრომლების გადაჭარბებული უფლებამოსილებები, რაც გულისხმობს მონაცემთა გაფართოებულ წვდომას, რომლებთან მუშაობა არ არის მათი სამუშაო პასუხისმგებლობის ნაწილი.
- არასანდო მეხსიერების გამოყენება, რომელზეც თანამშრომლების უმეტესობას აქვს წვდომა.
- კონფიდენციალურ ინფორმაციასთან ურთიერთქმედების მკაფიო ალგორითმების ნაკლებობა.
- მომხმარებლის ქმედებებზე სათანადო კონტროლის ნაკლებობა.
- მონაცემების გამოყენება შეუძლიათ არა მხოლოდ გარე თავდასხმელებს, რომლებსაც სურთ მისი მოპარვა ან კომპანიის რეპუტაციის შელახვა. არამედ, არ არის გამორიცხული საფრთხეები შიდა თანამშრომლებისგანაც მოდიოდეს, რომელთაგან შეიძლება შემთხვევით ან განზრახ გაჟონოს ინფორმაციამ ან გამოიყენონ იგი პირადი სარგებლობისთვის. ასევე არსებობს კომერციული ჯაშუშობა, რომელიც დაკვეთილია კონკურენტების მიერ.

### 3. ინფორმაციის გაჟონვის მიზეზები [4].

შიდა საფრთხეები შეიძლება გამოწვეული იყოს სხვადასხვა ფაქტორებით, როგორცაა:

- კომპანიის უსაფრთხოების პოლიტიკის შესახებ თანამშრომელთა ინფორმირებულობის არასაკმარისი დონე.
- კონფიდენციალური ინფორმაციის დამუშავების მკაფიო ინსტრუქციებისა და პროცედურების ნაკლებობა.
- მონაცემთა წვდომის უფლებების ბოროტად გამოყენება.
- კონფიდენციალური ინფორმაციის არასათანადო შენახვა და გადაცემა.
- თანამშრომლების შეგნებული და შემთხვევითი ქმედებები, რომლებიც მიზნად ისახავს მონაცემების მოპარვას ან განადგურებას.

აუცილებელია მკაფიოდ განისაზღვროს ვის შეუძლია კონფიდენციალურ ინფორმაციაზე წვდომა და რა პირობებში. ამისათვის აუცილებელია წვდომის დონეების სისტემის შემუშავება, რომელიც უზრუნველყოფს ორგანიზაციის თანამშრომლებისთვის განსხვავებულ როლებს და წვდომის უფლებებს.

დაშიფვრა გულისხმობს მონაცემთა დაშიფვრას ისეთ ფორმას, რომ მისი წაკითხვა შეუძლებელია. ეს ღონისძიება იცავს არავტორიზებული წვდომისგან, ჯაშუშური პროგრამებისგან და სხვა თავდასხმებისგან, რომლებიც მიზნად ისახავს ინფორმაციის

მოპარვას. ინფორმაციის წასაკითხად დაგჭირდებათ სპეციალური გასაღები. თუგამოყენებული იყო სიმეტრიული დაშიფვრის ტექნოლოგია, ეს იგივე იქნება კოდირებისთვის და დეკოდირებისთვის. ასიმეტრიული მიდგომის შემთხვევაში გამოიყენება ორი გასაღები - საჯარო მონაცემების გარდაქმნის მიზნით და კერძო პირვანდელ ფორმატში გადასაყვანად.

უსაფრთხოების აუდიტი შეიძლება განხორციელდეს როგორც კომპანიის, ასევე მესამე მხარის ექსპერტების მიერ. ინსპექტირების ოპტიმალური სიხშირე არის 6 თვეში ერთხელ.

**Firewalls და Access Controls:** Firewall-ები უსაფრთხოების სავალდებულო ინსტრუმენტებია, რომლებიც შექმნილია მონაცემთადაუცველობის აღმოსაჩენად, ტრაფიკის რულოვინგის საშუალებად და საექსპოზიციის კავშირებისა და შეტყობინებების პაკეტების დაბლოკვისთვის. ასევე არის ახალი თაობის firewalls - NGFW. შემდეგი თაობის Firewall-ის პროდუქტებს აქვთ უფრო ფართო ფუნქციონირება, რადგან ასეთი გადაწყვეტილებები ახორციელებს რამდენიმე დამცავ ინსტრუმენტს, რომლებსაც შეუძლიათ პარალელურად მუშაობა.

შიდა რესურსებზე წვდომის გასაკონტროლებლად და მომხმარებლის ანგარიშების მართვისთვის გამოიყენება IdM და Identity Management კლასის გადაწყვეტილებები. ისინი საშუალებას იძლევა თავიდან იქნეს აცილებული გადაჭარბებული უფლებების გაჩენა, ოპტიმიზაცია გაუწიოთ მუშაობას სისტემებს, მონაცემებზე წვდომის მოთხოვნით და დაინერგოს უფლებების მინიჭების როლური მოდელი.

#### **მომხმარებლის იდენტიფიკაცია და ავთენტიფიკაცია:**

**იდენტიფიკაცია** - არის პროცესი, რომლითაც რესურსი ან სისტემა ადასტურებს მომხმარებლის არსებობას, რომელიც ცდილობს მასში შესვლას. ტიპიური მაგალითია სისტემაში შესვლა. სისტემა ამოწმებს არის თუ არა ასეთი მომხმარებელი რეგისტრირებული. თუ კი, შემდეგი ეტაპი იწყება.

**ავთენტიფიკაცია** - არის პროცედურა, რომელიც ადასტურებს მომხმარებლის ავთენტურობას. მაგალითი - პაროლის შეყვანა შესვლის დადასტურების შემდეგ. ეს არის ჩვეულებრივი ერთფაქტორიანი ავთენტიფიკაცია, რომელიც არასრულყოფილად ითვლება, რადგან თავდამსხმელებს შეუძლიათ პაროლის მოპარვა ან უბრალოდ გამოცნობა. მრავალფაქტორიანი (ყველაზე ხშირად ორფაქტორიანი) პროცედურა მოიცავს დამატებით გადამოწმებას, მაგალითად, კოდის შეყვანას ტელეფონიდან ან ელექტრონული ფოსტიდან, ბიომეტრიული მახასიათებლების (თითის ანაბეჭდის, ხმის ჟღერადობის და ა.შ.) წარმოდგენას. ორივე ეს პროცესი ერთმანეთთან მჭიდრო კავშირშია და ძალიან მნიშვნელოვანია ინფორმაციის უსაფრთხოების უზრუნველსაყოფად და მონაცემთადაუცველობის აღმოსაფხვრელად.

შეჭრის აღმოჩენისა და პრევენციის სისტემები ეს არის IPS და IDS გადაწყვეტილებების კლასები (სრული სახელები - Intrusion Prevention System და Intrusion Detection System), რომლებიც საშუალებას გაძლევთ ამოცნობილი იქნეს თუნდაც ატიპიური საფრთხეები. არჩეული პროდუქტის სახეობიდან გამომდინარე, მათ შეუძლიათ შეისწავლონ ანომალიები, ჩაატარონ კვლევა ხელმოწერების ან წესების საფუძველზე [5].

DLP სისტემები - ეს არის მონაცემთადაკარგვის პრევენციის კლასის პროდუქტები, რომლებიც ხელს უშლიან მონაცემთადაუცველობის ექსპლუატაციას, აკონტროლებენ ქსელის აქტივობას, აკონტროლებენ ინფორმაციის გადაცემის არხებს და აწარმოებენ დეტალურ ანგარიშებს ინფორმაციის მდგომარეობის შესახებ. ეს ფუნქციებით მდიდარი ინსტრუმენტები განიხილება, როგორც ყველაზე ეფექტური შიდა ინციდენტების თავიდან ასაცილების საშუალება. DLP სისტემაში ფოსტის კონექტორი - აკონტროლებს მონაცემთა გადაცემას ელექტრონული ფოსტით. მოდული მუშაობს როგორც მონიტორინგის, ასევე აქტიური საწინააღმდეგო რეჟიმებში, ანუ მას შეუძლია დაბლოკოს საექსპოზიციო ოპერაციები.

Endpoint Agent - აკონტროლებს თანამშრომლების ქმედებებს სამუშაო სადგურებზე, ფინანსური ინფორმაციის ჩათვლით.

Solar Dozorსისტემა ეხმარება აღმოაჩინოს და თავიდან აიცილოს გაჟონვა, ებრძვის კორპორატიულ თაღლითობას და უზრუნველყოფს თაღლითობისეფექტურპრევენციას. კონფიდენციალური ინფორმაციის გაჟონვისგან საიმედო დაცვის უზრუნველსაყოფად, Solar Dozor იყენებს სპეციალიზებულ მოდულებს - ჩამჭრელებს. ისინი აგროვებენ და ანალიზისთვის გადასცემენ თანამშრომელთა კომუნიკაციებს სხვადასხვა არხებიდან, აკონტროლებენ მომხმარებლის ქმედებებს პერსონალურ კომპიუტერებზე, ასევე აწარმოებენ ინვენტარიზაციას და აკონტროლებენ ადგილობრივ და ღრუბლოვან ფაილურ რესურსებს [1].

ტექნიკური მახასიათებლებიდან გამომდინარე, თითოეული არხისთვის შეირჩევა ინფორმაციის ჩასმის ოპტიმალური წერტილი. ეს შეიძლება იყოს ფოსტის სერვერი, ქსელის კარიბჭე, პროქსი სერვერი ან სამუშაო სადგური. ეს მიდგომა საშუალებას იძლევა თანაბრად გადაანაწილდეს დატვირთვა IT ინფრასტრუქტურაზე და უზრუნველყოფილი იქნეს ორგანიზაციის ბიზნეს პროცესების უწყვეტობა, მინიმუმამდე იქნეს დაყვანილი სისტემის გადატვირთვის გამო მუშაობის შეფერხების რისკები.

OCR (ოპტიკური სიმბოლოების ამოცნობა) - საშუალებას იძლევა გადაყვანილი იქნეს გრაფიკული ფორმით გადაცემული მონაცემები (ფოტოები, ეკრანის ანაბეჭდები, სკანირება) და განზრახ დეფორმირებული, რათა ამოცნობა გართულდეს წასაკითხ ფორმატში.

File Crawler - საშუალებას იძლევა დადგინდეს კონფიდენციალური ინფორმაციის შენახვის წესების დარღვევა.

დოკუმენტის ნაკადის ანგარიში სხვადასხვა საკომუნიკაციო არხებზე დოკუმენტების განაწილების ავტომატურად თვალყურის დევნებისთვის. საშუალებას იძლევა სწრაფად და ეფექტურად გააკონტროლოდეს კონფიდენციალური ინფორმაციის მოძრაობა, განისაზღვროს მიმღებები და გამგზავნები, გადაცემის დრო, ასევე მოვლენის კრიტიკულობის დონეები.

#### 4. ქსელში ინფორმაციის უსაფრთხოების საფრთხის სახეები:

**უნებლიე თუ შემთხვევით.** ისინი წარმოიქმნება პროგრამული უზრუნველყოფის შეცდომების, ტექნიკის გაუმართაობის და მომხმარებლების და სისტემის ადმინისტრატორების არასწორი ქმედებების შედეგად. არ არსებობს მიზანმიმართული ხასიათი - ეს დამახასიათებელია მეორე კატეგორიისთვის [5].

**განზრახ.** მიზნად ისახავს ქსელის მომხმარებლების დაზიანებას. შეიძლება იყოს აქტიური და პასიური. პასიური მიზნად ისახავს ქსელის საინფორმაციო რესურსების უნებართვო გამოყენებას და არ ახდენს რაიმე განსაკუთრებულ გავლენას ქსელების ფუნქციონირებაზე. უსაფრთხოების აქტიურ საფრთხეებს აქვს მიზანმიმართული ზემოქმედება აპარატურულ, პროგრამულ და საინფორმაციო ქსელის რესურსებზე, რაც იწვევს ამ უკანასკნელის მუშაობაში ჩავარდნას. ეს ეხება საკომუნიკაციო ხაზების, ოპერაციული სისტემების და კომპიუტერული აღჭურვილობის განადგურებას. აქტიური საფრთხეები ასევე მოიცავს მომხმარებლის მონაცემთა ბაზებიდან ინფორმაციის დამახინჯებას.

ყველაზე გავრცელებული პრობლემები, რომლებსაც ონლაინ მომხმარებლები აწყდებიან, არის მონაცემთა ქურდობა, ვირუსები და ჰაკერები. თითოეული საფრთხის მახასიათებლები: სანამ განვიხილავთ ინტერნეტში ინფორმაციის დაცვის აუცილებლობას, ჩვენ გავანალიზებთ საფრთხეების ძირითად ტიპებს, რომლებსაც მომხმარებლები აწყდებიან. როდესაც ვსაუბრობთ უსაფრთხოების საფრთხეებზე, ვგულისხმობთ ქმედებებს

და მოვლენებს, რომლებიც ამახინჯებენ, იწვევენ მონაცემთა დაკარგვას და უკანონო გამოყენებას.

**ჰაკინგი.** თავდამსხმელები იღებენ წვდომას პროფილების, ელ.ფოსტის, ვებსაიტების და კომპიუტერული სისტემების ანგარიშის ინფორმაციაზე. თუ ქსელის დაუცველობაზე თავდასხმა წარმატებულია (მათ შორის RDP პროტოკოლის გამოყენებით, რომლის მეშვეობითაც ხდება კავშირები დისტანციურ სამუშაო სადგურებთან), თაღლითები შეძლებენ მიიღონ სრული დისტანციური წვდომა მიმდინარე მომხმარებლის მოწყობილობებზე.

**მავნე პროგრამები და ვირუსები.** ჩვენ ვსაუბრობთ ჭიებზე, ტროიანებზე და სხვა მავნე პროგრამებზე. ასეთი პროგრამული უზრუნველყოფა შექმნილია სპეციალურად სერვერების, კომპიუტერების, ქსელების დაზიანების მიზნით, კონფიდენციალური ინფორმაციის მოპარვის მიზნით. ვირუსები შეიძლება გავრცელდეს მავნე რეკლამის სახით. მომხმარებელი აჭერს შეტყობინებას, რის შემდეგაც მის მოწყობილობაზე დაინსტალირდება ვირუსი. ასევე, მრავალი მოწყობილობის მფლობელი „იჭერს“ მავნე პროგრამას ინფიცირებული საიტების მონახულების შემდეგ. ამიტომ, ნუ გახსნით გაუგებარ ბმულებს, თუნდაც მეგობრების შეტყობინებებიდან, ნუ უგულებელყოფთ ანტივირუსულ გაფრთხილებებს და აუცილებლად გამოიყენეთ ანტივირუსული პროგრამები.

**პირადობის ქურდობა.** თავდამსხმელები დაინტერესებულნი არიან მომხმარებელთა პერსონალური მონაცემებით, რათა გამოიყენონ ისინი საკუთარი ინტერესებისთვის ან შემოსავლის გამომუშავების მიზნით გადაყიდვის გზით. ყველაზე ხშირად, ფინანსური და სხვა ინფორმაცია მიზანმიმართულია. ყველა თანამედროვე მომხმარებლის ამოცანაა მიიღოს ყველა შესაძლო ზომა, რომელიც გაზრდის პერსონალური მონაცემების უსაფრთხოებას. ინფორმაციის ქონა საგრძნობლად ამცირებს მომავალში წარმოქმნილი პრობლემების რისკს.

**ფიშინგი.** ასევე ელ.ფოსტის საერთო საფრთხეა. ეს ძველი ონლაინ უსაფრთხოების საფრთხე ჯერ კიდევ არსებობს. საუბარია მიზანმიმართულ კიბერშეტევაზე, რომლის მთავარი ინსტრუმენტი ყალბი ელ.წერილების გაგზავნაა. მომხმარებელი იღებს შეტყობინებას ბანკიდან ან სხვა სანდო კომპანიისგან, ხსნის მას და მიჰყვება ბმულს. ამ უკანასკნელს მომხმარებელი გადაჰყავს მავნე საიტზე, ამიტომ ვირუსი ავტომატურად იტვირთება მოწყობილობაში. თავდამსხმელები იღებენ წვდომას მომხმარებლის პირად ინფორმაციაზე და შეუძლიათ გამოიყენონ ისინი საკუთარი შეხედულებისამებრ[8].

## 5. ინფორმაციის გაჟონვის შედეგები.

საინფორმაციო სისტემაშიყოველთვის არის მონაცემთა დაკარგვის, მოდიფიკაციის, ქურდობისა და ანადგურების რისკი.

ამის საპირისპიროდ გამოიყენება ინფორმაციის დაცვის სხვადასხვა მეთოდი, რომელიც ხორციელდება სპეციალიზებული პროგრამული უზრუნველყოფის დაყოფის მომცველი უსაფრთხოების სისტემების დანერგვით.

პერსონალური მონაცემების დაცვა არის სახელმწიფოებრივ დონეზე, ერთ-ერთი უმნიშვნელოვანესი მიმართულება ინფორმაციული უსაფრთხოების უზრუნველყოფის ერთიან სისტემაში[7].

რა ითვლება პერსონალურ მონაცემებად? განსაზღვრის შესაბამისად – ეს არის ნებისმიერი ინფორმაცია, რომელიც პირდაპირ ან ირიბად ეხება გარკვეულ (ან გასარკვევ) ფიზიკურ პირს (პერსონალური მონაცემების სუბიექტს). მაგალითად, თუ მითითებულია სუბიექტის მისამართი, მაგრამ ამ მონაცემებს არ ახლავს სახელი და გვარი, ესეც აგრეთვე არის

პერსონალური მონაცემები, მაგრამ უსახური, რადგანაც პერსონალური მონაცემების სუბიექტის დადგენა შეუძლებელია დამატებითი მონაცემების გარეშე. პერსონალური მონაცემების დაცვასთან დაკავშირებით არსებობს მნიშვნელოვანი შედეგები, თუ რა შეიძლება ზემოქმედებდეს პერსონალური მონაცემების გაქონვის ალბათობაზე - ძირითადად, დასამუშავებელ პერსონალურ მონაცემებში ცნობების მოცულობა [7] (ცხრილი 1, ცხრილი 2).

**ცხრილი 1. პერსონალური მონაცემების შესახებ ჩანაწერების რაოდენობა**

პერსონალური მონაცემების შესახებ ჩანაწერების რაოდენობა	რესპოდენტების რაოდენობა პროცენტებში, რომლებიც ამუშავებენ პერსონალურ მონაცემებს
მილიონზე მეტი	16%
500 ათასიდან მილიონამდე	6%
100 ათასიდან 500 ათასამდე	5%
50 ათასიდან 100 ათასამდე	4%
10 ათასიდან 50 ათასამდე	20%
1000-დან 10 ათასამდე	20%
1000-ზე ნაკლები	19%
ანალიზს არ ექვემდებარება	10%

(ინფორმაციის წყარო [6])

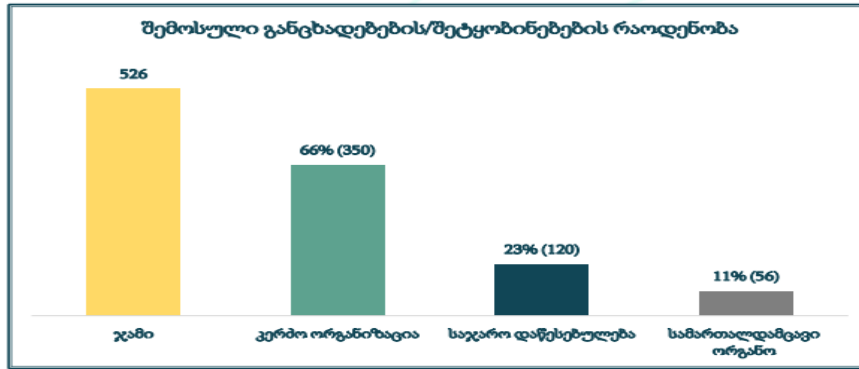
**ცხრილი 2. პერსონალურ მონაცემებზე წვდომის შესაძლო მაჩვენებლები**

მონაცემთა უსაფრთხოების დაცვის მოთხოვნათა შეუსრულებლობა	30%
მონაცემთა დამუშავება კანონით გათვალისწინებული საფუძვლების გარეშე	20%
მონაცემების დამუშავების პრინციპების დარღვევა	15%
პირდაპირი მარკეტინგის მიზნებისათვის მონაცემთა წესების დარღვევით გამოყენება	9%
მონაცემთა სუბიექტის ინფორმირების წესების დარღვევა	8%
ვიდეოთვალთვალის წესების დარღვევა	6%
განსაკუთრებული კატეგორიის მონაცემთა დამუშავება კანონით გათვალისწინებული საფუძვლების გარეშე	4%
უფლებამოსილი პირის მიერ მონაცემთა დამუშავება კანონით გათვალისწინებული წესების დარღვევით	3%
მონაცემთა დამუშავებლის მიერ მონაცემთა დამუშავების უფლებამოსილი პირისთვის დავალება წესების დარღვევით	2%
მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის წესის დარღვევა	1%

(ინფორმაციის წყარო [6])

პრაქტიკულად, მხოლოდ უსაფრთხოების სამსახურის თანამშრომლების დაშვება პერსონალურ მონაცემებთან შეესაბამება 4%, ხოლო ინფორმაციული ტექნოლოგიების სამსახურის თანამშრომლები ყველაზე ხშირად (41%) არიან პერსონალურ მონაცემებთან, რაც ძალზე დამაფიქრებელია.

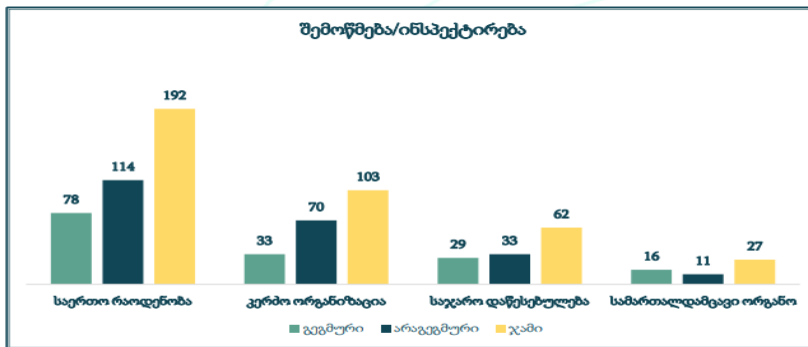
საანგარიშოპერიოდში, სამსახურამიილო 526 განცხადება/შეტყობინება, რომელთაგან 350 (66%) შეეხებოდა მონაცემთა დამუშავებას კერძო ორგანიზაციებში, 120 (23%) — საჯარო უწყებებში, ხოლო 56 (11%) — სამართალდამცავ ორგანოებში (ფიგურა 1).



მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება)

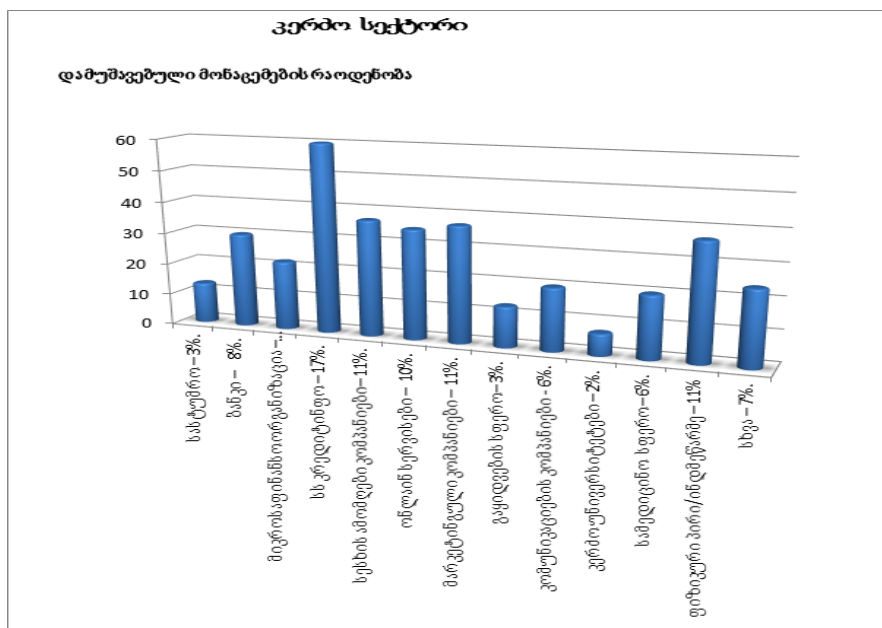
ფიგურა 1. მონაცემთა დამუშავების კანონიერების შემოწმება [6]

სამსახურმა ჩაატარა მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება) 192 ფაქტზე. მათგან 41% (78) ჩატარდა გეგმურად, ხოლო 59% (114) — არაგეგმურად (ფიგურა 2, ფიგურა 3).



გამოვლენილი ადმინისტრაციული სამართალდარღვევები

ფიგურა 2. გამოვლენილი ადმინისტრაციული სამართალდარღვევები [6]



ფიგურა 3. საქართველოს, პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის 2018 წლის ანგარიშიდან – მდგომარეობა კერძო სექტორში

## 6. ინფორმაციის დაცვის საშუალებები

ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი, ემყარება ინფორმაციის დაცვის საშუალებების ურთიერთგადაფარვის შესაძლებლობების არსებობას.

**ინტერნეტ ქსელებში მონაცემთა დაცვის მეთოდები** [3].

ქსელებზე ინფორმაციის დაცვა მნიშვნელოვანი ღონისძიებაა ყველასთვის, ვინც იყენებს ქსელის რესურსებს პირადი და საქმიანი მიზნებისთვის. ოპტიმალური შედეგის მიღწევა შესაძლებელია მხოლოდ ინტეგრირებული მიდგომით. ის მოიცავს ანტივირუსულ დაშიფვრის პროგრამებს, ფაიერვოლებს, ლოკალურ ქსელებზე წვდომის უფლებებს და/ან პასუხისმგებელია კომპანიის შიდა ქსელების ადექვატურ ფიზიკურ იზოლაციაზე სხვა სუბიექტებისგან.

**კრიპტოგრაფია ან დაშიფვრა.** ასეთი არხების გამოყენებისას მონაცემთა დაცვის დონე დამოკიდებულია დანერგილი ალგორითმების სირთულეზე. ორიგინალური ინფორმაცია იქნება კოდირებული და გადაეცემა მომხმარებლებს შორის. მასალების გამოყენებისას გამოიყენება სპეციალური დეკოდირების გასაღები. ტექნოლოგია უზრუნველყოფს გადაცემული ინფორმაციის სრულ უსაფრთხოებას.

**ქსელის დაცვა.** ეს ინსტრუმენტები მოიცავს მიმდინარე მოვლენების აუდიტს, ორფაქტორიან ავტორიზაციას და ავთენტიფიკაციას. მრავალფაქტორიანი ავთენტიფიკაცია არის მომხმარებლის იდენტიფიკაციის მრავალი დონის შემოწმება. ორი ან მეტი გადამოწმების მეთოდი შეიძლება გამოყენებულ იქნას ერთდროულად. შესვლა-პაროლის წყვილის სტანდარტული მოთხოვნის გარდა, სისტემას შეუძლია მოითხოვოს ერთჯერადი დამატებითი პაროლები, კოდის კითხვები ან ბიომეტრიული ინფორმაცია (თითის ანაბეჭდი, სახის ID და ა.შ.).

**პროგრამული უზრუნველყოფის დაცვა.** ჩვენ ვსაუბრობთ სპეციალიზებული პროგრამული უზრუნველყოფის გამოყენებაზე, რომელიც ხელს შეუშლის თავდამსხმელებს მონაცემთა მოპარვისკენ მიმართული მოქმედებების ერთობლიობის განხორციელებაში. დაცვის პროგრამული ტიპი მოიცავს ინფორმაციის დაშიფვრას და წვდომის დონის განაწილებას მომხმარებლებს შორის. თქვენ უბრალოდ უნდა ყურადღებით აკონტროლოთ ანტივირუსული განახლებების დროულობა და სამუშაო ოპერაციების განსახორციელებლად ონლაინ ბრაუზერების არჩევანი. ბრაუზერები არის ადგილი, სადაც კონფიდენციალური მონაცემები გაჟონავს.

**ჩაშენებული ანტივირუსული დაცვა.** ხელს უშლის ქსელებში არაავტორიზებულ წვდომას ინფიცირებული ობიექტების ჯერ აღმოჩენით და შემდეგ იზოლირებით[9].

**კავშირის მონიტორი.** აკონტროლებს ყველა დამყარებულ კავშირს, განსაზღვრავს არხის დატვირთვას, ტრაფიკის ტიპებს და სამუშაოს ხელმისაწვდომ მიმართულებებს.

**ანტივირუსი.** პროგრამა ამოწმებს FTP, HTTP ნაკადებს და ფაილებს მათში, ქსელის სიჩქარის შენელების გარეშე. ანტივირუსი საჭიროა ინტერნეტ რესურსებზე წვდომის დასარეგულირებლად, გამორიცხავს პოტენციურად საშიშ საიტებს კლიენტის ქსელების დასაცავად.

**პორტის გადაზავნის წესები.** უსაფრთხოების ამჟამინდელი დონის გაზრდის მიზნით, ცენტრალიზებულ დონეზე დაყენებული პორტის ნომრები შეიცვლება თვითნებურად შერჩეული პროტოკოლებისთვის. ამ შემთხვევაში, ICS სისტემები გადაამისამართებენ მიმდინარე პაკეტებს ახალზე. ეს გაართულებს ადგილობრივ ქსელებზე გარედან წვდომას და იქნება ეფექტური ღონისძიება დამატებითი დაცვის უზრუნველსაყოფად.

**IDS Snort .** შეჭრის გამოვლენის სისტემა არის თავისუფალი ტიპის პროტოკოლი, რომელიც შეიქმნა გარე შეტევების მცდელობების იდენტიფიცირებისა და ანალიზისთვის და



მუშაობს რეალურ დროში განუწყვეტლივ. შეჭრის გამოვლენას და ყველაზე ცბიერ შეტევებსაც კი აქვთ საერთო მახასიათებლები - ისინი ტიპიურია და მათი ზუსტად გამოვლენა შესაძლებელია. შესაბამისად, მონაცემთა ქურდობა შეიძლება ეფექტურად იქნას აცილებული.

**მაგიდის ARP ტრეკერი.** როდესაც ვსაუბრობთ ARP-ზე, ვგულისხმობთ პროტოკოლს, რომელიც ჩაწერს ფაქტებს MAC მისამართების შესატყვისი IP მისამართების სესიის ბოლოს ან სანამ მისამართი რაიმე მიზეზით შეიცვლება. თუ კორესპონდენციაში მოხდა არასანქცირებული ცვლილება, თვალთვალის მოდული ნებისმიერ მოქმედებას აღიქვამს, როგორც შენიღბვის ან ჩანაცვლების მიზანმიმართულ მცდელობას და დაიწყებს განგაშის ატეხვას [10].

დღეს საინფორმაციო ქსელის უსაფრთხოება ახალ დონეს აღწევს. ტრაფიკი უნდა გაანალიზდეს რაც შეიძლება სრულყოფილად - განაცხადიდან ფიზიკურ დონებამდე. კერძოდ, ICS იყენებს მონაცემთა დაცვის სხვადასხვა მეთოდს. ეს საშუალებას იძლევა მიიღწეს ქსელებში ინფორმაციის უსაფრთხოების მაქსიმალური დონე. თქვენ თავად შეგიძლიათ გამოიყენოთ სხვადასხვა მეთოდი, მაგრამ ICS ითვლება მოწინავე, ყველაზე ეფექტურ სისტემად. მისი არჩევით თქვენ მიიღებთ გარანტირებულ შედეგებს. გარდა ამისა, ჩვენ გირჩევთ, მიჰყევთ მიმოხილვაში მითითებულ რეკომენდაციებს და გამოიყენოთ მონაცემთა დაცვის გაფართოებული ტექნიკა [7].

ინფორმაციის დაცვის საშუალებების შერჩევა წარმოადგენს რთულ ამოცანას, რადგანაც ინფორმაციის დაცვის უკვე არსებულ სისტემაზე ნებისმიერი დამატება, ზემოქმედებს სისტემის ქმედითუნარიანობასა და მომსახურების სახეობების წვდომაზე.

## 7. მოსალოდნელი საფრთხეების მოდელის შედგენა

ობიექტების ინფორმაციული უსაფრთხოების უზრუნველყოფის შემდეგი ზომები, მეთოდები და საშუალებები არსებობს [1]:

- საკანონმდებლო (სამართლებრივი) ზომები;
- ორგანიზაციული (ადმინისტრაციული) დაცვის ზომები;
- პროგრამულ - ტექნიკური ზომები;
- არასანქცირებული ჩართვებისა და მიერთებებისაგან დაცვის საშუალებები;
- იდენტიფიცირებისა და აუტენტიფიცირების საშუალებები;
- შეღწევების გამიჯვნის საშუალებები;
- საინფორმაციო და პროგრამული რესურსების მთლიანობის უზრუნველყოფისა და კონტროლის საშუალებები;
- მოვლენების ოპერატიული კონტროლისა და რეგისტრაციის საშუალებები;
- ინფორმაციის დაცვის კრიპტოგრაფიული საშუალებები;
- ინფორმაციის უსაფრთხოების უზრუნველყოფის სისტემის მართვა;
- დაცვის სისტემის ეფექტურობის კონტროლი;
- საინფორმაციო - სატელეკომუნიკაციო სისტემებისა და ქსელების დაცვის ფიზიკური ზომები და საშუალებები.

მიზანშეწონილია მოსალოდნელი საფრთხეების მოდელის შედგენა, მაგალითად:

$$A_j = (P_j ; X_j), \quad (1)$$

სადაც,  $P_j$  - არის მოსალოდნელი საფრთხის ალბათობა;

$X_j$  - ზიანის ხარისხი, რომელიც განისაზღვრება უსაფრთხოების დარღვევით გამოწვეული შედეგებით (კონფიდენციალურობა, ინფორმაციის სისრულე, მიღწევადობა).

ცხადია, თუ ცნობილი იქნება ობიექტის დაცულობის ალბათობა და ბოროტმოქმედის შესაძლო პოტენციალი, ობიექტისათვის მოსალოდნელი საფრთხის, ლოგიკურ-ალბათური ფუნქციის გამოსახულება ასე ჩაიწერება:

$$P_j = (P_1, P_2), \quad (2)$$

სადაც  $P_1$  – არის მისაღწევი დაცულობის ალბათობა;

$P_2$  – ბოროტმოქმედის შესაძლებლობების (პოტენციალის) ალბათობა;

ობიექტზე უკვე არსებული დაცვის სისტემის შესაძლებლობებიდან გამომდინარე, მოსალოდნელი საფრთხის ლოგიკურ-ალბათური ფუნქციის გამოსახულებას ექნება შემდეგი სახე:

$$P_j = (P_1 \text{ საწყისი}, P_2), \quad (3)$$

სადაც,  $P_1$  საწყისი – პროექტით გათვალისწინებული დაცულობის ალბათობა, ინფორმაციის დაცვის კომპლექსური სისტემის შექმნამდე.

ინფორმაციის დაცვის  $M$  რაოდენობის საშუალებებიდან, დასაცავი ობიექტის მოთხოვნებიდან გამომდინარე, ვირჩევთ  $N$  რაოდენობის ინფორმაციის დაცვის საშუალებებს, ანუ  $N$  არის  $M$  სიმრავლის ქვესიმრავლე,  $N \in M$ , სადაც  $N \equiv \{n_j\}, j=1, k$ , ცხადია  $k$  არის ინფორმაციის დაცვის კომპლექსურ სისტემაში გამოყენებული დაცვის საშუალებების რაოდენობა.

შესაბამისად  $n_i = n_i(X_i)$ , სადაც  $X_i$  არის  $i$ -იური დაცვის საშუალების ტექნიკური მახასიათებლების და ფუნქციების ამსახველი მაჩვენებელი.

თუ დავუშვებთ, რომ ინფორმაციის დაცვის  $i$ -იური საშუალება უზრუნველყოფს დაცვის  $N_i$  რაოდენობის ფუნქციებს, მაშინ

$$\sum_{i=1}^K N_i = N_{\text{დაცვის}}$$

სადაც  $N_{\text{დაცვის}}$  - არის ინფორმაციის დაცვის კომპლექსური სისტემის ფუნქციების რაოდენობა. იმის გათვალისწინებით, რომ ინფორმაციის დაცვის საშუალებებისათვის შერჩეულ კრიტერიუმებს უზრუნველყოფს განსხვავებული დანიშნულებების სისტემები. ცხადია:

$$\sum_{i=1}^K N_i < N_{\text{დაცვის}}$$

რადგანაც

$$X_i \cong X_{i\text{მოთხოვნილი}}$$

სადაც  $X_{i\text{მოთხოვნილი}}$  - არის  $i$ -ური დაცვის საშუალებისადმი წაყენებული მოთხოვნების შესაბამისად შერჩეული დაცვის ფუნქციების რაოდენობა, მაშინ ჩვენი ამოცანის მიზნობრივ ფუნქციას ექნება შემდეგი სახე:

$$\left\{ \begin{array}{l} \sum_{i=1}^K N_i < N_{\text{დაცვის}} \\ X_i \cong X_{i\text{მოთხოვნილი}}, \quad i=1, K \end{array} \right.$$

## 8. დასკვნა

ობიექტებისათვის სატელეკომუნიკაციო ქსელებსა და სისტემებს უნდა გააჩნდეთ მზადყოფნის კოეფიციენტები კრიტიკულობის კოეფიციენტების შესაბამისად, სადაც მზადყოფნის კოეფიციენტების მნიშვნელობები განსაზღვრული იქნება მდგრადობის (სიცოცხლისუნარიანობის) შესაბამისად. აუცილებელია ახალი, ფუნდამენტური შედეგი, როგორც ინფორმაციაზე შემოტევებისაგან დაცვის პრობლემების მეცნიერულად

ფორმულირებისათვის, ასევე ინფორმაციის ზემოქმედებების აცილების მეთოდებისა და საშუალებების ანალიზისა და სინთეზისათვის. იმის გათვალისწინებით, რომ შემოტევების მეთოდები და მექანიზმები აგრეთვე, განიცდიან სრულყოფას, აუცილებელია ინფორმაციის დაცვის კომპლექსური სისტემის გათვალისწინება საერთო სარგებლობის ქსელებში. ტექნიკურ სრულყოფასთან ერთად შეიძლება შეიქმნას დაცული ინფორმაციული საზოგადოება. ამისათვის ტექნიკური საშუალებები არსებობს, მაგრამ არ არსებობს ნორმატიული ბაზა. ინფორმაციის მიმოცვლის პროცესში, სატელეკომუნიკაციო ქსელში შესაძლო ხიფათის წარმოქმნის გათვალისწინება და მისი მართვის უნარის არსებობა წარმოადგენს ინფორმაციული დაცულობის უზრუნველყოფის საფუძველს. საქართველოსთვის არსებულ განსაკუთრებულ საფრთხეს წარმოადგენს ყველაზე მაღალი ალბათობით სახელმწიფო საინფორმაციო რესურსებზე შემოტევები. აუცილებლად უნდა არსებობდეს შესაბამისი 3 – 5 წლიანი სახელმწიფო პროგრამა, დაცული ბიუჯეტით, რომელშიც, გარდა სახელმწიფო ორგანოებისა, ჩართული იქნება საგანმანათლებლო სისტემა, ვინაიდან ამ პროგრამის შედეგებს ესაჭიროება დანერგვა და კომპეტენტური ექსპლუატაცია.

### **ბიბლიოგრაფია**

1. <https://rt-solar.ru> (15.11.2024)
2. ИСО / МЭК 27032:2012 – Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Information technology - Security techniques – Guidelines for cybersecurity).  
URL: [http://www.iso.org/iso/ru/catalogue\\_detail?csnumber=44375](http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375), (15.11.2024).
3. ITU – T Recommendation X. 800: Security architecture for Open Systems Interconnection for CCITT applications. – URL: <http://www.itu.int/rec/T-REC-X.800-199103-I>
4. Jaap de Waard. The Private Security Industry in International Perspective // European Journal on Criminal Policy and Research. 1999. V. 7. Issue 2. P. 143 – 174.
5. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии. // Электросвязь, №5, 2014 стр. 44-47.
6. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის საქმიანობის სტატისტიკა.  
URL: <https://shorturl.at/wugEF>
7. ყიფიანი ქ. „ინფორმაციის დაცვის მეთოდების კვლევა სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით“. დისერტაცია. 2019. გვ. 106.
8. <https://sky-dynamics.ru/> (15.11.2024).
9. <https://xserver.a-real.ru/blog/useful/zashchita-informatsii-v-seti-internet/> (15.11.2024).
10. <https://sky-dynamics.ru/stati/metody-i-sredstva-zashchity-informacii-v-internete/> (15.11.2024).
11. <https://www.edpb.europa.eu/> (15.11.2024).

## LI-FI ტექნოლოგიით აგებული ქსელის კიბერუსაფრთხოება

სალომე მახარაძე<sup>1</sup>, ელვირა ბჟინავა<sup>2</sup>, მანანა გოგბერაშვილი<sup>3</sup>  
<sup>1,2,3</sup>ციფრული სატელეკომუნიკაციო ტექნოლოგიების დეპარტამენტი, საქართველოს  
ტექნიკური უნივერსიტეტი  
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

### CYBERSECURITY OF A NETWORK BUILT WITH LI-FI TECHNOLOGY

Salome Makharadze <sup>1</sup>, Elvira Bzhinava <sup>2</sup>, Manana Gogberashvili<sup>3</sup>  
<sup>1,2,3</sup> Department of Digital Telecommunication Technologies, Georgian Technical University  
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

**რეზიუმე:** თანამედროვე საზოგადოების ყოველდღიურობა წარმოდგენილია ინფორმაციის გაცვლისთვის უსადენო ტექნოლოგიების გამოყენების გარეშე. მონაცემთა უსადენოდ გადაცემა ხორციელდება 3G, 4G, LTE, 5G, Wi-Fi და სხვა ტექნოლოგიების გამოყენებით. აღნიშნული ტექნოლოგიების ფუნქციონირებისთვის საჭიროა რადიოსიხშირეების გამოყენება. შეზღუდული სიხშირული ზოლი და მონაცემთა გადაცემის სიჩქარე, რომელიც დამოკიდებულია ქსელში ერთდროულად ჩართულ მომხმარებელთა რაოდენობაზე, ასევე რამდენიმე წყაროს ერთმანეთზე გავლენა, განაპირობებს ახალი ტექნოლოგიის შექმნის აუცილებლობას. უფრო მეტად სრულყოფილ ტექნოლოგიას წარმოადგენს Li-Fi (Light Fidelity) ტექნოლოგია, რომელშიც დასახელებული პრობლემები არ არსებობს. Li-Fi ტექნოლოგია დაფუძნებულია სინათლის ენერჯის გამოყენებაზე, ინფორმაციის უსადენოდ გადასაცემად იყენებს ხილულ ან უხილავ სინათლეს, რომელსაც ასხივებს შუქდიოდი, რის საშუალებითაც შესაძლებელია ორმხრივი მაღალსიჩქარული კავშირის უზრუნველყოფა. სტატიის წარმოდგენილია Li-Fi ტექნოლოგიის სისტემის არქიტექტურა, ტექნოლოგიის უპირატესობები და ნაკლოვანებები, მახასიათებლები, გამოყენების სფეროები. დასახელებულია უსადენო კავშირის ქსელებში არსებული კიბერუსაფრთხოების სახეობები. ნებისმიერ ტექნოლოგიაში მნიშვნელოვანია უსაფრთხოების შესაბამისი ზომების მიღება პოტენციური საფრთხეებისგან თავის დასაცავად, უსაფრთხოების რისკების მინიმუმის მიზნით Li-Fi ტექნოლოგია გამოირჩევა მონაცემთა დაცულობისა და კონფიდენციალურობის უპირატესობით Wi-Fi-ისთან შედარებით. ის უზრუნველყოფს მონაცემთა უსაფრთხოდ გადაცემას და ქსელის საიმედოდ მუშაობას. ნაშრომში ასევე მოცემულია Li-Fi ტექნოლოგიაში გამოყენებული კიბერუსაფრთხოების საშუალებები და მეთოდები.

**საკვანძო სიტყვები:** უსადენო კავშირი; Wi-Fi; შუქდიოდი; LED განათება; Li-Fi; კიბერუსაფრთხე; კიბერუსაფრთხოება; შიფრაცია.

**ABSTRACT:** The daily life of modern society is unimaginable without the use of wireless technologies for information exchange. Wireless data transmission is performed using 3G, 4G, LTE, 5G, Wi-Fi and other technologies. For the functioning of the mentioned technologies, it is necessary to use radio frequencies. A limited frequency band, dependence of data transfer speed on the number of users connected to the network simultaneously, the influence of several sources on each other leads to the need to create new technology. A more perfect technology is Li-Fi (Light Fidelity) technology, in which

the mentioned problems are excluded. Li-Fi technology is based on the use of light energy, using visible or invisible light to wirelessly transmit information, which is emitted by a light-emitting diode, which enables two-way high-speed connection. In the article presents the architecture of the Li-Fi technology system, the advantages and disadvantages of the technology, it's characteristics, and areas of use. Are named the types of cyberthreats in the wireless networks. In any technology, it is important to take appropriate security measures to protect against potential dangers, in order to minimize security risks, Li-Fi technology offers data security and privacy advantages than Wi-Fi. It ensures secure data transmission and reliable network operation. In the paper also given the tools and methods of cybersecurity used in Li-Fi technology.

**KEYWORDS:** Wireless connection, Wi-Fi, Light-emitting diode, LED lighting, Li-Fi, Cyberthreat, Cybersecurity, Encryption.

## 1. შესავალი

ინტერნეტი არის ტექნოლოგია, რომელმაც მთელი მსოფლიო შეცვალა. მსოფლიოში ინტერნეტ ტრაფიკის მოცულობა ყოველწლიურად იზრდება და მოითხოვს საკომუნიკაციო ტექნოლოგიების მუდმივ განვითარებას და ცვლილებას. მონაცემთა გადაცემის მხრივ ალტერნატიული მეთოდების შექმნის საჭიროება დგება, მონაცემთა მაღალი სიჩქარით, საიმედოდ და უსაფრთხოდ გადაცემისთვის. ამჟამად ინოვაციურ ტექნოლოგიას წარმოადგენს Li-Fi ტექნოლოგია, რომელიც მონაცემთა გადასაცემად არა რადიოტალღებს, არამედ სინათლის სხივებს იყენებს. ჩვეულებრივი ნათურისა და უსადენო ინტერნეტის ინტეგრირებით პოტენციურად შესაძლებელია Wi-Fi ტექნოლოგიასთან შედარებით 10-ჯერ მძლავრი და სწრაფი შეერთების მიღწევა (მონაცემების გადაცემა 10 გბიტ/წმ-ზე მეტი პიკური სიჩქარით).

Li-Fi ტექნოლოგია იყენებს ხილული სინათლის ოპტიკურ დიაპაზონს 400 ტერაჰერციდან 800 ტერაჰერცამდე. აღნიშნული სიხშირული დიაპაზონის გამოყენება საშუალებას იძლევა თავიდან იქნას არიდებული სიგნალის სიმძლავრის შემცირება. მარშრუტიზატორის ნაცვლად LED-სინათლის გამომსხივებელი დიოდის (Light Emitting Diode) გამოყენების იდეა პირველად გერმანელ ფიზიკოს ჰარალდ ჰაასს 2011 წელს გაუჩნდა. ექსპერიმენტისას ლაბორატორიულ პირობებში მონაცემთა გადაცემის სიჩქარემ 224 გბიტ/წმ-ს მიაღწია. IEEE-ის (Institute of Electrical and Electronics Engineers-ელექტროტექნიკის და ელექტრონიკის ინჟინერთა ინსტიტუტი) მიერ განსაზღვრული იქნა Li-Fi-ის ტექნოლოგიის - 802.11bb სტანდარტი.

მეცნიერებს მუდმივად უწყვეტ უსადენო ქსელების ორგანიზების ტექნოლოგიების შემუშავება, განვითარება და ტექნოლოგიური ცვლილების განხორციელება, რითაც მომხმარებელს შესთავაზებენ მონაცემთა გადაცემას მაღალი სიჩქარითა და უსაფრთხოდ. Li-Fi ტექნოლოგია სწრაფად ვითარდება და მოსალოდნელია, რომ გახდება სიცოცხლისუნარიანი ფართოზოლოვანი ინტერნეტის წყარო [1].

## 2. Li-Fi სისტემის არქიტექტურა

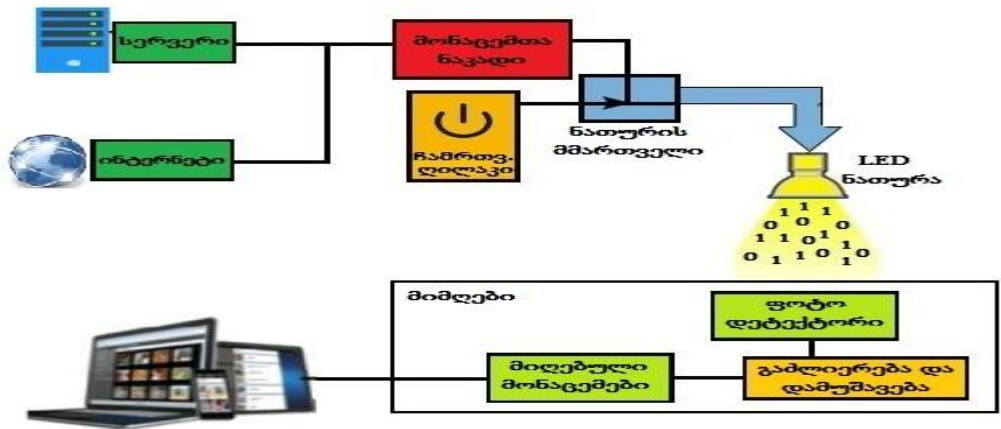
Li-Fi ტექნოლოგია ტელეკომუნიკაციაში შემოვიდა როგორც რევოლუციური ტექნოლოგია სიჩქარის, საიმედოობისა და უსაფრთხოდ შეერთების თვალსაზრისით. მიუხედავად Wi-

Fi-ის ქსელებზე ფართო წვდომის შესაძლებლობისა, მომხმარებლებს უჩნდებათ მოთხოვნილება შეერთების საუკეთესო სტაბილურობის, მონაცემთა კონფიდენციალურობისა და ქსელში ნაკლები არასანქცირებული შეჭრის მხრივ. Li-Fi ტექნოლოგია წარმოადგენს რადიოტალღების საფუძველზე ტრადიციული ქსელების რევოლუციურ ალტერნატივას.

Li-Fi ორმხრივი უსადენო ქსელური ტექნოლოგიაა, რომელიც იყენებს სინათლის ტალღებს მონაცემთა გადასაცემად. Li-Fi სთავაზობს მომხმარებლებს ამაღლებულ სტაბილურობას და უსაფრთხო შეერთებას. გადამცემიდან მიმღებამდე Li-Fi იყენებს უხილავ ან ინფრაწითელ სხივებს მონაცემთა გადასაცემად. ჩვეულებრივი შუქდიოდი ნათურები გადასცემენ ინფორმაციას Li-Fi ქსელით პულსირებადი სინათლის სიგნალების სახით, რაც ქმნის მონაცემთა გადაცემის უსაფრთხო მექანიზმს, ქსელის უფრო დიდი გამტარუნარიანობით.

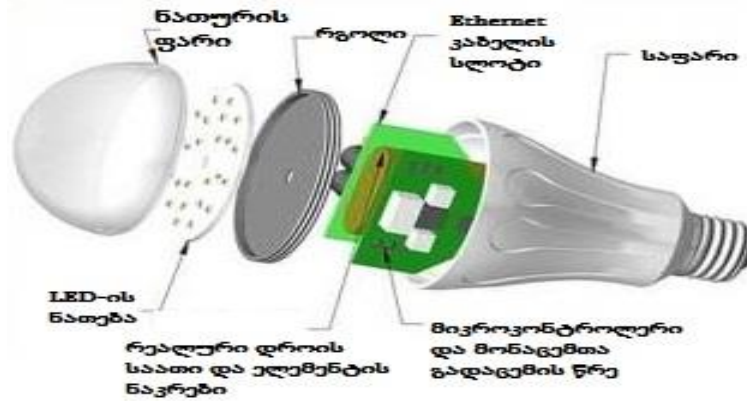
Li-Fi ქსელის არქიტექტურა შედგება გადამცემისა და მიმღებისგან. **გადამცემს** წარმოადგენს - თეთრი სინათლის წყარო - შუქდიოდი – LED ნათურა. **მიმღები** - მგრძობიარე ფოტო სენსორი – ფოტოდეტექტორი, რომელიც აკონტროლებს ნებისმიერ ცვლილებას განათების დონეში (ფიგურა 1).

Li-Fi ტექნოლოგიაში ხდება გადასაცემი მონაცემების გარდაქმნა ორობითი კოდის სახით და გაგზავნა მომხმარებლის მოწყობილობაზე, რისთვისაც გამოიყენება ჩვეულებრივი განათების დიოდური ნათურის (LED) ციმციმი, ხოლო **მიმღები** (ფოტოდეტექტორი) ახდენს სინათლის ამ იმპულსების დეკოდირებას ელექტრულ სიგნალად ანუ კვლავ ინფორმაციად გარდაქმნას ახორციელებს. მომხმარებლებისთვის საერთოდ შეუმჩნეველია ასეთი ციმციმი, რამდენადაც ის ხდება 60 ჰც-ზე მაღალი სიხშირით [2].



ფიგურა 1. Li-Fi (Light Fidelity) ქსელის არქიტექტურა [5]

LED (Light Emitting Diode) ნათურაში სპეციალური ჩიპი გარდაქმნის გადასაცემ ინფორმაციას ორობით კოდში და აგზავნის მომხმარებლის მოწყობილობაზე, რომელიც აღჭურვილია ფოტოდეტექტორით (ფიგურა 2).



ფიგურა 2. LED ნათურის სტრუქტურა [5]

### 3. Li-Fi ტექნოლოგიის უპირატესობები და ნაკლოვანებები

Li-Fi ტექნოლოგიის უპირატესობები:

- რადიოსიხშირული ზოლის არასაკმარისი გამტარუნარიანობის საკითხის გადაწყვეტა, სინათლის სხივების გამოყენების ხარჯზე;
- ქსელის ფუნქციონირება არ საჭიროებს ლიცენზიას;
- მონაცემთა გადაცემის მაღალი სიჩქარე. 10 გბიტ/წმ-ზე მეტი, 100-ჯერ უფრო სწრაფია ვიდრე Wi-Fi;
- ინტერნეტის ჩართვის შესაძლებლობა ყველგან, სადაც სინათლეა. მთელ მსოფლიოში დაახლოებით 19 მილიარდი ნათურა უნდა შეიცვალოს შუქდიოდებით, რომლებიც გადასცემენ მონაცემებს;
- ინფორმაციული უსაფრთხოება - ერთ ერთი მთავარი უპირატესობა, სინათლე არ აღწევს კედლებს მიღმა. მცირე მანძილზე მონაცემთა გადაცემა ქსელში არასანქცირებული შეღწევის საფრთხეს ამცირებს.
- მთელ მსოფლიოში ტექნოლოგიის რეალიზება, ყოველი ქუჩის განათებას გახდის ინტერნეტში უფასო წვდომის წერტილად;
- ელექტრომაგნიტური გამოსხივების არ არსებობის გამო უსაფრთხოება. თვითმფრინავებში, სამედიცინო მოწყობილობებსა და საავადმყოფოებში გამოყენების შესაძლებლობა;
- განათებაზე ენერჯის ეკონომია, ქსელის რეალიზაციის სიმარტივე და დაბალი ღირებულება.

Li-Fi ტექნოლოგიის ნაკლოვანება:

- სინათლის წყაროს გარეშე ქსელის ფუნქციონირება შეუძლებელია; ტექნოლოგია არ მუშაობს ბუნებრივ ან არასტაბილურ განათების პირობებში;
- მონაცემთა გადაცემა შეიძლება განხორციელდეს მხოლოდ პირდაპირი ხედვის საზღვრებში მიმდებსა და გადამცემს შორის;
- ფიზიკური ბარიერების გამო ტექნოლოგიის მუშაობა იზღუდება;
- დაფარვის მანძილი (სიგნალის გავრცელების არე). შეზღუდულია 10-30 მეტრის დიაპაზონში, ეს თვისება ამავედროულად დადებით მხარესაც მიეკუთვნება ინფორმაციის დაცულობის თვალსაზრისით;

- მზის სხივების ზემოქმედებით სტაბილურობის შემცირება, ხელშეშლები, კავშირის წყვეტა;
- ახალი ინფრასტრუქტურის შექმნის აუცილებლობა, რაც დამატებით ხარჯებს მოიცავს. დანერგვის პროცესში მყოფი თანამედროვე Li-Fi-ი ტექნოლოგია Wi-Fi-სთან შედარებით უზრუნველყოფს უფრო სწრაფ, საიმედო და უსაფრთხო შეერთებას. ცხრილი 1. Li-Fi და Wi-Fi ტექნოლოგიის მახასიათებლების შედარება [3-4].

ცხრილი 1. Li-Fi და Wi-Fi ტექნოლოგიის მახასიათებლების შედარება

მახასიათებლები	Li-Fi (Light Fidelity)	Wi-Fi (Wireless Fidelity)
IEEE სტანდარტი	802.11 bb	802.11
სიხშირული დიაპაზონი	380 ნმ-დან 780 ნმ-მდე ტალღის სიგრძის დიაპაზონში 400-800 ტერაჰერცი	2.4 გჰც, 5 გჰც და 6 გჰც
ღირებულება	დაბალი	მაღალი
მონაცემთა გადაცემის საშუალება	ხილული სინათლე	რადიოტალღები
ქსელის ტოპოლოგია	წერტილი-წერტილი	წერტილი-მრავალწერტილი
მონაცემთა გადაცემის სიჩქარე	1-3,5 გბიტ/წმ	2 მგბიტ/წმ-9.6 გბიტ/წმ
დაფარვის მანძილი	10 მ	20-100 მ
უსაფრთხოება	მაღალი	საშუალო
სისტემური კომპონენტები	სინათლის დიოდური ნათურა, დრაივერი, ფოტოდეტექტორი	მარშრუტიზატორი, აბონენტის მოწყობილობა
მუშაობის პრინციპი	მონაცემთა გადაცემა სინათლით, სინათლის დიოდური ნათურით	მონაცემთა გადაცემა რადიოტალღებით Wi-Fi როუტერით
კონფიდენციალობა	მონაცემთა უსაფრთხო გადაცემა	რადიოტალღები აღწევენ კედლებს მიღმა, ამიტომ მონაცემთა უსაფრთხოდ გადაცემა დაბალია
დაყოვნება	მიკროწამი	მილიწამი

#### 4. Li-Fi ტექნოლოგიის გამოყენების სფეროები

ბოლო ათწლეულში Li-Fi უსადენო კავშირის სისტემა გამოყენებული იქნა სხვადასხვა ინდუსტრიაში, როგორც ტრადიციული Wi-Fi-სა და 5G (Generation) შეერთების ალტერნატივა.

Li-Fi-ის გამოყენება შესაძლებელია ისეთ ადგილებში სადაც რადიოსიხშირული კავშირის გამოყენება ვერ ხერხდება:

- წყლის ზედაპირს ქვემოთ განთავსებული სივრცეები - Li-Fi-ის სინათლის სხივი თავისუფლად ვრცელდება წყალქვეშა გარემოში, ამ მოვლენამ შეიძლება შეცვალოს კომუტაციის პროცესი წყალქვეშა მოწყობილობებს შორის.
- უაღრესად საიდუმლო და კონფიდენციალურ ადგილებში (სამხედრო და სამთავრობო). Li-Fi-ის მოქმედების დიაპაზონის სიმცირის გამო შესაძლებელია საიდუმლო ინფორმაციაზე წვდომის შეზღუდვა.



– ნაკლებად განათებულ გარემოში (კარავი) და იმ ადგილებში, სადაც მობილური ტელეფონი არ შეიძლება იქნეს გამოყენებული, მაგალითად, საბრძოლო მარაგების საწყობში.

– საგნების ინტერნეტი IoT (Internet of Things). მონაცემების გადაცემის უფრო მაღალი სიჩქარე დააჩქარებს ინფორმაციის გაცვლას მოწყობილობებს შორის, შესაძლებელი იქნება უფრო მეტი რაოდენობის მოწყობილობის ჩართვა ქსელში და Wi-Fi ქსელის დატვირთვის განტვირთვა. 5G-სთან ერთად და მასიურად გამოყენების შემთხვევაში, შესაძლებელია „ჭკვიანი“ (Smart) მოწყობილობების შექმნა: „ჭკვიანი ქალაქი“, „ჭკვიანი სახლი“.

– ადამიანის ან ქსელში ჩართული ობიექტების ადგილმდებარეობის განსასაზღვრად. ადგილმდებარეობის განსაზღვრის სიზუსტე ძალიან მაღალია და შეადგენს 10-20 სმ-ს.

– სამედიცინო მოწყობილობებში და დაწესებულებებში გამოყენება, რადგან ტექნოლოგიას არ აქვს რადიოტალღებთან კავშირი, ამიტომ მისი გამოყენება შესაძლებელია ისეთ ადგილებში სადაც Bluetooth, IR-პორტის, Wi-Fi ინტერნეტის გამოყენება აკრძალულია, დისტანციური გამოკვლევების, პაციენტის ჯანმრთელობის მდგომარეობის და სასიცოცხლო ნიშნების რეალურ დროში მონიტორინგისა და პროცედურების ჩასატარებლად. საავადმყოფოს დერეფნები, მოსაცდელი ოთახები, პაციენტების პალატები და საოპერაციოები შეიძლება აღიჭურვოს ამ ტიპის ინტერნეტით.

– ჯანდაცვაში ინფორმაციული უსაფრთხოების უზრუნველსაყოფად. Wi-Fi-ისთან შედარებით Li-Fi ტექნოლოგიის დაფარვის რადიუსი რადგან მცირეა, ამიტომ ის უფრო უსაფრთხოა მონაცემთა გადაცემის მხრივ. ეს თვისება შეიძლება ძალიან სასარგებლო იყოს იმ სფეროებში, რომლებშიც ამუშავებენ დიდი რაოდენობით კონფიდენციალურ მონაცემებს.

– გარე განათებებში. უახლოეს მომავალში შესაძლებელი იქნება შუქდიოდების გამოყენება ინფორმაციის გადაცემისთვის ქალაქის ინფრასტრუქტურაში, ქალაქის განათების ქსელში, საავტომობილო გზების ქსელში, ავტონდუსტრიაში – ავტომობილებში და საგზაო ინფრასტრუქტურაში მანქანებს შორის (ავტომობილები აღჭურვილი იქნება შუქდიოდი ფარებით, მანქანებს შესაძლებლობა ექნებათ ერთმანეთთან და შუქნიშანთან „ურთიერთობის“), ქვეითთა გადასასვლელებზე, ობიექტებს შორის, საზოგადოებრივ ტრანსპორტში და მილიონ ობიექტს შორის, რომლებიც ჩართული არიან ქსელში.

– რადიოელექტრონული ხელშეშლების არარსებობის გამო, გადამწყვეტი უპირატესობა ექნება თვითმფრინავის ბორტზე შეღწევის წერტილების შექმნისათვის. Li-Fi-ის გამოყენება ასევე აქტუალურია აეროპორტებში.

– ვირტუალური რეალობა VR (Virtual reality). Li-Fi-ის გამოყენებით მონაცემთა გადაცემის მაღალი სიჩქარე, შემცირებული დაყოვნება, ჩართვის სტაბილურობა და კონფიდენციალურობა შესაძლებელს გახდის VR დამატებების ამოცანები შეუფერხებლად შესრულებას [6-7].

## 5. კიბერსაფრთხეები უსადენო კავშირში

უსადენო ქსელები ხშირად გამოიყენება საიმედო ინტერნეტ-შეერთების უზრუნველსაყოფად, მაგრამ ასეთმა ქსელმა შესაძლოა მომხმარებელს გარკვეული კიბერსაფრთხე შეუქმნას. ქსელის გატეხვამ და სხვა უსაფრთხოების დარღვევებმა შეიძლება კონფიდენციალურობის მთლიანობა და მონაცემთა გადაცემის მთლიანი სისტემის

რეპუტაცია დააყენოს საფრთხის ქვეშ. უსადენო კავშირის ქსელების კონფიდენციალობას შეიძლება საფრთხე შეუქმნას შემდეგმა ძირითადმა შეტევებმა:

### **მოსმენა**

მოსმენის შეტევა იყენებს დაუცველ ქსელს მოწყობილობებს შორის გადასაცემი მონაცემების უნებართვოდ წვდომის მოსაპოვებლად. უსადენო საკომუნიკაციო სისტემებში ბოროტმოქმედებმა შეიძლება მიითვისონ კონფიდენციალური ინფორმაცია, როგორცაა პაროლი, ელექტრონული წერილები, პირადი მონაცემები. ჰაკერებს შეუძლიათ წაშალონ ან შეცვალონ ქსელური მონაცემები, მას შემდეგ რაც აღმოაჩინენ ქსელურ დარღვევებს.

### **შეტევა „ადამიანი შუაში“ (Man in the Middle Attack-MitM)**

კიბერდამნაშავე ორ მხარეს შორის ერთგვარ კავშირში, რაც შეუმჩნეველია მხარეებისთვის, აკონტროლებს კავშირს, ახდენს მონაცემების მოდიფიკაციას, ცვლის ადრესატს, ქურდობს.

### **თაღლითური შეღწევის წერტილები**

თაღლითური შეღწევის წერტილები - უსადენო შეღწევის წერტილები, რომელიც შეიძლება სისტემაში მოეწყოს ქსელის ადმინისტრატორის ნებართვის გარეშე. ასეთმა შეღწევის წერტილებმა მოტყუებით შეიძლება მომხმარებლები მიუერთოს ქსელს და მათი მონაცემები დაექვემდებაროს მრავალ კიბერუსაფრთხოების რისკებს. თაღლითური შეღწევის წერტილების აღმოჩენა და მართვა მნიშვნელოვანია უსადენო კავშირის ქსელის საერთო უსაფრთხოების მხარდასაჭერად.

### **მავნე პროგრამული უზრუნველყოფის გავრცელება**

მავნე პროგრამული უზრუნველყოფის გავრცელება დანიშნულია პროგრამირებადი მოწყობილობის ან ქსელის მანიპულირებისა და დაზიანებისთვის. კიბერდამნაშავეებს შეუძლიათ შეაღწიონ მონაცემთა გადაცემის უსადენო არხში, ჩანერგონ მავნე პროგრამული უზრუნველყოფა მომხმარებლის მოწყობილობაში ან კავშირის ქსელში. დაყენებულ მავნე პროგრამულ უზრუნველყოფას შეუძლია მოწყობილობის ფუნქციონირების მოშლა, მომხმარებლის მონაცემების მოპარვა და შემდგომი შეტევების განხორციელება.

### **სუსტი შიფრაცია**

კიბერდამნაშავეებმა შეიძლება გამოიყენონ უსაფრთხოების სუსტად დაშიფრული ალგორითმები დეკოდირებისა და პირად მონაცემებში შეღწევისათვის. ცუდათ პროექტირებულმა კრიპტოგრაფულმა ალგორითმებმა შეიძლება გამოიწვიოს კონფიდენციალური მონაცემების მოპარვა, აუტენტიფიკაციის დარღვევა და „სპუფინგ“ შეტევები. ბოროტმოქმედები ცდილობენ გვერდი აუარონ დაცულ შიფრირების გასაღებს, იყენებენ კრიპტოგრაფიაში სისუსტეებს და გასაღებების მართვის ცუდ მეთოდებს. რასაც მიყვავართ კონფიდენციალობის სერიოზულ ზიანთან და უსადენო ქსელში კონფიდენციალური მონაცემების მთლიანობის დარღვევასთან.

### **განმეორებითი შეტევები**

შეტევა განმეორებით - შეტევა უსადენო ქსელზე, როდესაც ჰაკერი წყვეტს კავშირს ორ მხარეს შორის, რათა დააყოვნოს, მიმართულება შეუცვალოს ან გააყალბოს მათი მონაცემები. მონაცემთა გადაცემის ნამდვილი არხები წყდება და მიმართულებას იცვლის, რათა მოატყუოს მიმღები და აიძულოს შეასრულოს არასანქცირებული მოქმედებები. რაც იწვევს კონფიდენციალურობის დარღვევას და ქსელში მონაცემთა ტრაფიკს ხდის დაუცველს მესამე პირისთვის.

## 6. Li-Fi-ში უსაფრთხოების უზრუნველყოფისთვის კიბერუსაფრთხოების ჩაშენებული ფუნქციები

Li-Fi ტექნოლოგია მხოლოდ ოპტიკურ სიგნალს იყენებს მონაცემთა გადასაცემად. შესაბამისად Li-Fi სიგნალების გავრცელებაზე გარშემოში არსებულ სხვა კავშირის ქსელების რადიოტალღებს არ გააჩნიათ მასზე გავლენა. ეს ამაღლებს შეერთების სტაბილურობას მჭიდრო გარემოში.

Li-Fi ტექნოლოგია უზრუნველყოფს უსაფრთხოების იდეალურ გადაწყვეტას თანამედროვე მომხმარებლებისათვის, რომლებიც უპირატესობას ანიჭებენ ქსელის სტაბილურობასა და სიჩქარეს, გაუმჯობესებული კონფიდენციალურობით. Li-Fi-ის მომხმარებლები დაცული არიან კიბერუსაფრთხისგან შემდეგი უსაფრთხოების ფუნქციებით:

### ფიზიკური უსაფრთხოება

სინათლის ტალღების თვისებებიდან გამომდინარე Li-Fi ქსელი წინასწარ შეზღუდულია განსაზღვრული დაფარვის ზონით, რამდენადაც სინათლის სიგნალს არ შეუძლია გააღწიოს გაუმჭირვალე ობიექტებში, როგორც კედელი. მოწყობილობა, რომელიც მდებარეობს Li-Fi ქსელის დაფარვის ფიზიკური დიაპაზონის საზღვრებს გარეთ, არ შეუძლიათ მიიღოს ქსელთან წვდომის შესაძლებლობა. არავტორიზებული მოწყობილობა Li-Fi ქსელის დაფარვის ზონის საზღვრებში ვერ შეძლებს სიგნალის მითვისებას. Li-Fi ქსელით კავშირის არხების შექმნა კი შესაძლებელია მხოლოდ პირდაპირი ხედვის საზღვრებში კონკრეტული შერჩეული მოწყობილობებისთვის. Li-Fi სისტემის შიგნით გადასაცემი მონაცემების დაცულობის ფუნქცია მოიცავს პაროლით დაცვას, ჟურნალების მართვას და მონაცემთა დაშიფრვას.

### მინიმალური ჩარევა

უმეტესობა ჩვეულებრივი ქსელები იყენებს რადიოტალღებს კავშირისათვის, მათი სიგნალები არ უშლიან ხელს Li-Fi-ის საფუძველზე არსებულ შეერთებებს. Li-Fi მომხმარებლები იღებენ სტაბილურ და უწყვეტ შეერთებას მჭიდროდ განთავსებული მოწყობილობების შემთხვევაში ან გადატვირთულ გარემოშიც კი. Li-Fi შეერთება გარე ქსელებისა და მოწყობილობების ხელშეშლებისადმი მდგრადია, რაც საშუალებას იძლევა უაღრესად უსაფრთხოდ გადაიცეს მონაცემები სხვადასხვა სფეროებში, როგორცაა თავდაცვა, სამთავრობო უწყება, ფინანსური ორგანიზაციები და კოსმოსის გამოკვლევა.

### ქსელური უსაფრთხოების სხვა პროტოკოლებთან ინტეგრაცია

Li-Fi ფიზიკური უსაფრთხოების თვისებას დამატებული ორმაგი კონფიდენციალურობის დონე, მონაცემთა შიფრირების, გასაღებების უსაფრთხო განაწილება, ჟურნალების მართვის გაფართოებული პროცესები და ქსელის მონიტორინგის საიმედო სტრუქტურის გაერთიანებით რეალურ დროში.

## 7. კიბერუსაფრთხოების არსებულ საშუალებებთან Li-Fi-ის უსაფრთხოების ინტეგრაცია

უკვე არსებულ კიბერუსაფრთხოების საშუალებებთან Li-Fi-ის უსაფრთხოების ინტეგრაცია გააუმჯობესებს მონაცემთა დაცვასა და ქსელის კონფიდენციალურობას, უზრუნველყოფს მუდმივ უსაფრთხოებას შენახული და გადასაცემი მონაცემებისას. სხვა კიბერ

უსაფრთხოების პროტოკოლებთან Li-Fi-ის ინტეგრაციის რამდენიმე ძირითადი მეთოდები არსებობს:

### **კიბერ უსაფრთხოების არსებულ ინსტრუმენტებთან თავსებადობა**

Li-Fi მოწყობილობები შექმნილი უნდა იყოს უკვე არსებულ უსაფრთხოების პროტოკოლებთან ინტეგრაციისთვის, როგორცაა შედარებით კონტროლი 802.1X, შიფრირება AES (Advanced Encryption Standard) ან TLS (Transport Layer Security) და სხვა პროგრამული უზრუნველყოფა, რათა მოემსახუროს გასაღებების ჟურნალს. Li-Fi-ის მრავალ სისტემაში შესაძლებელია API (Application Programming Interface) კიბერუსაფრთხოების არსებულ პლათფორმის ინტეგრაცია, რათა უზრუნველყოფილი იქნეს კავშირის უწყვეტი მთლიანობა და დაცულობა.

### **ორმხრივი შიფრირება**

შიფრირების პროტოკოლები DES, RSA, Twofish და CR4 შეიძლება გამოყენებული იქნეს მონაცემთა კონფიდენციალობის საიმედოობის უზრუნველსაყოფად, რომელიც გადაიცემა უსადენო ქსელებით. Li-Fi ქსელისთვის აერთიანებენ სხვადასხვა შიფრირების ალგორითმებს ინდივიდუალური უსაფრთხოების შესაქმნელად.

### **შედარებით კონტროლი ბრანდმაუერის გამოყენებით**

ბრანდმაუერის და VLAN (Virtual LAN) გამოყენება შესაძლებელია სისტემის შედარებით კონტროლის შესაქმნელად, რომლებიც არეგულირებენ მონაცემთა გადაცემას და ქსელში ტრაფიკის ნაკადს. უსაფრთხოების ეს პროტოკოლები შეიძლება ინტეგრირებული იქნეს პროგრამულ უზრუნველყოფასთან, Li-Fi-ში ჩართვის არხების სეგმენტაციისთვის მონაცემთა სამართავად. ბრანდმაუერი მოქმედებს, როგორც შედარებით კონტროლის მცველი, რომელიც თვალყურს ადევნებს სისტემაში შემოსულ და გამავალ ტრაფიკს უსაფრთხოების წინასწარგანსაზღვრული წესების საფუძველზე.

### **უსაფრთხოების აუდიტის ჩატარება**

ქსელური აუდიტი - ტესტების სერიაა, სისტემის დაუცველობის, შედარებით სუსტი წერტილების და პროგრამული უზრუნველყოფის ცუდი კონფიგურაციის აღმოსაჩენად. Li-Fi ჩართვისას უნდა განხორციელდეს უსაფრთხოების რეგულარული შემოწმება სისტემური ხარვეზების აღმოსაჩენად და გამოსასწორებლად, იქამდე სანამ ამით ისარგებლებენ კიბერდამნაშავენი. უსაფრთხოების კომპლექსური შემოწმება და ტესტები შედარებითადობაზე გამოიყენება, სისტემაში მონაცემების გადაცემის პოტენციური დაუცველობის გამოსავლენად. სწრაფი აღმოჩენა და ოპერატიული გამოსწორება მნიშვნელოვანია ოპტიმალური კონფიდენციალურობისა და ქსელის მთლიანობის შესანარჩუნებლად.

## **8. Li-Fi-ის უსაფრთხოების სფეროში სამომავლო ტენდენციები და კიბერუსაფრთხოება**

უახლოეს წლებში Li-Fi ტექნოლოგიის სამომავლოდ უსაფრთხოების ძირითადი ტენდენციები იქნება:

### **გაფართოებული შიფრირება**

მომხმარებლის ქსელის უკეთესი დაცვისათვის ორმხრივი შიფრირების მეთოდებია საჭირო. კვანტური კრიპტოგრაფიის და შიფრირების მეთოდების ინტეგრაცია იძლევა გაფართოებული პროტოკოლების შექმნის შესაძლებლობას ქსელური

უსაფრთხოებისთვის. მანქანური სწავლების ტექნოლოგია შეიძლება გამოყენებული იქნეს უსაფრთხოების სისტემურ-სპეციფიკური ალგორითმების შემუშავებისთვის, რომელსაც შეუძლია ადაპტირდეს კიბერუსაფრთხოების საფრთხეების მიმართ დროის რეალურ რეჟიმში.

### **ქსელების დაცვა უფრო მკაცრი აუტენტიფიკაციის მეთოდების გამოყენებით**

Li-Fi ქსელში აუტენტიფიკაციის საიმედო მექანიზმების ინტეგრაცია აამაღლებს უსაფრთხოებას ინტერნეტ-მომხმარებლებისთვის. აუტენტიფიკაციის მეთოდები, როგორცაა საიმედო პაროლები, ბიომეტრია და თითის ანაბეჭდის ამოცნობა იქნება დამატებითი ფუნქცია Li-Fi ტექნოლოგიის უსაფრთხოების. იგეგმება ბლოკჩეინ ტექნოლოგიის გამოყენება და მომხმარებლების ჟურნალის დანერგვა ქსელში წვდომის მართვისთვის.

### **საგნების ინტერნეტის უსაფრთხოებასთან ინტეგრაცია**

IoT (Internet of Things) საგნების ინტერნეტის გავრცელება ახალ ერას იწყებს, გაუმჯობესებული კავშირი მოითხოვს უფრო მაღალ უსაფრთხოებას. Li-Fi-ინტერნეტის განვითარება IoT მოწყობილობების ჩართვის შესაძლებლობას იძლევა. მთელი სისტემის კონფიდენციალურობა დამოკიდებულია ქსელურ უსაფრთხოებაზე, რომელსაც Li-Fi ტექნოლოგია გვთავაზობს. საჭიროა უსაფრთხოების კომპლექსური გადაწყვეტები, რომელიც შეამცირებს მონაცემების გაჟონვის რისკს IoT სისტემებში [8].

## **9. დასკვნა**

Li-Fi გამოირჩევა გარკვეული დადებითი თვისებებით, მაგრამ მიუხედავად წარმოუდგენელი სიჩქარისა და გაზრდილი უსაფრთხოებისა, ახალი ტექნოლოგია Wi-Fi ტექნოლოგიას ვერ ჩაანაცვლებს. ის კარგი დამხმარე იქნება გლობალური საკომუნიკაციო ქსელების განვითარებაში. Li-Fi გამოყენებადი გახდება უახლოეს მომავალში იქ სადაც Wi-Fi-ის გამოყენება შეუძლებელია, პირველ რიგში ინდუსტრიაში და მედიცინაში. მომხმარებლებს შეეძლება ისარგებლონ უფრო სწრაფი ინტერნეტით შიგა სივრცეში, ხოლო გარე სივრცეში ისარგებლებენ Wi-Fi-ით და 5G-მობილური სწრაფი ინტერნეტით.

მომავალში Li-Fi და Wi-Fi შეძლებს გახდეს ერთიანი ჰიბრიდული უსადენო საკომუნიკაციო სისტემის ნაწილი, სადაც Li-Fi-ი მხოლოდ მოკლე მანძილზე იქნება პასუხისმგებელი მონაცემთა სწრაფ გადაცემაზე, იქ სადაც რადიოტალღები ვერ აღწევს.

ეს ახალი ტექნოლოგია შეიძლება გახდეს უახლოეს მომავალში ყველაზე ეკოლოგიური და ეკონომიური ინფორმაციის გადაცემის საშუალება, სტაციონალური აბონენტისთვის, შენობაში ადგილობრივი კავშირისთვის.

Li-Fi ტექნოლოგიის განვითარებასთან ერთად საჭიროა ინტეგრაცია უკვე არსებულ საკომუნიკაციო ტექნოლოგიებთან მომხმარებელთა მოთხოვნილებების დასაკმაყოფილებლად, ასევე აუცილებელია უსაფრთხოების პროტოკოლების შესაბამისი გათვლები, რომელიც იცავს ინტერნეტის მომხმარებელს კიბერდანაშაულისგან. მსხვილი საწარმოები, დაწესებულებები და კერძო პირები უფრო მეტად იყენებენ ინტერნეტს მაღალპრიორიტეტული ფუნქციებისა და ტრანზაქციების შესასრულებლად. ინტერნეტ ქსელით გადასაცემი მონაცემები ექვემდებარება მოპარვას, მითვისებასა და შეტევებს. Li-Fi ინტერნეტი შექმნილია იმისათვის, რომ მომხმარებელს შესთავაზოს უსაფრთხო ქსელი და ამაღლებული კონფიდენციალურობა. Li-Fi პროდუქტები აერთიანებენ სინათლის სიგნალების შიდა უსაფრთხოებას კიბერუსაფრთხოების თანამედროვე მეთოდებთან ერთად, რომ შეიქმნას მომხმარებლებისათვის საიმედო მონაცემების დაცვის სტრუქტურა.

ბიბლიოგრაფია

1. Biswas B., Nakhale A., Roshan Sinha A., Lighting up data: the future of wireless data transfer with Li-Fi technology, Telecommunications and Radio Engineering. 2024.
2. Gorozheev M., Pirogov R., Prospects for of Li-Fi Technology in the aspect of ensuring information security, A collection of scientific articles, 2023, 1, p.740-746.
3. Sharma A.K., Agarwal A., Changder S., Kumar A., Bhutiani M., Singh Ch.Sh., Bibar S., Singh A.K., Roy A., Dey A. Data Transfer Using Li-Fi. International Journal of Innovative Research in Physics. 2023. T. 4. № 4. p. 22-24.
4. Shavgulidze S., Ugrelidze N., Wi-Fi: Modern Standards and Development Trends (1st ed.). Georgia, ComCom, 2021, p.160.
5. URL: <https://shorturl.at/ofLKa> (18.11.2024)
6. Ahmad R., Soltani M. D., Safari M., Srivastava A., and Das A., Reinforcement learning based load balancing for hybrid Li-Fi Wi-Fi networks, IEEE Access, 2020, 8, p.132273–132284.
7. Siddique I., Awan Z., Yousaf Khan M., Mazhar A., Li-Fi the Next Generation of Wireless Communication through Visible Light Communication (VLC) Technology, International Journal of Scientific Researc in Computer Science, Engineering and Information Technology, 2019, 5, no 1, p.30-37.
8. URL: <https://shorturl.at/GJ1yE> (18.11.2024)

## OVERVIEW OF RESEARCH TRENDS AND CHALLENGES IN 6G MOBILE NETWORKS AND THE COMPUTING CONTINUUM

Stojan Kitanov<sup>1</sup>, Dragi Kimovski<sup>2</sup>, Fisnik Doko<sup>1</sup>, Kurt Horvath<sup>2</sup>, Shpresa Tuda<sup>1</sup>, Blerta Idrizi<sup>1</sup>

<sup>1</sup> Mother Teresa University, Faculty of Information Sciences, Skopje, Republic of North Macedonia

<sup>2</sup> Alpen Adria University of Klagenfurt, Department of Information Technology, Klagenfurt, Republic of Austria

**ABSTRACT:** The rapid proliferation of IoT devices, coupled with the generated exponential growth of data, has necessitated the development of advanced network architectures. As a result, 5G mobile networks have already begun to face challenges such as network congestion, latency, and scalability limitations. Therefore, the need for a robust and future-proof solution becomes increasingly evident. In this direction, many research initiatives and industrial communities started to work on the development of 6G mobile networks. On the other hand, the emerging concept of Computing Continuum encompasses the seamless integration of edge, fog, and cloud computing resources to provide a unified and distributed computing environment, and it aims to enable real-time data processing, low-latency response, and intelligent decision-making at the network edge. The primary objective of this research paper is to address the shortcomings of existing network infrastructures and to overcome these shortcomings by integrating advanced AI capabilities in 6G mobile networks with the Computing Continuum. Moreover, it would be proposed a Computing Continuum Middleware for Artificial Intelligence over 6G networks, which would offer high-level and well-defined (“standardized”) interfaces which would create an automated, sustainable loop for managing IoT applications utilizing AI approaches over 6G networks.

**KEYWORDS:** *AI (Artificial Intelligence), Cloud Computing, Computing Continuum, Distributed AI, Fog Computing, Mobile Edge Computing, 5G, B5G, 6G.*

### 1. INTRODUCTION

Recently we have witnessed a significant increase in the use of distributed network-sensitive applications following the industrial revolution of Artificial Intelligence (AI) and the Internet of Things (IoT) (Rashid, Adib Bin, and Md Ashfakul Karim Kausik, 2024 & Seng, Kah Phooi, Li Minn Ang, and Ericmoore Ngharamike, 2022). An important pillar in this revolution represents the evolution in mobile network technologies across five generations, roughly ten years long each: 1G in the 1980s (analog voice), 2G in the 1990s (digital voice), 3G in the 2000s (mobile data), 4G LTE-A, and WiMAX 802.16 in the 2010s (mobile broadband internet), and finally reaching 5G in the 2020s (ultra-low latency, mm-waves, gigabit throughput), to be extended to 6G (blockchain and terahertz bandwidth) by the end of this decade (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023).

Currently, multiple innovative applications that rely on artificial intelligence approaches (e.g., smart city, virtual reality, robotics, swarms) exploit the radio communication improvements and architectural changes in the edge and core networks. Such distributed applications attract mobile participants who connect through smartphones, virtual reality glasses, drones, robots, or any special IoT end device. Processing these interactions in real-time and meeting the requirements of the utilized AI algorithms is essential for their wider integration into our daily lives and for ensuring a responsive and fluent user experience.

The traditional solution to this problem is to offload the workload (i.e., AI model training) to a Cloud data center offering high-performance computing and storage capabilities (Choudhury, Alok, Manojit Ghose, Akhirlul Islam, and None Yogita, 2024 & Hao, Tianshu, Jianfeng Zhan, Kai Hwang, Wanling Gao, and Xu Wen, 2021). Unfortunately, the latencies required to reach remote Cloud data centers are

often unacceptably high, although the 5G technology promises to keep the user latency between 1 and 4 ms for ultra-reliable low latency communications (URLLC) and enhanced mobile broadband (eMBB) network slices.

Therefore, many industrial and research initiatives started to focus on next 6<sup>th</sup> generation of mobile networks, or simply 6G (Letaief, Khaled B., Wei Chen, Yuanming Shi, Jun Zhang, and Ying-Jun Angela Zhang, 2019 & Saad, Walid, Mehdi Bennis, and Mingzhe Chen, 2019 & Tariq, Faisal, Muhammad R. A. Khandaker, Kai-Kit Wong, Muhammad A. Imran, Mehdi Bennis, and Merouane Debbah, 2020). The main driving force in designing and optimizing 6G architectures, protocols, and operations is Distributed Artificial Intelligence in the core, radio access, and the network edge, which would provide support of ubiquitous and mobiquitous smart services from the core to the end devices of the network, which would exceed the mobile data traffic used today. It is expected that AI would transform the wireless evolution of future Internet of Everything (IoE) from “connected things or objects” to “connected intelligence.”

Moreover, despite the scarcity of networking technologies that support modern IoT applications, the provisioning of low-end wireless Edge and high-end Cloud resources to the use case applications is still a tedious and time-consuming manual process.

Therefore, recently, efforts have been made to consolidate these resources across a unified cloud and edge ecosystem, named Computing Continuum, that brings the Cloud services closer to the end users. The Computing Continuum encompasses the seamless integration of edge, fog, and cloud computing resources to provide a unified and distributed computing environment, and it aims to enable real-time data processing, low-latency response, and intelligent decision-making at the network edge (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023 & Tarneberg, William, Emma Fitzgerald, Monowar Bhuyan, Paul Townend, Karl-Erik Arzen, Per-Olov Ostberg, Erik Elmroth, Johan Eker, Fredrik Tufvesson, and Maria Kihl, 2022). For example, smart city IoT applications require clear differentiation between latency-critical tasks, such as AI-based routing of cars or pedestrians, and latency-permissive tasks, like localization of free, or occupied parking spaces. Furthermore, moving critical workloads onto edge devices (e.g., single-board computers, smartphones, routers) enables important data preprocessing, which reduces the traffic on the radio interface.

Therefore, without advanced middleware services offering high-level and well-defined (“standardized”) interfaces, every IoT application provider must design and deploy its own ad-hoc solutions to such problems. This makes the entire research and development effort in 5G and 6G technologies fragmented, often redundant, inefficient, and costly. Obviously, such manual and isolated approaches without integrated IoT application modelling and automated service orchestration do not scale with the long-term vision of millions of interconnected IoT devices relying on distributed AI approaches.

The primary objective of this research paper is to address the shortcomings of existing network infrastructures and to overcome these shortcomings by integrating advanced AI capabilities in 6G mobile networks with the Computing Continuum. It is organized in the following. Section 2 provides an overview of 6G Mobile Networks and its features. Section 3 explains the meaning and the importance of the Computing Continuum. Section 4 provides an explanation about our proposed Computing Continuum Middleware for Artificial Intelligence over 6G networks, which would offer high-level and well-defined (“standardized”) interfaces which would create an automated, sustainable loop for managing IoT applications utilizing AI approaches over 6G networks. Finally, Section 5 concludes the paper and provides directions for future research.

## **2. OVERVIEW OF 6G MOBILE NETWORKS**

The 2030 UN Agenda for sustainable development goals, adopted by all UN members in 2015, contains a set of 17 objectives for “shared blueprint for peace and prosperity for the people and the planet,” which should be accomplished by 2030 (“Transforming Our World: The 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs.”). The rapid advancements of mobile networks may play a major role in fulfilling these sustainable development goals. The deployment of 5G mobile networks have marked the beginning of a true digital society, and have achieved significant



improvements in terms of latency, data rates, spectral efficiency, mobility and number of connected smart mobile devices (Jiang, Dajie, and Guangyi Liu, 2016 & Kitanov, Stojan, Edmundo Monteiro, and Toni Janevski, 2016).

However, the rapid development of artificial intelligence (AI), virtual reality (VR), three-dimensional (3D) media, and the internet of everything (IoE), has led to an exponential traffic growth and a massive volume of traffic. The growth of the global mobile traffic according to ITU predictions in 2030 is predicted to be around 5000 EB/month (“Report ITU-R M.2370-0.” IMT Traffic Estimates for the Years 2020 to 2030, 2015).

As a result, 5G network would not be able to cope with these rapid increased demands of data traffic (Nawaz, Syed Junaid, Shree Krishna Sharma, Shurjeel Wyne, Mohammad N. Patwary, and Md. Asaduzzaman, 2019). For example, the holographic communication would require a data rate up to terabits per second (Tb/s), which is three times higher than the 5G’s data rate and massive low latency (hundreds of microseconds), which is three time less than 5G’s latency (Clemm, Alexander, Maria Torres Vega, Hemanth Kumar Ravuri, Tim Wauters, and Filip De Turck, 2020 & Du, Jun, Chunxiao Jiang, Jian Wang, Yong Ren, and Merouane Debbah, 2020 & Strinati, Emilio Calvanese, Sergio Barbarossa, Jose Luis Gonzalez-Jimenez, Dimitri Ktenas, Nicolas Cassiau, Luc Maret, and Cedric Dehos, 2019). In addition, due to the rapid deployment of Internet of Things (IoT) and future Internet of Everything (IoE) devices, it would be necessary to enhance the connection density and coverage of 5G enabled IoT networks (Tang, Fengxiao, Yuichi Kawamoto, Nei Kato, and Jiajia Liu, 2019 & Zhang, Shangwei, Jiajia Liu, Hongzhi Guo, Mingping Qi, and Nei Kato, 2020). Moreover, the new emerging services of Internet of Everything (IoE) such as extended reality (XR), telemedicine systems, mind-machine interface (MMI), and flying cars would demand very high transmission rates, high reliability, and low latency, which significantly surpass the original goals of 5G networks (Huang, Yakun, Boyuan Bai, Yuanwei Zhu, Xiuquan Qiao, Xiang Su, Lei Yang, and Ping Zhang, 2023 & Khan, Latif U., Ibrar Yaqoob, Muhammad Imran, Zhu Han, and Choong Seon Hong, 2020). In addition, the future mobile networks are expected to be ultra-large-scale, highly dynamic, and incredibly complex system, where the manual optimization and configuration tasks used in the existing mobile networks would be no longer suitable for the next generation mobile networks (Zhang, Shangwei, Jiajia Liu, Hongzhi Guo, Mingping Qi, and Nei Kato, 2020). As a result, 5G networks have already begun to face challenges such as network congestion, latency, and scalability limitations.

*Table.1. Description of the table*

<b>KPI</b>	<b>5G</b>	<b>6G</b>
<b>Traffic Capacity</b>	10 Mbps/m <sup>2</sup>	~ 1-10 Gbps/m <sup>3</sup>
<b>Peak Data rate of the device</b>	10 to 20 Gbps	1 Tbps
<b>End-to-End Latency</b>	5 - 10 ms	10 - 100 μs
<b>Uniform user experience</b>	50 Mbps 2D everywhere	10 Gbps 3D everywhere
<b>Localization precision</b>	10 cm on 2D	1 cm on 3D
<b>Mobility</b>	500 km/h	Up to 1000 km/h
<b>Application Types</b>	eMBB, URLLC, mMTC	mBRLLC, mURLLC, meMBB
<b>Spectral Efficiency</b>	30 bps/Hz	100 bps/Hz
<b>Energy Efficiency</b>	1x	10 - 100x of 5G
<b>Processing Delay</b>	100 up to 50ns	10ns
<b>Frequency Bands</b>	Sub-6 GHz; MmWave for fixed access at 26 GHz and 28 GHz.	Sub-6 GHz; MmWave for mobile access; THz band above 300 GHz; Non RF

Therefore, the need for a robust and future-proof solution becomes increasingly evident. At the moment the main network infrastructure problem is that currently exists no cloud data center, with a dedicated

connection to a telecommunication network offering sufficiently low latency and high throughput to support the execution of novel low-latency AI-based IoT applications and bring us into the 6G era by the beginning of the next decade.

As a result, sixth generation (6G) networks have been proposed as a way to enhance the 5G solutions (Kitanov, Stojan, Petrov, Ivan and Toni Janevski, 2021). Moreover, their potential is claimed to facilitate further development of smart IoT solutions. In this direction machine learning (ML) and generally Artificial Intelligence (AI) are becoming necessity for further expansion of the beyond 5G mobile world.

A comparison between 5G and 6G network is given in Table 1. It can be noticed that all parameters such as traffic capacity, data rate, end-to-end delay, processing delay, spectral and energy efficiency, etc. are improved several times over the value provided by 5G.

6G network should provide support for greater number of massive machine type connected devices, than 5G network. In that direction 6G should provide scalability, efficient connectivity with connectivity and reliability, coverage improvement, as well as, QoS and QoE provisioning. In order to manage such complex network, artificial intelligence (AI) with machine learning (ML) techniques are used to support the network autonomy, as well as, to get a knowledge of the surrounding environment in with 6G network would operate. 6G network would possess self-healing, self-organization, self-reconfiguration, self-optimization, self-aggregation, and self-protection capabilities.

6G network and 6G devices would require much higher energy consumption than 5G, increased by a factor of 1000 or even 10000, since they would operate on terahertz frequency bands (from 0.1 THz to 10 THz), and they would should provide support of a very high traffic capacity (10 Gbps/m<sup>3</sup>), and ultra large number of ubiquitous connected wireless nodes. Therefore, 6G network should have improved energy efficiency than 5G network.

With the technological innovations such as artificial intelligence, augmented reality, virtual reality, and holographic telepresence, 6G would offer many new possibilities in the e-health, since it would provide very high reliability (99,99999 %), very high precision, and very ultra-low latency, less than 1 ms (Shahraki, Amin, Mahmoud Abbasi, Md. Jalil Piran, and Amir Taherkordi, 2021).

New services such as would be introduced in 6G. In addition, 6G network should require higher frequency bands in the terahertz spectrum, i.e., millimeter waves. In addition, a very high and opportunistic data rate is required to support new emerging applications, such as immersive multimedia. Also, 6G network would require much end-to-end delay of less than 1 millisecond, in order to support some 6G services such as augmented reality, and telepresence. Furthermore, 6G network must require too high reliability, in order to enable mission and safety-critical applications.

As it is already known, there are 3 main key services introduced by 5G: Enhanced Mobile Broadband (eMBB), massive Machine Type Communication (mMTC) and Ultra-Reliable Low-Latency Communication (URLLC) (Shahraki, Amin, Mahmoud Abbasi, Md. Jalil Piran, and Amir Taherkordi, 2021). In 6G network, all services would require low latency, high reliability, high data rate, massive connectivity, and full mobility. Therefore, the following potential 6G services could be: massive URLLC (mURLLC), enhanced mobile broadband URLLC (eURLLC), and massive eMBB (meMBB). The mURLLC is the 5G URLLC service type increased to a massive scale, and combines the URLLC with mMTC (mMTC + URLLC). One potential application in this class could be autonomous intelligent driving. The eURLLC service combines both eMBB and URLLC classes (eMBB + URLLC). AR, VR and holographic meetings are some of the applications that fit into this service type. The meMBB service type combines the mMTC and eMBB types (mMTC + eMBB). The tactile Internet fits into this class which would be used to improve the operations and functions in industrial IoT devices (IIoT) in Industry 4.0.

6G network would provide many new use cases, which cannot be completely supported by 5G (Clemm, Alexander, Maria Torres Vega, Hemanth Kumar Ravuri, Tim Wauters, and Filip De Turck, 2020). Some of them are holographic telepresence, industrial automation (industry 4.0 transform), e-health, tactile internet, augmented, and virtual reality.

An overview of the 6G network architecture together with the artificial intelligence is given on Fig. 1. Artificial intelligence together with Machine Learning (ML) is introduced at any horizontal or vertical level, at all TCP/IP layers, at any slice configuration and cloud-based network resource (edge computing) (Kitanov, Stojan, and Vladimir Nikolikj, 2022).

The 6G network design would introduce descriptive, diagnostic, predictive and prescriptive AI data analytics (Balali, Farhad, Jessie Nouri, Adel Nasiri, and Tian Zhao, 2020 & Kibria, Mirza Golam, Kien Nguyen, Gabriel Porto Villardi, Ou Zhao, Kentaro Ishizu, and Fumihide Kojima, 2018). The network analytics would analyze the collected historical data in order to get insights of the network status especially of the physical, data link, network and transport layer. Artificial intelligence (AI) together machine learning (ML) techniques are used for network autonomy, as well as, to get a knowledge of the surrounding environment in which 6G network would operate. AI would provide network status and utilization opportunities. Work data which is obtained as an output of the network analytics processes would be used by Core data analytics for detecting and predicting the network anomalies in order to improve reliability and security of the network. The obtained data would be used to detect future faults based at historical and current information and network behavior. Predictive analytics would use data to forecast future resource availability based at user mobility prediction, traffic patterns and overload. Finally, 6G would possess self-capabilities in healing, organization, reconfiguration, optimization, aggregation, and protection.

The conventional centralized ML algorithms need the availability of a large amount of centralized data and training on a central server (e.g., cloud server or centralized machine). However, this would result with a bottleneck in the future ultra-large scale mobile networks. Therefore, 6G networks would adopt ubiquitous AI solutions from the network core to the edge devices, i.e., Edge Intelligence (EI), or edge AI located at the edge of the network would be introduced in 6G. As a result, there would be a significant of big data sources from the cloud data centers to the increased number of smart edge devices (smartphones and IoT devices). Because of this data shift, these edge devices would move the AI solutions to the edge of the network in order to exploit completely the available potential of the edge big data sources. One possible emerging distributed ML technique is federated learning (FL) which would realize ubiquitous AI in the 6G networks. FL does not rely on storing all data to a central server where model training can occur. Instead, the innovative idea of FL is to train an ML model at each device (participant or data owner) where data is generated, or a data source has resided, and then let the participants send their individual models to a server (or aggregation server) and like that to achieve an agreement for a global model. However, despite the considerable potential advantages of FL for the 6G networks, FL is still in its infancy and encounter various challenges for fully operationalize in the 6G networks (Kitanov, Stojan, and Vladimir Nikolikj, 2022).

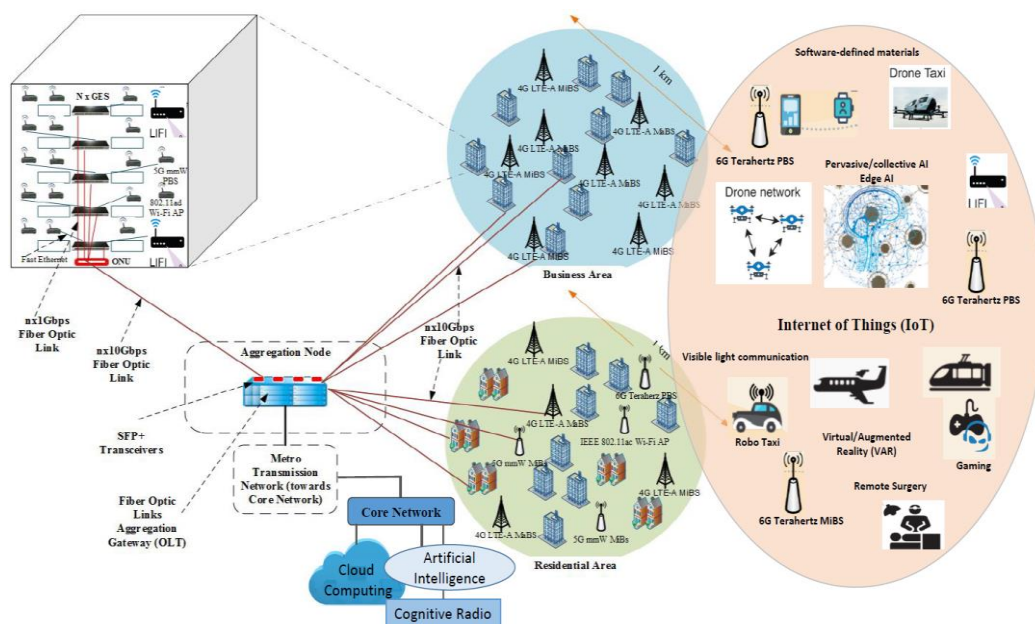


Fig.1. 6G Network Architecture

Regarding the security aspects, the security vision of 6G would integrate AI to produce security automation which would ensure user/data privacy, would ensure trust, would provide prediction, detection and prevention of attacks, and would limit vulnerability propagation (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023). Due to the new technologies in 6G network architecture, 6G new applications, and 6G new services, and the new policy regulations, the “Adversaries” also work non-stop to produce new kinds of security risks. Therefore, the identification and detection of zero-day attacks wouldn't be easy. As a result, the best practical defense would be to stop and prevent the zero-day attacks. In order to assess the value of network security in 6G, new set of Key Performance Indicators (KPIs) and Key Value Indicators (KVI) such as level of protection, response time, network coverage, autonomicity level, AI robustness, Secure AI model convergence time, security function chain round-trip-time, and deployment cost for security functions, should be defined. In addition, several factors, including network information security, and security-related to AI/ML, should be taken into account when characterizing security (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023).

### **3. OVERVIEW OF COMPUTING CONTINUUM**

The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities. Cloud computing is a computing paradigm, where a large pool of systems is connected in private or public networks, in order to provide dynamically scalable infrastructure for application, data and file storage (Khan, Atta Ur Rehman, Mazliza Othman, Sajjad Ahmad Madani, and Samee Ullah Khan, 2014). The beginning of 21st century has been characterized by a general trend in which “business solutions migrate to the cloud”, due to the following benefits:

- At the same time, the shared cloud resources (networks, servers, data warehouses, applications and services) can be rapidly provisioned and managed with minimal interaction by service providers;
- The cloud computing users may use these resources for development, hosting and running of services and applications on demand in a flexible way at any device, at any time and at any place in the cloud; and
- With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

However, cloud-centric solutions cannot support fast growing sizes of IoT deployment due to the following (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023):

- the amount of data generated by the sensors is so large, that networking infrastructure between the sensors and the Cloud may not be able to efficiently transfer them;
- between the sensors and the cloud, within the ecosystem, multiple computing nodes with reasonable capabilities exist and the cloud-centric model does not support their utilization;
- large IoT ecosystems may require extremely time-constraint decision loops, which cannot be realized in cloud-centric deployments; and
- privacy and security of travelling data is put at stake.

The progressive convergence between Cloud Computing and the Internet of Things resulted in the appearance of the Computing Continuum (Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al, 2023 & Tarneberg, William, Emma Fitzgerald, Monowar Bhuyan, Paul Townend, Karl-Erik Arzen, Per-Olov Ostberg, Erik Elmroth, Johan Eker, Fredrik Tufvesson, and Maria Kihl, 2022). Initially, the concept of Edge Computing represented a middle ground between data centers and IoT hyper-local networks of sensors and actuators. Then a much more nuanced paradigm emerged and placed computing infrastructure on a spectrum covering from the Cloud Data Centers to Edge Nodes with many intermediate levels. High-Performance Computing (HPC), Artificial Intelligence, 5G/6G networks are also part of this Continuum for which hardware and software need to be jointly considered.

Moreover, the role that 6G networks can play in the transition from the IoT, to the Edge-Cloud 6G Computing Continuum.

The computing continuum seamlessly combines resources and services at the center (e.g., in Cloud datacenters), at the Edge, and in-transit, along the data path. Typically, data is first generated and preprocessed (e.g., filtering, basic inference) on Edge devices, while Fog nodes further process partially aggregated data. Then, if required, data is transferred to HPC enabled Clouds for Big Data analytics, Artificial Intelligence model training, and global simulations. Fig. 2. illustrates the implementation of a highly distributed infrastructure with resources spanning the entire computing continuum (Kimovski, Dragi, Roland Matha, Josef Hammer, Narges Mehran, Hermann Hellwagner, and Radu Prodan, 2021).

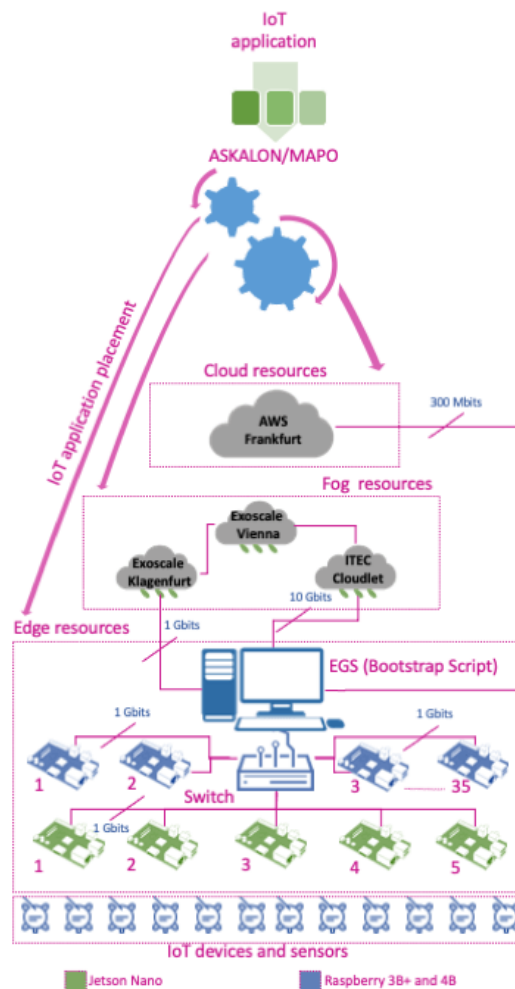
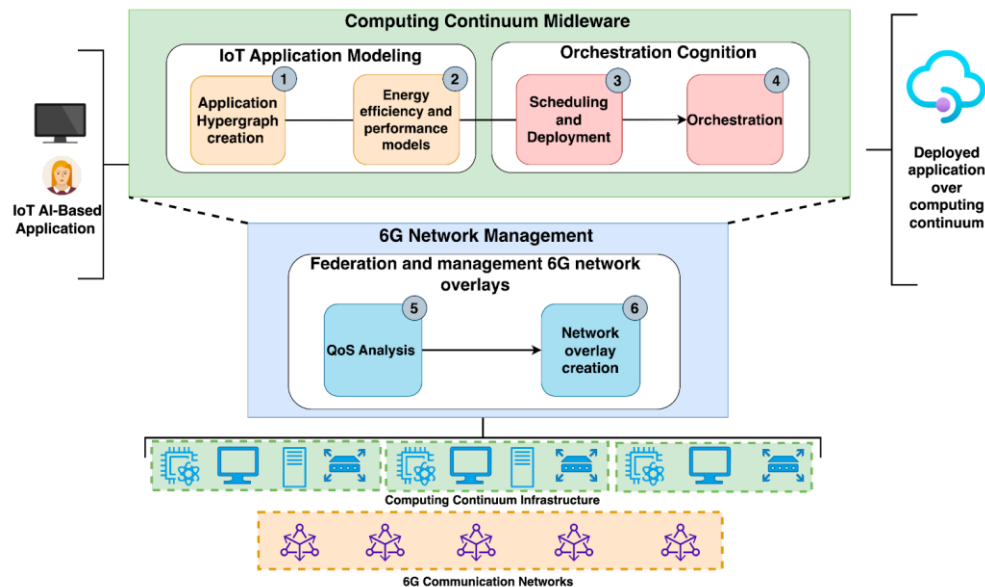


Fig.2. Overview of Computing Continuum

#### 4. THE COMPUTING CONTINUUM MIDDLEWARE FOR ARTIFICIAL INTELLIGENCE OVER 6G NETWORKS

Apart from the main network infrastructure problem mentioned in Section 2, there is also an operational problem which needs to be addressed. Actually, the novel IoT applications beyond the 5G networks and 6G networks would require a solid computing infrastructure, such as the computing continuum, which provides a near and rich set of computing devices and smart networking technologies to support their AI computation, storage, and low-latency communication (in 5G and future 6G standards). In addition, the modern AI-based IoT applications suffer from manual orchestration and device communication. They lack advanced middleware support to automate their operation with optimized resource and application modelling, scheduling and performance adaptation in response to low communication latency and throughput constraints.

One possible solution to the network infrastructure problem and the operational problem is our proposed computing continuum middleware for artificial intelligence over 6G mobile networks, that would create an automated, sustainable loop for managing IoT applications utilizing AI approaches over 6G networks, which is depicted in Fig. 6. It consists of Computing Continuum Middleware which is managed and controlled by 6G network management using the distributed edge artificial intelligence.



**Fig.3.** Computing Continuum Middleware for Artificial Intelligence over 6G Mobile Networks

The computing continuum middleware facilitates creating and optimizing the IoT applications’ workflows comprising performance and energy models and facilitates the scheduling, deployment and orchestration. It consists of IoT Application Modelling and Orchestration Cognition.

IoT Application Modelling provides the following functionalities: application hypergraph creation and optimization and energy efficiency and performance modelling. The Application hypergraph creation and optimisation analyzes the IoT application with its interactions with the computing continuum, 6G networks and environment and represents them as hypergraphs (HG), which is a powerful higher-order mathematical tool for systems modelling. Unlike classical approaches for managing IoT applications, which model the applications in isolation from the infrastructure and environment, this approach would generalize the applications and the infrastructure as hypergraphs. The Hypergraph models not only the IoT application components but also all multi-dimensional interactions, including the interactions with the environment.

Furthermore, the IoT Application Modelling encompasses energy efficiency analysis by considering multiple sustainability metrics, including energy wastage estimation. It utilizes benchmarks for energy profiling various computing resources available across the computing continuum, including single-board computers, powerful cloud instances and even open-source hardware, including RISC-V-based processors. Moreover, the IoT Application Modelling supports a set of benchmarks for improved hardware performance models, which are essential for improved energy efficiency and sustainable execution.

The Orchestration Cognition would be responsible for the following functionalities: scheduling and deployment and orchestration.

The scheduling and deployment support a preemptive scheduling approach capable of reacting to the changes in the computing infrastructure and the available 6G networks. The scheduling approach utilizes multi-objective heuristics, considering energy efficiency and performance as optimization objectives, to find IoT application scheduling solutions. Besides, it enables transparent deployment of IoT applications using the principle of infrastructure-as-a-code.

The orchestration component enables efficient orchestration and adaptation of the execution of the IoT application concerning the communication performance of the utilized 6G network overlays. It utilizes

a Prometheus-based monitoring system to constantly monitor the communication performance of the network and the computing performance of the resources. Based on the gathered monitoring data, the component uses machine learning to detect anomalies in the execution and the resources and adapt the execution in real time. For the given purpose, the component could rely on a Kubernetes orchestrator. The 6G network management layer enables the federation of multiple network technologies to support IoT application execution with high QoS and dynamic overlay network creation. It consists of QoS analysis and network overlay creation.

To achieve the fundamental goals of 6G, it is necessary to foster higher system capacity, higher data rate, lower latency, and improve the quality of service (QoS). The dynamic QoS analysis through novel, dynamic queue management would imply dynamic queues parameter configuration according to the requirements specified through the service management on the application layer. The QoS traffic management would utilize dynamic queues management and apply mechanisms to make intelligent decisions for max rates of service groups. The QoS analysis would be dynamically performed on the following key performance indicators (KPIs): latency, user data throughput, energy efficiency and power consumption. The KPIs would be dynamically collected from different RATs, and would be analyzed to determine which RAT would offer the best QoS for various profile users. This analysis would be performed by distributed artificial intelligence located at the core and the edge of the 6G network.

Once the QoS analysis is completed, it would be created an automatic network overlay. For that, a virtual or logical network would be created on top of an existing physical network. The overlay creates a new layer where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links. Overlays enable administrators to define and manage traffic flows, irrespective of the underlying physical infrastructure. Some of the advantages that network overlay provides over the physical network are scalability, flexibility, management, security, redundancy, and efficiency. The network overlay would provide a better QoS to all users that have different service requirements for IoT applications. The 6G network would be about distributed artificial intelligence at the edge of the 6G network, which would be enabled by using the computing continuum middleware.

#### **4. CONCLUSION**

The exponential increase in broadband multimedia wireless communications, as well as the rapid proliferation of smart mobile devices would shape the creation of the future 6G mobile and wireless networks. Terahertz, visible light communication and technologies like compressed sensing theory, new channel coding, large-scale antenna, flexible spectrum usage, AI-based wireless communication and special features as Space-Air-Ground-Sea integrated communication and wireless tactile network are few of the novelties that are expected to become a common network standard of 6G. 6G network should provide scalability, efficient connectivity with connectivity and reliability, coverage improvement, as well as, QoS and QoE provisioning.

The main driving force in designing and optimizing 6G architectures, protocols, and operations is Distributed Artificial Intelligence in the core, radio access, and the network edge, which would provide support of ubiquitous and ubiquitous smart services from the core to the end devices of the network, which would exceed the mobile data traffic used today. It is expected that AI would transform the wireless evolution of future Internet of Everything (IoE) from “connected things or objects” to “connected intelligence.”

The security vision of 6G would integrate AI to produce security automation which would ensure user/data privacy, would ensure trust, would provide prediction, detection and prevention of attacks, and would limit vulnerability propagation. new set of Key Performance Indicators (KPIs) and Key Value Indicators (KVI) should be defined, in order to assess the value of network security in 6G.

The Computing Continuum encompasses the seamless integration of edge, fog, and cloud computing resources to provide a unified and distributed computing environment, and it aims to enable real-time data processing, low-latency response, and intelligent decision-making at the network edge. The role that 6G networks can play in the transition from the IoT, to the Edge-Cloud 6G Computing Continuum.

The computing continuum middleware for artificial intelligence over 6G mobile networks, that would create an automated, sustainable loop for managing IoT applications utilizing AI approaches over 6G networks.

Although AI learning algorithms provide many benefits in terms of learning and recognition ability, still they require very high level of computational complexity, high power consumption, and many computing and processing resources. Therefore, significant research efforts are needed to advocate the inter-working collaboration and cooperation among hardware components and AI learning algorithms. In addition, scalability, great robustness, and flexibility of learning frameworks are important aspects to provide support of the potential unbounded number of interacting entities and to provide high-quality QoS and QoE services in 6G networks. Thus, the design of scalable, robust and flexible AI learning frameworks for 6G networks is still an open issue.

## **ACKNOWLEDGEMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

This research paper is a part of the bilateral national research project entitled: 6G Continuum: Computing Continuum Middleware for Artificial Intelligence over 6G Networks, funded by the governments of the Republic of North Macedonia and the Republic of Austria, in which participates the following institutions: Mother Teresa University, Faculty of Information Sciences, Skopje, Republic of North Macedonia and Alpen Audria University of Klagenfurt, Department of Information Technology, Klagenfurt, Republic of Austria.

## **REFERENCES**

1. Balali, Farhad, Jessie Nouri, Adel Nasiri, and Tian Zhao. *Data Intensive Industrial Asset Management*. Springer eBooks, 2020. <https://doi.org/10.1007/978-3-030-35930-0>
2. Choudhury, Alok, Manojit Ghose, Akhirlul Islam, and None Yogita. "Machine Learning-based Computation Offloading in Multi-access Edge Computing: A Survey." *Journal of Systems Architecture* 148 (February 16, 2024): 103090. <https://doi.org/10.1016/j.sysarc.2024.103090>.
3. Clemm, Alexander, Maria Torres Vega, Hemanth Kumar Ravuri, Tim Wauters, and Filip De Turck. "Toward Truly Immersive Holographic-Type Communication: Challenges and Solutions." *IEEE Communications Magazine* 58, no. 1 (January 1, 2020): 93–99. <https://doi.org/10.1109/mcom.001.1900272>.
4. Du, Jun, Chunxiao Jiang, Jian Wang, Yong Ren, and Merouane Debbah. "Machine Learning for 6G Wireless Networks: Carrying Forward Enhanced Bandwidth, Massive Access, and Ultrareliable/Low-Latency Service." *IEEE Vehicular Technology Magazine* 15, no. 4 (September 25, 2020): 122–34. <https://doi.org/10.1109/mvt.2020.3019650>.
5. Hao, Tianshu, Jianfeng Zhan, Kai Hwang, Wanling Gao, and Xu Wen. *AI-oriented Workload Allocation for Cloud-Edge Computing*, 2021. <https://doi.org/10.1109/ccgrid51090.2021.00065>.
6. Huang, Yakun, Boyuan Bai, Yuanwei Zhu, Xiuquan Qiao, Xiang Su, Lei Yang, and Ping Zhang. "ISCom: Interest-Aware Semantic Communication Scheme for Point Cloud Video Streaming on Metaverse XR Devices." *IEEE Journal on Selected Areas in Communications* 42, no. 4 (December 22, 2023): 1003–21. <https://doi.org/10.1109/jsac.2023.3345430>.
7. Jiang, Dajie, and Guangyi Liu. "An Overview of 5G Requirements." In *Springer eBooks*, 3–26, 2016. [https://doi.org/10.1007/978-3-319-34208-5\\_1](https://doi.org/10.1007/978-3-319-34208-5_1).
8. Khan, Atta Ur Rehman, Mazliza Othman, Sajjad Ahmad Madani, and Samee Ullah Khan. "A Survey of Mobile Cloud Computing Application Models." *IEEE Communications Surveys & Tutorials* 16, no. 1 (July 4, 2013): 393–413. <https://doi.org/10.1109/surv.2013.062613.00160>.
9. Khan, Latif U., Ibrar Yaqoob, Muhammad Imran, Zhu Han, and Choong Seon Hong. "6G Wireless Systems: A Vision, Architectural Elements, and Future Directions." *IEEE Access* 8 (January 1, 2020): 147029–44. <https://doi.org/10.1109/access.2020.3015289>.
10. Kibria, Mirza Golam, Kien Nguyen, Gabriel Porto Villardi, Ou Zhao, Kentaro Ishizu, and Fumihide Kojima. "Big Data Analytics, Machine Learning, and Artificial Intelligence in Next-



- Generation Wireless Networks.” *IEEE Access* 6 (January 1, 2018): 32328–38. <https://doi.org/10.1109/access.2018.2837692>.
11. Kimovski, Dragi, Roland Matha, Josef Hammer, Narges Mehran, Hermann Hellwagner, and Radu Prodan. “Cloud, Fog, or Edge: Where to Compute?” *IEEE Internet Computing* 25, no. 4 (February 9, 2021): 30–36. <https://doi.org/10.1109/mic.2021.3050613>.
  12. Kitanov, Stojan, Edmundo Monteiro, and Toni Janevski. *5G And the Fog — Survey of Related Technologies and Research Directions*, 2016. <https://doi.org/10.1109/melcon.2016.7495388>.
  13. Kitanov, Stojan, Ivan Petrov, and Toni Janevski. “6G MOBILE NETWORKS: RESEARCH TRENDS, CHALLENGES AND POTENTIAL SOLUTIONS.” *Journal of Electrical Engineering and Information Technologies* 6, no. 2 (January 1, 2021): 67–77. <https://doi.org/10.51466/jeeit2162186067k>.
  14. Kitanov, Stojan, and Vladimir Nikolikj. “The Role of Edge Artificial Intelligence in 6G Networks.” *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, June 16, 2022, 1–4. <https://doi.org/10.1109/icest55168.2022.9828567>.
  15. Kumar, Jaydip, Jitendra K Samriya, Marek Bolanowski, Andrzej Paszkiewicz, Wiesław Pawłowski, Maria Ganzha, Katarzyna Wasielewska-Michniewska, et al. “Towards 6G-Enabled Edge-Cloud Continuum Computing – Initial Assessment.” In *Communications in Computer and Information Science*, 1–15, 2023. [https://doi.org/10.1007/978-3-031-25088-0\\_1](https://doi.org/10.1007/978-3-031-25088-0_1).
  16. Letaief, Khaled B., Wei Chen, Yuanming Shi, Jun Zhang, and Ying-Jun Angela Zhang. “The Roadmap to 6G: AI Empowered Wireless Networks.” *IEEE Communications Magazine* 57, no. 8 (August 1, 2019): 84–90. <https://doi.org/10.1109/mcom.2019.1900271>.
  17. Nawaz, Syed Junaid, Shree Krishna Sharma, Shurjeel Wyne, Mohammad N. Patwary, and Md. Asaduzzaman. “Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future.” *IEEE Access* 7 (January 1, 2019): 46317–50. <https://doi.org/10.1109/access.2019.2909490>.
  18. Rashid, Adib Bin, and Md Ashfakul Karim Kausik. “AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications.” *Hybrid Advances* 7 (August 23, 2024): 100277. <https://doi.org/10.1016/j.hybadv.2024.100277>.
  19. “Report ITU-R M.2370-0.” *IMT Traffic Estimates for the Years 2020 to 2030*, 2015.
  20. Saad, Walid, Mehdi Bennis, and Mingzhe Chen. “A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems.” *IEEE Network* 34, no. 3 (October 15, 2019): 134–42. <https://doi.org/10.1109/mnet.001.1900287>.
  21. Seng, Kah Phooi, Li Minn Ang, and Ericmoore Ngharamike. “Artificial Intelligence Internet of Things: A New Paradigm of Distributed Sensor Networks.” *International Journal of Distributed Sensor Networks* 18, no. 3 (March 1, 2022): 155014772110628. <https://doi.org/10.1177/15501477211062835>.
  22. Shahraki, Amin, Mahmoud Abbasi, Md. Jalil Piran, and Amir Taherkordi. “A Comprehensive Survey on 6G Networks: Applications, Core Services, Enabling Technologies, and Future Challenges.” arXiv.org, January 29, 2021. <https://arxiv.org/abs/2101.12475>.
  23. Strinati, Emilio Calvanese, Sergio Barbarossa, Jose Luis Gonzalez-Jimenez, Dimitri Ktenas, Nicolas Cassiau, Luc Maret, and Cedric Dehos. “6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication.” *IEEE Vehicular Technology Magazine* 14, no. 3 (August 8, 2019): 42–50. <https://doi.org/10.1109/mvt.2019.2921162>.
  24. Tang, Fengxiao, Yuichi Kawamoto, Nei Kato, and Jiajia Liu. “Future Intelligent and Secure Vehicular Network Toward 6G: Machine-Learning Approaches.” *Proceedings of the IEEE* 108, no. 2 (December 6, 2019): 292–307. <https://doi.org/10.1109/jproc.2019.2954595>.
  25. Tariq, Faisal, Muhammad R. A. Khandaker, Kai-Kit Wong, Muhammad A. Imran, Mehdi Bennis, and Merouane Debbah. “A Speculative Study on 6G.” *IEEE Wireless Communications* 27, no. 4 (August 1, 2020): 118–25. <https://doi.org/10.1109/mwc.001.1900488>.
  26. Tarneberg, William, Emma Fitzgerald, Monowar Bhuyan, Paul Townend, Karl-Erik Arzen, Per-Olov Ostberg, Erik Elmroth, Johan Eker, Fredrik Tufvesson, and Maria Kihl. *The 6G*

*Computing Continuum (6GCC): Meeting the 6G Computing Challenges*, 2022. <https://doi.org/10.1109/6gnet54646.2022.9830459>.

27. “Transforming Our World: The 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs,” n.d. <https://sdgs.un.org/2030agenda>.
28. Zhang, Shangwei, Jiajia Liu, Hongzhi Guo, Mingping Qi, and Nei Kato. “Envisioning Device-to-Device Communications in 6G.” *IEEE Network* 34, no. 3 (March 27, 2020): 86–91. <https://doi.org/10.1109/mnet.001.1900652>.

## CYBERSECURITY IN AZERBAIJAN: LEGISLATIVE MEASURES TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

Dr Balajanov Elvin  
Chairman of the Association of Cybersecurity Organizations of Azerbaijan  
ebalajanov@akta.az

**ABSTRACT:** The scope of information infrastructures underpinning business operations and technological processes within Azerbaijan's national security sectors is rapidly expanding. These infrastructures are essential for ensuring operational continuity and resilience, with any compromise posing a risk of significant disruption and damage. Consequently, safeguarding these infrastructures has become a core priority within the nation's broader information security strategy. To this end, substantial measures, including enhanced legal regulations, have been implemented to strengthen the security of infrastructures deemed critical, as well as the information systems, communication networks, and automated management systems vital to the interests of the state, society, and its citizens. This article examines the legal frameworks established for the protection of critical information infrastructure (CII) in Azerbaijan, while also identifying areas needing further development and optimization.

**KEYWORDS:** critical information infrastructure, CII, Azerbaijan, legal regulation, criticality criteria, security requirements, cybercrime, legal liability.

### INTRODUCTION

In the rapidly evolving global information space, states are consistently broadening their efforts to secure national information independence and sovereignty while reliably safeguarding their national interests. Consequently, a comprehensive set of measures in information security and cybersecurity is being implemented to address these challenges. In the Republic of Azerbaijan, where digital transformation is progressing rapidly, a robust information infrastructure is being established to address issues of society and state significance through information technologies. In particular, the scope of information infrastructures underpinning business functions and technological processes in critical sectors, including state and private entities as well as civil organizations, is expanding swiftly. Any compromise in the security of these infrastructures could lead to substantial harm, thereby making their protection a crucial component of the nation's core interests in the information sphere.

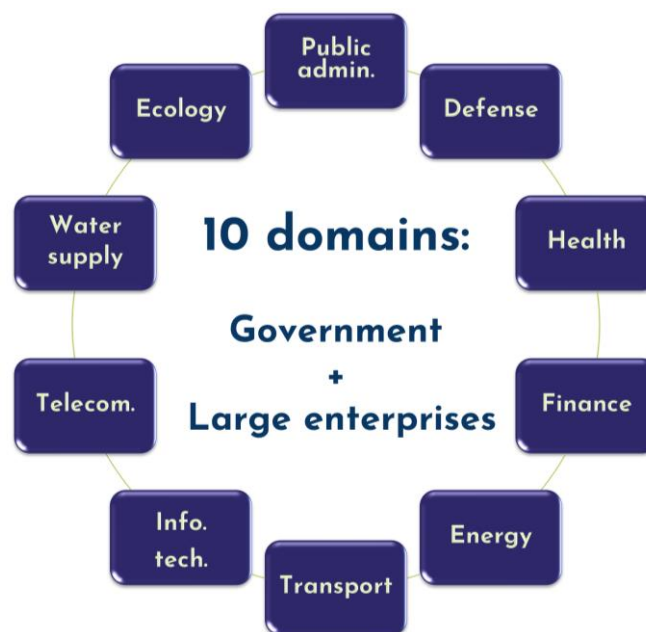
It should be particularly noted that ensuring the security of critical information infrastructure (CII) is one of the nine priority areas outlined in the *Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027* approved by the Decree of the President of the Republic of Azerbaijan No. 4060, dated August 28, 2023. The strategy emphasizes the critical importance of ensuring the information security of infrastructures that are pivotal in supporting the vital functions of society and the state, as any failure or disruption in their operation can have profound consequences on public health, safety, economic stability, social welfare, and the uninterrupted functioning of state institutions. Thus, the security of CII must remain a primary focus, regardless of its ownership, and appropriate measures must be implemented to safeguard it. (*Information Security and Cybersecurity Strategy 2023*, 6.4.)

Consequently, significant steps have been undertaken across various sectors in Azerbaijan, including legal regulation, to address issues essential to the state, society, and citizens and to enhance the security of CII, along with the associated information systems, communication networks, and automated management systems.

## FACTORS CHARACTERIZING THE CRITICALITY OF INFORMATION INFRASTRUCTURE AND THE LEGAL MECHANISMS APPLIED FOR THIS PURPOSE

As outlined in the *Presidential Decree* of the Republic of Azerbaijan dated April 17, 2021, "*On Certain Measures for Ensuring the Security of Critical Information Infrastructure*", the continuous development of information technologies and the globalization of information and information systems have become crucial tools for the country's progress. Thus, in the Republic of Azerbaijan, an appropriate information infrastructure is being developed to address matters of national importance, and its integration into global information networks, including the internet, has exposed infrastructure objects to cyberattacks. The disruption or malfunction of the systems and networks within CII, established to safeguard the rights and interests of the state, society, and citizens, can result in severe damage, which makes the cybersecurity of CII a priority issue (*the Presidential Decree "On Certain Measures for Ensuring the Security of Critical Information Infrastructure"* (2021)).

It should be noted that the Law of the Republic of Azerbaijan No. 539-VIQD, dated May 27, 2022, introduced a new chapter titled "Security of Critical Information Infrastructure" and several related concepts to the *Law on "Information, Informatization, and the Protection of Information."* According to this law, CII encompasses a set of information systems, automated management systems, and information-communication networks that ensure the functioning of sectors such as public administration, defense, healthcare, financial markets, energy, transportation, information technology, telecommunications, water supply, and ecology, the disruption of whose functionality could cause significant harm to the state, society, and citizens' interests (*Law "On Information, Informatization, and the Protection of Information"* 1998, article 2) Thus, ten sectors have been identified in the Republic of Azerbaijan as having CII:



*Figure 1. Critical Information Infrastructure Sectors in Azerbaijan*

According to the *Law on "Information, Informatization, and the Protection of Information"*, a CII object refers to an information system, automated management system, or information and communication network that is part of CII, while "a CII subject" refers to the state bodies (organizations) that own (or use) the CII object, including state-owned legal entities, public legal entities created on behalf of the state, as well as other legal entities and individual entrepreneurs (excluding micro, small, and medium-sized enterprises). (Ibid., article 2)

In both national and international practice, one of the most crucial and complex issues is determining the criteria for identifying CII objects. In the Republic of Azerbaijan, the list of CII objects is approved based on several requirements. According to the Law, an object is considered a CII object if its disruption could result in the following outcomes:

- “ - threats to the independence, sovereignty, constitutional order, territorial integrity, and defense capabilities of the state;
- significant threats to public safety;
- below situations leading to the deprivation of essential services for the population:
  - disruption of the functioning of state bodies (institutions);
  - serious obstacles to the normal functioning of life-supporting infrastructure;
  - interruption of transportation and communication links;
  - significant limitations on the provision of healthcare services;
- disruption of economic and financial stability;
- severe damage to the formation of the state budget;
- disruption of ecological balance and sharp deterioration of the environmental situation.” (*Law on "Information, Informatization, and the Protection of Information" 1998, Article 20-2*)

Although the criteria set by the law are somewhat clear, the lack of definitions for descriptive terms such as "significant threats", "serious obstacles", "severe damage", and "sharp deterioration" could create difficulties in determining the scope of CII objects in practice. Specifically, the meaning of the "significance" of threats, the "severity" of damage and restrictions, and the "sharpness" of deterioration remains unclear.

## SECURITY REQUIREMENTS FOR CII OBJECTS

In general, according to Article 20-1.1 of the Law, the security of CII is ensured through the establishment of security requirements for the infrastructure, the assessment of its compliance with these requirements, the elimination of identified non-compliance, the implementation of an information security management system corresponding to these requirements, and the monitoring of the security of CII. (Ibid., Article 20-1.1)

Furthermore, the Law stipulates that both general and specific requirements for the security of CII must be determined, taking into account its purpose and operational characteristics, and these requirements must be included in the registry of CII objects. (Ibid., Article 20-4)

It should be noted that the rules for ensuring the security of CII, including the general requirements for the security of CII and the requirements for cybersecurity service providers, their personnel, technological resources, and operational processes, are established by the "Rules for Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan", approved by the Cabinet of Ministers of the Republic of Azerbaijan on July 17, 2023, Decision No. 229. According to the Rules, CII entities must comply with 29 general requirements across 7 areas/objectives, as well as specific requirements:

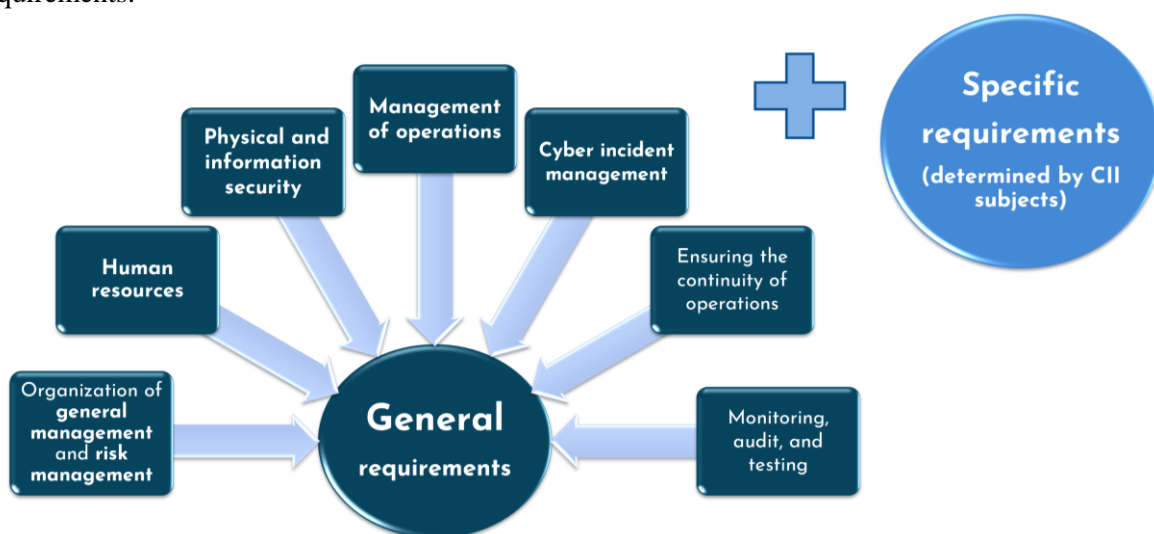


Figure 2. Security requirements for CII objects

The "Decree of the President of the Republic of Azerbaijan on the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and Information Protection" (1998) determines that the responsibility for ensuring the security of critical information infrastructure (excluding the information infrastructure of protected persons and protected objects), including combating cyber threats, lies with the State Security Service of the Republic of Azerbaijan. The State Security Service, along with the Special Communications and Information Security State Service of the Republic of Azerbaijan, carries out these functions with respect to government bodies, public legal entities created on behalf of the state, and state-owned legal entities. (Article 2.2-1) In turn, the CII subject ensures the security of its infrastructure in accordance with the established general and specific security requirements.

The competent authority and CII subjects are responsible for monitoring the security of critical information infrastructure, ensuring compliance with both general and specific security requirements. The competent authority should support CII subjects in safeguarding state and societal interests, while overseeing the overall security of CII. It is also specified that the oversight of the security of CII is carried out through the evaluation of compliance with general and specific requirements, the resolution of identified non-compliance, verification of adherence to these requirements, continuous (24/7) monitoring of the security of CII, conducting penetration tests, and performing external audit inspections. ("Rules for Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan" 2023, Article 9).

Additionally, it should be noted that the "Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects" approved by the Cabinet of Ministers of the Republic of Azerbaijan on July 17, 2023, define the legal, organizational, and technological foundations for the creation and operation of the registry. According to these regulations, the registry is an information system intended for carrying out information processes related to CII objects (such as data creation, collection, processing, storage, retrieval, protection, and exchange), as well as for ensuring the security of CII, including planning and executing measures for combating cyber threats and conducting analyses. ("Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects" 2023, Article 1.2). The operator of the registry is the Cybersecurity Operations Center of the State Security Service of the Republic of Azerbaijan. Regarding state institutions, the operator's functions are carried out in cooperation with the cyber center of the Special Communications and Information Security State Service of Azerbaijan. (Ibid, Article 1.4). The organization and functionality of the registry's operation are ensured based on the information submitted by CII subjects. The submission of data is done in line with the operator's methodological recommendations and provided templates. (Ibid, Articles 5.1-5.2).

## **LEGAL RESPONSIBILITY MEASURES IN THE FIELD OF CRITICAL INFORMATION INFRASTRUCTURE SECURITY**

The legal responsibility measures for ensuring the security of CII seem to take a more reactive approach, rather than proactively and effectively addressing potential risks. While penalties for non-compliance or failure to report incidents are in place, these measures may not be stringent enough to prevent or minimize threats effectively.

According to Article 371-1.1 of the *Administrative Offenses Code of the Republic of Azerbaijan* (2015), in case of violation of general and specific requirements by the owner of the infrastructure, its officials, or the provider (supplier) providing cybersecurity services, the officials are fined between 500 and 1000 AZN, and legal entities are fined between 3000 and 4000 AZN.<sup>1</sup> As per Article 371-1.2 of the same Code, officials who violate requirements related to the creation and functionality of the information security management system are fined between 1000 and 1500 AZN, and legal entities are fined between 4000 and 5000 AZN. Additionally, if the subject fails to report cyberthreats, cyberattacks, cyber incidents, and attempts to commit these actions against CII objects to the relevant state authority, officials are fined between 300 and 500 AZN, and legal entities are fined between 500 and 1000 AZN.

---

<sup>1</sup> Note: 1 AZN = 0.55 EUR as of the time of writing this article.

Moreover, according to Article 602-3 of the Administrative Offenses Code, if an official or the relevant authority fails to comply with the requirement to eliminate violations of general and specific requirements, or fails to create the necessary conditions or obstructs the detection, prevention, and investigation of cyber threats, cyberattacks, and security incidents, officials are fined between 1000 and 1500 AZN, and legal entities are fined between 4000 and 5000 AZN.

Additionally, it should be noted that according to the *Criminal Code of the Republic of Azerbaijan*, illegal access to, illegal interference with, and the illegal acquisition of data concerning the computer system of a CII object ("publicly significant infrastructure object") lead to criminal liability. The perpetrators of these crimes can face imprisonment for a period of four to six years, along with disqualification from holding certain positions or engaging in specific activities for up to three years (*Criminal Code of the Republic of Azerbaijan 1999*, Articles 271-273). This implies that cybercrimes targeting critical information infrastructure (CII) objects are classified as "minor crimes" under the Criminal Code.<sup>2</sup>

In general, the classification of cybercrimes committed against critical information infrastructure — considered crucial for the state's, society's, and citizens' interests, and whose security breaches could result in severe damage — as "minor crimes" can be disputed. For similar actions, such as those in the United Kingdom, penalties of up to fourteen years of imprisonment and even life imprisonment are imposed. (see, *UK Computer Misuse Act 1990*, 3ZA) This raises questions about whether the penalty set in the United Kingdom's legislation is excessively severe. However, it can also be argued that the penalty established in the *Criminal Code of the Republic of Azerbaijan* is not entirely proportional to these criminal acts, and in some cases, may be considered lenient.

## **CONCLUSION**

Significant steps have been taken in various fields, including legal regulation, to strengthen the security of CII and its components, such as information systems, communication networks, and automated control systems in Azerbaijan. These initiatives aim to address key concerns that affect the state, society, and citizens, ensuring greater protection of vital infrastructure and enhancing national security efforts. Specifically, criteria for identifying CII objects have been established, and security requirements for these objects have been clearly defined. Moreover, legal mechanisms for ensuring the security of CII, including organizational measures and oversight of safety conditions, have been implemented.

Additionally, it would be valuable to clarify certain descriptive terms used in the relevant normative legal acts mentioned above. A reassessment of the adequacy of the legal responsibility measures outlined in the legislation concerning violations related to CII would also be beneficial to ensure that they align with the evolving nature of cyber threats and security challenges.

## **ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## **REFERENCES:**

- Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027* (Approved by Decree No. 4060 of the President of the Republic of Azerbaijan, dated August 28, 2023).  
*Decree of the President of the Republic of Azerbaijan "On Certain Measures for Ensuring the Security of Critical Information Infrastructure"* (Decree No. 1315, April 17, 2021).  
*Law of the Republic of Azerbaijan "On Information, Informatization, and Information Protection"* (Law No. 460-IQ, April 3, 1998).

---

<sup>2</sup> Note: According to Article 15.3 of the Criminal Code of the Republic of Azerbaijan, offenses that are punishable by imprisonment for a term not exceeding seven years, whether committed intentionally or through negligence, are classified as minor crimes.

*Decree of the President of the Republic of Azerbaijan "On the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and Information Protection" (No. 729, 19 June 1998).*

*NIS2 Directive - Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures for ensuring a high common level of cybersecurity across the Union.*

*Decree of the President of the Republic of Azerbaijan "On the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and the Protection of Information" (Decree No. 729, June 19, 1998).*

*"Rules on Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan" (approved by the Cabinet of Ministers of the Republic of Azerbaijan, Decree No. 229, July 17, 2023).*

*"Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects" (approved by the Cabinet of Ministers of the Republic of Azerbaijan, Decree No. 230, July 17, 2023).*

*Administrative Offenses Code of the Republic of Azerbaijan (2015) (<https://e-qanun.az/framework/46960>).*

*Criminal Code of the Republic of Azerbaijan (1999) (<https://e-qanun.az/framework/46947>).*

*UK Computer Misuse Act 1990 (<https://www.legislation.gov.uk/ukpga/1990/18/contents>).*



## IMPLEMENTATION AND DEPLOYMENT OF POST-QUANTUM CRYPTOGRAPHY

Gabriel Chênevert<sup>1</sup>

<sup>1</sup> ICL, Junia, Université Catholique de Lille, LITL, F-59000 Lille, France.

**ABSTRACT:** This short expository note aims to share some of the insight gained by implementing “from scratch”, in C++, the ML-KEM and ML-DSA quantum resistant cryptographic primitives. Proper understanding of the inner workings of these recently standardized algorithms allows one to produce test vectors to verify compliance of any new implementation, as well as provide small (unsafe) parameter values that can be used for pedagogical purposes.

**KEYWORDS:** *post-quantum cryptography, module learning with errors, number-theoretic Fourier transform, ML-KEM, ML-DSA*

### ML-BASED POST-QUANTUM PRIMITIVES

In 2024, the US National Institute of Standards and Technology (NIST) published, after a 7-year-long international selection process, standards for three quantum-resistant algorithms: ML-KEM [2] (formerly known as CRISTALS-Kyber), ML-DSA [3] (CRISTALS-Dilithium) and SLH-DSA [4] (SPHINCS<sup>+</sup>). The first two of these, based on the *module-learning with errors* (M-LWE) problem, share many conceptual ideas and certain practical considerations. A blog post aimed at computer engineers [6] prompted this author, aided by a team of masters-level students, to come up with their own implementations of the then-drafts for the would-be standards in order to be able to provide feedback and compare them to reference implementations. This endeavour fits into a larger goal of being able to assess both the performance and total cost of deploying quantum-resistant primitives, in terms of development effort, scaling of infrastructures, and the actual migration to new primitives.

The basic *learning with errors* (LWE) problem [5] is a problem in linear algebra that can be used as a basis for cryptographical primitives. Given a vector  $\mathbf{x}$  and matrix  $\mathbf{A}$ , it is easy to compute, via matrix multiplication,  $\mathbf{y} = \mathbf{Ax}$ . The inverse process, recovering  $\mathbf{x}$  from  $\mathbf{y}$  knowing  $\mathbf{A}$ , is just solving a compatible system of linear equations and can be readily performed using Gaussian elimination. However, if noise is added:

$$\mathbf{y} = \mathbf{Ax} + \mathbf{e},$$

where  $\mathbf{e}$  is “small” in some suitable sense, then it becomes considerably more difficult to solve the noisy system of linear equations

$$\mathbf{y} \approx \mathbf{Ax}.$$

This asymmetrical problem can be used as the basis for a public-key encryption primitive as follows.

**Private key:** a secret (column) vector  $\mathbf{x}$ .

**Public key:** a matrix  $\mathbf{A}$  along with a vector  $\mathbf{y}$  such that  $\mathbf{y} \approx \mathbf{Ax}$ .





- $q$  is a prime number used as modulus for the integral coefficients of the polynomials;
- $n$  is the size of the negacyclic polynomials used (typically a power of 2 in order to have access fast multiplication through FFT);
- $\zeta$  an  $\ell^{\text{th}}$  root of unity in  $\mathbf{Z}/q\mathbf{Z}$  (which requires that  $q$  divides  $\ell - 1$  in order to exist).

Algorithm	$n$	$q$	$\zeta$	$\ell$
ML-DSA	256	$8380417 = 2^{23} - 2^{13} + 1$	1753	512
ML-KEM	256	$3329 = 2^8 \cdot 13 + 1$	17	256

Table 1: Algebraic parameters for ML-KEM and ML-DSA

Table 1 references the constants used by the ML standards, chosen for the balance they bring between the security level of the primitives and the efficiency of computations involved. We may remark that, in the case of ML-KEM,  $\ell = n$  and not  $2n$ , which complicates matters a bit because a non-split version of the Fourier transform needs to be used, grouping together the factors

$$(X - \zeta^{-i})(X + \zeta^{-i}) = X^2 - \zeta^i$$

in the factorization of  $X^{2n} - 1$ .

## COMPARISON WITH CLASSICAL PRIMITIVES

The main asymmetrical cryptographic primitives in use today for signature and key establishment, either based the difficulty of factorization or the discrete logarithm problem (DLP) over the modular integers and elliptic curves, would be vulnerable to an adversary having access to a large enough fault-tolerant quantum computer able to run Shor’s algorithm. The main advantage of ML-KEM and ML-DSA over these is that they are oblivious to such attacks; however, there is a price to pay, in terms of both spatial and temporal performances, to achieve this quantum resistance.

For instance, Table 2 references the sizes of the public keys needed in each case to achieve a given level of security.

## CONCLUDING REMARKS

The main takeaway from this experiment is that both ML-KEM and ML-DSA, as described by the standards, are considerably more subtle to grasp for the average working software developer than modular integer-based classical algorithms (which are relatively well understood by the community) and even elliptic curve-based ones (which still carry an aura of mystery despite being around for almost as long and having seen widespread usage for the last 25 years). In our opinion, this is due in no small part to the fact that the

security level	elliptic curve-based	integer-based	ML-DSA	ML-KEM
128	256	3072	10496	13056
256	512	15360	20736	25344

Table 2: Size (in bits) of the public keys for a given security level

$n$ (non-split)	$n$ (split)	$q$	$\zeta$	$\ell$
2	4	5	2	4
4	8	17	2	8
8	16	17	3	16
16	32	97	3	32

Table 3: Toy parameters that can be used for M-LWE

number-theoretic Fourier transform (NTT) is not used merely as an implementation optimization, but rather embroidered directly into the standards, rendering them somewhat more cumbersome to get a hold on.

Ready availability of test vectors since the publication of the final versions of the standards helps greatly to assess whether an implementation is functionally compliant or not. We suggest that, *for pedagogical purposes*, some implementations may support as "hazardous material" some smaller (unsafe) parameter choices that would allow people to get a better understanding of the inner workings of these new algorithms, such as those in Table 3. In particular, when speed of execution is not an issue, a modified version of the algorithm might skip altogether the NTT parts and work instead with the slower convolution-style multiplication (for the same functional results).

## ACKNOWLEDGEMENTS

Many thanks to friend and colleague Pierre Dubois for his precious help with the TikZ figures; as well as to JUNIA ISEN Cybersecurity students Rémi Protin, Aurélien Degain, Hamza Berbache, Enzo Barea Fernandez, Clément Gorse and Benoît Wattinne for their work on our C++ ML-KEM implementation.

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES

- [1] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "(Leveled) Fully Homomorphic Encryption without Bootstrapping." *ITCS*, ACM (2012): 309–325.
- [2] National Institute of Standards and Technology. *Module-Lattice-Based Key Encapsulation Mechanism Standard*, (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203 (2024). <https://doi.org/10.6028/NIST.FIPS.203>.
- [3] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*, (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204 (2024). <https://doi.org/10.6028/NIST.FIPS.204>.
- [4] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*, (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205 (2024). <https://doi.org/10.6028/NIST.FIPS.205>.
- [5] O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography." *STOC*, ACM (2005): 84–93.

- [6] F. Valsorda. "Enough Polynomials and Linear Algebra to Implement Kyber." *Cryptography Dispatches* (2023). <https://words.filippo.io/dispatches/kyber-math/>.

## CYBERTERRORISM: RISING THREATS AND STRATEGIC RESPONSES

Andro Gotsiridze

Cybersecurity Education and Research Centre

**ABSTRACT.** Cyberspace, as one of the domains of conflict, often gives a weak actor with few resources an asymmetric advantage over a strong opponent, as it provides the development and use of offensive capabilities with limited financial, human or organizational resources. With this, cyberoperations increase area of disinformation penetration and distribution, the ability to influence the audience, which is why they are widely used in information campaign production.

Nowadays, the most of cyber-attacks that cause immense damage, disruptions of financial loss are carried out by criminal organizations or state actors, not terrorist organizations. Nevertheless, cyber capabilities are developing all over the world, and proliferation control tools, financial and technical barriers are scarce and ineffective, which is why new technologies and intelligence vital to conduct cyber operations are becoming more and more accessible for terrorist organizations.

This article overviews those technical and organizational factors that increase the threat of cyber terrorism; it also provides a list of countermeasures to be implemented by the state and critical infrastructure.

**KEYWORDS:** Cyber attacks, cyber terrorism, RaaS, MaaS, DDoS- for-hire

### INTRODUCTION

Non-state actors, financially motivated organized crime groups, hacktivists, and ideologically motivated cyber groups are spending increasingly more time developing their cyber capabilities and integrate cyber operations into their strategic agendas and means of achieving their goals.

The trend also applies to terrorist organizations. They have significant motivation to conduct offensive cyber operations, thus analyzing their cyber capabilities and the threats they pose is of great importance for both state and individual security.

Today, the cyber capabilities of even major terrorist organization, such as Daesh and Al-Qaeda, are rudimentary. There is no evidence that these groups are competent to conduct large scale cyber-attack that could cause casualties, significant damage, or destruction, however, there is evidence of the development of cyber capabilities and the increasing integration of cyber operations into terrorist operations.

Based on the analysis of the attacks described so far, the cyber potential of terrorist organizations can be characterized as Low Skill/Low Value Target (LS/LT) capabilities. Strategic planning of cyber operations is weak, vulnerability detection of target networks - ineffective, and the attacks themselves have little effect and are limited to defacement and low-tech DoS techniques. None of the known cyber-attacks to this day has caused any operational disfunctions, nor has resulted in damage of long-term strategic or tactical significance.<sup>1</sup> The attacks of cyber groups rarely have shown economic nature, their goal is propaganda, information retrieval, and publishing jihadist calls (including threats) on websites with large number of visitors, as well as recruiting followers through social media.

Given the significant conventional successes of anti-terrorist coalition in recent years, the necessary base of human or material resource for traditional terrorist attacks shrunk drastically, and the territories controlled by these organizations' state-like entities became almost nonexistent, which pushed them to use asymmetric methods to achieve their goals. Moreover, certain areas of cybercrimes developed

---

<sup>1</sup> A notable exception is Hamas' cyber capabilities, which actively use malware and sophisticated, high-tech cyberespionage techniques. This is likely due to cooperation with Iranian state actors.

significantly over the past decade, giving terrorist organizations access to previously inaccessible cyber capabilities with an even higher level of conspiracy.

Based on the above, the threat of cyberterrorism is growing and significant, and in order to develop effective countermeasures, it is important to consider the factors that are driving the significant growth of cyber capabilities of terrorist organizations.

### **Organizational and technical factors leading to the growth of cyber capabilities of terrorist organizations**

#### **ORGANIZATIONAL FACTORS**

Due to the loss of controlled territories, a large part of terrorist organizations has transformed into a network coalition with a horizontal vector of expansion. The fragmentation of the territory led to the shift of focus from military and territorial goals to traditional terrorist acts. At the same time, the market for hacking tools has become more diverse, and the opportunity to use hacking services has emerged on the dark web, which has led to terrorist organizations' increased interest in cyberspace.

The following organizational factors should be considered as contributors in the significant growth of terrorist organizations' cyber capabilities:

- Radicalization or recruitment of Western resident lone wolves with relevant skills who can carry out cyberattacks against the targets of interest with minimal communication with the organization.
- Expanding the scope of recruitment: Intentions to develop cyber capabilities are detected in Southeast Asia, where compromise of websites are means to raise funds for terrorist activities or to support incarcerated extremists.
- Cooperation with states with highly developed destructive potential, which increases the threat of high-tech terrorist cyber-attacks.

#### **TECHNICAL ENABLERS**

While organizational factors like recruitment and collaboration have expanded the reach of terrorist groups, their growing access to advanced cyber tools and technologies further amplifies their potential for disruptive cyber operations.

**RaaS<sup>2</sup>, MaaS<sup>3</sup> and DDoS- for-hire<sup>4</sup>** services, as well as other tools accessible on illegal forums, give terrorist organizations a chance to expand their capabilities in an easy, cheap way. The ability to coordinate actions remotely from a secure environment makes such attacks much more attractive to a new, technology-savvy generation of terrorist organizations, increasing the intensity of cyber operations.

---

<sup>2</sup> Ransomware-as-a-Service is a criminal business model wherein an interested party or organization can commission a cybercriminal group to carry out ransomware attacks on a chosen target. Over the past five years, several significant cyberattacks on critical U.S. infrastructure, such as the Colonial Pipeline incident, have been executed via Russian-based criminal operators like ReVil and DarkSide.

<sup>3</sup> Malware-as-a-Service refers to a cyberattack model in which cybercriminals offer malicious software and its deployment on a target's digital infrastructure through illegal online marketplaces. This model is particularly appealing to resource-constrained, less capable actors as it eliminates the need for them to invest financial, human, and time resources in developing their own cyber capabilities, allowing them instead to leverage the offered service.

<sup>4</sup> An illegal service that involves renting out infrastructure required for conducting DDoS attacks. The proliferation of such services creates additional risks by enabling individuals or organizations without the necessary technical or intellectual capabilities to carry out such attacks.



The usage of DDoS- for-hire enables terrorist organizations to conduct these types of attacks more effectively. There is data on attempts to purchase such a tool on illegal forums.

RaaS technology, widely spread on illegal forums, could become a source of additional income for terrorist organizations, as well as a tool to disrupt the functioning of an adversary's critical infrastructure or sow fear.

Another common illegal service, MaaS, allows terrorist organizations to penetrate industrial control systems or other critical infrastructure networks. However, it should be noted that using such a service is quite expensive and requires technological skills from the user's part, in this case the terrorist organization, and a high degree of coordination with the provider.

Aside from aforementioned areas, the growth of cyber capabilities can be achieved by acquiring high-level **zero-day exploits**,<sup>5</sup> hiring information security specialists, or recruiting them with the prospect of further education.

In order to obtain the information needed to cause cyber incidents with significant damage, terrorist organizations are likely to become more active in terms of collaborating with insiders of the critical infrastructure of target countries. Radicalization of the insider or recruitment with financial motives and obtaining sensitive information from them significantly increases the likelihood of a successful cyberattack.

## **PROPOSED COUNTERMEASURES**

The potential targets of high-impact terrorist cyberattack are critical infrastructure facilities, which require robust defenses to mitigate risks.

To address the growing threat of cyberterrorism, the following measures are recommended:

- **Strengthen International Cooperation:** Enhance information-sharing between nations and agencies to improve incident detection and response.
- **Develop Public-Private Partnerships:** Foster collaboration between governments and private sector stakeholders to strengthen critical infrastructure defenses.
- **Implement Insider Threat Mitigation:** Introduce programs to monitor and counteract insider threats at critical infrastructure facilities.
- **Leverage Social Media Analysis:** Integrate social media content analysis into signals intelligence (SIGINT) to detect and disrupt planning for terrorist cyberattacks.

## **CONCLUSION**

The evolving cyber capabilities of terrorist organizations pose a growing threat to global security. Although their current capabilities are limited, their access to advanced tools and the growing availability of cybercrime services signal an urgent need for proactive countermeasures. Strengthening collaboration, improving defenses, and addressing insider threats are critical steps to mitigate the risks of cyberterrorism effectively.

## **ACKNOWLEDGEMENTS**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

---

<sup>5</sup> . A zero-day exploit refers to a cyberattack that leverages an undisclosed software vulnerability, giving developers no time to patch it. These exploits are highly dangerous and often used in targeted attacks by cybercriminals or nation-state actors.

**BIBLIOGRRAPHY**

1. Cyber Terrorism: Assessment of the Threat to Insurance, Cambridge: Centre for Risk Studies, November 2017.
2. ICCT Press Publication. Handbook of Terrorism Prevention and Preparedness. July 2021. Chapter 29. Shashi Jayakumar. Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. DOI: 10.19165/2020.6.01 ISSN: 2468-0486 ISBN: 9789090339771
3. G. Weimann; 2005. 'Cyberterrorism: The Sum of All Fears?', Studies in Conflict & Terrorism. 28:129-149, 2005
4. Simon P. Handler. THE CYBER STRATEGY AND OPERATIONS OF HAMAS: Green Flags and Green Hats. Atlantic Council Cyber Statecraft Initiative. 2022.
5. Michael Schmitt, "Normative Voids and Asymmetry in Cyberspace," Just Security, December 29, 2014

## ALGORITHMS FOR IDENTIFICATION AND ELIMINATION OF RISKS IN PACKET FILTERING RULES

<sup>1,a)</sup>Sherzod Gulomov, <sup>1,b)</sup>Sherzod Sayfullaev

<sup>1</sup>Tashkent university of information technologies named after Muhammad al-Khwarizmi

<sup>a)</sup>[sherhisor30@gmail.com](mailto:sherhisor30@gmail.com)

<sup>b)</sup>[sherzodsay@gmail.com](mailto:sherzodsay@gmail.com)

**ABSTRACT:** This study focuses on the development and optimization of algorithms to enhance network security and traffic management in information and communication systems. Advanced methods were designed to adaptively modify rule actions based on traffic behavior, reducing risks in network packets and improving security responses. The research emphasizes minimizing vulnerabilities by implementing a dynamic rule-prioritization mechanism that ensures optimal decision-making when accepting or rejecting network packets.

Key contributions include the creation of algorithms that effectively identify and mitigate harmful biases in network traffic, enhancing workstation security. Additionally, strategies for optimizing traffic filtering in Software-Defined Networks (SDN) were explored to address evolving network threats. Methods for detecting and managing anomalies in network packets, as well as tools for securing packet headers through the use of inter-network screens, were also developed.

The outcomes align with global advancements, incorporating principles from research institutions worldwide, such as cognitive inter-network screens, Next-Generation Firewalls, and Honeypot systems. This work significantly contributes to the development of efficient packet filtering rules and protective measures, ultimately reducing the likelihood of phishing attacks and other network-based threats. These advancements hold promise for bolstering the resilience of modern information systems against increasingly sophisticated cyberattacks.

**KEYWORDS:** *fuzzy petri net, packet filtering, fuzzy filtering, risk, network*

### INTRODUCTION

According to world experience, there is a scientific and practical research work on the development of traffic filtering models, methods and algorithms based on the detection and elimination of network attacks in information and communication systems, methods for detecting anomalies in network packages and Means for detecting suspicious packages. Research on the development of methods and tools for filtering network traffic in information and Communication Systems has yielded a number of scientific results, including the development of data proxy and cognitive inter-network screens (Massachusetts Institute of Technology, USA); the capabilities of the COAST inter-network screen reference model have been improved by adding a transfer block change function and attribute value mapping function (Zhejiang University, people's Republic; classification of protocols and services, The Next Generation Firewall new generation inter-network screen of the OSI model, which allows monitoring and blocking traffic at different levels from the network level to the application level, has been developed (TexArgos company, Russian Federation); authorization and denial algorithms have been developed that serve to effectively work network security, and the effectiveness of the algorithm; based on optimizing package filtering rules, a protection strategy and a Honeypot system has been developed that reduces the number of phishing attacks (Idaho State University, USA); a method has been developed that ensures data security in package headers by installing inter-network screens between Networks-on-Chip (NoC) routers (Technical University of Munich, Germany and the University of São Paulo, Brazil). In this regard, optimization of package filtering rules, methods for performing traffic filtering on SDN networks, improvement and development of harmful bias detection algorithms at workstations are considered one of the current pressing problems.

### MAIN PART

*Fuzzy Petri net.* A fuzzy Petri net is a combination of fuzzy logic and Petri nets. Fuzzy Petri nets

represent imprecise knowledge about the state of a system and allow the description of imprecise event and action rules. As a set of models of a fuzzy Petri net, it is expressed as follows  $N_f(P, T, D, \alpha, \beta)$  [1], here,

- $P \subset P_i$  for;  $(i = 1, i \leq n, i++)$  – set of finite position
- $T \subset T_i$  for;  $(i = 1, i \leq m, i++)$  – set of finite transitions
- $D \subset D_i$  for  $(i = 1, i \leq j, i++)$  – the last set of transitions
- $P = \{T: (T, P) \in f\} \cup P = \{T: (P, T) \in f\}$  – unwanted reflection;
- $T = \{P: (P, T) \in f\} \cup T = \{P: (P, T) \in f\}$  – outgoing reflection;
- $f \Rightarrow [0,1]$  – reflect associations [2];
- $\alpha: P \rightarrow [0,1]$ ;
- $\beta: P \rightarrow D$ ;
- $P \cap T \cap D = \phi \quad |P| = |D|$ .

Represented by the value of the token  $\alpha(p_i) \in [0,1]$  in position  $p_i \in P$ .

Fuzzy Petri nets are suitable for modeling parallel distributed systems where regulated information flows are important, and for inter-network screens that implement access control policies on network packets [3]. Therefore, it is appropriate to use the fuzzy Petri net for risk detection in network packet rules.

Fig. 4.1 Filter performance based on fuzzy Petri netA two-level fuzzy packet filtering architecture is proposed.

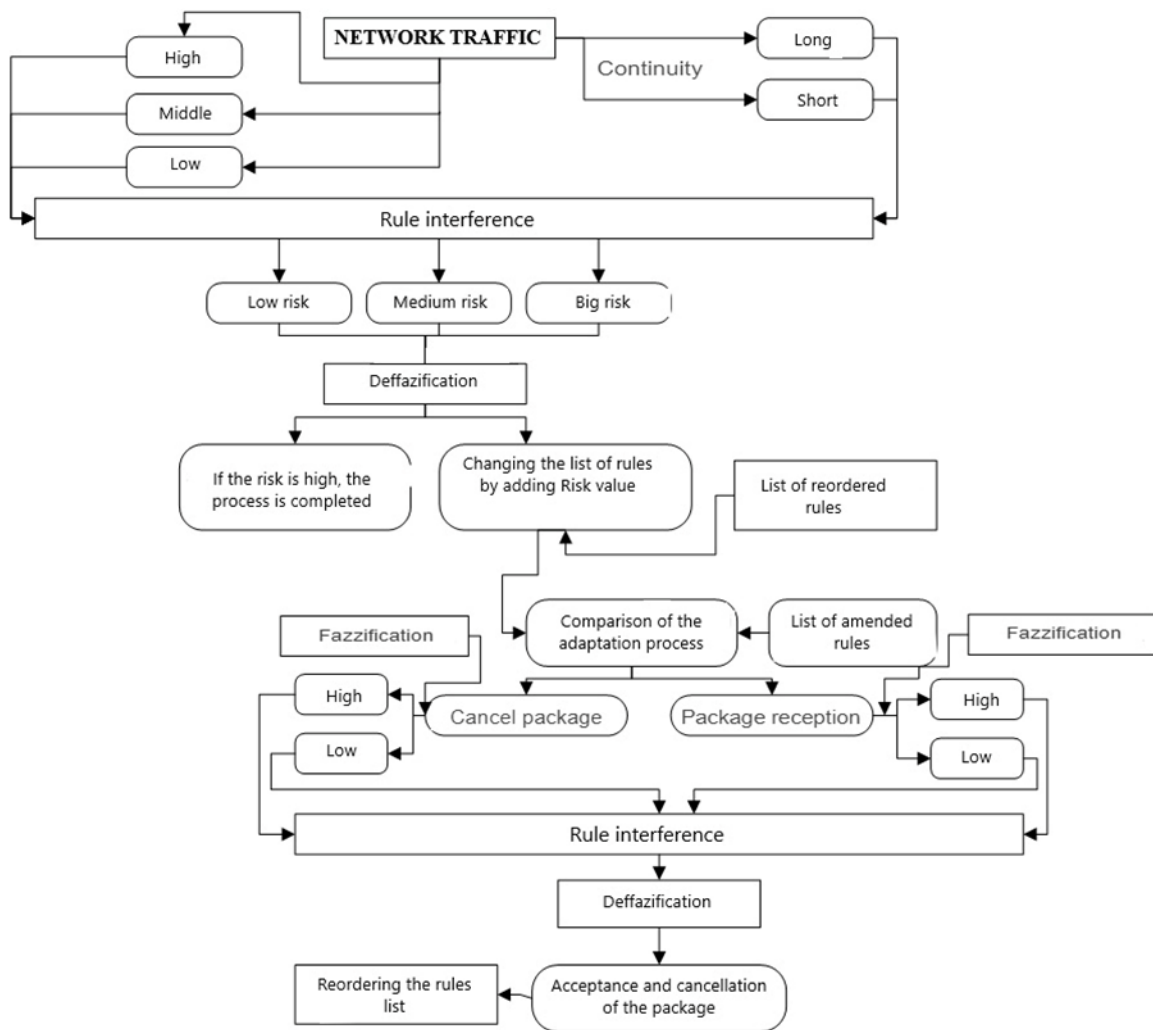


Fig. 1. Two-level fuzzy packet filtering architecture

The proposed architecture uses a fuzzy Petri net as a graphical method to describe the fuzzy logic control

of packet traffic through an inter-network screen. The following two levels of ambiguity are applied to filtering packets:

- the first level allows to determine the level of possible threat to packets from the Internet;
- the second level is used to reorder the ACL by determining the packet acceptance and discard rates.

*First level: fuzzy filtering.* This level is based on capturing and classifying all incoming packets based on packet related information such as IP address, packet time and protocol type, impersonation and packet tracking. A packet is represented by a token through a fuzzy Petri net, and a fuzzy Petri net is responsible for the processing of the packet, moving it from one place to another.

After the packet is intercepted by the gateway, it is moved to the location where it is inspected and matched with the ACL, in addition, a snapshot of this packet is moved to the traffic analysis part to extract the parameters of the packet, for example, the IP that arrived after a certain time or the number of ICMP protocol packets. These two parameters are fed into a fuzzy logic engine, which is used to determine the level of risk. This risk level represents the threats posed by the transfer of packets from untrusted sources. It is well known that IP and ICMP protocols are used in many stages of hacker advancement in system hacking. In addition, IP and ICMP protocols are sometimes used as a hidden communication channel for attackers. This layer can also deal with attack methods using other protocols such as TCP SYN and UDP Flood [4]. UDP protocol flooding occurs when an attacker sends IP packets containing UDP datagrams to slow down the victim to the point where it cannot handle real connections. A characteristic feature of SYN-Flood attacks is that attackers send a large number of TCP SYN request packets with a fake source IP address. This causes the server side to consume too many resources to maintain a very large list of open connections, resulting in the server running out of resources and unable to provide normal services.



Figure 2. Block diagram of packet filtering rule algorithm (first level: fuzzy filtering)

$p_{echo}$  – The rationale for choosing the ICMP echo request packet count and  $p_{time}$  – packet arrival time

interval is that they are simple and suitable for most attack protection situations, especially when the number of whole packets is large. To meet the membership degree function (MDF) requirements used in the proposed fuzzy logic, the feature vectors are scaled by Gaussian normalization method, i.e., in the range [0,1]. Fuzzy logic is the most efficient and flexible way to filter packets, and it allows you to control the combination of measurements according to their degree of ambiguity. The fuzzy logic system consists of the following functions:

- A fuzzifier that receives input values through MDF and determines their degree of belonging to each fuzzy set;
- fuzzy inference system, which determines the non-linear mapping of input data vector to scalar inference using fuzzy rules;
- a defuzzifier that maps the output fuzzy sets to a precise number.

Thus, using fuzzy logic with two inputs and one output given:

$$f: U \subset \bigcup_{i=1}^n (R_i \cap V),$$

here,

$U = U_1 \times U_2$  –incoming space;

$V$  –outgoing space;

$R$  –risk level.

$p_{echo}$  three fuzzy low, medium and high variables are used to describe the characteristics and  $p_{time}$  two fuzzy long and short variables are used to describe the function. All MDF parameters are provided to assess the level of risk caused by packet filtering. When the system has vague descriptions of the characteristics of the packets, it begins to build a rule base to determine their similarity. Fuzzy reasoning represents the presence or absence of relationships or degrees of interaction between two or more set elements formed by a group of If-Then rules. Figure 2 presents a block diagram of the algorithm of packet filtering rules (first level: fuzzy filtering).

Fuzzy logic processes all cases in parallel, which in turn allows you to make the right decision. The result of the fuzzy logic is the  $r_l$  risk level, which describes the risk inherent in packet filtering.

*Second level: fuzzy filtering.* Typically, each interface has two sets of packets associated with it: a set of packets accepted by the interface and a set of packets discarded by the interface. Figure 3 presents a block diagram of the algorithm of packet filtering rules (second level: fuzzy filtering).

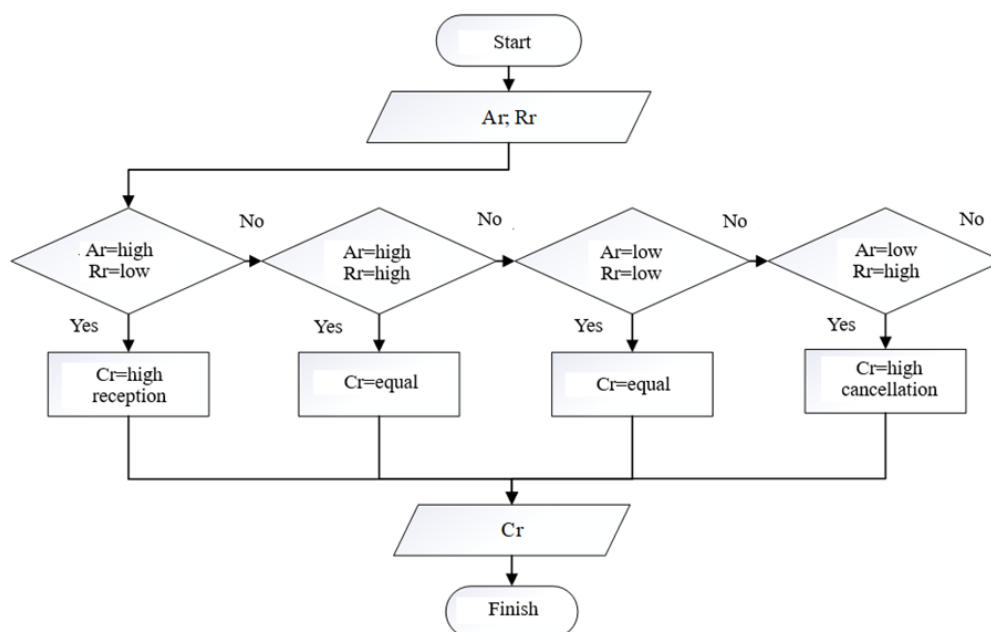


Figure 3. Block diagram of packet filtering rule algorithm (second level: fuzzy filtering)

This algorithm uses packet filtering by applying second-level fuzzy filtering to monitor the rate of packet acceptance or rejection while minimizing the rule-matching time. Here, the ambiguity in the rate of receiving or discarding packets using a fuzzy scheme is reflected [5]. In this case, fuzzy logic with two inputs and one output is used. Network packet acceptance rate  $A_r$  and discard rate  $R_r$  two fuzzy variables, including low and high, are used to describe. The output of fuzzy logic is a calculated quantity that describes the  $C_r$  rate of cancellation or acceptance in traffic, and is characterized by three fuzzy variables, i.e., high cancellation, equal, and high acceptance.

The output fuzzy values are defuzzified to generate the precise value of the variables. Here, if  $C_r =$  there is a high admission rate, then all rules that have a permit action are reordered and moved to the top of the ACL with the highest priority to execute. Otherwise, if  $C_r =$  there is a high cancellation rate, then the ACL rules with the highest priority will be moved to the beginning to execute all the rules with the cancellation action, and the resulting ACL with the acceptance action will stabilize at the end of the rules.

## **CONCLUSION**

Based on the Fuzzy Petri net proposed two-level fuzzy packet filtering architecture and algorithms allow to change rule actions according to traffic behavior based on information security risk levels and minimize risks in network packets.

In summary, two-level non-linear packet filtering algorithms based on the Petri network allow changing rule actions in packets according to traffic behavior, minimizing risks in network packets, and reflecting the highest rule of thumb when accepting and rejecting network packets.

## **ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## **REFERENCES**

1. И.Ю. Терёхина, А.А. Грушо, Е.Е. Тимонина, С.Я. Шоргин, Построение моделей процесса с помощью простых сетей Петри, Системы и средства информ., 2020, том 30, выпуск 4, – С.61–75
2. Саидахмедов Ш.Х. Модели поведения передачи данных с установлением соединения и их математические формы. РИ, 1999, №4. –С.94–96
3. Гуломов Ш.Р., Шамшиева Б.М. Моделирование атак для активного анализа уязвимостей компьютерных сетей. “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари” Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – С.112-116
4. Гуломов Шерзод Ражабоевич. Применение математических моделей для оценки Flood атак. “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари” Республика миқёсидаги илмий-техник конференция. Тошкент-2018. – С.300-304
5. Sh.R.Gulomov. Risk detection model in packet filtering rules based on Fuzzy Petri Net. “Technical science and Innovation Journal”, 2021, №3. – P.181-189

## CYBER WEAPONS AND NATION-STATES: THREATS AND RISKS

Dr. Nato Jiadze

Officer retired, MoD of Georgia, Invited lecturer at the Caucasus University  
email: [jiadzenatalia@gmail.com](mailto:jiadzenatalia@gmail.com), [njiadze@cu.edu.ge](mailto:njiadze@cu.edu.ge), [njiadze@mod.gov.ge](mailto:njiadze@mod.gov.ge)

**ABSTRACT:** As the digital landscape evolves, cyber weapons have become pivotal tools for nation-states to assert dominance, engage in espionage, and conduct warfare. This article will explore the growing role of cyber weapons in state-sponsored operations, focusing on how these digital tools are used to disrupt critical infrastructure, compromise national security, and manipulate political landscapes. By examining recent case studies and analyzing the evolving tactics of nation-states in cyberspace, the presentation will highlight the key threats posed by cyber warfare. It will also address the different levels of nation-state attackers, the dual-use nature of cyber weapons, the role of cyber-arms manufacturers, and the challenges of attribution.

**KEYWORDS:** Cyber weapons, Nation-states, APT, Dual use cyber weapons, cyber Militia, cyber-arms manufacturers.

### INTRODUCTION:

The fundamental nature of national security threats has not changed, but cyberspace has introduced a new domain for conflict and warfare. It offers a delivery mechanism that amplifies the speed, stealth, precision, diffusion, and power of attacks. While activity in cyberspace does not automatically constitute a hybrid threat, cyber operations frequently complement other forms of harmful activity in hybrid scenarios.

Cyber interference consists of operations by state or non-state actors conducted in cyberspace. If this activity targets critical infrastructure, for instance, by cyber means to achieve political/military aims alongside other activity by an outside hostile actor – we have hybrid action. Cyber interference, in its priming phase, can effectively spy on and manipulate electronic and information systems. At this juncture, it would be premature to talk in terms of waging war. It is not possible at this point to know whether the activity will escalate into war.

Since the 1970s Information and Communication Technologies (ICTs) and digital technologies have become an increasingly crucial part of military command and control. The integration of digital technologies has allowed military operations to transform the defense industry, advances like smart weapons, real time battlefield management, network-centric solutions, superiority in air and outer space, and software-based solutions to ground troops all have key roles today.

### HOW HACKERS CHANGE STATECRAFTS

Today one of the primary ways governments shape geopolitics is by hacking other countries. Government hackers continually find ways to advance their states interests and hinder those of their adversaries. Cyber operations show up again and again in the sophisticated modern states playbook. Hackers wiretap, spy, alter, sabotage, disrupt, attack, manipulate, interfere, expose, steal and destabilize. Government hacking has evolved and accelerated over past two decades.

A hack is any means of subverting a system's rules in unintended ways. The tax code isn't computer code, but a series of complex formulas. It has vulnerabilities; we call them "loopholes." We call exploits "tax avoidance strategies." And there is an entire industry of "black hat" hackers intent on finding exploitable loopholes in the tax code. We call them accountants and tax attorneys. Hacking



underpin our society: from tax laws to financial markets to democracy. Powerful actors using hacking tools to bend our economic, political, and legal systems to their advantage. [1]

## GOVERNMENT CYBER THREATS AND CYBER-ARMS MANUFACTURERS

### Nation-state cyber threats can be categorized into three levels:

- **Advanced Persistent Threats (APTs):** Highly sophisticated, state-sponsored cyber units with extensive resources and expertise. Examples include APT29 (Russia) and APT41 (China).
- **Cyber-Arms Customers:** States that purchase cyber weapons from external manufacturers due to a lack of domestic capability.
- **Cyber Militias:** Non-state actors or patriotic hackers who support state objectives, often with plausible deniability.

### Advanced Persistent Threats (APTs)

APTs are typically nation-states with the capability to develop and deploy sophisticated cyber weapons. These countries possess the resources, expertise, and motivation to create their own tools and execute advanced cyber operations. While the list of such countries is debatable, it commonly includes the United States, the United Kingdom, Russia, China, Israel, North Korea, Iran, India, and, to a lesser extent, Argentina.

These nations engage in cyber activities that range from espionage to destructive attacks. APTs are often used for state-sponsored operations, targeting other countries to gain intelligence, disrupt critical systems, or achieve strategic objectives [2] [3].

Examples of notable cyber-attacks include:

- **2012:** The U.S. under President Obama, accelerated cyber operations against Iran[4].
- **2018:** Russian hackers compromised DNS-based systems, with WikiLeaks revealing sensitive information.
- **2020:** China was implicated in a massive breach of U.S. government data.
- **2013:** The NSA was caught spying on Brazil.
- **2021:** The United Arab Emirates (UAE) launched its own cyber operations.
- **2008:** Russia conducted cyber-attacks against Georgia.
- **2022:** Russia deployed destructive malware against Ukraine ahead of its invasion[3]

These cases highlight the dual nature of cyber-attacks: some are focused on espionage, while others aim to cause tangible destruction. A particularly striking example is the ongoing conflict between Russia and Ukraine. In 2022, Russia utilized destructive malware against Ukraine in the early stages of its invasion, causing significant disruption. Interestingly, this cyber campaign was more effective in creating chaos before the physical conflict began. However, the effectiveness of cyber-attacks tends to diminish during active warfare, where kinetic operations often take precedence.

### Cyber Militia

Some countries are not sophisticated enough to develop their own cyber weapons, so they purchase them from external sources. There is an entire industry of cyber arms manufacturers that produce and sell cyber weapons to nations that lack the in-house capability to create their own.

For example, in 2013, the Syrian Electronic Army used commercially available cyber weapons to attack Sweden and several other countries. Interestingly, instead of relying solely on commercial

tools, they also used hacker tools from the dark web. They downloaded criminal hacking tools and repurposed them for national interests.

Countries like China use both Advanced Persistent Threats (APTs), which are highly organized and state-sponsored cyber units, as well as cyber militias. Russia also benefits from cyber militias and patriotic hackers—individuals or groups who voluntarily assist the government in cyber operations. These hackers often carry out attacks on behalf of the state, and Russia does not sanction them because they are serving the state's objectives.

In this way, cyber militias provide governments with a flexible, cost-effective way to engage in cyber operations while maintaining plausible deniability.

Sometimes they are patriotic hackers, Russia do not prosecute them because they do the states work. The other case is patriotic hackers help to Ukraine, there were involved about 4000 hackers to support Ukraine at the beginning of war-they hacked Russian Transport system and slowed down movement of troops and transport.

## CYBER ARMS MANUFACTURERS

Cyber-arms manufacturers are entities, often supported by their governments, that develop and distribute cyber weapons. These manufacturers are based in various countries, including Italy, Germany, the UK, and Israel. Interestingly, Israel has emerged as a prominent player in this domain. Israeli firms not only develop cyber tools for national security but also export these technologies as a tool of diplomacy, providing capabilities to other countries in exchange for political or strategic agreements.

Many of the products developed by these manufacturers are dual-use technologies, meaning they can be employed for legitimate purposes, such as surveillance and law enforcement, or for oppressive activities like censorship and political repression. For example:

- **FinSpy:** A surveillance tool used for monitoring individuals [5].
- **Pegasus:** A piece of spyware that has been used in both democratic and authoritarian states. While some governments, such as the FBI in the United States, use tools like Pegasus to track criminals, others, such as Uzbekistan, have employed it to suppress dissent [6]

Numerous documented cases highlight the misuse of Pegasus for attacks on journalists, activists, and opposition members.

Other products, such as Blue Coat Systems' tools, illustrate how seemingly legitimate security technologies can be misused. In Syria, for instance, Blue Coat tools have been deployed to censor the internet. Similarly, some police forces have used cyber tools for lawful criminal investigations while others have exploited them to spy on political parties, raising significant ethical concerns.

Compounding the problem, international restrictions on the sale of such tools can be circumvented by third-party transactions, allowing repressive regimes to acquire these technologies indirectly. This gray area makes regulating the industry particularly challenging, as it is often difficult to control who ultimately uses these products and for what purposes [7].

## CONCLUSION

Unchecked, cyber weapons pose significant risks to global stability. They threaten to destabilize financial markets, undermine democratic systems, and disrupt societal norms. As artificial intelligence begins to amplify these capabilities, the potential for catastrophic consequences grows. However, understanding the hacker mindset and leveraging defensive technologies can mitigate

these threats. By fostering international collaboration and strengthening cyber defenses, the global community can strive for a more secure digital future.

cyber weapons have become indispensable tools for nation-states to assert influence and achieve geopolitical goals. As cyberattacks continue to evolve, the line between peace and warfare is becoming increasingly blurred. Nation-states, cyber militias, and cyber arms manufacturers all play significant roles in this landscape, and the dual-use nature of cyber technologies makes it challenging to regulate their development and deployment. As the cyber arms race intensifies, understanding the tactics, threats, and risks associated with cyber warfare is essential for maintaining global stability and security.

## **ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## **REFERENCES**

- [1] Bruce Schneier - A Hacker's Mind. February 7, 2023.
- [2] David E. Sanger -Obama Order Sped Up Wave of Cyberattacks Against Iran June 1, 2012.
- [3] National Institute of Standards and Technology (NIST). "Advanced Persistent Threat Definition," 2011.
- [4] Nicolae. Sfetcu, Cyber Warfare: A Comprehensive Overview. Chapter: APT Definition, History, and Features
- [5] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton You Only Click Twice FinFisher's Global Proliferation, March 13, 2013
- [6] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert-Pegasus Spyware to Operations in 45 Countries, September 18, 2018
- [7] Ben Buchanan - The hacker and the state cyber-attacks and new normal of geopolitics

## APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

Joanna Kulesza, PhD

Assistant Professor, Department of Public International Law, University of Lodz Law School;  
Executive Director, Lodz Cyber Hub, University of Lodz, Poland.

**ABSTRACT:** This paper examines the evolving role of international law in cyberspace, with a focus on the contributions of the United Nations through its Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG). It analyzes key principles affirmed by the UN GGE, such as sovereignty, non-intervention, and due diligence, while highlighting challenges stemming from limited participation and divergent state views. The paper also explores the OEWG's broader approach to inclusivity and its efforts to address unresolved issues. Furthermore, it assesses the 2024 European Declaration on the Application of International Law in Cyberspace, emphasizing its role in complementing UN initiatives and strengthening global cyber governance. By bridging theoretical frameworks with actionable measures, the paper underscores the importance of multilateral cooperation in addressing cyber threats and advancing a rules-based international order in the digital age.

**KEYWORDS:** international law, cybersecurity, Internet governance, human rights, due diligence.

### INTERNATIONAL LAW IN CYBERSPACE: UN GGE, OEWG, AND THE EUROPEAN DECLARATION

The rapid evolution of cyberspace has posed significant challenges to the application of international law, requiring enhanced dialogue and collaboration among states and non-state actors. As the digital domain increasingly shapes global interactions, international institutions have become necessary to effectively address legal questions surrounding state behaviour in and governance of cyberspace. The establishment of norms and principles to govern this domain highlights the importance of balancing state sovereignty with collective security. In this context, the United Nations has played a vital role in advancing discussions on the applicability of international law to cyberspace, fostering multilateral cooperation, multistakeholder governance and addressing complex global issues of security, responsibility and human rights.

Among its numerous initiatives, two platforms have played a key role: the Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG). The UN GGE, established in 2004, has made significant contributions, particularly through its 2013 and 2015 reports, which affirmed that existing international law, including the UN Charter, applies to cyberspace.<sup>1</sup> These reports also introduced foundational principles such as state sovereignty, non-intervention, and the peaceful settlement of disputes in the digital domain. However, the GGE's limited membership and difficulty achieving consensus have underscored challenges in addressing diverse state perspectives.

To overcome these limitations, the OEWG was established in 2018, offering a more inclusive platform for dialogue among all UN member states. Its broader participation aimed to address contentious issues left unresolved by the GGE, including interpretations of sovereignty and the principle of due diligence in cyberspace. Despite these efforts, divergent views among states persist, particularly concerning the extent of state responsibility for cyber operations and how international law should evolve to address emerging cyber threats.

The European Council Declaration on a Common Understanding of International Law in Cyberspace complements similar efforts of individual states and those of the UN by providing clarity and reinforcing

---

<sup>1</sup> See respectively: UN GGE 2013 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013). Available at: <https://digitallibrary.un.org/record/752462>; UN GGE 2015 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015). Available at: <https://digitallibrary.un.org/record/799853>.

key legal principles in a vital geopolitical region.<sup>2</sup> Adopted in November 2024, the Declaration emphasizes state responsibility for cyber activities within their jurisdiction and highlights the applicability of sovereignty, non-intervention, and due diligence in cyberspace. By aligning with existing UN principles and frameworks, the Declaration strengthens the global legal regime governing state behaviour in cyberspace, addressing critical gaps and advancing collective understanding. It reflects Europe's commitment to fostering a rules-based international order while supporting ongoing multilateral discussions at the UN and complementary multistakeholder efforts in various Internet governance venues. Through its practical contributions, the Declaration bridges theoretical principles with actionable measures, setting a benchmark for responsible state behaviour in the digital age.

### **SHIFT TO INFRASTRUCTURES IN INTERNET GOVERNANCE AND RESPONSIBLE STATE BEHAVIOUR**

The focus of internet governance has evolved significantly within the UN and in its members states since the adoption of the 2005 Tunis Agenda approved by the World Summit on the Information Society (WSIS), shifting from the establishment of normative frameworks toward the protection of critical infrastructures such as undersea cables and satellites. These infrastructures form the backbone of global connectivity, with undersea cables handling over 95% of international data traffic and satellites supporting a wide range of services, from communications to navigation. As cyberspace increasingly integrates terrestrial and orbital systems, the complexity of protecting this hybrid infrastructure grows, amplifying the need for effective governance and technical measures.

Under international law, states bear responsibilities to protect cyber infrastructure within their jurisdiction and ensure its resilience against attacks. These obligations stem from principles such as sovereignty and due diligence. Recent incidents, such as the severing of undersea cables disrupting internet access in regions like Northern Europe, and reports of satellite cyberattacks targeting communication networks, highlight the vulnerabilities of these systems. Such incidents not only compromise connectivity but also pose risks to national security, economic stability, and humanitarian operations.

Addressing these challenges requires collaboration across sectors and between various stakeholder groups. Public-private partnerships are particularly vital, as much of the critical infrastructure is owned and operated by private entities. The multistakeholder approach to Internet governance complements existing international law frameworks and brings together governments, corporations, technical experts, and civil society to ensure comprehensive policies and avoid fragmentation. These include setting technical standards for infrastructure security, implementing state policies that mandate protection, and fostering international agreements to manage shared vulnerabilities. Integrating these efforts into existing internet governance mechanisms strengthens the resilience of the digital ecosystem, emphasizing that securing infrastructure is as crucial as establishing norms. By prioritizing infrastructure security alongside legal frameworks, the international community can better safeguard the foundations of the interconnected world.

### **THE EUROPEAN DECLARATION ON INTERNATIONAL LAW IN CYBERSPACE**

The recent European Declaration on a Common Understanding of International Law in Cyberspace, adopted by the Council of the European Union on November 18, 2024, represents a landmark for a shared regional understanding of legal norms for state behaviour in cyberspace. The Declaration draws heavily from established international frameworks, notably the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), reinforcing principles such as the attribution of wrongful acts and the conditions under which states may respond

---

<sup>2</sup> European Council, "Declaration on a Common Understanding of International Law in Cyberspace," Brussels, November 18, 2024, Document 15833/24, CYBER 334, COJUR 111, COPS 622.

to cyber operations. It stipulates that states are responsible for the actions of their organs and, under Articles 8 and 11 of ARSIWA, may also be held accountable for non-state actors acting under their instruction or whose actions they adopt as their own. The Declaration emphasizes discretion in whether to disclose attribution publicly or keep it confidential, balancing transparency and operational security.

In addressing responses to cyber incidents, the Declaration categorizes permissible actions into peaceful dispute resolution, retorsions, and measures under specific exceptions to wrongfulness, such as self-defense and countermeasures. Peaceful means remain paramount, aligning with Articles 2(3) and 33(1) of the UN Charter. At the same time, it recognizes retorsions, such as economic or diplomatic sanctions, as legitimate tools that do not breach international law. This nuanced framework reflects the EU's commitment to a stable, rules-based international order in cyberspace, linking existing legal principles to the realities of modern digital infrastructure.

By adopting this Declaration, the EU solidifies its role as a normative leader in cyberspace governance. It builds upon previous international consensus, such as the work of the UN GGE and the OEWG, while promoting practical guidance for state behaviour. Its implementation could enhance global cyber stability and set a model for broader international cooperation.

The European Declaration also underlines key principles of sovereignty, self-defence, and due diligence in cyberspace, affirming the need for state responsibility and liability. It explicitly addresses the responsibility of states for cyber operations originating within their jurisdiction, reinforcing that states must not allow their territories to be used for activities that breach international peace or security.

In terms of its impact on EU cyber diplomacy, the Declaration strengthens Europe's collective stance on cybersecurity and legal cooperation, fostering unified responses to cyber threats. It positions the EU as a leader in advocating for a rules-based international order in cyberspace, promoting collaboration between member states and external partners to enhance cybersecurity resilience. This approach strengthens law enforcement cooperation and shows the EU's commitment to a safe, stable, and accountable cyber environment.

## **CONCLUSIONS AND RECOMMENDATIONS**

The evolving discourse on international law in cyberspace highlights its critical relevance in shaping responsible state behaviour and securing digital infrastructures. The European Declaration follows the path set by the UN GGE and the OEWG, numerous national positions on the application of international law in cyberspace, and the African Union one adopted earlier in 2024. It exemplifies a significant step toward harmonizing global perspectives. It reaffirms the applicability of established international law, emphasizing principles such as sovereignty, state responsibility, and due diligence, while promoting peaceful resolutions to disputes. Its alignment with multilateral frameworks and emphasis on practical state accountability strengthens the global cybersecurity architecture.

To ensure the effective implementation of these principles, several recommendations should be made. First, global adherence to agreed norms should be promoted through capacity-building initiatives and widespread educational programs. These efforts can help states, particularly those with limited resources, to internalize and operationalize the legal frameworks and technical safeguards necessary for cyberspace governance. Second, states should be encouraged to adopt transparent policies, which include effective incident reporting mechanisms. Such transparency builds trust, enhances accountability, and facilitates timely responses to cyber incidents. Finally, fostering research into vulnerabilities of critical infrastructures, such as undersea cables and satellites, is essential. Coordinated international efforts to develop protocols for managing cyber risks and responding to attacks will ensure the resilience of global connectivity.

It is recommended for states to prioritize the implementation of the confidence-building measures (CBMs) established by the UN Group of Governmental Experts to promote trust and prevent conflicts

in cyberspace. These measures, including information-sharing, establishing points of contact, and promoting transparency in cyber operations, play a critical role in reducing risks of misperception and escalation. Adherence to CBMs fosters collaboration, enhances mutual understanding, and strengthens international stability in the digital domain. By committing to these practices, states can support a secure and predictable cyber environment, reinforcing the broader framework of international law and contributing to peaceful interactions in an increasingly interconnected world.

#### **ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

#### **REFERENCES**

1. UN GGE 2013 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013). Available at: <https://digitallibrary.un.org/record/752462>;
2. UN GGE 2015 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015). Available at: <https://digitallibrary.un.org/record/799853>
3. European Council, "Declaration on a Common Understanding of International Law in Cyberspace," Brussels, November 18, 2024, Document 15833/24, CYBER 334, COJUR 111, COPS 622.

## CHALLENGES OF IMPLEMENTING THE PAYMENT CARD DATA SECURITY STANDARD (PCI DSS) IN PRACTICE

Audrius Lopata, Kaunas University of Technology  
audrius.lopata@ktu.lt

**ABSTRACT:** The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem. Challenges of Implementing the Payment Card Data Security Standard (PCI DSS) in Practice presented in this article

**KEYWORDS:** *PCI DSS, Cyber security, Payment Gateways, Security standards*

### BRIEF SUMMARY ABOUT PCI DSS STANDARD

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework designed to secure payment card data handling. It was established by the Payment Card Industry Security Standards Council (PCI SSC), comprising major credit card companies like Visa, MasterCard, American Express, Discover, and JCB. The standard applies to all entities involved in card payment processing, including merchants, processors, and service providers.

Key goals of PCI DSS include:

1. Protect Cardholder Data: Safeguarding sensitive data, such as card numbers and security codes, through encryption and secure storage.
2. Implement Strong Access Controls: Restricting access to cardholder data to authorized personnel only.
3. Maintain a Secure Network: Ensuring robust firewall configurations and secure network protocols.
4. Regular Monitoring and Testing: Conducting routine audits, vulnerability scans, and penetration testing to identify and mitigate risks.
5. Develop a Security Policy: Promoting a security-conscious culture through documented policies and employee training.

The standard is divided into 12 key requirements covering areas like network security, vulnerability management, and monitoring. Compliance is mandatory for businesses handling payment cards and is enforced through audits and penalties. By adhering to PCI DSS, organizations can mitigate risks of fraud, data breaches, and financial loss while ensuring customer trust.

### PCI DSS COMPLIANCE LEVELS

These levels categorize businesses based on the volume of annual payment card transactions. Below is a brief summary of these compliance levels:

Level 1: For businesses processing over 6 million transactions annually or those that have experienced data breaches. This level has the most rigorous requirements, including an annual audit by a Qualified Security Assessor (QSA) and quarterly network scans.

Level 2: For businesses processing 1 to 6 million transactions annually. They typically need to complete a self-assessment questionnaire (SAQ) and conduct quarterly network scans.

Level 3: For businesses processing 20,000 to 1 million e-commerce transactions annually. They also complete a self-assessment questionnaire and perform quarterly scans.

Level 4: For businesses processing fewer than 20,000 e-commerce transactions annually or up to 1 million other payment card transactions annually. This level has the least stringent requirements but still includes completing an SAQ and conducting quarterly scans.



## **PCI DSS – 5 MOST COMMONLY OBSERVED CONTROL FAILURES**

### **Challenge No.1**

It is of utmost importance for businesses dealing with cardholders' data to be aware of the locations where the data resides. However, most businesses have failed to do so only because a lot of payments card data remains unmanaged and uncategorized, dispersed across multiple databases of an enterprise. Proposed Solution:

To meet this PCI DSS compliance control, businesses must map the business systems through which the cardholder data enters the organization and leaves all the way through.

To establish a diagram that shows how cardholder data flows across systems and networks, businesses can depict the cardholder data environment, devices and systems with all payment channels, applications and associated protections on CHD based on locations, using a labelling method for identifying the transport mechanism and crucial dependencies.

### **Challenge No.2**

Many businesses even though have established security policies, they fail to maintain the same that open multiple vulnerabilities in the payments lifecycles.

This has been noticed to happen with companies that have documented and published a security policy for the PCI DSS compliance requirement but have not actually used them.

Proposed Solution:

When creating a security policy for the PCI DSS compliance requirements, the organizational design must be brought into work. First and foremost, create a policy to address every requirement of PCI DSS and ensure that it is structured to match the order and language of the PCI DSS sub requirements.

Moreover, businesses must review and update at least annually to effectively maintain the security policy.

### **Challenge No.3**

Tracking card data is directly proportional to tracking the people that process and store it.

However, most of the businesses attempting to comply to PCI DSS compliance requirements fail due to this important control. It happens only because companies do not track the devices well.

Proposed Solution:

Assurance and operations members of risk and compliance teams must update the device lists with changing employees. The best solution to tackle this PCI DSS control is to maintain an accurate inventory with proper labelling and set a shorter frequency for updating the list with 4 columns – device, employee, data type, and access type.

### **Challenge No.4**

Off-the-shelf security incident response plans remain outdated and ineffective against the ever-changing threat landscape. For compliance analysts and managers, verification of plans only goes so far.

Each year, SISA performs hundreds of incident response exercises across the globe.

During these engagements, we have observed incident response plan failures mostly because of organizational shortcomings that form a major part of the PCI DSS requirements. Failing to plan means planning to fail.

Proposed Solution:

Businesses opting to verify their incident response plans for PCI DSS compliance must simulate a real-world attack every 6 months and assess how key stakeholders respond to it.

Operational security teams must, in such events, document issues and lessons against specific scenarios of PCI DSS incident response requirements including organizational coordination, business recovery, data backup, and analysis of legal requirements.

### **Challenge No.5**

All data custodians and key management professionals that give access to data based on a business' need to know must be solely responsible to monitor the access hygiene.. However, businesses ignore

the importance of bestowing this responsibility to an individual with formal accountabilities. This has become crucial ever since remote working has increased as companies aren't able to ensure that the type of access given is appropriate and all technical safeguards are in place for data access.

Proposed Solution:

A data security specialist with a straight-line reporting to the executive authority of the firm (CIOs, CISOs, Information Security Managers, Chief Data Officers, Risk and Compliance Managers, etc.) must be nominated for such responsibilities. QSAs at SISA recommend such professionals to implement privileged access management and update the data access charts on a monthly basis.

## **MAIN RECOMMENDATIONS HOW TO SUCCESSFULLY IMPLEMENT THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)**

### **Understand PCI DSS Requirements**

Familiarize with PCI DSS version: Ensure that you are working with the most current version of PCI DSS (as of 2024, it's v4.0).

Identify scope: Understand which systems, processes, and personnel are involved in the storage, processing, or transmission of cardholder data.

Review the 12 PCI DSS requirements: These include securing network systems, protecting cardholder data, maintaining a vulnerability management program, and monitoring network access.

### **Scope and Segmentation**

Define scope: Identify all locations where cardholder data is stored, processed, or transmitted. This includes all systems that can affect the security of the cardholder data environment (CDE).

Network segmentation: Implement network segmentation to isolate systems that handle cardholder data from other parts of your network, reducing the compliance scope.

### **Create a PCI DSS Compliance Team**

Appoint a compliance manager/team: A dedicated team should oversee the implementation of PCI DSS standards.

Cross-functional collaboration: Include members from IT, security, legal, and operations to ensure all areas are covered.

### **Data Protection Measures**

Encryption: Ensure sensitive cardholder data is encrypted both in transit (e.g., SSL/TLS for web traffic) and at rest (e.g., disk encryption).

Masking and truncation: Mask PAN (Primary Account Number) where necessary and store only the minimal necessary information.

Secure storage: Avoid storing sensitive authentication data (e.g., CVV, magnetic stripe) after authorization unless absolutely necessary.

### **Access Control**

Limit access to cardholder data: implement strong access control measures, ensuring only authorized personnel can access the cardholder data environment (CDE).

Role-based access: Enforce role-based access control (RBAC) with the principle of least privilege.

Two-factor authentication: Use multi-factor authentication (MFA) for personnel accessing critical systems.

### **Regular security testing**

Vulnerability scanning: Conduct regular internal and external vulnerability scans.

Penetration testing: Perform annual penetration testing to identify vulnerabilities in the systems.

Application security testing: Ensure secure software development practices by conducting code reviews and application vulnerability testing.

**Monitoring and logging:**

Log management: Implement logging mechanisms to track access to network resources and cardholder data.

Intrusion detection and monitoring: Utilize tools to monitor network traffic and alert administrators of suspicious activities.

Retain logs: Store logs for at least one year, with the last three months available for immediate review.

**Regular Audits and Assessments**

Self-assessment questionnaire (SAQ): Smaller merchants may be required to complete an SAQ annually.

Qualified Security Assessor (QSA) audit: For larger organizations, hire an external QSA to perform annual assessments and provide formal validation.

Gap analysis: Conduct a gap analysis to identify areas that need improvement before formal audits.

**Employee training and awareness**

Security awareness training: Provide regular training on PCI DSS requirements, phishing, and secure handling of cardholder data.

Incident response training: Ensure that personnel are familiar with the organisation’s incident response procedures in case of a security breach.

**Incident Response Plan**

Develop a plan: Establish an incident response plan for handling security breaches that involve cardholder data.

Test regularly: Regularly test and update the incident response plan to ensure effectiveness.

Notify stakeholders: Have a communication plan to notify necessary stakeholders, including banks, card brands, and customers, in the event of a breach.

**CONCLUSIONS**

The implementation of the Payment Card Industry Data Security Standard (PCI DSS) is essential for businesses handling payment card data to ensure its security and maintain customer trust. While the framework provides robust guidelines for safeguarding cardholder data, its practical application poses significant challenges, such as identifying data locations, maintaining effective security policies, tracking data and devices, updating incident response plans, and ensuring proper access controls. Addressing these challenges requires comprehensive strategies, such as mapping data flows, creating and maintaining security policies, appointing dedicated compliance teams, and leveraging advanced tools for encryption, logging, and monitoring.

Successful PCI DSS implementation involves a clear understanding of requirements, proper scoping and segmentation, regular testing and audits, and fostering a culture of security awareness. Organizations must also invest in employee training, simulate real-world scenarios for incident response, and establish effective collaboration across departments. With these measures, businesses can overcome the hurdles of PCI DSS compliance, enhance their security posture, and reduce the risk of fraud or data breaches, thereby safeguarding both the business and its customers.

**ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

**REFERENCES:**

1. Stephen Hancock, PCI DSS Version 4.0 - A guide to the payment card industry data security standard. Released February 2024. Publisher(s): IT Governance Publishing, ISBN: 9781787785090

2. Arthur B. Cooper Jr. (Author), Jeff Hall (Author), David Mundhenk (Author), Ben Rothke (Author). The Definitive Guide to PCI DSS Version 4: Documentation, Compliance, and Management 1st ed. Edition
3. Chad M. Barr (Author). Fortifying The Digital Castle: A Strategic Guide to PCI DSS Compliance and Cyber Defense Kindle Edition 2024
4. Branden Williams (Author), James Adamson (Author) PCI Compliance 5th Branden Williams (Author), James Adamson (Author) Publisher: CRC Press; 5th edition (December 22, 2022). ISBN-13:978-0367570033
5. PCI DSS: A pocket guide (Compliance) 6th Edition by IT Governance (Editor) 2019, ISBN-13 : 978-1787781627
6. Bharat Nishad, PCI DSS Compliance Masterclass - Foundation to Mastery, ASIN : B0CWPPGPQS, Publisher : Bharat Nishad (February 26, 2024).
7. PCI Compliance A Complete Guide - 2021 Edition Paperback – December 17, 2020 by The Art of Service - PCI Compliance Publishing (Author), ISBN-13: 978-1867414933
8. ENYINAYA OKAFOR, The Plague Of Cyber Threats In The Financial Industry: PCI-DSS COMPLIANCE Kindle Edition, February 29, 2024, ASIN : B0CW1HM6JR

## THE ROLE OF 5G/6G CELLULAR NETWORK TECHNOLOGIES IN ACHIEVING THE GOALS OF SUSTAINABLE DEVELOPMENT

Roman Odarchenko<sup>1</sup>, Oleh Polihenko<sup>1</sup>, Vladyslav Fesenko<sup>1</sup>, Maksym Riabenko<sup>1</sup>

<sup>1</sup>National aviation university, Kyiv, Ukraine

**ABSTRACT:** The main global goals of sustainable development of humanity by 2030 have been identified. It is obvious that information technologies can play one of the key roles in their successful achievement. In this context, within the framework of this work, the existing potential of cellular networks for the impact on the successful achievement of sustainable development goals was analyzed. The main domains where a significant contribution can be made through the use of mobile technologies were analyzed. But there are also risks that can have a negative impact on the achievement of global goals of sustainable development. The result of this study is also reflected in this article. And finally, the potential of the introduction of modern cellular networks within countries with developing economies was demonstrated.

**KEYWORDS:** *Sustainable Development, Cellular Network, 5G, 6G, New Technologies, SDG*

### INTRODUCTION

The United Nation's Sustainable Development Goals (SDGs) are a universal call to achieve a sustainable future and promote equality, human rights, and justice for all by 2030 [1 Adopted by UN Member States in 2015, the 2030 Agenda for Sustainable Development provides a shared strategy for peace and prosperity for all people and our planet, now and into the future. The SDGs are a collection of 17 interlinked goals designed to guide reflection and action on the most pressing challenges and opportunities facing humanity and the natural world, including inequalities (SDG 10), climate change (SDG 13), peace and justice (SDG 16), and global cooperation to meet global targets (SDG 17). These goals and their targets acknowledge that ending poverty and other deprivations must go hand-in-hand with strategies that improve health and education, social inequalities, and economic disparities—all while tackling climate change and working to preserve our natural surroundings.

The SDGs establish a blueprint for global citizens to work together to build a better world, for it is only by working collectively—across borders and disciplines and with community partners—that these goals might be achieved. Through research, teaching and learning, community engagement, and global collaborations, IU Indianapolis is playing a leading role in tackling the SDGs and achieving the 2030 Agenda.



Fig. 1. Global goals of sustainable development [1]

## MOBILE NETWORKS DEVELOPMENT

In order to achieve the global goals of sustainable development, it is necessary to use all available high-tech tools, which to one degree or another will bring the world community closer to the realization of the most ambitious ideas for global well-being. The potential contribution of the ICT industry to achieving the goals of sustainable development should be noted separately.

According to a research paper by Ericsson [3] on the potential of ICT to reduce greenhouse gas emissions, the ICT sector has the potential to reduce total industrial emissions worldwide by up to 15%, although it accounts for only 1.4% of the global carbon footprint. The study highlights the importance of 5G as a key building block for a future Net Zero [4].

One of the key drivers of the development of the ICT industry is cellular networks. They are developing at a very rapid pace and this is evidenced by a number of studies and the results of the analysis of the subscriber base (Fig. 2).

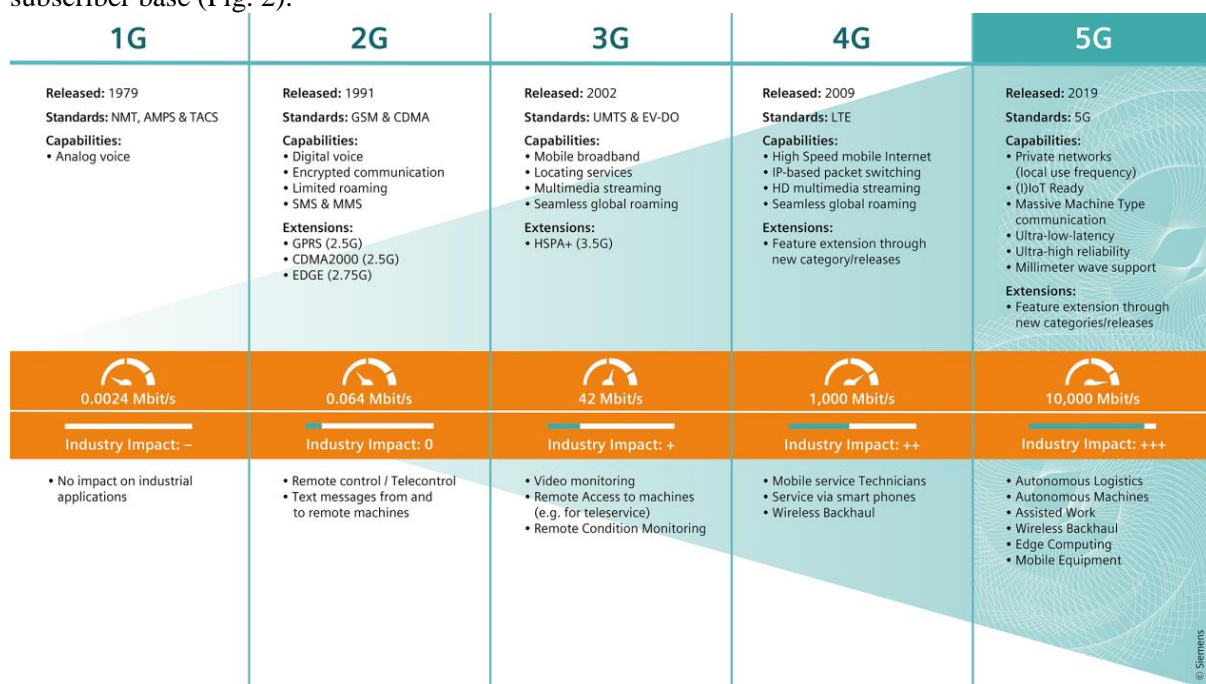


Fig. 2. Cellular networks evolution [3]

## POTENTIAL OF MOBILE NETWORKING IN ACHIEVING THE SDGs AND POTENTIAL RISKS

Thus, the latest cellular network technologies can also make a significant contribution to achieving sustainable development goals. The main areas in which mobile technologies can make a contribution are discussed below.

**Ultra-Low Latency.** Both 5G and 6G networks are designed to offer incredibly low latency, which is crucial for real-time applications. This feature supports innovations in healthcare (remote surgeries), transportation (autonomous vehicles), and smart grids for efficient energy management.

**Massive Connectivity.** 5G enables the connection of billions of IoT devices globally, paving the way for smart cities, smart agriculture, and smart industries, all of which contribute to more sustainable practices by optimizing resources and reducing waste.

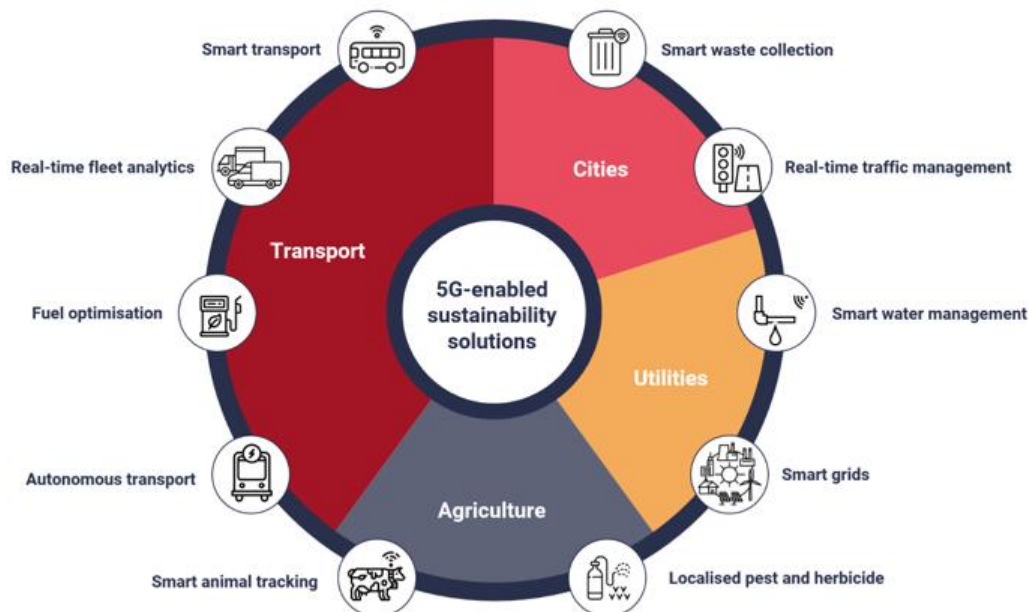
**Energy Efficiency.** 5G and future 6G networks are designed to reduce energy consumption through more efficient data transmission and smarter infrastructure, contributing to a reduction in the global carbon footprint.

**Enhanced Network Reliability and Speed.** These networks ensure reliable, high-speed connectivity, which can drive digital inclusion by enabling access to education, telemedicine, and other essential services, even in remote areas, supporting goals like quality education and health.

**Integration with Advanced Technologies.** 5G/6G will integrate with AI, edge computing, and blockchain to enable innovations like predictive maintenance in industries, smart environmental monitoring systems, and secure data sharing for sustainable development initiatives.

The latest generation of mobile radio communication networks today are 5G networks. However, the benefits of 5G are not limited to the ICT sector. The technology represents an open innovation platform that serves a multitude of sustainable uses – from smart farms to smart factories – by improving automation, increasing productivity, increasing energy efficiency, conserving resources and increasing resilience to climate change. 5G can also contribute to the decarbonisation of the world's largest carbon-emitting sectors, namely energy, manufacturing and transport, by improving data sharing, optimizing systems and increasing operational efficiency, thereby accelerating global efforts to reduce carbon emissions.

In general, projecting the role of 5G on the process of achieving the goals of sustainable development, we can draw a conclusion about the opportunities that this technology opens up in various sectors of the economy (Fig. 3).

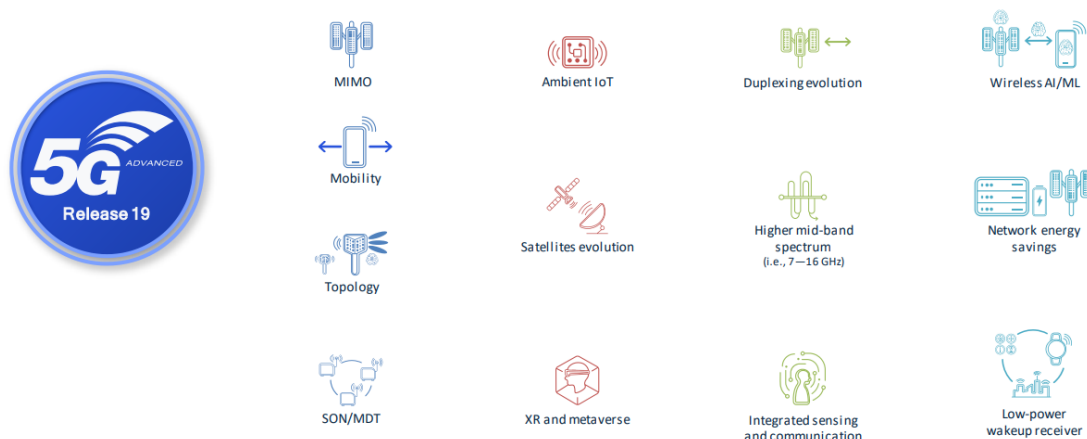


*Fig. 3. Contribution of 5G to achieving the goals of sustainable development [6]*

5G networks have more advanced features than networks of previous generations. They are equipped to handle large amounts of data with minimal latency (ultra-low latency) and support an extremely high density of connected devices (machine-type mass communication). This improved connectivity has unlocked a range of new 5G-enabled sustainability services that individuals, companies and governments can implement to reduce their carbon footprint and achieve other sustainability goals. But improved connectivity will also mean that more devices will be connected to the network, increasing the energy consumption of the network. Telecommunications companies and service users need to take immediate action to limit this environmental impact.

The environmental impact of 5G thus encompasses more energy-efficient network technology that helps telcos minimize their environmental impact, as well as enabling technology that telcos can use to help businesses, governments and consumers reduce their own environmental impact.

Along with this, cellular communication networks continue to develop at a rapid pace. Currently, development is underway to coordinate Release 19, which will have a significant number of new advanced technologies that will open the possibility of achieving the goals of sustainable development, including (Fig. 4).



*Fig. 4. Technological innovations in 5G Release 19*

But there are already many examples of using 5G to achieve the UN's sustainable development goals. Below are some of them.

Nokia and Elisa's 5G Liquid Cooling Station uses wasted energy from Elisa's networks to heat buildings and water. This allowed Elisa to reduce the energy consumption of its 5G networks by 30% and reduce overall CO<sub>2</sub> emissions by 80% [7].

Some operators use intelligent network software that allows base stations to turn off power depending on quiet times of day (such as at night) or periods of general low traffic. Such innovations are key to the telecommunications industry, which now produces c. 0.8% of all global emissions. We explored these topics in more detail in our report, *Why Power Management is Critical to 5G Success*.

e& is decarbonizing its network with sustainable 5G solutions. They plan to achieve this by partnering with Ericsson to implement changes such as RAN's intelligent energy-saving software features, as well as other initiatives such as its global product return program to increase recycling and responsible disposal of e-waste across e&'s network [8].

The Telia and Ericsson Autonomous Electric Bus solution relies on 5G network capabilities for live video positioning and prioritization [9]. During the trials, 5G control towers were used to remotely control buses and transmit real-time video to track journeys and ensure passenger safety. Automated vehicles enabled by 5G IoT technologies are more fuel-efficient than manual alternatives, reduce greenhouse gas emissions from public transport, make public transport more accessible and lower operating costs.

Proximus [10] solutions for weed and pest control use drones to capture images of agricultural plots and artificial intelligence to identify the nature of weeds or diseases in crops. Proximus provides 5G connectivity that allows data to be sent from the drone to the analytics platform. The analytics platform then creates a task map for a robot equipped with a torch (for weeds) or a pesticide sprayer (for pests or diseases). Instead of treating the entire field for pests or diseases, this allows farmers to treat only the affected areas. By 2030, European farmers will have to reduce their use of pesticides by 50%. In this test case, Proximus found that pesticide use could be reduced by 80%.

The City of Rotterdam's smart waste management system [] uses IoT sensors in bins and other waste disposal areas to monitor fill percentages. This data is transmitted via the KPN 5G LoRa network to a centralized control system that determines dynamic routes for waste collection vehicles. 165 dynamic waste collection routes replaced 203 static routes, resulting in a 20% reduction in vehicle kilometers driven for waste collection. In turn, this resulted in a 20% reduction in CO<sub>2</sub> emissions, as well as a 25% reduction in labor and equipment costs.

Thus, in summary, it can be argued that 5G and future 6G cellular network technologies have significant potential to promote sustainable development. Their high throughput, low latency and high scalability make them key tools for various initiatives to improve the quality of life and preserve the environment. With the help of 5G/6G technologies, it is possible to ensure efficient use of resources, develop the "Internet of Things" and "smart" systems, increase the availability of education and health services,



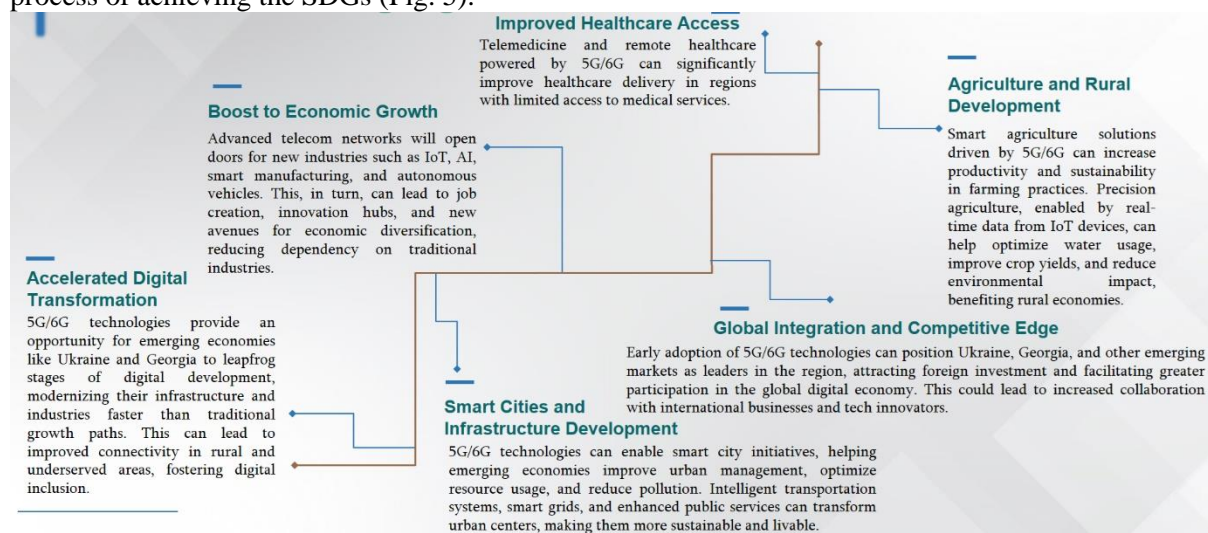
promote the development of remote work and mobility, and also increase the competitiveness of the economy. Therefore, the role of 5G/6G cellular network technologies in sustainable development cannot be overestimated. Their implementation and use open up new opportunities for creating more efficient, intelligent and ecologically clean communities.

But also with the introduction of new mobile network technologies, a number of risks also arise, presented in Table 1.

**Table.1.** Potential risks while introducing 5G/6G technologies for achieving the SDG

<b>High Energy Consumption and Environmental Impact</b>	While 5G/6G networks promise energy efficiency, the infrastructure deployment (like base stations and data centers) can consume substantial power. Without renewable energy sources, this may increase carbon emissions, counteracting the environmental benefits.
<b>Digital Divide</b>	The rapid rollout of 5G/6G may widen the gap between regions with access to advanced networks and those without, particularly in rural or underdeveloped areas. If not addressed, this digital divide can limit the global equity and inclusiveness intended by the SDGs.
<b>Cybersecurity Risks</b>	As 5G/6G expands the Internet of Things (IoT) and connects billions of devices, it also increases the potential for cyber-attacks. Ensuring robust cybersecurity measures is essential to prevent data breaches, identity theft, and other forms of cybercrime, which could undermine trust in digital solutions.
<b>Cost and Infrastructure Requirements</b>	The infrastructure needed to support 5G/6G networks, such as base stations and fiber-optic connections, is capital-intensive. For many countries, especially developing ones, the costs of implementation might be prohibitive, slowing down adoption and limiting the impact on sustainable development goals.
<b>Privacy Concerns</b>	With billions of connected devices gathering personal and industrial data, privacy concerns are heightened. There is a need for strong data governance policies to ensure that sensitive information is protected, and individuals' privacy rights are upheld.

But despite the risks presented above, mobile technologies can still have a significant impact on the process of achieving the SDGs (Fig. 5).



**Fig. 5.** The potential of using cellular networks to achieve sustainable development goals

## CONCLUSIONS

Considering this figure, the next conclusion can be drawn. In any case, there are a lot of opportunities for Ukraine, Georgia, and other emerging economies while developing the novel mobile network technologies.

5G/6G technologies offer immense opportunities to drive innovation, economic growth, and sustainability across industries and sectors. Their ability to improve connectivity, support smart cities, enhance healthcare, and enable efficient resource use aligns directly with the UN's Sustainable Development Goals (SDGs).

By connecting people, industries, and technologies, 5G/6G networks will serve as key enablers for addressing critical challenges like climate action, education inequality, and urbanization.

While 5G/6G bring significant benefits, challenges such as digital inequality, high energy consumption, and cybersecurity risks need to be addressed through policy, investment, and innovation.

Thus, to maximize the potential of 5G/6G, collaboration between governments, industries, and communities is essential to ensure that the technology is accessible, secure, and environmentally friendly.

## ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES

1. <https://sdgs.un.org/goals>
2. <https://business.dii.gov.ua/handbook/sustainable-development-goals/cili-stalogo-rozvitku>
3. <https://www.ericsson.com/en/reports-and-papers/research-papers/exploring-the-effects-of-ict-solutions-on-ghg-emissions-in-2030>
4. [https://www.ecohz.com/what-is-net-zero?utm\\_term=&utm\\_campaign=Net+Zero&utm\\_source=adwords&utm\\_medium=ppc&hsa\\_acc=4127008299&hsa\\_cam=15634661673&hsa\\_grp=132743177455&hsa\\_ad=575732957491&hsa\\_src=g&hsa\\_tgt=dsa-1649357561718&hsa\\_kw=&hsa\\_mt=&hsa\\_net=adwords&hsa\\_ver=3&gad\\_source=1&gclid=CjwKC-Ajw14yyBhAgEiwADSEjeMxAZ7dhls-buGITY1dC8ltdl8qY9Bfk0RTfSG4SonST4MhxfuHTRoCbdkQAvD\\_BwE](https://www.ecohz.com/what-is-net-zero?utm_term=&utm_campaign=Net+Zero&utm_source=adwords&utm_medium=ppc&hsa_acc=4127008299&hsa_cam=15634661673&hsa_grp=132743177455&hsa_ad=575732957491&hsa_src=g&hsa_tgt=dsa-1649357561718&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKC-Ajw14yyBhAgEiwADSEjeMxAZ7dhls-buGITY1dC8ltdl8qY9Bfk0RTfSG4SonST4MhxfuHTRoCbdkQAvD_BwE)
5. <https://www.quora.com/Which-is-the-largest-mobile-network-operator-in-the-world>
6. <https://stlpartners.com/articles/sustainability/5g-and-sustainability/>
7. <https://www.nokia.com/about-us/news/releases/2020/06/03/nokia-and-elisa-see-sustainability-leap-in-world-first-5g-liquid-cooling-deployment/>
8. <https://www.eand.com/en/news/7-dec-etisalat-by-eand-takes-significant-strides-toward-a-green-and-sustainable-network.html>
9. <https://www.teliacompany.com/en/news-articles/5g-powered-self-driving-electric-bus-propels-stockholm-into-the-future>
10. <https://proximus.com/news/2021/20210624-news-proximus-and-partners-demonstrate-weed-control-via-5g.html>
11. <https://cities-today.com/rotterdam-increases-efficiency-of-waste-collection/>

## STATE OF MEMORY SAFETY IN C++

René Pfeiffer

DeepSec GmbH / University of Applied Sciences Technikum Wien

**ABSTRACT:** The C++ programming language shares its ancestry with C, but it is a language on its own. Memory safety has always been a challenge, but recently government bodies addressed defects in software applications and recommended a strategy for securing memory access. The C++ standard started to adopt a security stance beginning with C++11. Later C++ specifications improved the language further. Modern C++ includes all features to develop memory-safe software applications provided the language specification C++11 and later is used.

**KEYWORDS:** *C++, memory safety, secure coding, C++ standards, information security, software development, data ownership, secure design*

### OVERCIEW OF MODERN C++

Modern C++ consists of the C++11 and all later language specifications (C++ standards). (Stroustrup et. al. 2015) The specifications eliminate ambiguities and clearly define how the language handles undefined behavior. Furthermore, the language features allow to track dynamic memory allocations by use of smart pointers and automatically deallocate memory blocks that go out of scope. These features require the cooperation of the developers, because the C++ constructs must be actively used. Smart pointers change the approach on how to implement memory operations. The new approach does not require the use of the operators *new[]* and *delete[]*. In fact, Modern C++ should completely avoid using these operators, because they are implicitly used by the smart pointers. The language features of Modern C++ for implementing secure code consist of the Resource Acquisition Is Initialization (RAII), object lifetime, scope exit, stack unwinding, constant declarations/expressions, and smart pointers. (Gregoire 2021)

- RAII ensures that objects stay in scope and that constructors/destructors are always called.
- Scopes consist of functions, member functions, and localized blocks of code.
- Function parameters and variables declared as *const* introduce immutable data structures.
- No use of raw pointers, *new[]* or *delete[]*.
- No use of references in functions.
- Use of unique and shared pointers with reference counting; creation must be implemented by calling *make\_unique<>()* and *make\_shared<>()*.
- Operations on unique pointers require move semantics to transfer ownership to code operating on data structures.

More specific advice for safety-critical code adds ten more rules for specific use cases. Among them is to avoid heap memory allocations, not using the preprocessor, and limit the use of references. These rules are known as The Power of 10. (Holzmann 2006) They are older than Modern C++ and can be applied to any programming language.

### STATIC AND DYNAMIC ANALYSIS OF CODE

Bjarne Stroustrup, the creator of C++, recommends using static analysis for all code. (Stroustrup 2022). The purpose is to periodically check for errors and code violating core guidelines and best practices. Static and dynamic analysis are a standard tool in software development in order to maintain and test the quality of the code. This analysis stage can catch bugs and undesired behavior of applications, but it is limited by Rice's Theorem. (Rice 1953) The theorem states that non-trivial and extensional code (expressed by functions) processing input data is undecidable. This means that there can be no complete formal test to check if the code behaves in a well-defined manner and as expected for all variations of

input data. The theorem limits the claims that any analysis tool can make about any application code. Therefore the selection and design of the unit and security tests for the application must be carefully created. Trivial tests should be avoided. Best practice is to test for the normal and exceptional operational situations. The latter is the primary task of security tests. Software quality and security is therefore mainly defined by the set of tests performed.

## FURTHER IMPROVING MEMORY SAFETY OF C++

The set of rules outlined by the Modern C++ standards serves as a baseline for all new code and refactoring. Memory safety can be improved by incorporating techniques from the programming languages Austral, Gel, Inko, Hyl/Val, and Vale. (Borretti 2021; Falcon and Cook 2009; Inko 2018; Racordon 2023; Ovadia 2022) The approach of the different proposals is similar, but the lead developer of Vale has compiled the most effective coding styles for protecting data structures in applications. (Ovadia 2023) The strategies are:

- Borrowless affine style for data structure
- Constraint references
- Generational references (for cases with limited memory use)
- Random generational reference
- Simplified unique borrowing

The borrowless affine style mandates to exclusively use stack objects and data referenced by unique pointers. No raw pointer and no C++ references are allowed. Raw arrays must be replaced by the `std::array` C++ STL container. When reading data it is always moved to the code that uses it. This ensures that the code acting on the data always has the full ownership and that all other code has no read and write access to the data. The C++ move operations utilize unique pointers in order to save expensive memory copy operations. The Rust programming language uses the same concepts.

Constraint references are implemented by explicitly adding the reference count into an object. The reference itself work similar to a shared pointer. The object has to check its reference counter and asserts a zero value once it gets out of scope. Any destructor can only deallocate the instance if there is no other reference to it. This protection mechanism is modeled after the foreign constraints in the Structured Query Language (SQL). The constraint references enables instances of objects to monitor its use by other parts of the code.

Generational references are an implementation of heap memory management. The design is a memory arena where created objects are referenced by their memory address and a generation number. All deallocation operations increment the generation number. All access verifies that the generation number matches the expected generation number when addressing an object instance. Generation numbers must not be reused, and the allocation process keeps the memory in order to protect it. This approach is only possible if the heap memory accommodates all storage requirements of the application at run-time, because all unreferenced memory regions are kept for protection.

Random generational reference use a pseudo-random generation number as object identifier instead of an increasing number. The purpose is to reduce the probability of generation number collisions. The random numbers act as a stochastic defense. These numbers are categorized as metadata and can be linked to the memory address of data structures. There are hardware features to support this, for example Arm v9 processors implement Memory Tagging Extensions (MTEs) for tracing memory allocations/deallocations. (Oracle® 2016, Arm Holding 2024, Serebryany 2019) Compilers developers implement memory tagging to assist with debugging. It is important to note that this technique is only useful for finding bugs. It is not recommended to build production code with it. (Clang Team 2007)

Simplified unique borrowing re-introduces mutable non-owning pointers. These pointers must never access the original object while it exists. They must never be returned by functions. They must not be stored in data structures or arrays. Also there must be no aliasing when using the pointer. A sample implementation in C++ shows how to integrate this method into existing code. (Ovadia 2023) The main reason to use simplified unique borrowing is to avoid using a full borrow checker or memory annotations such as references.

## IMPLEMENTING NEW CODE

The rules can be integrated into secure coding guidelines to help with the implementation. Using the rules requires discipline, because the memory protection techniques add extra code constructs and change the way traditional C++ code was designed. This is especially important for the C++ move semantics. Testing also requires specific code to test for memory safety violations. The effort is less than a complete reimplementation in a new programming language.

The compiler tool chains can support the development process. Compilers have added check features and assistance by taking advantage of processor features. (Wei 2021) This is only a measure to support the implementation. The code must be written in a manner to enable the compilers to use the protection and debugging features.

## CONVERTING EXISTING CODE

The techniques can be gradually integrated into existing code. The C++ code needs to be reduced or adapted to the language features described in this document. The most important step is to introduce unique pointers and move semantics. References may be added if the processor has hardware support and the compiler toolchain can use these features. As a bonus, all techniques can be implemented in a concurrency-safe way. The borrowless affine style is already concurrency-safe. The necessary C++ standards are available in all compilers for standards platforms. The first step should always be to port the code to Modern C++. The use of generational references should be checked with the availability of the heap memory in the target system.

The testing phase can take advantage of all standard test methods for memory safety. This is an advantage, because no adaptations to the toolchain are necessary.

## SUMMARY

The described memory safety techniques are available with modern C++ compilers. The methods are implemented in other programming languages. The abstraction layers and the hardware running the compiled code may introduce subtle changes in storage or execution order. All concurrent code is affected by this behavior due to the optimizations present in the run-time environment. Applications with a parallel execution design have to add synchronization techniques.

The proposed memory safety need to be evaluated for their impact. The research of the sources and related publications yielded no quantitative studies of code with a statistically significant sample size of tests. Further work is needed to test how well the proposed programming approach can counter memory safety problems with test data.

## ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES

Stroustrup, Bjarne et. al. 13 September 2015. “C++ Core Guidelines”. Updated 3 October 2024. <https://github.com/isocpp/CppCoreGuidelines>

Gregoire, Marc. 13 February 2021. “Professional C++”. John Wiley & Sons, Inc.

Holzmann, Gerard J. June 2006. “The Power of 10: Rules for Developing Safety-Critical Code”. NASA/JPL Laboratory for Reliable Software. IEEE Computer. **39** (6): 95–99. doi:10.1109/MC.2006.212.

Stroustrup, Bjarne. December 2022. “A call to action: Think seriously about “safety”; then do something sensible about it”. Doc. no. P2739R0. Columbia University.

Rice, H. G. (1953). "Classes of recursively enumerable sets and their decision problems", Transactions of the American Mathematical Society, **74** (2): 358–366, doi:[10.1090/s0002-9947-1953-0053041-6](https://doi.org/10.1090/s0002-9947-1953-0053041-6), JSTOR 1990888

Borretti, Fernando. 2021. The Austral Programming Language. Updated 2023. <https://austral-lang.org/>.

Falcon, J., Cook, W.R. (2009). Gel: A Generic Extensible Language . In: Taha, W.M. (eds) Domain-Specific Languages. DSL 2009. Lecture Notes in Computer Science, vol 5658. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-642-03034-5\\_4](https://doi.org/10.1007/978-3-642-03034-5_4)

Inko development team. 2018. “The Inko programming language”. Updated October 2024. <https://inko-lang.org/>

Racordon, Dimitri. 2023. “The Hylo Programming Language”. Updated October 2024. <https://www.hylo-lang.org/>.

Ovadia, Evan. 2022. “The Vale Programming Language”. Updated October 2024. <https://vale.dev/>.

Ovadia, Evan. 22 June 2023. “Making C++ Memory-Safe Without Borrow Checking, Reference Counting, or Tracing Garbage Collection”. <https://verdagon.dev/blog/vale-memory-safe-cpp>

Oracle® Corporation. 2016. “Application Data Integrity (ADI) operations”. Updated July 2017. [https://docs.oracle.com/cd/E86824\\_01/html/E54765/adi-2.html](https://docs.oracle.com/cd/E86824_01/html/E54765/adi-2.html)

Arm Holding plc. “Arm memory tagging extension”. Updated 1 November 2024. <https://source.android.com/docs/security/test/memory-safety/arm-mte>

Serebryany, Konstantin. 2019. “ARM Memory Tagging Extension and How It Improves C/C++ Memory Safety”. ;login: Magazine Vol. 44 ,No. 2.

The Clang Team. 2007. “Hardware-assisted AddressSanitizer Design Documentation”. Updated 2024. <https://clang.llvm.org/docs/HardwareAssistedAddressSanitizerDesign.html>

Wei, Song, et. at. 2021. “A Comprehensive and Cross-Platform Test Suite for Memory Safety - Towards an Open Framework for Testing Processor Hardware Supported Security Extensions”. Computing Research Repository (CoRR). November 2021.

## ML-BASED PREDICTING PRNG OUTPUT WITH SEQUENTIAL ANALYSIS

Dmytro Proskurin<sup>1</sup>, Maksim Iavich<sup>2</sup>, Sergiy Gnatyuk<sup>1</sup>, Tetiana Okhrimenko<sup>1</sup>,  
<sup>1</sup>State University “Kyiv Aviation Institute”, <sup>2</sup>Caucasus University

**ABSTRACT:** This research goes into the predictive capabilities of neural network models, mainly focusing on recurrent neural networks (RNNs) and long-term short-term memory networks (LSTMs), and their combination in a hybrid architecture to predict the outcomes of various pseudo-random number generators (PRNGs). In this work Continuous-Output Scenario Analysis is shown.

**KEYWORDS:** *Random numbers, Neural Networks, AI, Hybrid model, PRNG, cybersecurity, critical information infrastructure.*

### INTRODUCTION

Neural networks are artificial intelligence systems designed to replicate the functioning of the human brain. Unlike traditional digital models that process binary data (zeros and ones), neural networks operate through connection processing units, akin to neurons in a biological brain. The performance of these networks depends on how their connections are structured and weighted. Neural networks are algorithms modelled after the human brain that recognize patterns. Sensory data is interpreted using machine perception, which labels or clusters raw information. They recognize numerical patterns in vectors, which must be converted into real-world data like as images, sounds, text, and time series [1]. *Artificial Neural Networks (ANNs)* are computing systems modelled such as biological neural systems, including the human brain. These systems consist of numerous interconnected computational units (neurons) that work collaboratively in a distributed manner. By learning from input data and optimizing outputs, they enhance performance and achieve accurate results [2].

Let's consider the main Neural Networks types:

- 1) *Convolutional Neural Networks (CNNs)* are comparable to standard ANNs because they utilize neurons and improve through learning [2]. CNNs have achieved significant breakthroughs and are now a key component of deep learning applications. They have revolutionized computer vision, enabling advancements such as facial recognition, autonomous driving, cashier-less retail systems, and intelligent healthcare technologies. Unlike traditional ANNs, CNNs are tailored for recognizing patterns in visual data. This specialization allows them to embed image-specific features directly into their structure, making them particularly effective for image-centric tasks. Furthermore, CNNs require fewer parameters to configure, enhancing their efficiency and performance in complex visual processing tasks [2, 3].
- 2) *Hybrid neural networks (HNNs)* are becoming increasingly popular in computer vision applications including picture captioning and action identification, and they integrate the strengths of many neural networks. However, there has been limited research on the effective use of hybrid architectures for time series data, particularly for trend forecasting purposes [4]. HNNs use their internal structure to limit the interactions between process variables in order to align with physical models. Compared to regular neural networks, coupled models are more accurate, dependable, and generalizable [5].
- 3) *Recurrent Neural Networks (RNNs)* represent a paradigm shift in neural networks, specifically designed to recognize patterns in sequences of data [6]. Unlike traditional feedforward neural networks, RNNs possess a unique feature: the output from the previous step is fed back into the output of the current step. This looping mechanism allows RNNs to maintain an internal state that captures information about the sequence they have processed so far, making them ideal for tasks like speech recognition, language modelling, and time series forecasting [6 7]. The core architecture of an RNN involves a hidden layer where the activation at a given time step is a function of the output at the same step and the activation of the hidden layer at the previous step [8]. This recurrent nature allows the network to maintain a form of memory [6]. However,

RNNs are often challenged by long-term dependencies due to issues like vanishing and exploding gradients during backpropagation [7, 9], where the network becomes unable to learn and retain information from earlier time steps in the sequence [10].

- 4) *Long Short-Term Memory networks*, a special kind of RNN, were developed to overcome the limitations of traditional RNNs. LSTMs are adept at learning long-term dependencies, thanks to their unique internal structure [9]. Unlike standard RNNs, LSTMs have a complex architecture with a series of gates: the forget gate, output gate, and output gate [9, 10]. These gates regulate the flow of information into and out of the cell, deciding what to keep in memory and what to discard, thereby addressing the vanishing gradient problem [8].

Both RNNs and LSTMs are designed for sequence processing, the key difference lies in their ability to handle long-term dependencies. Standard RNNs, while simpler and computationally less intensive, struggle with retaining information over longer sequences. LSTMs, with their intricate gating mechanism, excel in scenarios where understanding long-range contextual information is crucial.

The choice between RNNs and LSTMs often boils down to the specific requirements of the task at hand, the complexity of the sequences involved, and the computational resources available. LSTMs are generally preferred for more complex tasks with longer sequences [9], while RNNs might suffice for simpler tasks with shorter temporal dependencies [11].

In our research, we utilized datasets produced by four different PRNG algorithms, each presenting unique challenges and features for sequence prediction with RNN and LSTM models. These datasets provided a platform to assess and contrast the performance of various neural network architectures in tackling sequence prediction tasks.

After generating the dataset, it was carefully divided into three distinct subsets to support the training, testing, and validation of our predictive models:

- **Training Set:** Used for model training, enabling the networks to learn and adapt to the patterns present in the pseudorandom sequences generated by each PRNG.
- **Testing Set:** Reserved for evaluating the models' performance on unseen data, providing an objective measure of their predictive accuracy.
- **Validation Set:** Applied during the model tuning process to adjust parameters and mitigate overfitting, ensuring the models can generalize effectively to new data.

This structured approach to dataset preparation and partitioning played a pivotal role in establishing a reliable framework for analyzing the predictability of PRNG outputs via sequential analysis. By standardizing generation parameters and implementing a methodical data split, we ensured a consistent and equitable evaluation environment for all predictive models used in the study.

## EVALUATION METRICS FOR TESTING

To evaluate how effectively our models predict PRNG outputs, we utilized a range of detailed assessment metrics. These metrics play a vital role in measuring prediction accuracy and enabling direct comparisons between the various neural network architectures examined in our research. The core of our evaluation framework includes the Mean Squared Error (MSE) and a custom-designed Model Performance Score.

MSE is a fundamental component of our evaluation approach, providing a robust measure of prediction accuracy. It calculates the average squared differences between predicted and actual values, highlighting the magnitude of prediction errors. By emphasizing larger discrepancies through squaring, MSE becomes particularly sensitive to outliers and significant inaccuracies.

When applied to predicting PRNG outputs, MSE offers a straightforward metric to assess how closely the model's predictions match the actual sequence of numbers produced by the PRNGs. A lower MSE signifies greater prediction accuracy, indicating the model's effectiveness in capturing and replicating the underlying patterns of the PRNG sequence [13-15].

Recognizing the need for a standardized metric that allows for an intuitive understanding of model performance, we introduced the Model Performance Score. This metric normalizes the MSE to a scale ranging from 0 to 1, where 0 represents the poorest performance (highest MSE) and 1 denotes perfect prediction accuracy (zero MSE).

The Model Performance Score is calculated by inversely scaling the MSE against a predetermined maximum error threshold. This approach ensures that the performance score is adjusted for the scale of



the data and the expected variation in prediction accuracy, allowing for a fair comparison across different models and datasets.

This normalized score simplifies the interpretation of our results, providing a straightforward metric to gauge model effectiveness. It allows stakeholders to quickly assess the relative performance of each model in predicting PRNG outputs without delving into the complexities of raw MSE values.

Together, these evaluation metrics form the foundation of our analytical approach, enabling a nuanced analysis of model performance. MSE offers a detailed view of the prediction accuracy, while the Model Performance Score provides a high-level, comparative perspective. By incorporating both metrics, our study ensures a balanced and comprehensive evaluation of how well each neural network architecture can predict the seemingly unpredictable: the output of pseudorandom number generators.

We carried out a comprehensive set of experiments to assess the predictive performance of various neural network architectures. These experiments were carefully structured to examine how different model parameters influence the accuracy of PRNG output predictions. In the following sections, we outline the key variables considered in these experiments and discuss significant insights regarding model performance.

To systematically assess the effects of various hyperparameters on model performance, we tested a wide array of combinations, encompassing:

- *Activation Functions*: experimented with two popular activation functions, ReLU (Rectified Linear Unit) and tanh (Hyperbolic Tangent). These functions were chosen for their distinct characteristics in handling nonlinearities in the data.
- *Number of Neurons*: the neuron counts tested were 8, 16, and 32. This range allowed us to explore the models' capacity to learn and generalize from the data, balancing complexity with computational efficiency.
- *Epochs*: all models were trained for [1000] epochs, providing ample opportunity for learning and convergence.
- *Model Layers*: varied the depth of the models by testing configurations with [2, 3, 5] layers. This variation aimed to understand how model depth influences learning and prediction accuracy.
- *Output Lengths*: for continuous value prediction, output lengths of [1, 2, 3, 5] were tested. This range was selected to assess the models' ability to forecast multiple steps ahead in the PRNG sequence.

## EXPERIMENT

The study on predicting the output of PRNGs using sequential analysis gave convincing results, which were obtained by analyzing the most effective models for each PRNG. In the following, we consider meaningful results for scenarios with a continuous output for different PRNGs: Xorshift, MT (Mersenne Twister), LCG (Linear Congruential Generator), and MiddleSquare.

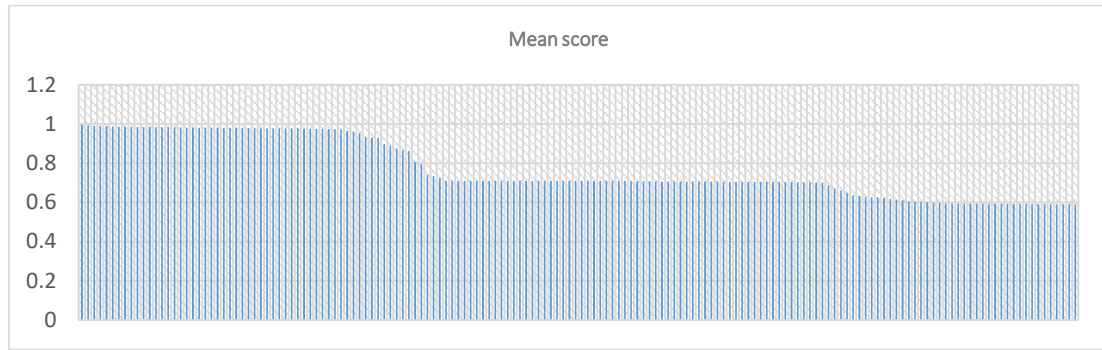
The continuous-output models demonstrated even higher predictive accuracy than single-output, with the Hybrid model configured for continuous predictions (Hybrid-C) achieving remarkable success.

For the MiddleSquare PRNG, the Hybrid-C model with tanh activation, 16 neurons, 3 layers, and an output length of 3 achieved a near-perfect mean score of 0.9955.

**Table 1. MiddleSquare, continuous output results**

Scenario	Model type	Neuron	Activation function	Epochs	Layers	Output length	Mean score
MiddleSquare	Hybrid-C	16	tanh	1000	3	3	0.995479
MiddleSquare	Hybrid-C	16	tanh	1000	2	2	0.992588
MiddleSquare	Hybrid-C	8	tanh	1000	5	2	0.990003
MiddleSquare	Hybrid-C	8	relu	1000	5	1	0.988989
MiddleSquare	Hybrid-C	32	relu	1000	5	3	0.988566
MiddleSquare	Hybrid-C	8	tanh	1000	3	1	0.988066
MiddleSquare	Hybrid-C	16	relu	1000	2	2	0.986359
MiddleSquare	Hybrid-C	16	tanh	1000	5	3	0.985923
MiddleSquare	Hybrid-C	16	tanh	1000	5	2	0.985797
MiddleSquare	Hybrid-C	8	tanh	1000	5	1	0.984813

Only 29% of the models managed to achieve a success rate exceeding 90% (Fig. 1).



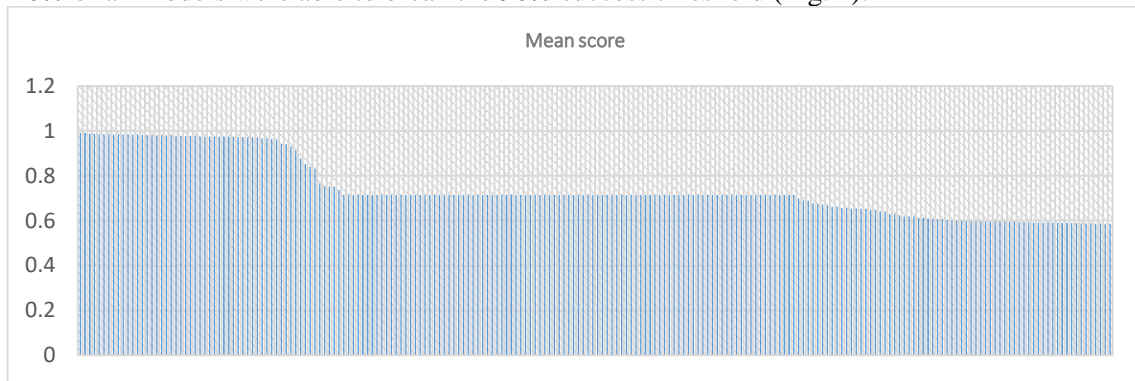
**Fig. 11.** MiddleSquare, continuous output, all models results

For the LCG PRNG, the Hybrid-C model with tanh activation, 8 neurons, 5 layers, and an output length of 2 achieved a near-perfect mean score of 0.992055.

**Table 2.** LCG, continuous output results

Scenario	Model type	Neuron	Activation function	Epochs	Layers	Output length	Mean score
LCG	Hybrid-C	8	tanh	1000	5	2	0.992055
LCG	Hybrid-C	8	tanh	1000	5	3	0.98973
LCG	Hybrid-C	16	tanh	1000	5	5	0.987614
LCG	Hybrid-C	8	tanh	1000	3	5	0.986818
LCG	Hybrid-C	8	tanh	1000	2	5	0.985174
LCG	Hybrid-C	16	tanh	1000	3	2	0.984808
LCG	Hybrid-C	32	tanh	1000	3	2	0.984462
LCG	Hybrid-C	16	tanh	1000	2	1	0.984411
LCG	Hybrid-C	32	tanh	1000	3	1	0.983866
LCG	Hybrid-C	32	tanh	1000	2	1	0.983706

20% of all models were able to break the 90% success threshold (Fig. 2).



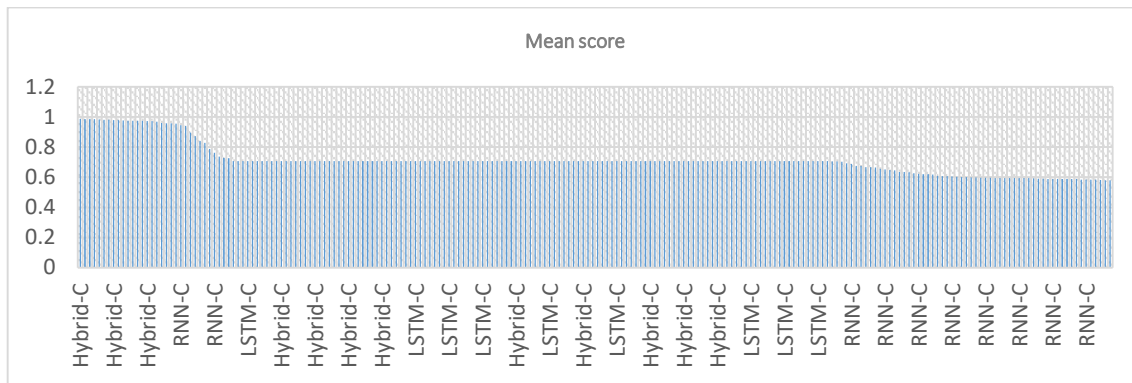
**Fig. 2.** LCG, continuous output, all models results

For the Xorshift PRNG, the Hybrid-C model with relu activation, 16 neurons, 2 layers, and an output length of 2 achieved a near-perfect mean score of 0.987906 (table 3).

**Table 3.** Xorshift, continuous output results

Scenario	Model type	Neuron	Activation function	Epochs	Layers	Output length	Mean score
Xorshift	Hybrid-C	16	relu	1000	2	2	0.987906
Xorshift	Hybrid-C	16	relu	1000	2	5	0.985753
Xorshift	Hybrid-C	8	relu	1000	5	5	0.985715
Xorshift	Hybrid-C	8	relu	1000	2	2	0.984238
Xorshift	Hybrid-C	32	relu	1000	2	2	0.983437
Xorshift	Hybrid-C	16	relu	1000	2	3	0.981247
Xorshift	Hybrid-C	8	relu	1000	2	1	0.980434
Xorshift	Hybrid-C	32	relu	1000	2	1	0.97893
Xorshift	RNN-C	32	tanh	1000	3	1	0.977685
Xorshift	Hybrid-C	32	relu	1000	2	3	0.976177

15% of all models were able to break the 90% success threshold (Fig. 3 Fig. 2).



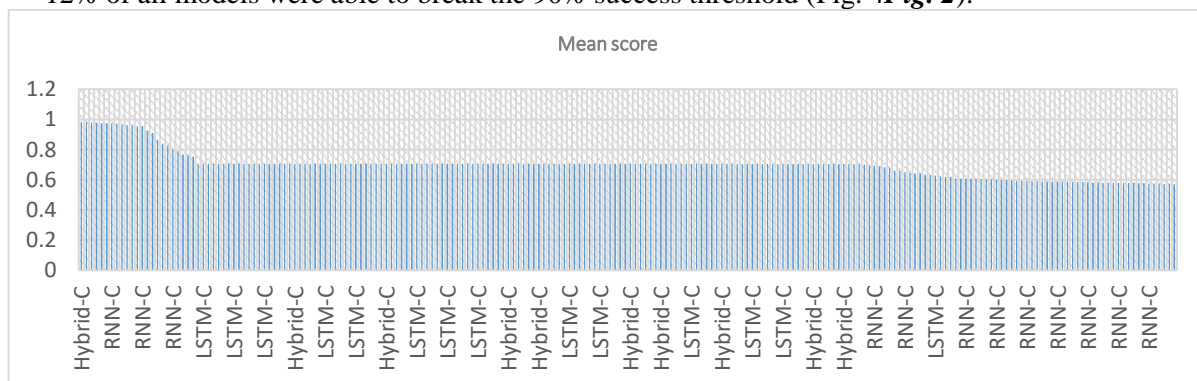
**Fig. 2.** Xorshift, continuous output, all models results

For the MT PRNG, the Hybrid-C model with relu activation, 32 neurons, 2 layers, and an output length of 2 achieved a near-perfect mean score of 0.985006 (table 4).

**Table 4.** MT, continuous output results

Scenario	Model type	Neuron	Activation function	Epochs	Layers	Output length	Mean score
MT	Hybrid-C	32	relu	1000	2	2	0.985006
MT	RNN-C	32	relu	1000	5	1	0.981523
MT	RNN-C	32	tanh	1000	5	1	0.980135
MT	Hybrid-C	16	tanh	1000	2	3	0.976324
MT	LSTM-C	32	relu	1000	5	1	0.976245
MT	Hybrid-C	8	tanh	1000	2	1	0.975258
MT	RNN-C	32	tanh	1000	3	1	0.97421
MT	RNN-C	32	relu	1000	3	1	0.972664
MT	RNN-C	32	relu	1000	2	1	0.965829
MT	RNN-C	32	tanh	1000	2	1	0.963914

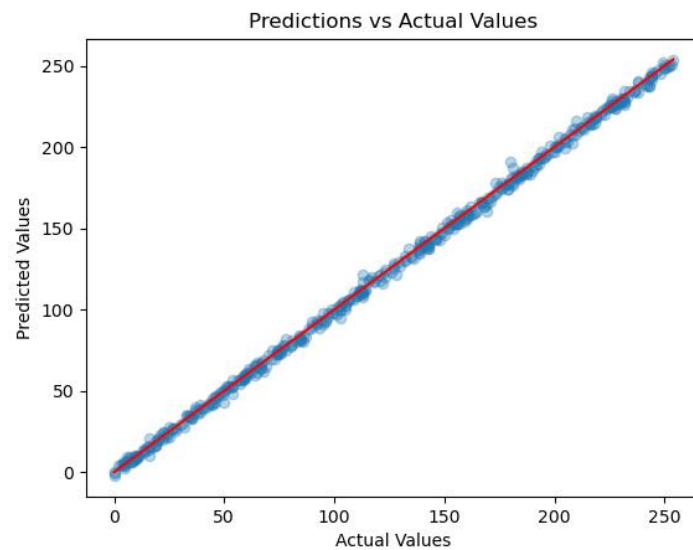
12% of all models were able to break the 90% success threshold (Fig. 4Fig. 2).



**Fig. 3.** MT, continuous output, all models results

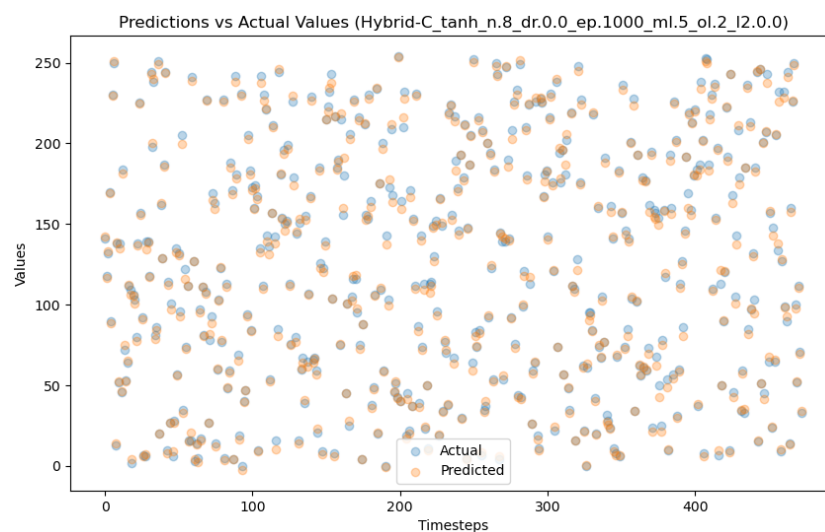
The examination of continuous-output models reveals a notable enhancement in predictive performance compared to single-output models. This is particularly evident in the context of predicting sequences generated by the MiddleSquare PRNG.

The performance plot illustrating the correlation between predicted and actual values (Fig. 4 5) for the continuous-output model shows an even tighter linear alignment than the single-output model. This near-perfect correlation, along with a high success score of 0.9955, reflects the model's exceptional predictive accuracy. The dense clustering of points along the diagonal suggests that the model can reliably predict the MiddleSquare PRNG's output with high confidence, and such precision is indicative of the model's ability to capture both the immediate and contextual dependencies within the PRNG's sequence.



**Fig. 4.** Prediction vs actual values, MiddleSquare with the best result (0.9955)

The scatter plot for the continuous-output Hybrid model, which integrates CNN and LSTM architectures (Hybrid-C), showcases a substantial concentration of points closely aligned with the line of perfect prediction (fig. 6). The model, employing tanh activation with 16 neurons across 3 layers, exhibits a remarkable ability to track the actual values throughout the sequence. This tight clustering indicates a substantial reduction in prediction errors and a strong alignment with the true PRNG sequence, suggesting a deeper understanding of the underlying patterns by the model.



**Fig. 5.** Prediction vs actual values, MiddleSquare with the best result (0.9955)

The continuous-output model's superior performance, as evidenced by the closer proximity of predicted to actual values and the higher success score, highlights the benefit of utilizing sequential context in PRNG output prediction. The ability to forecast the sequence with a success score reaching 0.9955 marks a significant milestone, suggesting that models incorporating sequence history can more effectively decode the deterministic yet complex structure of PRNG outputs.

This analysis implies that continuous-output models hold great promise for applications where forecasting accuracy over sequences is critical. The insights gleaned from this research can inform the development of more secure PRNGs, capable of withstanding sophisticated sequential analysis. Future work will likely explore the expansion of this approach to more complex and higher-dimensional

sequences, potentially integrating additional layers of complexity and exploring the impact on model performance.

Our study's findings highlight the nuanced nature of PRNG output prediction, with different models excelling for specific generators. This variation underscores the importance of model selection tailored to the characteristics of the PRNG being analyzed. For instance, the best-performing model for the Xorshift generator might leverage its unique XOR and shift operations, whereas the optimal model for the Mersenne Twister (MT) would need to account for its complex bit manipulation and tempering techniques.

Remarkably, the single-output models consistently achieved a 98% success rate across various PRNGs, demonstrating a high level of accuracy in predicting the next output value based solely on a single preceding value. This success rate is indicative of the models' ability to decipher the underlying deterministic patterns that govern PRNG outputs.

Even more impressive, the continuous-output model, which utilizes sequences of values to predict subsequent outputs, reached a 99% success rate. This improvement suggests that incorporating more context in the form of continuous output sequences enables the models to better capture the PRNGs' inherent algorithms, leading to more accurate predictions.

The success of our models in predicting PRNG outputs with such high accuracy has profound implications for the fields of cryptography and random number generation. While PRNGs are designed to produce sequences that are difficult to predict, our results suggest that advanced neural network models can uncover and exploit hidden patterns within these sequences. This finding calls for ongoing efforts to enhance the unpredictability and security of PRNGs, ensuring they remain robust against sophisticated analytical techniques.

## **CONCLUSION**

This study investigates the predictability of PRNGs using advanced neural network architectures. Our analysis highlights the impressive ability of the tested models to accurately predict PRNG outputs, particularly in continuous output scenarios where their capacity to capture long-term dependencies within PRNG sequences proves highly effective. This underscores their potential for tackling complex sequence prediction challenges.

Future research should focus on integrating more sophisticated neural network architectures and exploring practical applications of these insights in areas such as secure communication and cryptographic key generation. The results of this work point to a critical need for the development of more secure and less predictable PRNG designs, strengthening defenses against adversarial predictions and enhancing the reliability of cryptographic systems.

## **ACKNOWLEDGMENT**

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## **REFERENCES**

- [1]. Islam, M., Chen, G., & Jin, S. (2019). An Overview of Neural Network. *American Journal of Neural Networks and Applications*, 5(1), 7-11. doi:10.11648/j.ajna.20190501.12.
- [2]. O'Shea, K., & Nash, R. (2015). *An Introduction to Convolutional Neural Networks*.
- [3]. Li, Z., Yang, W., Peng, S., & Liu, F. (2021). *A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects*.
- [4]. Lin, T., Guo, T., & Aberer, K. Hybrid Neural Networks for Learning the Trend in Time Series.
- [5]. Psychogios, D. C., & Ungar, L. H. A Hybrid Neural Network-First Principles Approach to Process Modeling.
- [6]. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems*, 30.
- [7]. Sutskever, I., Vinyals, O., & Le, Q. V. (2014). Sequence to Sequence Learning with Neural Networks. *Advances in Neural Information Processing Systems*, 27.

- [8]. Karpathy, A. (2015). The Unreasonable Effectiveness of Recurrent Neural Networks. Andrej Karpathy blog.
- [9]. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. *Neural Computation*, 9(8), 1735-1780
- [10]. Gers, F. A., Schmidhuber, J., & Cummins, F. (2000). Learning to Forget: Continual Prediction with LSTM. *Neural Computation*, 12(10), 2451-2471.
- [11]. Cho, K., van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., & Bengio, Y. (2014). Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. arXiv:1406.1078.
- [12]. Brownlee, J. (2018). Deep Learning for Time Series Forecasting: Predict the Future with MLPs, CNNs and LSTMs in Python. *Machine Learning Mastery*.
- [13]. Maksim Iavich, Tamari Kuchukhidze, Giorgi Iashvili, Sergiy Gnatyuk Hybrid quantum random number generator for cryptographic algorithms. *RADIOELECTRONIC AND COMPUTER SYSTEMS*, 4, 2021. DOI: <https://doi.org/10.32620/reks.2021.4.09>
- [14]. Maksim Iavich, Tamari Kuchukhidze, Giorgi Iashvili, Sergiy Gnatyuk, Razvan Bocu," Novel Quantum Random Number Generator with the Improved Certification Method ", *International Journal of Mathematical Sciences and Computing (IJMSC)*, Vol.7, No.3, pp. 41-53, 2021. DOI: 10.5815/ijmsc.2021.03.05
- [15]. Maksim Iavich, Tamari Kuchukhidze, Giorgi Iashvili, Sergiy Gnatyuk, Razvan Bocu," Novel Quantum Random Number Generator with the Improved Certification Method ", *International Journal of Mathematical Sciences and Computing (IJMSC)*, Vol.7, No.3, pp. 41-53, 2021. DOI: 10.5815/ijmsc.2021.03.05

## ARTIFICIAL INTELLIGENCE APPLICATIONS FOR THE SECURITY OF IOT DEVICES IN HEALTHCARE

A.Ravishankar Rao, PhD, IEEE Fellow  
Fairleigh Dickinson University  
Teaneck, NJ 07666 USA  
ravirao@fdu.edu

**ABSTRACT:** The integration of Internet of Things (IoT) devices in healthcare has revolutionized patient care but also introduced significant cybersecurity challenges. This paper explores the vulnerabilities of IoT systems in healthcare, drawing from high-profile cyberattacks like the Mirai botnet, Hackensack Meridian ransomware incidents, and the Colonial Pipeline breach. It examines the role of artificial intelligence (AI) in enhancing IoT security, particularly through techniques such as User and Entity Behavioral Analytics (UEBA) and predictive modeling. While AI offers promising solutions for detecting anomalies and predicting threats, it also faces limitations, including embedding drift, resource constraints, and the generation of insecure code. Case studies illustrate how IoT devices like pacemakers and webcams can be exploited without proper safeguards. Future directions for AI-driven IoT security include multi-source data integration, explainability, and ethical oversight. It is important to safeguard the security of IoT systems in healthcare through high levels of vigilance.

**KEYWORDS:** *cybersecurity, internet of things, medical devices, healthcare*

### INTRODUCTION

The Internet of Things (IoT) has transformed the healthcare industry, enhancing patient outcomes and operational efficiency (Rao and Clarke 2019, Rao, Mishra et al. 2020, Zhou, Ye et al. 2023). These devices, ranging from pacemakers to barcode scanners and wearable health monitors, enable seamless communication and real-time data sharing. However, their integration into critical systems has significantly expanded the attack surface, making healthcare facilities attractive targets for cybercriminals. IoT devices often lack robust security mechanisms, which, when coupled with the critical nature of healthcare environments, create significant vulnerabilities.

Cybersecurity incidents like the Mirai botnet (Antonakakis, April et al. 2017), Hackensack Meridian ransomware attack (Karambelas 2020), and Colonial Pipeline shutdown (Beerman, Berent et al. 2023) demonstrate the growing risks posed by IoT systems. Artificial intelligence (AI) offers promising solutions to address these challenges, particularly through techniques like User and Entity Behavioral Analytics (UEBA) (Datta, Dasgupta et al. 2021, IBM 2024). This paper examines the role of AI in IoT security for healthcare, discussing its potential, limitations, and implications for the future.

### THE IOT SECURITY LANDSCAPE: CHALLENGES AND HISTORICAL CONTEXT

IoT security encompasses a wide array of threats, ranging from ransomware attacks to unauthorized device access. A notable example is the Mirai botnet of 2017, orchestrated by a Rutgers University student, which leveraged insecure IoT devices to launch distributed denial-of-service (DDoS) attacks (Antonakakis, April et al. 2017). This incident underscored the vulnerability of IoT systems due to poor password practices and lack of firmware updates.

Healthcare institutions have also been frequent targets. In 2019, Hackensack Meridian Health, New Jersey's largest healthcare provider, was forced to pay a ransom after a cyberattack crippled its systems (Karambelas 2020). Despite improving security protocols and reducing vulnerabilities by 90% over subsequent years, another attack in 2023 highlighted the persistent nature of these threats. Similarly,

the Colonial Pipeline attack in 2021 revealed the fragility of operational technology (OT) systems (Beerman, Berent et al. 2023). The attackers infiltrated critical control equipment, forcing the shutdown of oil pipelines and resulting in a \$5 million ransom payment. This incident drew attention to the interplay between IT (information technology) and OT in ensuring cybersecurity.

Hospitals rely on IoT for functions such as patient monitoring, medication delivery, and administrative tasks. Yet, many devices operate with outdated protocols or lack proper encryption, making them susceptible to hacking. Open cameras found on platforms like Shodan (Tundis, Modo Nga et al. 2021) serve as a cautionary example. In one case, a network camera monitoring a building entrance in Hackensack, New Jersey, was publicly accessible, exposing individuals to potential privacy violations and unauthorized facial recognition (Rao and Elias-Medina 2024).

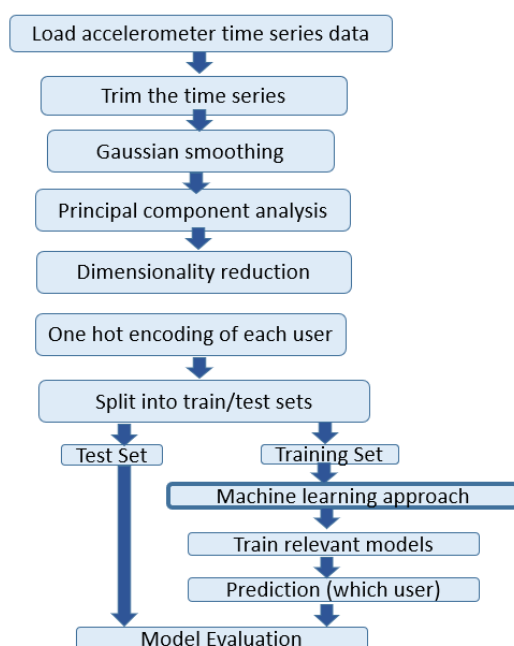
Established best practices exist for protecting the security of hospital IT systems. For instance, (405d.hhs.gov 2023) mentions that a medical device such as a blood pressure monitor should only be connected to the technologies it needs to function. For example, the blood pressure monitor should not be connected to the HVAC system because an attacker could leverage the HVAC system for access.

### AI AND IOT SECURITY: OPPORTUNITIES AND USE CASES

Artificial intelligence has emerged as a game-changer in the field of cybersecurity. One prominent application is User and Entity Behavioral Analytics (UEBA). By analyzing baseline behavior patterns of users and devices, UEBA systems can detect anomalies that signal potential security threats (IBM 2024). For instance, in a hospital setting, if a network-connected heart monitor begins transmitting data outside predefined parameters, a UEBA system could flag the activity as suspicious.

UEBA systems employ machine learning algorithms to monitor user activities and device behavior. This capability is particularly relevant for identifying insider threats, where malicious actors may use legitimate credentials to bypass conventional security measures. UEBA enhances zero trust security frameworks (Buck, Olenberger et al. 2021) by providing contextual insights into device activities.

We developed a proof-of-concept study leveraging user interactions with a doorknob. Our DeepKnob system (Vegas, Rao et al. 2024) combined user behavior patterns with deep learning to identify individual users with an accuracy of 90%. An overview of the system is presented in **Fig. 1**.



**Fig. 1:** Sensory data processing pipeline. The first six blocks on the top show the initial data acquisition and processing. The processed data is fed into a machine learning algorithm utilizing deep learning. This model performance is evaluated using cross-validation by splitting the data in test and training sets.



Real-world implementation of such models in healthcare faces challenges related to scalability, resource constraints, and the need for high-throughput systems. Combining multiple data sources and measurements may improve accuracy, but practical deployment in large-scale environments remains a significant hurdle.

### **CASE STUDIES: IOT IN HEALTHCARE**

Healthcare environments offer a fertile ground for understanding the intersection of IoT, AI, and cybersecurity. Critical devices, such as pacemakers, insulin pumps, and pulse sensors, are integral to patient care but are often vulnerable to attacks. For example, researchers demonstrated that pacemakers could be hacked to deliver incorrect shocks, posing life-threatening risks (Alexander, Haseeb et al. 2019). This example highlights the need for stringent security measures in healthcare IoT systems.

Another example involves the use of barcode scanners and webcams in hospitals. These devices often lack secure configurations, allowing hackers to exploit them (Siddiqi, Singh et al. 2023). Such breaches could enable attackers to gather sensitive information or launch larger coordinated attacks.

We have developed a Secure Embedded Systems Lab, which represents an educational initiative to equip students with the skills necessary to design secure IoT systems. By incorporating sensors, cameras, and real-world security scenarios into laboratory exercises, the lab aims to bridge the gap between academic knowledge and practical cybersecurity applications (Rao and Elias-Medina 2024).

### **AI'S ROLE IN PREDICTIVE ANALYTICS FOR HEALTHCARE**

Beyond anomaly detection, AI plays a crucial role in predictive analytics, helping hospitals manage resources and anticipate patient needs. For example, we have developed models to forecast healthcare costs and predict patient length of stay (Jain, Singh et al. 2024, Rao, Jain et al. 2024). These predictive tools rely on interpretable machine learning techniques, such as decision trees and regression models, which allow healthcare providers to make data-driven decisions.

However, predictive analytics also introduces cybersecurity risks. The aggregation of sensitive patient data into AI systems makes them attractive targets for hackers. Securing these systems requires robust encryption, access controls, and regular audits to mitigate risks.

### **CHALLENGES AND LIMITATIONS OF AI IN CYBERSECURITY**

Despite its potential, AI faces several limitations when applied to IoT security:

1. **Embedding Drift:** As device behaviors and cyberattack techniques evolve, AI models may fail to adapt, reducing their effectiveness. For instance, a model trained on past ransomware attacks may struggle to detect new variants that employ novel strategies.
2. **AI-Generated Code Vulnerabilities:** A survey by Snyk, a cybersecurity firm, found that 91.6% of AI coding tools generated insecure code suggestions (Synk 2023). This problem is exacerbated by the lack of automated scanning tools to detect vulnerabilities in open-source components.
3. **Resource Constraints:** Deploying AI solutions in healthcare environments often requires significant computational resources, which may not be readily available. Furthermore, training and maintaining AI models can be expensive and time-consuming.
4. **False Positives and False Negatives:** High false-positive rates can overwhelm security teams with unnecessary alerts, while false negatives may allow threats to go undetected.
5. **Ethical Concerns:** The dual-use nature of AI raises ethical questions. Cybercriminals have begun experimenting with generative AI tools to create phishing campaigns and malware, complicating efforts to combat cybercrime.

## FUTURE DIRECTIONS FOR AI-DRIVEN IOT SECURITY

To address these challenges, healthcare organizations must adopt a multi-faceted approach to AI-driven IoT security:

1. **Integrating Multi-Source Data:** Combining data from multiple devices and sensors can improve the accuracy of anomaly detection systems. For example, correlating data from pacemakers, insulin pumps, and hospital network traffic could provide a comprehensive view of security events.
2. **Enhancing Explainability:** Developing explainable AI models ensures that security professionals can understand and trust the system's decisions. This transparency is crucial for addressing ethical concerns and mitigating biases in AI algorithms.
3. **Collaborative Research:** Partnerships between academic institutions, healthcare providers, and cybersecurity experts can accelerate the development of scalable, secure AI solutions. Initiatives like the Secure Embedded Systems Lab provide valuable platforms for collaboration (Rao and Elias-Medina 2024).
4. **Continuous Monitoring and Updates:** Regularly updating AI models and IoT devices is essential to stay ahead of evolving threats. Incorporating feedback loops into AI systems can help them learn from new data and improve over time.
5. **Policy and Regulation:** Establishing cybersecurity standards, such as ANSI/CTA-2088-A, ensures that IoT devices meet baseline security requirements. Regulatory frameworks should also address the ethical implications of AI deployment.

The interplay between automated attacks and defenses will likely define the future of IoT security. Organizations must remain vigilant, adopting proactive measures to anticipate and counter emerging threats. Cybersecurity is no longer a reactive process; it requires forward-thinking strategies that leverage AI's potential while acknowledging its limitations.

## CONCLUSION

IoT security in healthcare presents a complex challenge, combining technical, operational, and ethical considerations. Historical cyberattacks highlight the vulnerabilities of IoT systems, while AI offers innovative solutions through techniques like UEBA and predictive analytics. However, the deployment of AI in healthcare cybersecurity must address challenges such as embedding drift, resource limitations, and ethical concerns.

By integrating multi-source data, enhancing model explainability, and fostering collaboration, healthcare organizations can harness AI to strengthen IoT security. As the threat landscape evolves, adopting a proactive, strategic approach to cybersecurity will ensure safer environments for patients and providers alike.

## ACKNOWLEDGEMENTS

I am grateful to the Shota Rustaveli National Science Foundation, Georgia, and Caucasus University for providing the funding to host this conference. I express my deep gratitude to Dr. Maksim Iavich, and Dr. Vladimer Svanadze for inviting me to present this paper. I greatly appreciate the kind hospitality of the event sponsors, and members of the Scientific Cybersecurity Association, especially Diana Popova and Irakli Pirtskhalava.

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES

- 405d.hhs.gov (2023). Technical Volume 2: Cybersecurity practices for medium and large healthcare organizations.
- Alexander, B., S. Haseeb and A. Baranchuk (2019). "Are implanted electronic devices hackable?" Trends in cardiovascular medicine **29**(8): 476-480.
- Antonakakis, M., T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi and M. Kallitsis (2017). Understanding the mirai botnet. 26th USENIX security symposium (USENIX Security 17).
- Beerman, J., D. Berent, Z. Falter and S. Bhunia (2023). A review of colonial pipeline ransomware attack. 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), IEEE.
- Buck, C., C. Olenberger, A. Schweizer, F. Völter and T. Eymann (2021). "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust." Computers & Security **110**: 102436.
- Datta, J., R. Dasgupta, S. Dasgupta and K. R. Reddy (2021). Real-time threat detection in ueba using unsupervised learning algorithms. 2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), IEEE.
- IBM (2024). What is UEBA (User entity behavioral analytics)?
- Jain, R., M. Singh, A. R. Rao and R. Garg (2024). "Predicting hospital length of stay using machine learning on a large open health dataset." BMC Health Services Research **24**(1): 860.
- Karambelas, C. (2020). "Health Care Technology: Ransomware Risk and Protection." American Bankruptcy Institute Journal **39**(5): 30-57.
- Rao, A., K. Mishra and N. Recharla (2020). Designing an Internet of Things Laboratory to Improve Student Understanding of Secure Embedded Systems. National Cyber Summit, Springer.
- Rao, A. R. and D. Clarke (2019). Capacity Building for a Cybersecurity Workforce Through Hands-on Labs for Internet-of-Things Security. National Cyber Summit, Springer.
- Rao, A. R. and A. Elias-Medina (2024). "Designing an internet of things laboratory to improve student understanding of secure IoT systems." Internet of Things and Cyber-Physical Systems **4**: 154-166.
- Rao, A. R., R. Jain, M. Singh and R. Garg (2024). "Predictive interpretable analytics models for forecasting healthcare costs using open healthcare data." Healthcare Analytics **6**: 100351.
- Siddiqi, R., S. Singh, L. Zuck and C. Kanich (2023). Tracking, But Make It Offline: The Privacy Implications of Scanning QR Codes Found in the World. Proceedings of the 2023 Workshop on Technology and Consumer Protection.
- Synk (2023). 2023 AI Code Security Report.
- Tundis, A., E. M. Modo Nga and M. Mühlhäuser (2021). An exploratory analysis on the impact of Shodan scanning tool on the network attacks. Proceedings of the 16th International Conference on Availability, Reliability and Security.
- Vegas, J., A. R. Rao and C. Llamas (2024). "Deep Learning System for User Identification Using Sensors on Doorknobs." Sensors **24**(15): 5072.
- Zhou, X., X. Ye, I. Kevin, K. Wang, W. Liang, N. K. C. Nair, S. Shimizu, Z. Yan and Q. Jin (2023). "Hierarchical federated learning with social context clustering-based participant selection for internet of medical things applications." IEEE Transactions on Computational Social Systems **10**(4): 1742-1751.

## SHORT NOTE REGARDING BLACKBOX ANDROID MALWARE DETECTION USING MACHINE LEARNING AND EVASION ATTACKS TECHNIQUES

Professor Dr. Razvan Bocu

Department of Mathematics and Computer Science, Transilvania University of Brasov, Romania

**ABSTRACT:** Over the past ten years, researchers have extensively explored the vulnerability of Android malware detectors to adversarial examples through the development of evasion attacks. Nevertheless, the feasibility of these attacks in real-world use case scenarios is debatable. Most of the existing published papers are based on the assumptions that the attackers know the details of the target classifiers used for malware detection. Nevertheless, in reality, malicious actors have limited access to the target classifiers. This proposed talk presents a problem-space adversarial attack designed to effectively evade blackbox Android malware detectors in real-world use case scenarios. The proposed approach constructs a collection of problem-space transformations derived from benign donors that share opcode-level similarity with malware applications through the consideration of an  $n$ -gram-based approach. These transformations are then used to present malware instances as legitimate entities through an iterative and incremental manipulation strategy. The proposed presentation will describe a manipulation model that is based on a query-efficient optimization algorithm, which can identify and implement the required sequences of transformations into the malware applications. The model has already been evaluated relative to more than 1,000 malware applications. This demonstrates the effectiveness of the reported approach relative to the generation of real-world adversarial examples in both software and hardware-related scenarios. The experiments that we conducted demonstrate that the proposed model may effectively trick various malware detectors into believing that malware entities are legitimate. More precisely, the proposed model generates evasion rates of 90%–95% relative to data sets like DREBIN, Sec-SVM, ADE-MA, MaMaDroid, and Opcode-SVM. The average number of required computational operations belongs to the range [1..7]. Additionally, it is relevant to note that the proposed adversarial attack preserves its stealthiness against the virus detection core of three popular commercial antivirus software applications. The obtained evasion rate is 87%, which further proves the proposed model's relevance for real-world use case scenarios.

**KEYWORDS:** *Blackbox Malware Detection, Android, Machine Learning, Evasion Attacks, Android APK Decompilation*

### INTRODUCTION

Machine Learning (ML) determines a references conceptual system, which may be considered to address the challenges posed by continues to show promise in detecting complex and zero-day malicious programs. Thus, the suggested bibliographic references report interesting machine learning-based contributions.

The first perspective relates to the feature representation of Android applications. Thus, the application of a slight change in the structure of the feature representation of a malware application may break its functionality, considering that malware features obtained from Android Application Packages (APK) are generally discrete (e.g., application permissions), as compared to continuous features, such as the pixel intensity in a grayscale image. A potential solution is represented by the manipulation of the features acquired from the Android Manifest file. Nevertheless, the feasibility of such structural changes relative to the generation of executable adversarial examples (AE) is debatable for a number of reasons. First, the modification of the features that are part of the Android Manifest, such as content providers, intents, is not meant to guarantee the proper function of the original applications that contain the malicious payload. Second, the addition of unused features to the Manifest file may be discarded through the application of preprocessing techniques. Additionally, the advanced Android malware

detectors especially consider the semantics of Android applications, which are represented by the Dalvik bytecode, in the detriment of the Manifest files.

Another difficulty is represented by the limitations of feature mapping techniques, which are considered to convert Android applications from the problem space, all the way to the feature space. These technical solutions are not reversible, which means that feature-space perturbations cannot be directly transformed into a malicious application. The proper approach to an inverse feature-mapping problem relates to a common approach to process real-world malware applications using problem-space transformations that relate to the features used as part of the respective ML models. Through the application of these feature-based transformations to the target Android applications the adversaries are able to create hazardous evasion attacks. Nevertheless, the determination of the proper transformations that address problem-space constraints is not determined by a simple process. First, certain modifications that mimic feature-space perturbations may not result in feasible adversarial examples, considering that they ignore feature dependencies generated from real-world objects. Moreover, certain transformations that meet problem-space constraints for manipulating real objects may introduce undesired or incompatible payloads into malware applications. These types of transformations not only might generate perturbations that are different from the reference that is expected by the attacker, but they may also lead to the functional crash of the adversarial malware applications.

The final problematic aspect is connected to the current methods, which generate adversarial examples based on the specific features of the target malware detectors, such as the ML algorithmic model, and the related features set. These solutions presume that attackers possess either Perfect Knowledge (PK), or Limited Knowledge (LK) regarding the target classifiers. Nevertheless, relative to real-world use case scenarios, adversaries usually possess Zero Knowledge (ZK) regarding the target malware detectors. This aligns in a closer manner with reality, considering that antivirus systems operate as blackbox engines that are interrogated. Thus, certain solutions have evaluated partial blackbox configurations to generate adversarial examples through leveraging the feedback from the target detectors. It is relevant to note that these approaches are inefficient relative to the evasion costs, which include the high number of queries that are necessary, and the extent of manipulation applied to the input sample. Thus, the efficiency of the involved interrogations is fundamental considering the associated costs, and the risk of detectors blocking suspicious queries. Moreover, the application of only the necessary manipulation operations is preferred, considering that, otherwise, the malicious functionality of the applications may be affected.

The research process, which this paper reports, determined the following contributions.

- We propose a comprehensive and generalized evasion attack, which can bypass blackbox Android malware classifiers through a two-step process: (i) *preparation* and (ii) *manipulation*. The first step involves implementing a donor selection technique to create an action set comprising a collection of problem-space transformations. This relates to code snippets known as *gadgets*.
- These gadgets are derived by conducting program slicing on benign apps, known as donors, which are publicly available. By injecting each gadget into a malware app, specific payloads from a benign donor can be incorporated into the malware application.
- The proposed technique utilizes an *n-gram-based similarity (sequence of n adjacent symbols in a particular order)* method to identify suitable donors, particularly benign apps that exhibit similarities to malware apps at the opcode level (**specifies operation to be executed**). Applying transformations derived from these donors to malware apps can enable them to appear legitimate (benign), or move them towards blind spots of ML classifiers.
- This approach aims to achieve the desired outcome of introducing transformations that not only ensure adherence to problem-space constraints (**preserved semantics, robustness to preprocessing, and plausibility**), but also possibly lead to malware classification errors.
- We propose a *blackbox evasion* attack that generates real-world Android Adversarial Attacks (AE-Adversarial Examples) that adhere to problem-space constraints. To the best of our knowledge, this is one of the few studies in the Android scope that successfully evades ML-based malware detectors by effectively manipulating malware samples without performing feature-space perturbations.

- We demonstrate this is a *query-efficient* attack capable of deceiving various blackbox ML-based malware detectors through minimal querying. Thus, our proposed problem-space adversarial attack achieves evasion rates of 92%, 88%, 89%, 98%, and 84% against DREBIN, Sec-SVM, ADE-MA, MaMaDroid, and Opcode-SVM, respectively.
- Our proposed attack can operate with either *soft labels* (confidence scores), or *hard labels* (classification labels) of malware apps, as specified by the target malware classifiers, to generate adversarial examples.
- We assess the practicality of the proposed evasion attack under real-world constraints by evaluating its performance in deceiving popular commercial antivirus products. Specifically, our findings indicate that proposed approach may significantly diminish the effectiveness of three popular commercial antivirus products, achieving an average evasion rate of approximately 86%.

## PROPOSED ATTACK METHOD

The purpose of the adversarial goal is to manipulate Android malware samples in order to deceive static ML-based Android malware detectors. The proposed attack is an untargeted attack (Carlini et al., 2019) designed to mislead binary classifiers considered in Android malware detection, causing Android malware apps to be misclassified. More precisely, the objective is to trick malware classifiers into classifying malware samples as benign.

Concerning the adversarial knowledge, the proposed evasion attack has blackbox access to the target malware classifier. Therefore, it does not have knowledge of the training data  $\mathcal{D}$ , the feature set  $\mathcal{X}$ , or the classification model  $f$ , more precisely to the classification algorithm and its hyperparameters. The attacker can only obtain the classification results (hard labels or soft labels) by querying the target malware classifier.

It is also relevant to discuss about the adversarial capabilities. Thus, the designed attack model is conceived to deceive blackbox Android malware classifiers during their prediction phase. Our attack manipulates an Android malware app by applying a set of safe transformations, known as Android gadgets (slices of the benign apps' bytecode), which are optimized through interactions with the blackbox target classifier. Furthermore, in order to avoid major disruptions to apps, the manipulation process of a malware app is conducted gradually, making it resemble benign apps. This is achieved by injecting a minimal number of gadgets extracted from benign apps into the malware app, and the process continues until the malware app is misclassified or reaches the predefined evasion cost. In addition to the problem-space constraints discussed in previous research contributions, our model must also adhere to two additional constraints highlighting the significance of minimizing evasion costs:

- **Number of queries.** Proposed approach is a decision-based adversarial attack that aims to generate AEs while minimizing the number of queries, thus reducing the associated costs.
- **Size of adversarial payloads.** In order to generate executable and visually inconspicuous AEs, such as those with minimal file size, proposed approach aims to minimize the size of injected adversarial payloads.

It is relevant to note that that each gadget consists of an organ, which represents a slice of program functionality, an entry point to the organ, and a vein, which represents an execution path that leads to the entry point. Proposed model extracts gadgets from benign apps by identifying entry points, which are typically API calls, through string analysis. The proposed attack assumes that the benign apps used for gadget extraction are not obfuscated, particularly in terms of their API calls. This is because the proposed model relies on string analysis to identify entry points, which limits its ability to extract gadgets from obfuscated apps. The gadget injection is **considered successful** when both the classification loss value of the manipulated app increases, and the injected adversarial payload conforms to the predefined size of the adversarial payload. Additionally, the injected gadgets are placed within the block of an obfuscated condition statement that is always evaluated as False during runtime, and cannot be analyzed during early preprocessing stages.

It is relevant to note that, concerning the defender's capabilities, it is assumed that the target ML models do not employ adaptive defenses that are aware of the operations performed by proposed model due to

disclosing detectors' vulnerability to the detection core of our proposed model. Specifically, these target models are unable to enhance their resilience by incorporating AEs generated by proposed model during adversarial training. Furthermore, they lack the capability to detect and block queries from proposed model, if they become suspicious of its origin. Additionally, our analysis suggests that proposed model can still be effective, even if we relax the second assumption regarding the defender's capabilities. This is supported by empirical evidence demonstrating that our attack often requires only a minimal number of queries to generate adversarial examples.

## METHODOLOGY

The primary goal of proposed model is to transform a malware app into an adversarial app insuch a way that it retains its malicious behavior, but is no longer classified as malware by ML-based malware detectors. This is achieved through an iterative and incremental algorithm used in the proposed attack, which aims to disguise malware APKs as benign ones. The attack algorithm generates real-world adversarial examples from malware apps using *problem-space transformations* that satisfy problem space constraints. These transformations are extracted from benign apps in the wild, which are similar to malware apps using an *n-gram*-based similarity model.

Considering this approach, a random search (RS) algorithm is used to optimize the manipulations of applications. Each malware app undergoes incremental tweaking during the optimization process, where a sequence of transformations is applied over different iterations. These transformations are extracted from benign apps in the wild, which are similar to malware apps using an *n-gram*-based similarity model.

The attack pipeline is structured according to the diagram, which is described in Figure 1.

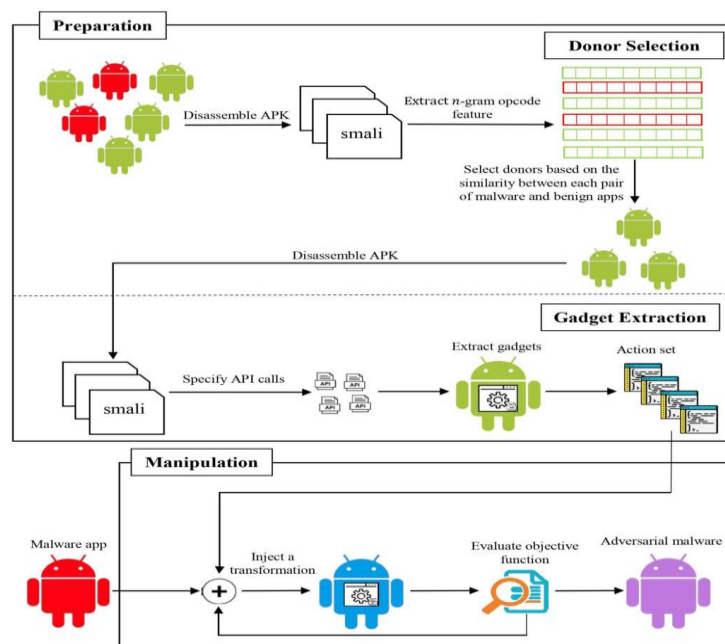


Fig.1. Logical flow of the attack pipeline

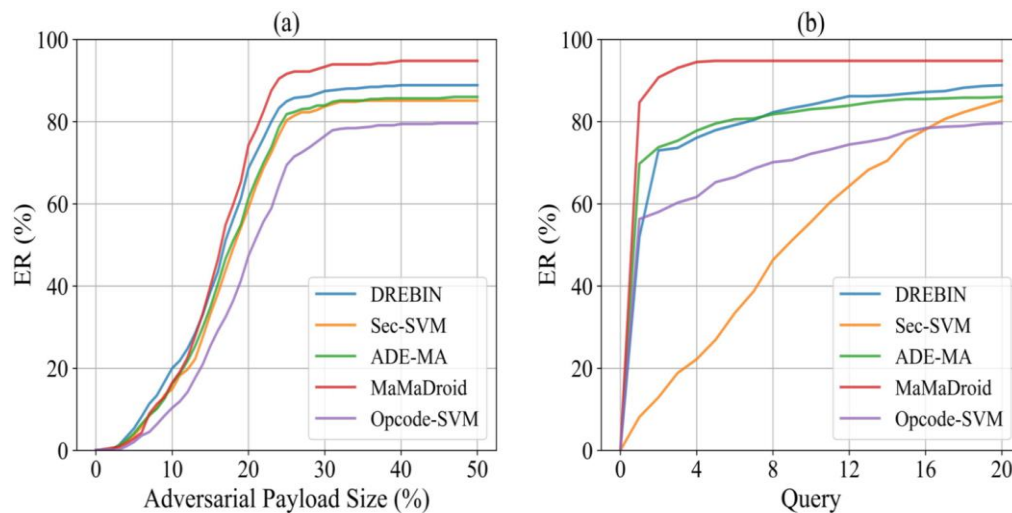
## EXPERIMENTAL PROCESS

The experimental dataset consists of  $\approx 170K$  samples, each represented using the DREBIN feature set (Arp et al., 2014). The samples are feature representations of Android applications collected from AndroZoo (AndroZoo, 2024). These collected applications were published between January 2017 and December 2018. Thus, an APK is considered malicious or clean if it has been detected by any 4+ or 0 VirusTotal (VT) (VirusTotal, 2024) engines, respectively. It is important to note that the threshold-

based labeling approach does not rely on specific engines, but instead considers the number of engines involved. Therefore, the engines used for labeling may vary from sample to sample.

Relative to the performance metrics, we consider the True Positive Rate (TPR), and False Positive Rate (FPR) as performance metrics for evaluating the effectiveness of malware classifiers in detecting Android malware. Additionally, we consider the Evasion Rate (ER) and Evasion Time (ET) as proposed model's performance assessment metrics in deceiving malware classifiers. Thus, ER is calculated as the ratio of correctly detected malware samples that are able to evade the target classifiers after manipulation, relative to the total number of correctly classified malware samples. Additionally, ET represents the average time, expressed in seconds, required by proposed model to generate an AE, encompassing both the optimization and query times. The optimization time primarily consists of the execution times of random search, injecting problem-space transformations, and performing feature extraction to represent manipulated applications within the feature space. Following, six research questions were considered.

**RQ1.** The evasion rates of proposed approach in fooling various malware detectors under different adversarial payload sizes and query numbers



*Fig.2. Experimental results related to RQ1*

**RQ2.** Effectiveness of proposed model in misleading different malware detectors. NoQ, NoT, and AS denote Avg. No. of Queries, Avg. No. of Transformations, and Avg. Adversarial Payload Size, respectively.

Type of Threat	Target Model	ER (%)	ET (s)	NoQ	NoT	AS (%)
Soft Label	DREBIN	88.9	210.3	3	2	15.5
	Sec-SVM	85.1	495.4	9	4	16.4
	ADE-MA	86.0	126.2	2	1	16.3
	MaMaDroid	94.8	131.4	1	1	15.9
	Opcode-SVM	79.6	114.1	3	2	18.3
Optimal Hard Label	DREBIN	84.5	240.6	4	2	16.2
	Sec-SVM	82.6	613.1	9	6	16.5
	ADE-MA	84.4	121.2	2	1	16.3
	MaMaDroid	94.8	133.7	1	1	15.9
	Opcode-SVM	74.1	101.2	2	1	18.2
Non-optimal Hard Label	DREBIN	79.7	357.2	4	4	16.9
	Sec-SVM	78.2	782.8	9	9	17.3
	ADE-MA	82.7	157.3	2	2	16.4
	MaMaDroid	94.8	132.6	1	1	15.9
	Opcode-SVM	66.6	76.2	1	1	18.3

*Fig.2. Experimental results related to RQ2*



Data in Figure 2 demonstrate a 15% improvement in the evasion rate(ER) of proposed model when considering Opcode-SVM in the soft-label setting, compared to the non-optimal hard-label setting. Furthermore, when operating in the soft-label setting, proposed model requires notably fewer transformations to bypass DREBIN and Sec-SVM, as compared to the non-optimal hard-label setting, which confirms the effectiveness of described approach in solving the optimization problem.

The table further illustrates that our optimization leads to a substantial reduction in evasion time (ET) compared to the non-optimal hard-label setting. Specifically, for DREBIN and Sec-SVM, this leads to a time reduction of  $\approx 41\%$  and  $\approx 37\%$ , respectively. This significant enhancement can be attributed to the reduction in the number of transformations, achieved through the utilization of our proposed optimization model.

Thus, the experimental results demonstrate that the proposed adversarial attack is a versatile blackbox attack that does not make assumptions about target detectors, including the ML algorithms or the features used for malware detection. As a consequence, it can operate effectively in various attack settings.

### RQ3. Proposed model relative to other attacks

We conduct an empirical analysis to assess how the proposed attack pattern performs in comparison to other similar attacks. We consider four baseline attacks: PiAttack, Sparse-RS, ShadowDroid, and GenDroid operating in whitebox, graybox, semi-blackbox, and blackbox settings, respectively. These attacks serve as suitable benchmarks, allowing us to assess the performance of described approach from different perspectives, such as evasion rate and the number of queries. Similar to our model, Sparse-RS, ShadowDroid, and GenDroid generate adversarial examples by querying the target detectors.

Additionally, PiAttack is a problem-space adversarial attack that employs a similar type of transformation to generate AEs. Although PiAttack is a whitebox evasion attack, it establishes a benchmark for optimal evasion performance, facilitating the evaluation of the comparative effectiveness of other attacks with limited or zero knowledge about the targeted detectors.

We selected DREBIN, Sec-SVM, and ADE-MA as the target detectors because they align with the threat models of PiAttack, Sparse-RS, and ShadowDroid. Although our model has zero knowledge about DREBIN, Sec-SVM, and ADE-MA, its evasion rates for bypassing these detectors are comparable to PiAttack, where the adversary has full knowledge of the target detectors.

Our empirical analysis shows that the reported model requires adding more features to evade DREBIN, Sec-SVM, and ADE-MA. Concretely, on average, proposed model makes 54–90 new features appear in the feature representations of the malware apps when it applies transformations to the apps for evading DREBIN, Sec-SVM, and ADE-MA, while the transformations used by PiAttack, on average, trigger 11–68 features. It is important to note that the reference attack's ability to add a smaller number of features is attributed to its complete knowledge of the details of DREBIN, Sec-SVM, and ADE-MA, while our model lacks this specific information.

The evasion rate of Sparse-RS for DREBIN and Sec-SVM demonstrates that random alterations in malware features do not necessarily result in the successful generation of AEs, even when adversaries have access to the target models' training set. Although proposed model operates solely in a blackbox setting, this attack outperforms Sparse-RS by a considerable margin for both DREBIN and Sec-SVM, i.e., 74.8% and 89.8% improvement, respectively. Moreover, GenDroid exhibits superior evasion rates compared to our model when targeting DREBIN and ADE-MA; nevertheless, its efficacy is substantially nullified when facing Sec-SVM, a resilient malware detector. Our empirical analysis also highlights the remarkable efficiency of our model in terms of the number of queries compared to other query-based attacks. Specifically, on average, our model requires only 1–7 queries to bypass DREBIN, Sec-SVM, and ADE-MA, while Sparse-RS, ShadowDroid, and GenDroid demand 2–195, 29–64, and 81–336 queries, respectively.

#### RQ4. Real-world effectiveness

We selected three popular antivirus engines in the Android ecosystem: Total AV, AVG, Avast. Thus, our proposed attack pattern can effectively evade all antivirus products with a few queries. Thus, the effectiveness of our model can be primarily attributed to the transformations rather than the optimization technique. This is evident from the fact that in most cases, only one query is required to generate adversarial examples.

It is relevant to mention that our model is capable to effectively deceive VirusTotal (VT) engines with an average of 73.97%. It is worth noting that the findings in this experiment validate the results observed in previous studies, such as (Ceschin et al., 2020).

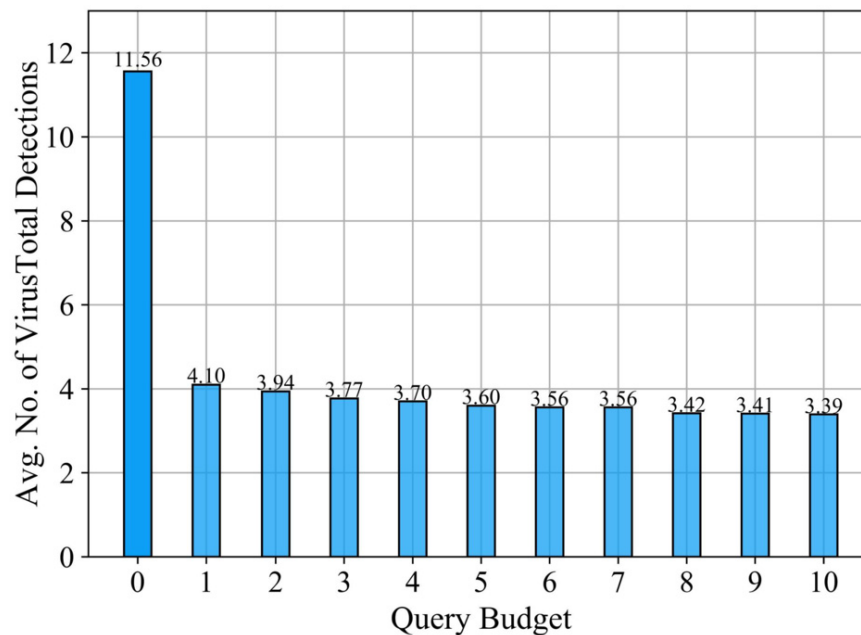


Fig.3. Experimental results related to RQ4

#### RQ5. Real-world relevance of advanced comparative performance analyses

We evaluated the evasion rates of adversarial examples generated on a model (e.g., Sec-SVM), which works as a surrogate model, in misleading other target models (e.g., DREBIN). This is a stricter threat model that evaluates the performance of our model in cases where adversaries are not capable of querying the target detectors. Thus, as soon as our model considers a stronger surrogate model, such as Sec-SVM, the adversarial examples exhibit higher transferability.

#### RQ6. Real-world effectiveness of proposed model when utilizing an alternative search strategy for manipulation.

We performed an empirical analysis to evaluate the performance of our model when utilizing an alternative search strategy for manipulation. We introduced a baseline manipulation method based on genetic algorithms (GA) for use relative to our model, where the fitness function of the baseline is the same as the RS-based method.

The inclusion of RS into the algorithmic model indicates that this strategy outperforms GA. Specifically, RS not only leads to a 36.5% enhancement in (Evasion Rate)ER but also accelerates our model by  $\approx 3\times$ . These improvements are achieved with only 3 queries compared to the GA's 24 queries.

## CONCLUSION

This paper reports a novel Android evasion attack in the problem space, designed to generate real-world adversarial Android malware, which is capable of evading ML-based Android malware detectors relative to a blackbox setting.

It is important to note that, unlike previous approaches, this directly operates in the problem space without initially focusing on finding feature-space perturbations. Experimental results demonstrate the effectiveness of this approach in deceiving various academic and commercial malware detectors. Therefore, the results of the experimental process suggest that this integrated approach may be used in order to further tweak the effectiveness of existing and future malware detectors.

## ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

## REFERENCES

Yousra Aafer, Wenliang Du, and Heng Yin, “DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android,” in *Springer eBooks*, 2013, 86–103, [https://doi.org/10.1007/978-3-319-04283-1\\_6](https://doi.org/10.1007/978-3-319-04283-1_6).

“Can Machine/Deep Learning Classifiers Detect Zero-Day Malware With High Accuracy?,” IEEE Conference Publication | IEEE Xplore, December 1, 2019, <https://ieeexplore.ieee.org/document/9006514>.

Cara, Fabrizio, Michele Scalas, Giorgio Giacinto, and Davide Maiorca. 2020. "On the Feasibility of Adversarial Sample Creation Using the Android System API" *Information* 11, no. 9: 433. <https://doi.org/10.3390/info11090433>

“DroidEye: Fortifying Security of Learning-Based Classifier Against Adversarial Android Malware Attacks,” IEEE Conference Publication | IEEE Xplore, August 1, 2018, <https://ieeexplore.ieee.org/document/8508284>.

Francesco Croce et al., “Sparse-RS: A Versatile Framework for Query-Efficient Sparse Black-Box Adversarial Attacks,” *Proceedings of the AAAI Conference on Artificial Intelligence* 36, no. 6 (June 28, 2022): 6437–45, <https://doi.org/10.1609/aaai.v36i6.20595>.

“Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection,” IEEE Journals & Magazine | IEEE Xplore, August 1, 2019, <https://ieeexplore.ieee.org/abstract/document/7917369>.

“Malware Detection and Classification Based on N-Grams Attribute Similarity,” IEEE Conference Publication | IEEE Xplore, July 1, 2017, <https://ieeexplore.ieee.org/document/8005908>.

“Program Slicing,” IEEE Journals & Magazine | IEEE Xplore, July 1, 1984, <https://ieeexplore.ieee.org/abstract/document/5010248>.

“ShadowDroid: Practical Black-box Attack Against ML-based Android Malware Detection,” IEEE Conference Publication | IEEE Xplore, December 1, 2021, <https://ieeexplore.ieee.org/document/9763777>.

Jinrong Bai, Junfeng Wang, and Guozhong Zou, “A Malware Detection Scheme Based on Mining Format Information,” *The Scientific World JOURNAL* 2014 (January 1, 2014): 1–11, <https://doi.org/10.1155/2014/260905>.

Daniel Arp, Michael Spreitzenbarth, Malte Hubner, Hugo Gascon, Konrad Rieck, „DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket“, 2014, [https://media.telefonicatech.com/telefonicatech/uploads/2021/1/4915\\_2014-ndss.pdf](https://media.telefonicatech.com/telefonicatech/uploads/2021/1/4915_2014-ndss.pdf) .

AndroZoo. Available online: <https://androzoo.uni.lu/> , (Accessed: 7 November 2024).

VirusTotal. Available online: <https://www.virustotal.com/gui/home/upload> , (Accessed: 7 November 2024).

Fabício Ceschin, Marcus Botacin, Heitor Murilo Gomes, Luiz S. Oliveira, and André Grégio. 2020. Shallow Security: on the Creation of Adversarial Variants to Evade Machine Learning-Based Malware Detectors. In Proceedings of the 3rd Reversing and Offensive-oriented Trends Symposium (ROOTS'19). Association for Computing Machinery, New York, NY, USA, Article 4, 1–9. <https://doi.org/10.1145/3375894.3375898> .

ინტერნეტ ფრაგმენტაცია როგორც ახალი გამოწვევა ინტერნეტის  
ერთიანობის, უსაფრთხოებისა და სტაბილურობისთვის

**INTERNET FRAGMENTATION AS A NEW CHALLENGE FOR THE  
UNIFIED, SECURITY AND STABILITY OF INTERNET**

ვლადიმერ სვანაძე  
კავკასიის უნივერსიტეტის ავილირებული პროფესორი  
საჯარო მმართველობის დოქტორი  
Vladimer Svanadze  
Affiliated Professor at the Caucasus University  
Doctor in the Public Administration

**აბსტრაქტი:** გლობალური ინტერნეტის ერთიანობისთვის, უსაფრთხოებისა და სტაბილური განვითარებისთვის ახალ გამოწვევად იქცა ფრაგმენტაციის სულ უფრო ღრმა პროცესი, ანუ შეიძლება ითქვას, რომ ინტერნეტს ემუქრება დაშლის საფრთხე ერთმანეთთან სუსტად დაკავშირებულ ცალკეულ ფრაგმენტებად. ფრაგმენტაციის გამოძწევ მთავრდება სახელდება მთელი რიგი შემთხვევითი ტენდენციები, რაც უკავშირდება ინტერნეტის ტექნოლოგიურ განვითარებას, ცალკეული ქვეყნების ინტერნეტ პოლიტიკებსა და კომერციულ საქმიანობას, ასევე არსებულ საერთაშორისო ვითარებას. ფაქტიურად, ფრაგმენტაციის პროცესმა გლობალური ინტერნეტ სივრცე დააყენა ახალი საფრთხის წინაშე, რაც გარდა აღნიშნულისა, ასევე უკავშირდება ცალკეული ავტორიტარული ხელისუფლებების მხრიდან მასზე ტოტალური კონტროლის დაწესებას, გლობალურად არსებულ ეთნოკონფლიქტებსა და საომარ მოქმედებებს, აგრეთვე გაზრდილ კიბერდანაშაულებებს. ყოველივე ეს კი არღვევს ინტერნეტის ერთიანობასა და მდგრადობას, საფრთხეს უქმნის მის სტაბილურ და უსაფრთხო განვითარების პროცესს. მოცემული პროცესი ასევე ეწინააღმდეგება გაერთიანებული ერების ორგანიზაციის ასამბლეის მიერ 2005 წელს მიღებულ ტუნისის დღის წესრიგს. ინტერნეტ ფრაგმენტაცია არის ახალი პროცესი და ის წარმოადგენს ფართო შესწავლის საკითხს. წინამდებარე ნაშრომი მოკლედ მიმოიხილავს ინტერნეტ ფრაგმენტაციის technical, commercial and governmental ფორმებს, და ამავდროულად, ყურადღებას ამახვილებს უფრო ფრაგმენტაციის political ასპექტზე. კერძოდ, მოცემული საკითხი განიხილება უკრაინის ომისა და რუსეთის ხელისუფლების ინტერნეტ პოლიტიკის კუთხით. სწორედ, ცალკეული ქვეყნების ინტერნეტ პოლიტიკები და მიდგომები ის, რაც მიიჩნევა ფრაგმენტაციის პოლიტიკურ ნაწილად, და რაც ყველაზე მნიშვნელოვანია ხშირ შემთხვევაში პოლიტიკურ ფრაგმენტაციას გავლენა აქვს ფრაგმენტაციის დანარჩენ სამ ფორმაზე. აქვე ყურადღებას იმსახურებს ის გარემოებაც, რომ ისეთი გლობალური ორგანიზაციები, როგორებიც არის ICANN და RIPE NCC ჯერ - ჯერობით ახერხებენ შეინარჩუნონ დამოუკიდებელი პოზიცია და არ მოახდინონ საკითხის პოლიტიკურ ჭრილში გადაყვანა, რადგან ინტერნეტის ტექნიკური მართვის პოლიტიზირება წარმოადგენს იმ საფრთხეს, რასაც შეიძლება მოყვეს ინტერნეტ ფრაგმენტაციის შეუქცევადი პროცესი.

**საკვანძო სიტყვები:** ინტერნეტის ფრაგმენტაცია, ერთიანობა, მდგრადობა, გამძლეობა, უსაფრთხოება, სტაბილურობა, განვითარება, პოლიტიკური, ტექნიკური, კომერციული, სამთავრობო, პოლიტიკა.

**ABSTRACT:** The deepening process of fragmentation has become a new challenge for the unity, security and stable development of the global Internet. That is, it can be said that the Internet is in danger of disintegrating into separate fragments that are weakly connected to each other. A number of

disturbing trends related to the technological development of the Internet, the Internet policies and commercial activities of individual countries, as well as the current international situation are called the causes of fragmentation. In fact, the process of fragmentation has put the global Internet space in front of a new threat, which is also related to the establishment of total control over it by individual autocratic governments, the global ethno-conflicts and hostilities, as well as increased cybercrimes. All this violates the unity and stability of the Internet and threatens its stable and safe development process. This process also contradicts the Tunisian Agenda adopted by the United Nations Assembly in 2005. Internet fragmentation is a new process and it is a subject of extensive research. This paper briefly reviews the technical, commercial and governmental forms of Internet fragmentation, and at the same time, focuses on the political aspect of fragmentation. In particular, this issue is discussed in terms of the war in Ukraine and the Internet policy of the Russian government. It is the Internet policies and approaches of individual countries that are considered the political part of fragmentation, and in many cases political fragmentation has an impact on the other three forms of fragmentation. The fact that such global organizations as ICANN and RIPE NCC still manage to maintain an independent position and not to turn the issue into a political one deserves attention here, because the politicization of the technical management of the Internet represents the danger that may follow the irreversible process of Internet fragmentation.

**KEYWORDS:** Internet fragmentation, unity, sustainability, robustness, security, stability, development, political, technical, commercial, governmental, policy.

## შესავალი

ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფი მიმართულებით განვითარების პოზიტიურ პროცესს თან ახლავს გარკვეული რისკები, რაც საფრთხეს უქმნის გლობალური ინტერნეტ ქსელის ერთიანობასა და უსაფრთხოებას, მის მდგრადობასა და სტაბილურ განვითარებას.

როცა ვსაუბრობთ გლობალური ინტერნეტ ქსელის ერთიანობაზე, უსაფრთხოებასა და სტაბილურობაზე, აუცილებლად უნდა აღვნიშნოთ გაერთიანებული ერების ორგანიზაციის გენერალური მდივნის მიერ მოწვეული ინტერნეტ მმართველობის ყოველწლიური ფორუმი, რომლის მუშაობაში ჩართული არის ყველა დაინტერესებული მხარე – საჯარო და კერძო სექტორები, სამოქალაქო საზოგადოება და აკადემიური წრეების წარმომადგენლები. ეს არის საუკეთესო პლატფორმა, სადაც ხდება ინტერნეტ სივრცეში მიმდინარე პროცესების შესახებ აზრთა გაცვლა, დისკუსია და გამოცდილებების გაზიარება დაინტერესებულ მხარეთა შორის, როგორც გლობალურ, ისე ეროვნულ და რეგიონულ დონეზე.

გაერთიანებული ერების ორგანიზაციის მხრიდან ინტერნეტ მმართველობის ფორუმის მოწვევას წინ უსწრებდა 2005 წელს საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგის მიღება. ეს მოიცავდა ტერმინის ინტერნეტის მმართველობის განმარტებასა და იმის აღიარებას, რომ ინტერნეტის მართვის პროცესი მოიცავს დაინტერესებულ მხარეთა ჩართულობას სხვადასხვა როლში. კერძოდ, საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგში ვკითხულობთ, რომ „ინტერნეტის მმართველობა არის მთავრობების, კერძო სექტორისა და სამოქალაქო საზოგადოების მიერ თავიანთი როლების შემუშავება და გამოყენება საერთო პრინციპების, ნორმების, წესების, გადაწყვეტილების მიღების პროცედურებისა და პროგრამების, რომლებიც აყალიბებენ ინტერნეტის ევოლუციას და გამოყენებას“. აქვე უნდა აღინიშნოს, რომ ტუნისის დღის წესრიგის 72 - ე პარაგრაფი ადგენს ინტერნეტ მმართველობის ფორუმის მანდატს, სადაც ვკითხულობთ, რომ ფორუმზე უნდა ხდებოდეს:

- a. „.....ინტერნეტის მართვის ძირითად ელემენტებთან დაკავშირებული საჯარო პოლიტიკის საკითხების განხილვა, რათა ხელი შეუწყოს ინტერნეტის მდგრადობას, გამძლეობას, უსაფრთხოებას, სტაბილურობას და განვითარებას.....“

ფაქტიურად, გაერთიანებული ერების ორგანიზაციის ასამბლეა აღიარებს ფორუმის მნიშვნელობას ინტერნეტის მდგრადობის, გამძლეობის, უსაფრთხოების, სტაბილურობისა და განვითარების ხელშეწყობაში.

### ინტერნეტ ფრაგმენტაციის ფორმები

სწორედ ინტერნეტ და ინტერნეტ ტექნოლოგიების სულ უფრო აქტიურმა გამოყენებამ კიდევ უფრო გაზარდა მისი მნიშვნელობა და მასზე დამოკიდებულება. გარდა ამისა, ინტერნეტი და ზოგადად, კიბერსივრცე დადგა ახალი საფრთხის წინაშე, რაც უკავშირდება ცალკეული ავტოკრატული ხელისუფლებების მხრიდან მასზე ტოტალური კონტროლის დაწესებას, გლობალურად არსებულ ეთნოკონფლიქტებსა და საომარ მოქმედებებს, გაზრდილ კიბერდანაშაულებს. ყოველივე ეს კი არღვევს ინტერნეტის ერთიანობასა და მდგრადობას, საფრთხეს უქმნის მის სტაბილურ და უსაფრთხო განვითარების პროცესს. მოცემული პროცესი ასევე ეწინააღმდეგება გაერთიანებული ერების ორგანიზაციის ასამბლეის მიერ თავის დროზე მიღებულ ტუნისის დღის წესრიგს [1-2].

ბოლო წლებში სულ უფრო ხშირად გამოითქმის შეშფოთება იმის თაობაზე, რომ ინტერნეტს ემუქრება დაშლის საფრთხე ერთმანეთთან სუსტად დაკავშირებულ ცალკეულ ფრაგმენტებად. მთელი რიგი შემაშფოთებელი ტენდენციები, რაც უკავშირდება ტექნოლოგიურ განვითარებას, სახელმწიფოების ინტერნეტ პოლიტიკასა და კომერციულ საქმიანობას, ასევე არსებულ საერთაშორისო ვითარებას, ვრცელდება ინტერნეტ ქსელში, მის ცალკეულ ფენებში, რაც გავლენას ახდენს პროცესზე, რასაც უწოდებს ინტერნეტ ფრაგმენტაცია. თუმცა, უნდა აღინიშნოს, რომ ჯერ კიდევ არ არსებობს ფართო გაგება იმისა თუ რა არის და რა არ არის „ფრაგმენტაცია“, ან რა რისკებს უქმნის ის ინტერნეტის, იგივე კიბერსივრცის ერთიანობას, სტაბილურობასა და უსაფრთხოებას.

აქ ჩნდება კითხვა რა არის „ინტერნეტ ფრაგმენტაცია“ და როგორ შეიძლება ეს ტერმინი თუ ქმედება განისაზღვროს? ინტერნეტ ფრაგმენტაცია, იგივე Splinternet, ეს არის ინტერნეტის საწინააღმდეგო მოვლენა, მისი საპირისპირო, რომლის მიხედვით ღია, უსაფრთხო და სტაბილური გლობალურად ერთიანი ინტერნეტი, რომლითაც ჩვენ ვსარგებლობთ, იყოფა ცალკეულ ერთმანეთისგან იზოლირებულ ქსელებად, რომლებიც კონტროლდება სახელმწიფოებისა და კორპორაციების მიერ. გარდა ამისა, „ინტერნეტ ფრაგმენტაციის“ მსგავს განსაზღვრებას, ბოლო დროს განვითარებული გლობალური მოვლენების გათვალისწინებით, შეიძლება დავუმატოთ ასევე საომარი მოქმედებები და ეთნოკონფლიქტები, რომლებიც უკვე ფიზიკურად აზიანებს კიბერსივრცის ერთიანობას [3-4].

არსებობს ინტერნეტ ფრაგმენტაციის ყველასთვის ნაცნობი სამი ფორმა:

1. **ტექნიკური ფრაგმენტაცია** – ეს არის საბაზისო ინფრასტრუქტურის პირობები, რომლებიც აფერხებენ სისტემების სრულყოფილ და თანხვედრილ ურთიერთობას, მონაცემთა პაკეტების გაცვლასა და ინტერნეტის ნორმალურ ფუნქციონირებას;
2. **სახელმწიფო ფრაგმენტაცია** – ცალკეული ქვეყნების მთავრობების ინტერნეტ პოლიტიკა და ქმედებები, რომლებიც ზღუდავს ან ხელს უშლის ინტერნეტის

გარკვეულ გამოყენებას საინფორმაციო რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის;

3. **კომერციული ფრაგმენტაცია** – ბიზნეს პრაქტიკა, რომელიც ზღუდავს ან ხელს უშლის ინტერნეტის გარკვეულ გამოყენებას საინფორმაციო რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის.

აქვე, ინტერნეტ ფრაგმენტაციის მეოთხე ტიპად შეიძლება დავამატოთ – ინტერნეტ ფრაგმენტაცია, რომელიც მივიღეთ ამა თუ იმ მთავრობების როგორც შიდა, ისე საგარეო ინტერნეტ პოლიტიკის, საომარი მოქმედებებისა და ზოგადად, გლობალურად თუ რეგიონულად არსებული არამდგრადი ვითარების შედეგად, რაც ზიანს აყენებს ინტერნეტის ერთიანობას, უსაფრთხოებასა და სტაბილურობას [5].

ამ მეოთხე ტიპს უწოდებენ პოლიტიკურ ფრაგმენტაციას, რომელსაც ზოგი მოიხსენიებს სახელმწიფო ფრაგმენტაციასთან ერთად. აუცილებელია აღინიშნოს ის გარემოება, რომ ინტერნეტ ფრაგმენტაციის თითოეული ტიპი შეიძლება ძალზედ განსხვავდებოდეს მთელი რიგი განზომილებების მიხედვით. ამ შემთხვევაში გამოვყოთ ოთხი ძირითადი მახასიათებელი, კერძოდ:

- **წარმოშობა** – ანუ არსებობს თუ არა ფრაგმენტაციის ესა თუ ის ფორმა და რა პოტენციური საფრთხის შემცველია ფრაგმენტაციის კონკრეტული ფორმა;
- **მიზანმიმართულობა** – ფრაგმენტაცია ეს არის მიზანმიმართული მოქმედების შედეგი თუ გაუთვალისწინებელი, სპონტანური შედეგი;
- **გავლენა** – არის ფრაგმენტაცია ღრმა, სტრუქტურული და კონფიგურაციული, თუ უფრო ზედაპირული, ვიწრო და შეზღუდული პროცესების ერთობლიობა;
- **ხასიათი** – ზოგადად, არის თუ არა ფრაგმენტაცია დადებითი, უარყოფითი ან ნეიტრალური.

### პოლიტიკური გამოწვევები და ინტერნეტ ფრაგმენტაციის არსებული საფრთხეები

როცა პოლიტიკური ფორმის ფრაგმენტაციაზე ვსაუბრობთ, მსჯელობა იწყება უკრაინა - რუსეთის ომით, რაც დიდ გავლენას ახდენს სწორედ კიბერსივრცეზე. უკრაინაში რუსეთის შეჭრის შემდეგ გაჩნდა საფრთხე, რომ რუსეთი გამოეყოფოდა გლობალურ ინტერნეტს, რაც მართალია არ მოხდა, მაგრამ ჩვენ შეიძლება გავხედოთ გლობალური ინტერნეტის უფრო ფუნდამენტური ფრაგმენტაციის დაწყების პროცესის მოწმენი.

რუსეთის ფედერაციის მთავრობამ დაავალა რუსეთის ოპერატორებს, რომ 2022 წლის 11 მარტისთვის გამხდარიყვნენ დამოუკიდებელი გლობალური ქსელისგან. თუმცა, მართალია, რომ გლობალური ქსელისგან გამოიყოფა მხოლოდ სახელმწიფო ვებგვერდი და სერვერები, მაგრამ რუსეთის გამოყოფა გლობალური ინტერნეტ ქსელისგან ისევ განიხილება და წარმოადგენს მსჯელობის საგანს.

უკრაინაში შეჭრის შემდეგ, რუსეთმა მართლაც გადადგა ქმედითი ნაბიჯები, კერძოდ, რუსეთის ხელისუფლებამ დაბლოკა მრავალი საინფორმაციო საიტი, აკრძალა მრავალი პოპულარული დასავლური ინტერნეტ სერვისი და სოციალური პლატფორმა, მათ შორის Facebook, Instagram და Twitter, შემოიღო ახალი კანონი ე. წ. „fake news“ და დეზინფორმაცია – პროპაგანდის გავრცელების შესახებ. მიუხედავად მსგავსი რეპრესიული ქმედებებისა, რუსეთმა არ გაწყვიტა კავშირი გლობალურ ინტერნეტთან. 2019 წელს მიღებული რუსეთის კანონი „ინტერნეტის სუვერენიტეტის“ შესახებ ინტერნეტის მომწოდებელი ოპერატორებისგან ითხოვს ტრაფიკის მარშრუტიზაცია განახორციელონ იმ გაცვლითი წერტილების საშუალებით, რომლებიც დამტკიცებულია Роскомнадзор - ის ფედერალური სააგენტოს მიერ. გარდა ამისა, კანონი Роскомнадзор - ს უფლებას აძლევს აიძულოს



ინტერნეტის მომსახურების მომწოდებელი კომპანიები განახორციელონ ტრაფიკის მარშრუტიზაცია ბლოკირების სპეციალური სისტემებით, რომელთა გამოყენება ხელისუფლებას შეუძლია ტრაფიკის ფილტრაციისა და მათთვის სასურველი მარშრუტიზაციისთვის. უფრო მეტიც, 2021 წლიდან რუსეთის ინტერნეტ მომწოდებელ კომპანიებს უნდა შეეძლოთ დაამუშაონ მოთხოვნები დომენური სახელების სისტემებზე, სერვერებზე, რომლებიც განლაგებულია ქვეყნის შიგნით და გლობალური ინტერნეტ ქსელიდან გათიშვის შემთხვევაში შესაძლებელი იქნება ინტერნეტ რესურსების მოძებნა. მწელი სათქმელია თუ როგორ იმუშავებს ეს სისტემები რეალურ სიტუაციაში, თუმცა ფაქტია, რომ ავტონომიური სეგმენტი, რომელიც იმეორებს გლობალური ინტერნეტის ფუნქციების დიდ ნაწილს, უფრო რთულად რეალიზდება ტექნიკური კუთხით, ვიდრე პოლიტიკურად. ყოველ შემთხვევაში, რუსეთის შესაძლებლობა შეწყვიტოს მონაცემთა გადაცემა არ წარმოადგენს რაღაც შეუძლებელს და ეს არ გამოიწვევს მომსახურების ხარისხის გაუარესებას.

და მაინც, ომმა უკრაინაში შესაძლოა მისცეს უფრო დიდი ბიძგი გლობალური ციფრული კავშირის ფუნდამენტურ ფრაგმენტაციას. ერთ - ერთ ასპექტს წარმოადგენს ინტერნეტის ტექნიკური მართვის პოლიტიზება, და ამასთან ერთად, ინტერნეტის ფრაგმენტაციის გრძელვადიანი რისკი, რაც იძლევა გარანტიას, რომ მონაცემები შეიძლება გადაეცეს მრავალი ქსელის საშუალებით, რომლებიც ერთად შეადგენს ინტერნეტს, როგორც ერთიან მთლიანობას. რუსეთის აგრესიის საპასუხოდ, უკრაინა შეეცადა გაეწყვიტა რუსეთის კავშირები გლობალურ ინტერნეტთან და ამით შეეზღუდა მისი შესაძლებლობები გადაეჭრა მოთხოვნები ქვეყნის შიგნით. ამ მიზნით, უკრაინამ გააგზავნა წერილი ICANN - თან, რომელიც კოორდინაციას უწევს დომენური სახელების სისტემებს, და მიმართა თხოვნით, გააუქმოს რუსეთის ფედერაციაში გამოშვებული უმაღლესი დონის დომენები (მაგ., „.ru“, „.pp“ და „.su“) და გაეთიშა რუსეთში მდებარე DNS root სერვერები. უკრაინის ხელისუფლებამ ასევე სთხოვა RIPE - ს, რეგიონულ ინტერნეტ რეესტრს ევროპის, ახლო აღმოსავლეთისა და ცენტრალური აზიის ნაწილისთვის, გაეუქმებინა რუსული IP მისამართები. თუმცა, ორივე ორგანიზაციამ, ICANN - მა და RIPE - მა უარყვეს უკრაინის მოთხოვნა და ხაზი გაუსვეს მათი ნეიტრალიტეტის მნიშვნელობას ტექნიკური ინტერნეტის მართვაში, გლობალური და თავსებადი ინტერნეტის შენარჩუნების მიზნით [6-8].

ფაქტობრივად, უკრაინის მოთხოვნის დაკმაყოფილება იქნებოდა საგარეო პოლიტიკისა და ტექნიკური ადმინისტრაციის შერწყმის პრეცედენტი, რაც, თავის მხრივ, ძირს უთხრის ამ ინსტიტუტების, როგორც საყოველთაოდ ლეგიტიმური მმართველობის ორგანოების როლს. თუ ინტერნეტის ტექნიკური მართვის შესახებ გლობალური კონსენსუსი გაქრება, კონკურენტი ინსტიტუტების გაჩენა იქნება ახალი გამოწვევა და მწვავე რისკი ინტერნეტის ერთიანობისთვის. მიუხედავად იმისა, რომ მმართველობითი ინსტიტუტები ეწინააღმდეგებოდნენ პოლიტიკურ დაკვეთებს, ციფრულ ინფრასტრუქტურაზე კონტროლის გაძლიერება, თავის მხრივ, გამოიწვევს ინტერნეტ ფრაგმენტაციის პროცესის კიდევ უფრო მეტ გაძლიერებას.

ფაქტობრივად, რუსეთის უკრაინაში შეჭრის შემდეგ, რუსეთის გლობალური ინტერნეტიდან გათიშვა ჯერ კიდევ არ მომხდარა. თუმცა, უნდა აღინიშნოს ის გარემოება, რომ ომი ხაზს უსვამს სახელმწიფოების დიდ ცდუნებას, ინტერნეტზე ტექნიკური კონტროლი და ინტერნეტის მთლიანი ინფრასტრუქტურა გამოიყენონ როგორც იარაღი. მიუხედავად იმისა, რომ დროულად აღიკვეთა მცდელობები კიბერსივრცის სრული კონტროლი გამოყენებული ყოფილიყო როგორც იარაღი, ომის გარშემო ფართო

გეოპოლიტიკური დაპირისპირება ამჟამინდელს გლობალური ციფრული კავშირის ღრმა ფრაგმენტაციას, ხდის მას უფრო ფუნდამენტურს.

როცა ვსაუბრობთ ინტერნეტის ინფრასტრუქტურაზე კონტროლის დაწესებაზე, აუცილებლად უნდა აღინიშნოს ირანისა და ჩინეთის ხელისუფლებების მიდგომები მოცემულ საკითხთან, რაც ძირითადად არის პოლიტიკური გადაწყვეტილებები და, რაც გარკვეულ ზიანს აყენებს გლობალური ინტერნეტის ერთიანობას, მდგრადობას, უსაფრთხოებასა და სტაბილურობას და ხელს უწყობს ინტერნეტ ფრაგმენტაციის პროცესს [9].

ირანის ისლამურ რესპუბლიკაში გამკაცრებულია კიბერსივრცის კონტროლი, რაზეც მეტყველებს არსებული ცენზურის წესები, დაბლოკილია მრავალი ვებგვერდი, ასევე ხელისუფლების მხრიდან არსებობს ბლოგერების მკაცრი კონტროლი და მათი საქმიანობის მუდმივი შევიწროება. ირანის ენერგოსისტემაზე განხორციელებულმა კიბერშეტევამ და ამით მიყენებულმა ზიანმა ირანის ხელისუფლება კიდევ ერთხელ მიიყვანა იმ დასკვნამდე, რომ საჭიროა ეროვნული ინტერნეტის შექმნა და საკუთარი კიბერსივრცის გაძლიერება. ხელისუფლებამ დაიწყო საერთაშორისო სოციალური ქსელების ალტერნატიული შიდა მოხმარების სოციალური ქსელების განვითარების პროცესის დაფინანსება, რაც ხელს უწყობს საკუთარ მოსახლეობაზე ვირტუალურ სივრცეში კონტროლის დაწესებას. შედეგად, ირანში დღეს არსებული სურათის მიხედვით, ქვეყანაში მაქსიმალურად არის შეზღუდული საერთაშორისო სოციალური ქსელები, რითაც გზა გაეხსნა მხოლოდ ქვეყნის ხელისუფლების ხელშეწყობით შექმნილ ეროვნულ ალტერნატიულ ონლაინ პლატფორმების ფუნქციონირებას. 2015 წელს ჩინეთის ხელისუფლებამ წარმოადგინა ახალი გეგმა ინტერნეტ პოლიტიკასთან დაკავშირებით, რომელიც ითვალისწინებს ქვეყნის ეკონომიკურ და ტექნოლოგიურ ზრდას კიბერსივრცის მეშვეობით. ფაქტობრივად, ჩინეთის ხელისუფლების ინტერნეტ პოლიტიკა მიმართულია გლობალური ინტერნეტ სივრციდან ნაწილობრივ გამოყოფაზე და მისი პოლიტიკა ცნობილია, როგორც “Great Firewall“. იმავე წელს შემოღებულ იქნა ახალი კანონი, რომლის თანახმად, ყველა მომხმარებელი ვალდებული იყო ონლაინ პლატფორმაზე სარეგისტრაციო ფორმაში შეეყვანა თავისი მონაცემები. ამ კანონის თანახმად, კომპანიებს (საუბარია ISP კომპანიებზე), რომელთა გვერდზეც რეგისტრირდებოდნენ მომხმარებლები, ევალებოდათ მყისიერად გადაემოწმებინათ მიწოდებული ინფორმაცია და მხოლოდ ამის შემდეგ დაეშვათ მომხმარებლისთვის ვებგვერდზე წვდომა, მათ უნდა ეკონტროლებინათ ყველა საჯარო ანგარიში და დაეხარისხებინათ ისინი ინფორმაციის მიხედვით. გარდა ამისა, ჩინეთმა დაიწყო კონტროლის განხორციელება არა მარტო საკუთარ მოქალაქეებზე, არამედ მათ შეუზღუდეს ინტერნეტ პლატფორმებზე წვდომა უცხო ქვეყნის მოქალაქეებსაც. ამჟამად, მხოლოდ ჩინური ტელეფონის ნომრით არის შესაძლებელი ონლაინ აპლიკაციაზე წვდომა და ვებგვერდები გამოსაყენებლად მიუწვდომელია ჩინეთის ტერიტორიის ფარგლებს გარედან. უცხოელი მოქალაქეებისათვის საგრძნობლად გაართულებულია ჩინურ ვებგვერდებზე და აპლიკაციებზე წვდომა. მათ უნდა გაიარონ საკმაოდ ხანგრძლივი და რთული პროცესი რეგისტრაციისთვის, რისთვისაც მოეთხოვებათ წარმოადგინონ თავისი პერსონალური ინფორმაცია. ქვეყანას გააჩნია დიდი ამბიციები და თუ გადავხედავთ მის აქტიურობას საერთაშორისო დონეზე, მაშინ ვნახავთ, რომ დღევანდელ მსოფლიოში არსებობს დიდი რაოდენობით ჩინური ინვესტიცია, რომელიც ინტერნეტ სივრცისკენ არის მიმართული. ფაქტია, რომ ჩინეთი აშენებს საკუთარ, ეროვნულ ინტერნეტს, რაც უკვე ნიშნავს ინტერნეტ ფრაგმენტაციას. ჩინეთის იდეოლოგიაში წარმოდგენილი ინტერნეტი სულაც არ არის ღია, თავსებადი და თავისუფალი. შეიძლება ითქვას, რომ ჩინეთს არ აქვს მიზანი მსოფლიო ინტერნეტი კიბერშეტევებისგან გახადოს

უფრო უსაფრთხო, არამედ ცდილობს შექმნას კიბერსივრცის სრულიად განსხვავებული არქიტექტურა, რომელიც მორგებული იქნება არა საერთაშორისო უსაფრთხოებაზე არამედ ჩინეთის ეროვნულ ინტერესებზე. ჩინეთი ქმნის ფრაგმენტულ კიბერლანდშაფტს და მისი მთავარი მიზანი გახლავთ გახდეს დომინანტი მსოფლიო საზოგადოებაზე ინტერნეტის გავლით.

### დასკვნა

და ბოლოს, დასკვნის სახით შეიძლება ითქვას, რომ გლობალურ ციფრულ ხელშეკრულებაზე მუშაობის ფარგლებში, გრძელდება გლობალური და ინკლუზიური პროცესი ციფრული სივრცის ერთიანი პრინციპების შემუშავების კუთხით. ეს არის შესაძლებლობა, რომლის მიხედვით მოხდება გლობალური ინტერნეტის აღიარება, როგორც საერთო პრობლემების გადაწყვეტის მნიშვნელოვანი ინსტრუმენტი. ამაზე მეტყველებს გაერთიანებული ერების ორგანიზაციის ბოლო შეხვედრაზე მიღებული გადაწყვეტილებებიც.

ზოგადად, უნდა აღინიშნოს, რომ ინტერნეტის ფრაგმენტაციის პროცესის შეჩერება რთული ამოცანაა, მაგრამ ეს შესაძლებელია სახელმწიფოთა შორისი მაღალი დონის შეხვედრებით, ფოკუსირებული დიალოგებითა და ძალისხმევით იმ ძირითად ფრაგმენტულ ფაქტორებზე, როგორცაა კიბერჯაშუშობა, ინტერნეტის ინფრასტრუქტურაზე კონტროლის დაწესების მცდელობა და ინტერნეტისა და ინტერნეტ ტექნოლოგიების გამოყენებაზე, როგორც იარაღის ქვეყნებისა და ადამიანთა წინააღმდეგ. და მაინც ჯერ ისევ რჩება კითხვა გვაქვს თუ არა ფრაგმენტაცია, და რას შეიძლება ვუწოდოთ ფრაგმენტაცია? რამდენად წარმოადგენს ის საფრთხეს გლობალური ინტერნეტისთვის, მისი უსაფრთხოების, სტაბილურობისა და ერთიანობისთვის?

### დადასტურება

აღნიშნული ნაშრომის შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მხარდაჭერით - CG-24-220

### ბიბლიოგრაფია

1. Vladimer Svanadze, Maksim Iavich, Impact of Internet Fragmentation on the Unity, Security, and Stability of Global Internet; CPITS 2024 Cybersecurity Providing in Information and Telecommunication Systems 2024; CEUR, Vol-3654, pp. 520–525. <https://ceur-ws.org/Vol-3654/>
2. Svanadze, Vladimer. 2023. “Challenges of Internet Fragmentation and Global Cyberspace.” Scientific and practical cyber security journal – SPCSJ № 4 vol. 07, December 2023;
3. Christopher Meinel, „Russia’s War Against Ukraine is Catalyzing Internet Fragmentation“, Council on Foreign Relations, 2023;
4. Kamaitis Konstantions, “Internet Fragmentation: Why It Matters for Europe”, 2023;
5. Stokel-Wallker Chris, “Russia Inches Toward Its Splinternet”, 2022;
6. Sullivan Andrew, “Misguided Policies the World over are slowly killing the Open Internet”, Internet society, 2023;
7. Drake J. drake, Cerf Vinton G., Kleinwachter Wolfgang, “Internet Fragmentation: An Overwiev”, 2016.
8. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019 <https://journal.scsa.ge/papers/cyber-security-european-standards-in-business/>.
9. Vladimer Svanadze, Maksim Iavich, and Sergiy Gnatyuk, Challenges and Solutions for Cybersecurity and Information Security Management in Organizations; CPITS 2024 Cybersecurity Providing in Information and Telecommunication Systems 2024; Vol-3654, pp. 497–504. <https://ceur-ws.org/Vol-3654/>

## CHALLENGES OF CYBER SECURITY IN MODERN SOCIETY: THE IMPACT OF SOCIAL ENGINEERING

Assoc. Prof. Dr. Ilona Veitaitė  
Institute of Social Sciences and Applied Informatics, Vilnius University, Lithuania

**ABSTRACT:** Social engineering is a significant cybersecurity vulnerability that exploits human psychology to manipulate individuals into exposing confidential information. Unlike other forms of cyberattacks that target technological weaknesses, social engineering attacks leverage psychological aspects such as emotions, trust, and authority. These tactics often involve the use of “weapons of influence,” which include reciprocity, commitment, social proof, authority, liking, and scarcity. Social engineering can manifest in various forms, such as phishing, pretexting, baiting, and reverse social engineering, where attackers manipulate targets into reaching out to them for assistance. In 2024, statistics show that social engineering remains a prevalent threat, accounting for a significant portion of cybersecurity breaches globally. According to recent reports, nearly 70% of businesses have experienced at least one social engineering attack in the past year. High-profile examples of social engineering attacks include phishing emails disguised as official communications, pretexting to gather personal information under false pretenses, and baiting with enticing offers that lead to malware installation. As cyber threats become more sophisticated, the trends in social engineering are expected to evolve, incorporating advanced techniques such as deep-fake technology and artificial intelligence to enhance their effectiveness. Attackers are leveraging these technologies to create more convincing scenarios, making it increasingly challenging for individuals and organizations to differentiate between legitimate and fraudulent communications. To combat these threats, it is crucial to implement comprehensive training programs focusing on the psychological aspects of social engineering, emphasizing the importance of skepticism and verification before divulging sensitive information. Organizations should also consider employing interactive methods such as short videos to illustrate real-world examples of social engineering attacks, enhancing employee awareness and engagement. By fostering a culture of vigilance and continuous learning, individuals and organizations can better protect themselves against the growing threat of social engineering, ensuring a more secure cyber landscape in the years to come.

**KEYWORDS:** *Social Engineering, Phishing, Manipulation, Persuasion, Cybersecurity Attack, Psychological Attack, Weapons of Influence.*

### MAIN DEFINITIONS

Cybersecurity has become a critical concern in today's interconnected world as individuals and organizations face an ever-growing array of digital threats. Among these, phishing and social engineering stand out as particularly pervasive, exploiting human trust and psychological manipulation to gain unauthorized access to sensitive information. As technology evolves, attackers leverage sophisticated techniques, including personalized phishing campaigns and AI-driven tools, making the fight against these threats more complex than ever (Lewallen, 2020).

Phishing is a form of cybercrime in which attackers use deceptive techniques to manipulate individuals into revealing sensitive information such as usernames, passwords, credit card details, or other personal data. This is typically done through fraudulent emails, messages, or websites that appear to come from legitimate sources. The primary goal of phishing is to exploit human trust and gain unauthorized access to systems, financial accounts, or sensitive information. Phishing attacks come in various forms, each tailored to exploit specific vulnerabilities. Email phishing involves sending fraudulent emails to large groups, often containing malicious links or attachments. Spear phishing targets specific individuals or organizations with highly personalized messages to increase credibility. Whaling attacks focus on high-profile targets, such as executives, by crafting convincing messages that exploit their authority or access. Smishing and vishing use text messages and phone calls to deceive victims into revealing

sensitive information. Angler phishing occurs on social media platforms, where social media capabilities are used to persuade people to expose sensitive information or download malware. Data people post on social media to create highly targeted attacks could also be used. Awareness of these attack types is vital for recognizing and avoiding phishing threats in an increasingly digital world (Craig et al., 2014).

The main phishing challenges in modern society can be divided into several fields. Modern phishing attacks often employ advanced tactics like spear phishing, where attacks are tailored to specific individuals or organizations. This makes them more convincing and harder to detect. The pervasive use of email, social media, and instant messaging provides attackers with many platforms to exploit. Phishing messages can reach millions of users quickly. Artificial Intelligence enables the creation of highly personalized phishing content, while deepfakes can mimic voices or images of trusted individuals, making attacks more credible. Phishing attacks are often perpetrated across borders, making it difficult for law enforcement to track and prosecute offenders due to jurisdictional challenges. Attackers continually adapt their methods, using text messages (smishing), phone calls (vishing), and even QR codes to execute phishing campaigns. Phishing can lead to financial losses for individuals and organizations, reputational damage, and a loss of trust in digital communication channels (Schats, 2017).

Efforts to address phishing include public education, implementation of multi-factor authentication, deployment of sophisticated email filters, and global cooperation among cybersecurity organizations and governments. However, as technology evolves, the arms race between attackers and defenders continues, making phishing a persistent challenge (Hadnagy, 2018).

And still, despite advancements in cybersecurity, human error remains a significant vulnerability. Many people are not adequately trained to recognize phishing attempts. People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. Technical security measures are constantly evolving, but people do not change. They remain the weakest link in information security with their weaknesses, stereotypes, and attitudes. As Albert Einstein said: “Only two things are infinite, the universe and human stupidity, and I’m not sure about the former”. Several facts can confirm this quote: during the past few years, the estimated cost of cyber-attacks on organizations globally was more than four hundred billion dollars; 35 percent of data breaches were attributed to human error or negligence; 47 percent of IT professionals describe collaboration between security risk management and business as poor or nonexistent (Walker, et al. 2020).

## **SOCIAL ENGINEERING**

In very common sense social engineering can be called an act that influences a person to take an action that may or may not be in his or her interests. Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to. Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to access buildings, systems, or data. In the more technical sense, social engineering is a cyber-attack focused on tricking the victim into believing the criminal is someone they know and trust. The attacker will then request important information like passwords or fund transfers to their account. These attacks have become highly sophisticated with the advent of social media since these platforms have made it easy for attackers to uncover personal or work-related information. Attackers use this data to convince their victims that they are their friends, family members, or coworkers (Washo, 2021). Also, social engineering is one of the most insidious threats to businesses, particularly to small and medium-sized enterprises (SMEs). Unlike conventional computer attacks, which exploit technical vulnerabilities, social engineering targets human psychology to gain access to confidential information and IT systems, and compromise corporate security. Attackers use a variety of techniques to abuse users’ trust, inducing them to divulge confidential information or perform harmful actions. Social engineering is one of the most widespread and effective methods of accessing confidential information. Statistics show that attacks combining social engineering and phishing are extremely effective, resulting in considerable financial losses for organizations. Here are a few figures illustrating the scale of social engineering:

- Social engineering is behind 98% of all computer attacks.

- Over 70% of data breaches begin with phishing or social engineering attacks.
- In 2021, Google counted more than 2 million phishing sites.
- Some 43% of phishing e-mails impersonate well-known entities, such as Microsoft.
- SMEs with fewer than 100 employees are 3 times more likely to be the target of social engineering.
- 43% of IT professionals targeted by social engineering in previous years.
- A study by the Cyber Security Hub revealed that 3 out of 4 cybersecurity professionals considered social engineering or phishing attacks to be the “most dangerous” threat to their organization’s cybersecurity.
- According to the Information Systems Audit and Control Association, social engineering was the #1 attack vector in 2022.
- According to IBM’s 2022 Cost of a Data Breach report, the average cost of a social engineering attack is 4,55 million dollars.
- The same IBM report says that social engineering attacks can take up to 270 days to be detected and contained on average.
- Social engineering attempts increased by more than 500% in the past few years.



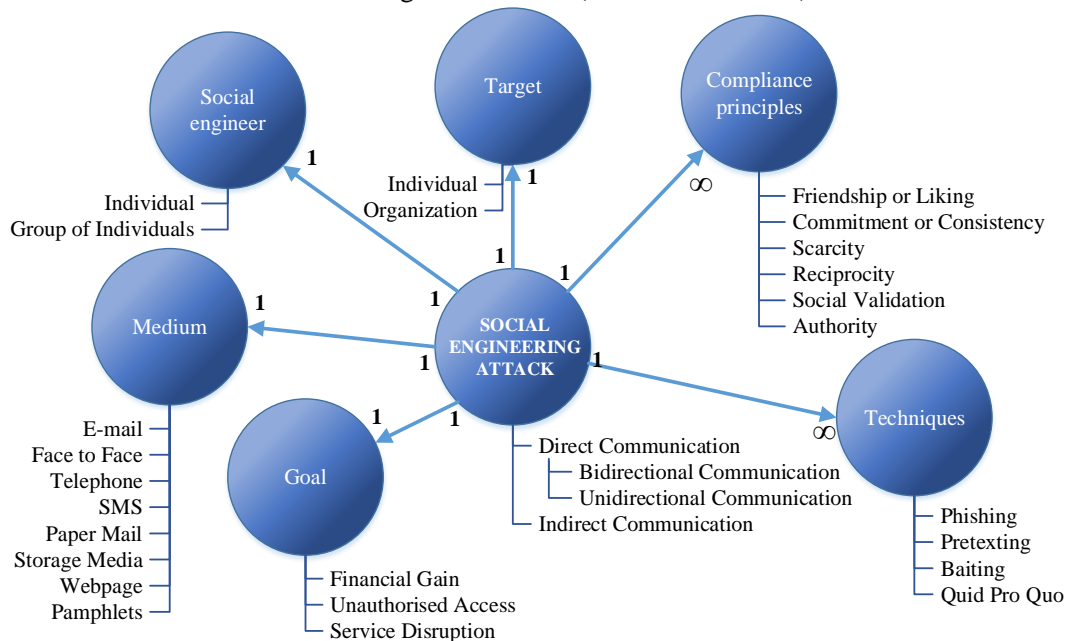
**Fig.1.** Steps of Social Engineering

Social engineering is a psychological manipulation technique attackers use to deceive individuals and gain access to sensitive information or systems. It typically follows a structured series of steps (Schats, 2017):

1. Targeting: The attacker identifies a specific individual, group, or organization to exploit, often selecting those with access to valuable information or systems.
2. Information Gathering: Detailed research is conducted on the target through publicly available sources, such as social media, corporate websites, or online databases, to gather information that can be used to build trust or craft convincing narratives.
3. Elicitation: The attacker engages the target in conversation, often using casual or indirect methods, to draw out additional information without raising suspicion.
4. Pretexting: The attacker creates a fabricated scenario or role to establish credibility and make the target believe they are interacting with a legitimate person or authority.
5. Mind Tricks: Psychological tactics, such as flattery, fear, urgency, or creating a false sense of trust, are employed to lower the target’s defenses and make them more likely to comply.
6. Persuasion: Using the information and rapport built so far, the attacker persuades the target to perform specific actions, such as clicking a link, sharing confidential information, or providing access credentials.

- Exploiting and Disengagement: The attacker uses the gained information or access to achieve their objective, such as stealing data, infiltrating systems, or committing financial fraud. After successfully exploiting the target, the attacker exits the interaction, often attempting to cover their tracks to avoid detection or suspicion.

The ontological model defines a social engineering attack as “employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles, and one or more techniques.” The attack can be split into more than one attack phase, each phase handled as a new attack according to the model (Merwe et al. 2017).



**Fig.2.** An Ontological Model of a Social Engineering attack (Merwe et al. 2017).

Direct communication in social engineering is divided into bidirectional and unidirectional communication. Bidirectional communication involves two-way interaction, such as when an attacker sends an email to a target and the target replies. In contrast, unidirectional communication is one-way, like when an attacker sends a letter with no return address, preventing a response from the target. Phishing attacks often use this form of communication. Indirect communication occurs when the attacker does not directly interact with the target but uses a third-party medium, such as leaving an infected flash drive for the target to find and unknowingly activate.

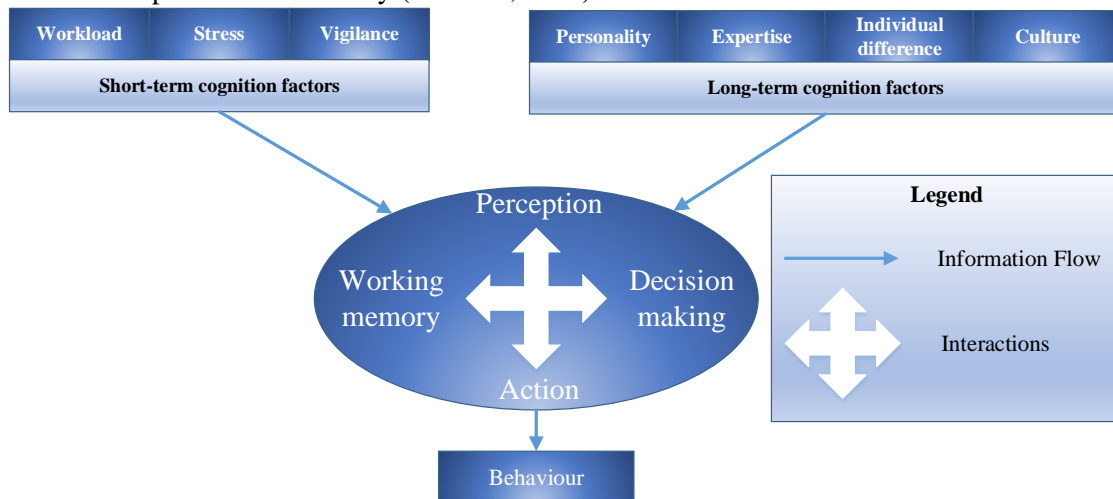
The ontological model of social engineering includes components such as the goal of the attack (e.g., financial gain, unauthorized access, or disruption), the medium (email, phone, face-to-face), the social engineer (individual or group), the target (individual or organization), compliance principles (why the target complies), and techniques (e.g., phishing, pretexting, baiting, and quid pro quo).

The social engineering attack implemented through one or several people can have serious consequences for a person or entire organization: leakage of sensitive data, and social engineering attacks are often aimed at obtaining confidential information. If successful, this can lead to the leakage of sensitive data, such as information on customers, employees, organization finances, or trade secrets; financial loss: attackers can use social engineering to defraud the organization of money, whether through fraud, unauthorized fund transfers or payments to fraudulent suppliers; reputational damage: successful social engineering attacks can seriously damage organization’s reputation. Customers and business partners may lose confidence in the organization if sensitive data is leaked or if it is involved in scams; disruption of operations: some social engineering attacks aim to disrupt organization operations. This can result in service disruption, loss of productivity, and significant costs to restore normal operations; legal liability: organizations can be held liable for breaches of their customers’ privacy or the financial consequences of a successful social engineering attack. This can lead to legal action; infiltration of networks and systems: social engineering attacks can enable attackers to break into corporate networks and systems, which can lead to cyber espionage, intellectual property theft, or

other forms of intrusion; malware propagation: attackers can use social engineering to induce employees to download malware, which can compromise the security of IT systems and data; loss of financial or accounting data: social engineering attacks can target employees responsible for finance or accounting, leading to the loss of crucial financial data or fraudulent manipulation (Bella, 2014).

### PSYCHOLOGICAL ASPECTS OF SOCIAL ENGINEERING

“Some authors advocate treating social engineering cyberattacks as a particular kind of psychological attack.” (Montañez et al. 2020). Social engineering is highly effective because it exploits fundamental aspects of human nature and behavior. People are inherently social, driven by a desire to connect and stand out, often influenced by others’ decisions. The instinct to be helpful and the tendency to trust strangers make individuals particularly susceptible to manipulation. Additionally, in an age of information overload, people often rely on mental shortcuts to save time and gravitate toward quick and effortless solutions, which attackers exploit. Fear of consequences, such as getting into trouble, can pressure targets into compliance. Compounding these factors, many lack sufficient security knowledge and share excessive personal information on social media, providing attackers with valuable tools to tailor their manipulations effectively (McLeod, 2023).



**Fig.3.** Steps of Social Engineering (Montañez et al. 2020)

Human cognitive functions, such as perception, memory, and decision-making, play a significant role in shaping behavior by influencing how individuals process information, respond to environmental changes, etc. In the context of social engineering, attackers exploit cognitive biases, such as the tendency to trust authority or react to urgency, to manipulate targets into making decisions against their best interests. A high cognitive workload, a high stress level, a low level of attentional vigilance, a lack of domain knowledge, and/or a lack of past experience make one more susceptible to social engineering cyberattacks (Montañez et al. 2020).

The psychology of online persuasion leverages cognitive biases and emotional triggers to influence individuals' decisions and actions in the digital realm. Various techniques are commonly used to create a sense of urgency, build trust, or induce a feeling of obligation, prompting users to comply with requests or make impulsive purchases. By understanding how people process information and respond to emotional cues, attackers and marketers alike can craft messages that exploit these psychological tendencies for manipulation or persuasion. Emotional manipulation provides attackers with a significant advantage in any interaction, as individuals are more prone to making irrational or risky decisions when experiencing heightened emotions.

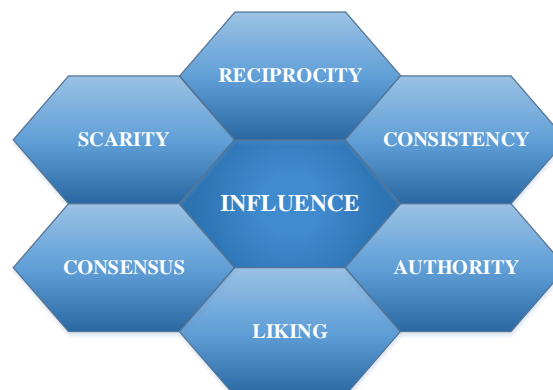




*Fig.4. Heightened emotions*

Heightened emotions are powerful tools in social engineering and cyberattacks, as they can cloud judgment and prompt hasty actions (Cialdini, 2007).

- Fear: A phishing email claiming a victim's bank account has been compromised and requiring immediate action can trigger panic, leading the target to click on a malicious link.
- Excitement: An attacker may send a fake message about winning a contest or prize, enticing the victim to share personal information to claim their reward.
- Curiosity: A message stating, "Check out this surprising news about you," can spark the victim's curiosity, encouraging them to click on a link that leads to a harmful site.
- Helpfulness: An attacker may pose as a coworker needing urgent assistance, convincing the target to provide login credentials or download malicious files to "help."
- Guilt: A scammer might impersonate a friend in distress, claiming to need financial help and making the victim feel guilty enough to send money or personal details.
- Urgency: A fake notification claiming that a victim's account will be suspended unless immediate verification is completed can rush the target into giving away sensitive information.
- Sadness: A message claiming a close relative is in an emergency can manipulate the target into making hasty decisions, such as transferring money or disclosing private information.
- Anger: An attacker may send a message impersonating a customer service agent demanding immediate action or threatening to cancel an important service, evoking frustration and prompting rash decisions.
- Greed: A phishing email offering an incredible financial opportunity or a "too good to be true" investment can provoke greed, leading the victim to provide personal details or funds.



*Fig.5. Weapons of Influence*

Weapons of Influence refer to psychological principles used to persuade and manipulate behavior (Cialdini, 2007). Here are short definitions of the main types:

- Reciprocity: The tendency to return a favor or feel obligated to give back when someone does something for you.
- Consistency: The desire to act in ways that align with one's past behaviors, commitments, or beliefs.

- Authority: The influence exerted by individuals perceived as experts or authority figures, leading others to comply with their requests.
- Liking: People are more likely to be influenced by those they like or feel connected to, such as friends or individuals with similar traits.
- Consensus: The tendency to follow the actions of others, believing that if many people do something, it must be the right thing to do.
- Scarcity: The perception that something is more valuable or desirable because it is limited or in short supply.
- Unity: 7th principle of persuasion was later added. The feeling of shared identity or connection makes individuals more likely to trust and act in alignment with others in their group.

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy Aesthetics Feelings Actions Ideas Values	Competence Order Dutifulness Achievement Striving Self-Discipline Deliberation	Warmth Gregariousness Assertiveness Activity Excitement Seeking Positive Emotion	Trust Straightforwardness Altruism Compliance Modesty Tender-mindedness	Anxiety Hostility Depression Self-Consciousness Impulsiveness Vulnerability to Stress

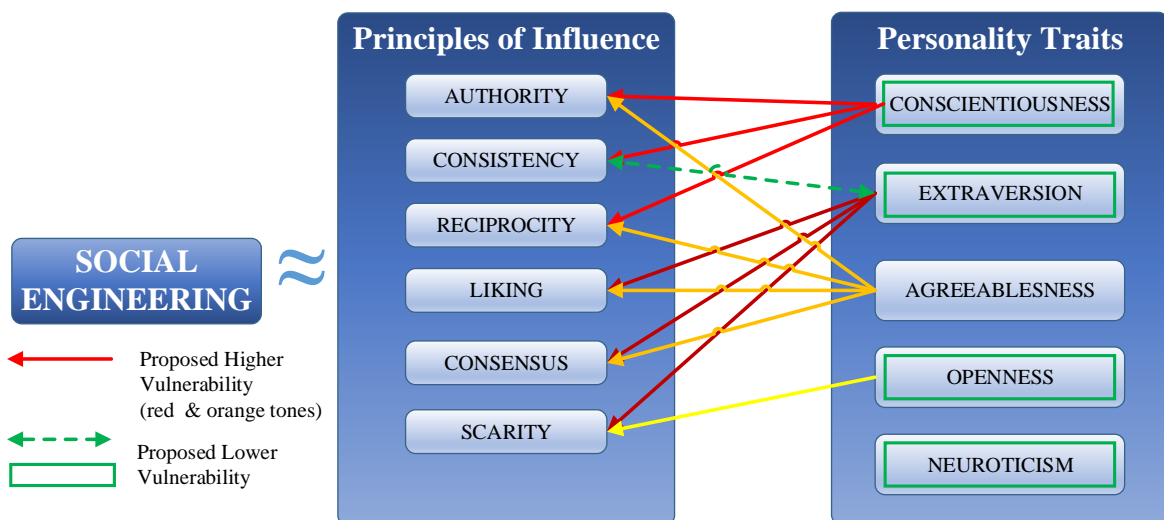


Fig.6. The Social Engineering Personality Framework (Cialdini, 2007).

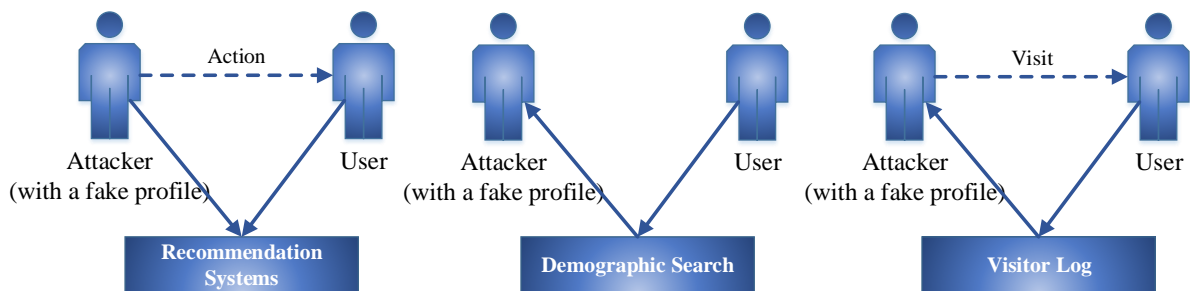
The Social Engineering Personality Framework (SEPF) is a model developed to understand how personality traits influence individuals' susceptibility to social engineering attacks. According to scientific literature, this framework categorizes personality traits that can make a person more vulnerable to manipulation, such as high levels of agreeableness (e.g., a willingness to help others), openness to experience (e.g., curiosity), and neuroticism (e.g., anxiety or fear). People with high conscientiousness may be less susceptible, as they tend to be more cautious and skeptical, while those with low self-esteem are often more easily manipulated by attackers preying on their insecurities. The framework also highlights the role of social traits, such as the need for affiliation or fear of conflict, which can drive individuals to comply with requests even when they might normally be suspicious. By understanding these personality factors, attackers can tailor their approach to exploit specific vulnerabilities in their targets, making the SEPF a valuable tool for both attackers and defenders in recognizing and mitigating social engineering risks.

## REVERSE SOCIAL ENGINEERING

Reverse social engineering is a psychological manipulation tactic where the attacker creates a situation in which the target seeks help or information from the attacker rather than the other way around. This technique often involves the attacker gaining the trust of the target through indirect means and then

waiting for the target to initiate contact. By positioning themselves as the solution to a problem, the attacker exploits the target's desire for assistance or resolution (Irani, 2011).

In reverse social engineering, the attacker does not make the first contact with the victim. Instead, the attack is designed in such a way that the victim reaches out to the attacker for assistance, establishing a relationship based on trust, as it is initiated by the victim. This process typically unfolds in three stages: first, a bait or pretext is created to spark the victim's interest or curiosity (for example, the victim's equipment is sabotaged or damaged). Second, the attacker ensures the target perceives them as an authoritative figure with the necessary skills to fix the issue. Finally, the attacker provides assistance, building trust and gaining access to the victim's information or other resources. Attacks can be classified as targeted or untargeted—in a targeted attack, the attacker focuses on a specific individual, whereas in an untargeted attack, the goal is to reach as many users as possible. They can also be direct or mediated—in a direct attack, the baiting action is visible to the victim, while in a mediated attack, an intermediary collects the bait and then distributes it, often in a different form, to the targeted users.



**Fig.7.** Reverse social engineering attacks examples

Several modern examples of reverse social engineering include recommendation systems, demographic searches, and visitor tracking (Irani, 2011).

- One example of reverse social engineering is through recommendation systems, which are commonly used by online platforms to suggest products, services, or content to users. These systems often rely on data collection and algorithmic predictions based on user behavior, creating a sense of personalized service. However, attackers can exploit these systems to manipulate individuals into making decisions that benefit the attacker. For instance, an attacker could set up a fake website or a malicious product recommendation that subtly persuades the target to click on a malicious link or purchase a fraudulent service, all under the guise of a trusted, personalized recommendation. The user, having been conditioned to trust recommendation systems, may unknowingly follow the suggestion, revealing personal information or falling into a trap.
- Another form of reverse social engineering occurs through demographic search, where attackers gather information based on demographic data to manipulate individuals. Attackers can identify personal details such as age, location, job, or interests by accessing publicly available information on social media profiles or other online sources. Using this information, they can tailor their approach, appearing as though they have a legitimate connection to the target's life. For example, an attacker might contact an individual claiming to be from a local organization offering exclusive deals for people of their demographic, leveraging the target's trust in personalized, relevant offers. Once the target engages, the attacker may then extract sensitive data or lead them into a phishing scam disguised as a legitimate transaction.
- Visitor tracking is another example of reverse social engineering that plays on an individual's online behavior. Websites often track visitors to gather data on their browsing habits, interests, and preferences. Attackers can use this information to create targeted and convincing interactions. For example, by tracking a user's online visits to certain websites, an attacker could craft a message that appears to be from a trusted vendor or service provider related to the user's interests. The message might offer support or solutions to a problem the user has not yet realized they need help with, prompting the target to reach out to the attacker. Once contact is made, the attacker can manipulate the victim into providing personal details, downloading malicious software, or engaging in harmful actions, all while the target feels they are receiving help from a trusted source.

In all of these examples, the core principle of reverse social engineering is the manipulation of trust and the creation of an environment where the victim feels compelled to initiate interaction with the attacker. By understanding and exploiting human behavior, attackers can effectively control the narrative and lead the target into a position where they willingly disclose information or make decisions that benefit the attacker.

## **TIPS TO PREVENT SOCIAL ENGINEERING**

Social engineering attacks pose a heightened risk to organizations in today's world, and this risk is only likely to increase in the future. As attacks become more sophisticated and techniques evolve, organizations must adapt to protect their data, assets, and reputation.

The key to defending against social engineering attacks is a combination of employee education, robust cybersecurity measures, and a proactive security culture. Organizations must continually update their defenses and prepare for evolving threats. The future of social engineering attacks is uncertain, but by staying vigilant and implementing best practices, organizations can better safeguard themselves against this growing menace.

Organizations and individual users need to prioritize education and awareness to prevent social engineering attacks. For organizations, this means regularly training employees on recognizing common social engineering tactics, such as phishing emails, pretexting, and baiting, and fostering a security-first culture. Training should cover identifying suspicious communication, verifying the legitimacy of requests for sensitive information, and understanding the risks of oversharing personal or organization data online. Implementing robust security measures like multi-factor authentication (MFA) and regularly updating software and security protocols can also significantly reduce the risk of successful attacks. Additionally, organizations should have clear incident response plans in place so employees know how to act if they suspect a social engineering attack.

Being vigilant about personal security and avoiding impulsive actions is key for individual users. Users should be cautious when receiving unsolicited emails, phone calls, or messages asking for sensitive information and always verify the source before responding. Password hygiene is crucial—using strong, unique passwords for different accounts and enabling MFA where possible can add an extra layer of defense. Users should also be mindful of their online presence and avoid oversharing personal details on social media, as attackers often use this information for targeted social engineering attempts. Lastly, fostering a healthy skepticism and always questioning the legitimacy of urgent requests or offers can help individuals recognize and avoid falling victim to social engineering attacks.

## **CyberPhish PROJECT**

The international project “Safeguarding against Phishing in the Age of 4th Industrial Revolution” (“CyberPhish”) initiated by Vilnius University Kaunas Faculty and partners started at the beginning of November 2020. The project duration period is 2 years. The objective of the project is to educate students of higher education institutions, educators, university staff (members of the community), education centers, and the business sector (employers and employees) and encourage critical thinking of the target group in the field of cyber security (CyberPhish, n.d.).

The project partners are going to design a curriculum, e-learning materials, a blended learning environment, knowledge and skills self-assessment, and knowledge evaluation system simulations for students and other users in order to prevent phishing attacks, raise competencies, which will help to focus attention to threats and take appropriate prevention measures (CyberPhish, n.d.).

The main intellectual outputs focus on enhancing cybersecurity competencies and addressing phishing threats. These include a study analysis with surveys on “Recognizing Phishing and Skills Gaps” and “Analysis of Existing Cybersecurity Training Programs” across multiple countries (EST, GR, LV, LT). A course curriculum was developed in both short and extended versions for dissemination and training material creation alongside an integrated CyberPhish online course. Additional outputs include online learning materials, gamified educational simulations, and self-evaluation tools, all incorporated into the online learning platform. Methodological guidelines for trainers and implementing “Phishing in the Age

of the 4th Industrial Revolution” were also created to support effective training and course delivery (CyberPhish, n.d.).

#### ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

#### REFERENCES

- [1] Jonathan Lewallen, “Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity,” *Regulation & Governance* 15, no. 4 (July 14, 2020): 1035–52, <https://doi.org/10.1111/rego.12341>.
- [2] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, “Defining Cybersecurity,” *Technology Innovation Management Review* 4, no. 10 (October 30, 2014): 13–21, <https://doi.org/10.22215/timreview/835>.
- [3] Daniel Schatz, Rabih Bashroush, and Julie Wall, “Towards a More Representative Definition of Cyber Security,” *The Journal of Digital Forensics, Security and Law*, January 1, 2017, <https://doi.org/10.15394/jdfsl.2017.1476>.
- [4] Robert B. Cialdini, *Influence: The Psychology of Persuasion* (Rev. ed.; 1st Collins business essentials ed. New York: Harper Collins, 2007).
- [5] Christopher Hadnagy, *Social Engineering: The Science of Human Hacking* (John Wiley & Sons, 2018).
- [6] Danesh Irani et al., “Reverse Social Engineering Attacks in Online Social Networks,” in *Lecture Notes in Computer Science*, 2011, 55–74, [https://doi.org/10.1007/978-3-642-22424-9\\_4](https://doi.org/10.1007/978-3-642-22424-9_4).
- [7] Saul McLeod PhD, “Techniques of Compliance in Psychology,” *Simply Psychology*, June 14, 2023, <https://www.simplypsychology.org/compliance.html>.
- [8] Johannes Van de Merwe, Francois Mouton. “Mapping the anatomy of social engineering attacks to the systems engineering life cycle”. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2017), pp. 24-40
- [9] Rosana Montañez, Edward Golob, and Shouhuai Xu, “Human Cognition Through the Lens of Social Engineering Cyberattacks,” *Frontiers in Psychology* 11 (September 30, 2020), <https://doi.org/10.3389/fpsyg.2020.01755>.
- [10] Giampaolo Bella and Giampaolo Bella et al., “A Socio-technical Methodology for the Security and Privacy Analysis of Services,” *Workshops* 376 (July 1, 2014): 401–6, <https://doi.org/10.1109/compsacw.2014.69>.
- [11] Emile Walker, Dave Witkowski, Sarah Benczik, Pilar Jarrin. *Cybersecurity –the Human Factor. Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce*. Retrieved from [https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017\\_Witkowski\\_Benczik\\_Jarrin\\_Walker\\_Materials\\_Final.pdf](https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf)
- [12] Amy Hetro Washo, “An Interdisciplinary View of Social Engineering: A Call to Action for Research,” *Computers in Human Behavior Reports* 4 (July 25, 2021): 100126, <https://doi.org/10.1016/j.chbr.2021.100126>.
- [13] “CyberPhish: Safeguarding Against Phishing in the Age of 4th Industrial Revolution,” CyberPhish: Safeguarding Against Phishing in the Age of 4th Industrial Revolution, n.d., <https://cyberphish.eu/>.

# THE IMPACT OF PERFORMANCE EXPECTANCY ON BEHAVIORAL INTENTION TO USE WIRELESS TECHNOLOGIES IN PUBLIC UNIVERSITIES IN UGANDA

Kyambadde Abdunool<sup>1</sup>, Mwase Ali<sup>2</sup>, Ssebanenya Muhammad<sup>3</sup>, Saunders Warda<sup>4\*</sup>

<sup>1,2,3</sup>Department of Marketing & Management, Makerere University Business School, Kampala, Uganda

<sup>4</sup>Department of Human Resource Management, Makerere University Business School Kampala, Uganda

\*Corresponding author: [akyambadde@mubs.ac.ug](mailto:akyambadde@mubs.ac.ug)

**ABSTRACT.** The rapid evolution of wireless technologies has transformed the educational landscape, particularly in higher education institutions. This study examines the impact of performance expectancy on the behavioral intention to use wireless technologies (WTs) in public universities in Uganda. Performance expectancy, defined as the degree to which individuals believe that using a technology will enhance their performance, is a critical factor influencing technology adoption. The study opted for cross sectional survey methodology and using a quantitative approach, data were collected from students and faculty across selected public universities in Uganda. Results of correlation and regression analysis indicated that a positive and significant relationship exists between Performance Expectancy and Behavioral Intention to Use. The findings suggest that enhancing users' expectations of performance benefits could significantly improve technology usage in educational settings. This study provides valuable insights for policymakers, university administrators, and technology providers aiming to foster wireless technology adoption in Uganda's higher education sector.

**KEYWORDS:** *UTAUT, Performance Expectancy, Behavioral Intention to Use and Wireless Technologies*

## 1. INTRODUCTION

Public universities in Uganda are witnessing rapid growth in the number of enrolled students, which requires further infrastructural development and the creation and construction of more colleges, schools and facilities, along with the required services. However, since the installation and use of wired technologies is highly expensive, and its maintenance is expensive, some universities resorted to the use of wireless technologies to link students and staff to their systems [1].

According to [22], wireless technologies consist of networking hardware and software which increase on the mobility of user access to internet since they eliminate the need for wired technologies. This can be achieved through the use of wireless technology devices like; cell phones which are used by students in learning, wireless modems used by students to connect to wireless networks instead of telephone systems, wireless hotspots installed at campuses for students to access internet using their personal laptops [13]. [12] considers two wireless technologies that is Wi-Fi and Bluetooth to link between access devices and access providers to address the needs of rural communities by exploring and implementing potential innovative low cost technologies for Internet access.

Wireless technologies were introduced in universities to be used for academic purposes like sending and receiving academic emails, use of chat communication technologies to join discussions or collaborate with classrooms worldwide, accessing electronic notes. Instead the students use them for non-academic purposes like chat rooms, downloading music and facebook, games among others [13]. In addition, a few years ago universities were struggling to keep mobile phones and other wireless devices away from students especially during lectures whereas now they are doing their best to encourage students to use smart phones, tablets, laptops among other wireless devices even during lectures. Wireless technologies are as well being considered as critical tools to enhance students'

learning experience and provide powerful educational opportunities [7]. [9] noted that mobile wireless technology promotes interactive lectures thereby enriching the learning process of students in classroom or online classes. The adoption of wireless technologies is increasing and students are more satisfied because it can solve math problems or issues using their own ideas [15]. [15] further argues that mobile learning should be developed using wireless technologies such as tablets and android. According to [11], the use of wireless technologies can provide opportunities for students to conduct an investigation and critical thinking skills of learning which is only done in the classroom and can effectively improve the learning behavior more positively.

Similarly, a report on socioeconomic impacts of wireless technology has revealed that the introduction of wireless technologies has enabled instant communication at all times and places, speedy transfer of information and services over long distances irrespective of the geographic barriers [7].

Despite the widely recognized benefits offered by wireless technologies, wireless technology adoption is underutilized in Ugandan Public Universities, with limited studies focusing on low-developed countries like Uganda. This study seeks to address this gap by examining the impact of performance expectancy on the behavioral intention to use wireless technologies in public universities in Uganda.

## **2. LITERATURE REVIEW**

### **2.1. Performance Expectancy**

Performance expectancy is the degree to which a user believes that using the technology will help him or her attain benefits or have better and effective performance. In other words, Performance expectancy means to what extent users believe their performance will improve if they adopted a technology. [17] from the work of [18]. Thus, UTAUT model is a set or series of previous models. Five factors from previous models assisted in the formation of performance expectancy variable consisting of perceived usefulness from Technology Acceptance Models (TAM), external motivation from Motivational Model (MM), job fit from utilization model, relative advantages from innovation diffusion theory (IDT) and an outcome from expectations social cognition theory (SCT) [17],[16]. Hence, several past studies uncovered that performance expectancy plays a significant role in intention to use information technology [3], [8], [23].

### **2.2. Performance Expectancy and Behavioral Intention**

Performance expectancy, defined as the degree to which users perceive a technological system as useful and beneficial in performing their tasks, is a key determinant of behavioral intention to use technology [28]. Studies have consistently shown that performance expectancy has a direct and positive impact on the adoption of various technologies.

In the context of mobile commerce, research has demonstrated that performance expectancy significantly influences consumers' behavioral intentions. For instance, a study conducted in Pakistan found that performance expectancy was a strong predictor of the intention to adopt mobile commerce technologies, highlighting its importance in shaping user behavior [29].

Similarly, in the realm of mobile health services, performance expectancy has been identified as a crucial factor in determining the intention to adopt such services. Studies have shown that when users perceive mobile health services as useful and beneficial, they are more likely to adopt and use these services [30].

### **2.3. Theoretical Analysis**

The Unified Theory of Acceptance and Use of Technology (UTAUT) is a widely used framework for understanding the adoption of new technologies. The Unified Theory of Acceptance and Use of Technology (UTAUT) posits that the intention to use information systems to follow-up use behavior [24]. The theory considers that the performance of key structures, anticipated value, anticipated workload, social inspiration and favorable surroundings are all through the elements of purpose and

they use performance of information systems [18]. Further, [25] proposed that sex, age, involvement and age voluntary procedures mitigate the influence of the four key structures on use intentions and performance. UTAUT is meant to be adjusted to fit the technology being queried; therefore, a certain amount of modification is expected. Therefore, in this study, UTAUT is used as baseline model while the moderating variables of age, gender, experience and voluntariness of use are excluded. The research model posits that behavioral intention to use wireless technologies is determined by Performance Expectancy (PE) as shown on the proposed model below;



### 3. RESEARCH METHOD

#### 3.1. Research Design

This study adopts a quantitative research design to investigate the relationship between performance expectancy and behavioral intention to use wireless technologies in public universities in Uganda. A cross-sectional survey was conducted to collect data from academic staff and students across selected public universities.

#### 3.2. Population and Sample

The target population included academic staff and students from five public universities in Uganda, including Makerere University and Kyambogo University. A sample size of 334 participants was determined using Krejcie and Morgan's sample size determination table. The sample was stratified to ensure that both students and academic staff were adequately represented.

#### 3.3. Data Collection

A structured questionnaire was used to collect data. The questionnaire was divided into two sections. The first section gathered demographic information about the respondents, while the second section focused on the constructs of performance expectancy and behavioral intention to use wireless technologies. Items in the questionnaire were adapted from established studies [2], [3] and measured using a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

#### 3.4. Validity and Reliability

To ensure the validity of the instrument, content validity was established through expert reviews. The content validity index (CVI) was found to be 0.70 or higher for all variables, which is acceptable according to [26]. Internal consistency was assessed using Cronbach's alpha, with all constructs showing reliability coefficients above 0.70, as suggested by [27]. The validity and reliability of the variables is indicated in Table 1 and Table 2 below respectively.

#### 3.5. Data Analysis



The data collected were analyzed using descriptive and inferential statistics. Pearson correlation analysis was conducted to examine the relationship between performance expectancy and behavioral intention. Additionally, regression analysis was performed to assess the predictive power of performance expectancy on behavioral intention to use wireless technologies.

**Table 1:** Content Validity Index

S/N	Variable	CVI	No. of items
01	Performance Expectancy	.71	6
02	Behavioral Intention	.70	6

**Table 2:** Reliability Test

S/N	Variable	Cronbach Alpha	No. of items
01	Performance Expectancy	.78	6
02	Behavioral Intention	.77	6

### 3. Results

In order to test the formulated hypothesis, we use the Pearson (r) correlation analysis and regression analysis to ascertain the predictive effect of Performance Expectancy on Behavioral Intention to use WTs and the results are displayed in table 3 and table 4 respectively;

**Table 3:** Correlation Analysis

S/N	Variable	1	2
01	BI	1	
02	PEXPT	.205**	1
<i>N=205</i>		<i>**P&lt;0.01</i>	<i>Level (1-tailed)</i>

*Source: Primary Data*

Key: BI = Behavioral Intention, PEXPT = Performance Expectancy

**Table 4:** Results of Simultaneous Regression Analysis of PEXPT on BI

Variable	Beta	T	P
(Constant)		9.095	.000
PEXPT	.205	3.399	.001
R = 205 R <sup>2</sup> = .042 Adjusted R <sup>2</sup> = .038 F = 11.553			

*Source: Primary Data*

Key: PEXPT = Performance Expectancy

From table 3 above, at a preliminary level, correlation results indicated that Performance Expectancy is positively and significantly related to Behavioral Intention ( $r = .205$ ;  $p < 0.01$ ). This is an indication that a positive change in Performance Expectancy is associated with a positive change in Behavioral Intention. Further evidence is adduced by the results of regression analysis as displayed in table 4. Results show that approximately 4 per cent of the total variance in Behavioral Intention is explained by Performance Expectancy ( $R^2 = .042$ ;  $p < .01$ ). The regression coefficient of Performance Expectancy was significant ( $\beta = .205$ ,  $t = 3.399$ ;  $p < .01$ ). On account of this, it can be adduced that Performance Expectancy is positively related to Behavioral Intention to use WTs in public universities in Uganda.

#### 4. DISCUSSION

Performance Expectancy was found to have a significant direct effect on the Behavioral Intention to use WTs in public universities in Uganda. According to the original Unified Theory of Acceptance and Use of Technology, Performance Expectancy is hypothesized to affect behavioral intention to use a particular technology and it relates to what users perceive as the performance benefits of using such a technology.

This study found out that academic staff in public universities in Uganda believe that behavioral intention to use WTs would be more useful in their job performance if successfully adopted for academic use. This might be because these academic staff want to adopt WTs for they think WTs experience will be beneficial for future job preparation and accomplishing, improved their job performance. Or, they feel it would give them competitive edge over other universities engaged in e-learning in terms of academic delivery. These findings are consistent with literature [4], [10], [19],[20],[21]. This stream of literature provides evidence of the significant effect of Performance Expectancy on behavioral intention to use a technology. The Performance Expectancy and Behavioral Intention relationship is strongly based on the idea that, people form intention toward behaviors they believe will increase their system use, over and above whatever positive or negative feeling may be evoked toward the behavior. These revelations further confirm studies by [14] which supports the view that stressing Performance Expectancy leads to Behavioral Intention to use. Another study by [5] found that Performance Expectancy is an important factor in determining actual usage via Behavioral Intention to Use.

Results of this research fill an important gap in literature by contributing the results of the determinants of individual's intention to use wireless technologies in developing economies context, with a theoretical based empirical investigation. Consequently, the empirical validation of model posits that model is valid and can generally be applied to explore and achieve better results in similar contextual setting.

#### 5. CONCLUSION AND RECOMMENDATIONS

This study investigated the impact of performance expectancy on behavioral intention to use wireless technologies in public universities in Uganda. The findings reveal that performance expectancy significantly influences behavioral intention among academic staff and students. Specifically, individuals who perceive that wireless technologies will enhance their performance are more likely to adopt and use them. This finding aligns with previous studies in both developed and developing countries, underscoring the importance of performance expectancy in technology adoption.

The results suggest that wireless technologies have the potential to enhance the teaching and learning experience in Ugandan public universities. However, for these benefits to be fully realized, universities must ensure that staff and students perceive the use of wireless technologies as advantageous to their academic and professional goals.

Future studies should investigate other factors, such as effort expectancy and social influence, that may affect the adoption of wireless technologies in public universities. Moreover, qualitative studies could explore the experiences of users to gain a deeper understanding of their motivations and challenges in using wireless technologies.

## REFERENCES

- [1] Aruba Networks. (2012). Islamic university in Madinah deploys wireless networks for students and staff. Aruba Networks.
- [2] Anderson, J. E., & Schwager, P. H. (2004). SME Adoption of Wireless Lan Technology: Applying the UTAUT Model. The 7th Annual Conference of the Southern Association for Information Systems (pp. 39-43). Southern Association for Information Systems.
- [3] Aytekin, A., Özköse, H., & Ayaz, A. (2022). Unified theory of acceptance and use of technology (UTAUT) in mobile learning adoption: Systematic literature review and bibliometric analysis. *COLLNET Journal of Scientometrics and Information Management*, 75-116.
- [4] Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies? *Decision Sciences*, 30(2), 361-391.
- [5] Alblooshi, M., & Abdul Hamid, R. (2022). Performance expectancy and behavioral intention to use new technologies: A comparative study. *Technology in Society*, 58, 101208.
- [6] Alraja, M. N. (2015). User acceptance of information technology: Exploring the role of social influence and perceived usefulness. *Journal of Social Sciences*, 41(1), 18-25.
- [7] BSR & CTIA-The Wireless Association. (2012). Socioeconomic impacts of wireless technology in education. *Journal of Wireless Communication*, 20(2), 5-10.
- [8] Carter, L., Schaupp, L. C., & McBride, M. E. (2011). The UTAUT model for understanding mobile commerce adoption: Cross-country analysis. *Journal of Electronic Commerce*, 17(1), 25-34.
- [9] Chin, M. L., & Vimala, K. (2016). Interactive learning and mobile wireless technologies in higher education. *Journal of Educational Research*, 35(2), 112-123.
- [10] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
- [11] Kutluk, F. A., & Gulmez, M. (2014). The effects of mobile learning on student performance. *Journal of Wireless Technologies*, 14(1), 45-55.
- [12] Morris, D. (2004). Wireless technologies for rural internet access. *Technology and Society Journal*, 12(3), 27-33.

- [13] Ndawula, P. (2011). The use of wireless technologies in Ugandan universities. *Educational Technology Journal*, 12(5), 23-27.
- [14] Nyembezi, L. S., & Bayaga, A. (2014). Technology acceptance model in South Africa's educational sector. *International Journal of Information Systems*, 30(4), 152-160.
- [15] Rif'at, M. (2015). Wireless technology in mobile learning: Opportunities and challenges. *Journal of Wireless Technologies*, 20(3), 89-95.
- [16] Salloum, S. A., & Shaalan, K. (2018). Factors affecting the adoption of information technologies: A review and research framework. *Information Systems Journal*, 23(1), 123-143.
- [17] Sair, S., & Danish, R. (2018). Performance expectancy and technology adoption in educational settings. *Educational Technology Review*, 11(2), 67-72.
- [18] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, 27(3), 425-478.
- [19] Venkatesh, V. (1999). Creation of favorable user perceptions: Exploring the roles of intrinsic motivation, extrinsic rewards, and user involvement. *Management Information Systems Quarterly*, 23(2), 239-260.
- [20] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.
- [21] Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *Management Information Systems Quarterly*, 24(1), 115-139.
- [22] Seymour, C. (2012). Wireless networks in education: Current trends and future directions. *Journal of Communication Technologies*, 7(3), 145-156.
- [23] Trybou, J. (2017). The role of performance expectancy in user adoption of technology in healthcare. *Health Information Technology Journal*, 12(6), 333-340.
- [24] Vrazalic, L., & Macgregor, R. (2009). Barriers to e-commerce adoption: A study of Australian and Croatian SMEs. *Journal of Electronic Commerce Research*, 7(1), 33-44.
- [25] Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, 26(4), 760-767.
- [26] Amin, M. E. (2007). *Social science research: Conception, methodology, and analysis*. Makerere University.
- [27] Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

[28] Chao, C. M. (2019). Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. *Frontiers in psychology*, 10, 1652.

[29] Sair, S. A., & Danish, R. Q. (2018). Effect of performance expectancy and effort expectancy on the mobile commerce adoption intention through personal innovativeness among Pakistani consumers. *Pakistan Journal of Commerce and social sciences (PJCSS)*, 12(2), 501-520.

[30] Mensah, I. K., Zeng, G., & Mwakapesa, D. S. (2022). The behavioral intention to adopt mobile health services: The moderating impact of mobile self-efficacy. *Frontiers in Public Health*, 10, 1020474.

## CYBERSECURITY VS INFORMATION SECURITY

Ketiladze Dachi<sup>1</sup>  
<sup>1</sup>JSG “TBC Insurance”

### კიბერუსაფრთხოების მეცნიერება VS ინფორმაციული უსაფრთხოების დარგი

კეთილაძე დაჩი<sup>1</sup>  
<sup>1</sup>სს „თიბისი დაზღვევა“

**ABSTRACT:** Some Georgian information security professionals, even those with international certifications, incorrectly claim that 'cybersecurity is part of information security.' This misplaces cybersecurity within the realm of information security, rather than recognizing it as a separate field of IT security. Such a viewpoint is clearly unprofessional and subjective. This study seeks to elevate understanding of information security, particularly among both experienced and novice professionals. It clearly delineates and substantiates the differences between information security and cybersecurity.

**KEYWORDS:** Cybersecurity, security awareness, information security, IT security, digital security

**ანოტაცია:** საქართველოში, ინფორმაციული უსაფრთხოების სფეროს, მათ შორის საერთაშორისო სერტიფიცირებების მქონე სპეციალისტების ნაწილი თვლის, რომ ციტატა: „კიბერუსაფრთხოება ინფორმაციული უსაფრთხოების შემადგენელი ნაწილია“. ამკარაა, რომ ისინი კიბერუსაფრთხოების მეცნიერებას ინფორმაციული უსაფრთხოების დარგის დაფარვის ზონაში მოიაზრებენ, და არა ზოგადად, ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს ქვეშ, - რაც გახლავთ არაპროფესიონალური და სუბიექტური შეფასება. მოცემული კვლევა ორიენტირებულია ცნობიერების დონის ამაღლებაზე როგორც ინფორმაციული უსაფრთხოების სფეროს სპეციალისტებს შორის, ასევე დამწყებ სპეციალისტებშიც. ის მკაფიოდ განმარტავს და ქვემოთ მოყვანილი, მყარი, დასაბუთებული არგუმენტებით ასაბუთებს ინფორმაციული უსაფრთხოების დარგსა და კიბერუსაფრთხოების მეცნიერებას შორის განსხვავებას.

**საკვანძო სიტყვები:** კიბერუსაფრთხოება, უსაფრთხოების ცნობიერების ამაღლება, ინფორმაციული უსაფრთხოება, IT უსაფრთხოება, ციფრული უსაფრთხოება

#### შესავალი:

ინფორმაციული უსაფრთხოების დარგის დეფინიცია: „ინფორმაციული უსაფრთხოება გულისხმობს ინფორმაციისა და საინფორმაციო სისტემების დაცვას არასანქცირებული წვდომის, გამოყენების, გამჟღავნების, შეცვლის ან/და განადგურებისგან, - კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფის მიზნით“. (nist n.d.)

კიბერუსაფრთხოების მეცნიერების დეფინიცია: „კიბერუსაფრთხოება არის ქსელების, მოწყობილობებისა და მონაცემების დაცვის მეცნიერება არასანქცირებული წვდომისა და დანაშაულებრივი გამოყენებისაგან, ასევე ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფის პრაქტიკა“. (cisa 2021)

ტერმინი „ინფორმაციული უსაფრთხოება“ გამოიყენება როგორც ინფორმაციული უსაფრთხოების სფეროს, ასევე ინფორმაციული უსაფრთხოების დარგის

განმარტებისთვისაც. სხვა სიტყვებით რომ ვთქვათ, ერთი და იგივე ტერმინი „ინფორმაციული უსაფრთხოება“ გამოიყენება როგორც ზოგადად სფეროს განმარტება (იგივე IT უსაფრთხოება), ასევე, ინფორმაციული უსაფრთხოების დარგის - როგორც ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული მიმართულების დარგის აღნიშვნისთვისაც.

ეს გახლავთ ამოსავალი წერტილი, რომელიც ინფორმაციული უსაფრთხოების სფეროს წარმომადგენელთა ნაწილისთვის ჰბადებს გაუგებრობას იქიდან გამომდინარე, რომ არცერთ ოფიციალურ, საერთაშორისო სტანდარტში, დეფინიციის დონეზე არ არსებობს მკაფიო ზღვარი ამ ორ ცნებას შორის და ინფორმაციული უსაფრთხოების დარგს, როგორც ასეთი, საკუთარი დასახელება არ გააჩნია, თუმცა სხვაგვარადაა მკაფიოდ გამოიხატული კიბერუსაფრთხოების მეცნიერებისაგან.

ამის შედეგად საქართველოში, ზოგიერთი, როგორც წესი - ინფორმაციული უსაფრთხოების დარგის სპეციალისტი თვლის, რომ ციტატა „კიბერუსაფრთხოება ინფორმაციული უსაფრთხოების შემადგენელი ნაწილია“, და რაც მთავარია, გულისხმობენ ინფორმაციული უსაფრთხოების დარგს და არა ზოგადად, ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს. სხვა სიტყვებით რომ ვთქვათ, კიბერუსაფრთხოების მეცნიერებას ინფორმაციული უსაფრთხოების დარგის დაფარვის ზონაში განიხილავენ და ვერ ანსხვავებენ ერთმანეთისგან, რაც თავისთავად არ შეესაბამება ობიექტურ რეალობას.

სწორი პასუხია - ინფორმაციული უსაფრთხოების დარგი და კიბერუსაფრთხოების მეცნიერება შედიან ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს დაფარვის ზონაში და ამის უამრავი ფაქტი და მტკიცე არგუმენტი არსებობს, ასე მაგალითად:

1. არცერთ საერთაშორისოდ აღიარებულ ან/და ოფიციალურ სტანდარტში არ არსებობს დეფინიცია ან/და განმარტება, რომელიც ადგენს ან/და განსაზღვრავს, რომ კიბერუსაფრთხოების მეცნიერება ინფორმაციული უსაფრთხოების დარგის შემადგენელი ნაწილია;
2. უფრო მეტიც, საერთაშორისოდ აღიარებული ინფორმაციული უსაფრთხოების სტანდარტში „ISO/IEC 27001“ სათაურშივე გამოკვეთილად გამოიხატულია ინფორმაციული უსაფრთხოების დარგი და კიბერუსაფრთხოების მეცნიერება. დამატებით, სათაურშივე, თავისთავად ცალკეა გატანილი ასევე პრივატულობის ცნება, რომელიც ნაწილობრივ იკვეთება ინფორმაციული უსაფრთხოების სფეროსთან, მაგრამ ასევე სცილდება მის ფარგლებს (ისევე, როგორც კიბერუსაფრთხოების მეცნიერება ნაწილობრივ იკვეთება, მაგრამ სცილდება ინფორმაციული უსაფრთხოების დარგის ფარგლებს): (ISO/IEC 2022)
3. ზემოთხსენებულს კიდევ ერთხელ ადასტურებს ის ფაქტიც, რომ პირობითად, თუ არსებობს “ISO/IEC 27001:2022”, რომელიც აუცილებელი ფორმით ადგენს ინფორმაციული უსაფრთხოების მართვის სისტემების შექმნის, დანერგვის, მხარდაჭერისა და მუდმივი გაუმჯობესების მოთხოვნებს, ასევე არსებობს „ISO/IEC 27032:2023 Cybersecurity“, რომელიც გახლავთ კიბერუსაფრთხოების მეცნიერების სახელმძღვანელო, რომელიც მოცემულ დოკუმენტში ფოკუსირებულია ინტერნეტის უსაფრთხოების უნიკალურ ასპექტებზე და მის კავშირზე ინფორმაციის უსაფრთხოებასთან, ქსელურ უსაფრთხოებასთან და კრიტიკული ინფრასტრუქტურის დაცვაზე. (ISO n.d.)
4. კიდევ ერთი ფაქტი და უტყუარი არგუმენტია ისიც, რომ ღია წყაროების ანალიზის მეთოდი (OSINT) (Gill 2023) და ე.წ. “Threat Intelligence” (IBM, <https://www.ibm.com> n.d.) - აბსოლუტურად სცდებიან ინფორმაციული უსაფრთხოების დარგის ფარგლებს და ამავედროულად წარმოადგენენ კიბერუსაფრთხოების მეცნიერების განუყოფელ ნაწილს.

5. კიდევ ერთ მაგალითად შეიძლება მოვიყვანოთ ინფორმაციული უსაფრთხოების სფეროს, საერთაშორისოდ აღიარებული სერთიფიცირების მქონე აკადემიების სასწავლო კურსები, მათი დასახელებები და მათში მოცემული სასწავლო მასალების განსხვავებები. განვიხილოთ საერთაშორისოდ ცნობილი და აღიარებული ორგანიზაცია “EC-Council”, რომლის მიერ გაცემულ სერთიფიკატებსაც გააჩნია საერთაშორისო აღიარება ინფორმაციული უსაფრთხოების სფეროში, როგორც ინფორმაციული უსაფრთხოების დარგის, ასევე კიბერუსაფრთხოების მეცნიერების მიმართულებებით.

შედარებისთვის, დავადართო მისი ორი, დამოუკიდებელი სასერტიფიკატო კურსი: “Certified Cybersecurity Technician” (C|CT)

ქართულად - „კიბერუსაფრთხოების სერთიფიცირებული სპეციალისტი / ტექნიკოსი“ სასწავლო მასალაში შემავალი საკითხები:

მოდული 01: ინფორმაციული უსაფრთხოების საფრთხეები და დაუცველობა

მოდული 02: ინფორმაციული უსაფრთხოების თავდასხმები

მოდული 03: ქსელის უსაფრთხოების საფუძვლები

მოდული 04: იდენტიფიკაცია, ავთენტიფიკაცია და ავტორიზაცია

მოდული 05: ქსელის უსაფრთხოების კონტროლი - ადმინისტრაციული კონტროლი

მოდული 06: ქსელის უსაფრთხოების კონტროლი - ფიზიკური კონტროლი

მოდული 07: ქსელის უსაფრთხოების კონტროლი - ტექნიკური კონტროლი

მოდული 08: ქსელის უსაფრთხოების შეფასების ტექნიკა და ინსტრუმენტები

მოდული 09: აპლიკაციის უსაფრთხოება

მოდული 10: ვირტუალიზაცია და ღრუბლოვანი ინფრასტრუქტურა

მოდული 11: უსადენო ქსელის უსაფრთხოება

მოდული 12: მობილური მოწყობილობის უსაფრთხოება

მოდული 13: „IoT“ (IBM, <https://www.ibm.com> n.d.) და „OT“ ტიპის მოწყობილობების (NIST n.d.) უსაფრთხოება

მოდული 14: კრიპტოგრაფია

მოდული 15: მონაცემთა უსაფრთხოება

მოდული 16: ქსელის პრობლემების მოგვარება

მოდული 17: ქსელური ნაკადის მონიტორინგი

მოდული 18: ქსელის ჟურნალების მონიტორინგი და ანალიზი

მოდული 19: ინციდენტზე რეაგირება

მოდული 20: კიბერ ექსპერტიზა

მოდული 21: ბიზნესის უწყვეტობა და კატასტროფის აღდგენა (cisco თ. გ.)

მოდული 22: რისკების მართვა

(eccouncil 2024)

“Chief Certified Information Security Officer” (C|CISO)

ქართულად - „ინფორმაციული უსაფრთხოების სერთიფიცირებული უფროსი ოფიცერი“ სასწავლო მასალაში შემავალი საკითხები:

დომენი 1: მმართველობა, რისკი, შესაბამისობა

დომენი 2: ინფორმაციის უსაფრთხოების კონტროლი და აუდიტის მართვა

დომენი 3: უსაფრთხოების პროგრამის მართვა და ოპერაციები

დომენი 4: ინფორმაციის უსაფრთხოების ძირითადი კომპეტენციები

დომენი 5: სტრატეგიული დაგეგმვა, ფინანსები, შესყიდვები და მესამე მხარის მართვა

(<https://www.eccouncil.org> 2024)

ამკარაა, რომ როგორც მოცემული სასერტიფიკატო კურსის დასახელებები, ასევე სასწავლო მასალებში შემავალი საკითხების აბსოლუტური უმრავლესობა მკვეთრად





განსხვავებულია და ორივე შემთხვევაში მკაფიოდაა გამოკვეთილი შესაბამისი დარგისა თუ მეცნიერებისთვის საჭირო და მნიშვნელოვანი პროფესიული სპეციფიკა და აქცენტები. ნ. თუ გადავხედავთ საერთაშორისოდ აღიარებულ სტანდარტებთან შესაბამისობაში მყოფ და მსოფლიოს წამყვანი ორგანიზაციებისა თუ ქვეყნების სახელმწიფო სტრუქტურული ერთეულების მიერ გამოქვეყნებულ ვაკანსიებს, - შევამჩნევთ, რომ აქაც მკაფიოდაა გამოკვეთილი ინფორმაციული უსაფრთხოების დარგის ან/და კიბერუსაფრთხოების მეცნიერების სპეციალისტების წინაშე წაყენებული, სპეციფიური ცოდნისა და გამოცდილების შესაბამისი მოთხოვნები და პასუხისმგებლობები.

ასე მაგალითად, შეგვიძლია განვიხილოთ დასაქმების საერთაშორისო ონლაინ პლატფორმაზე “Indeed”-ზე გამოქვეყნებული ორი დამოუკიდებელი ვაკანსია, - ინფორმაციული უსაფრთხოების დარგის სპეციალისტისა და კიბერუსაფრთხოების მეცნიერების სპეციალისტის პოზიციაზე და შევადაროთ ერთმანეთს მათ წინაშე წაყენებული სპეციფიური მოთხოვნები და პასუხისმგებლობები:

### INFORMATION SECURITY SPECIALIST

The State of Florida | 250 Marriott Dr, Tallahassee, FL 32301 | \$55,000 a year

[Apply now](#)  

#### Full job description

Requisition No: 828027

Agency: Department of Law Enforcement

Working Title: INFORMATION SECURITY SPECIALIST- 71001685

Pay Plan: Career Service

Position Number: 71001685

Salary: \$55,000.00

Posting Closing Date: 06/26/2024

#### Total Compensation Estimator Tool

INFORMATION SECURITY SPECIALIST

INFORMATION TECHNOLOGY SERVICES

NETWORK AND INFORMATION SECURITY - RISK

**\*\*Open-Competitive Opportunity\*\***

#### POSITION SUMMARY:

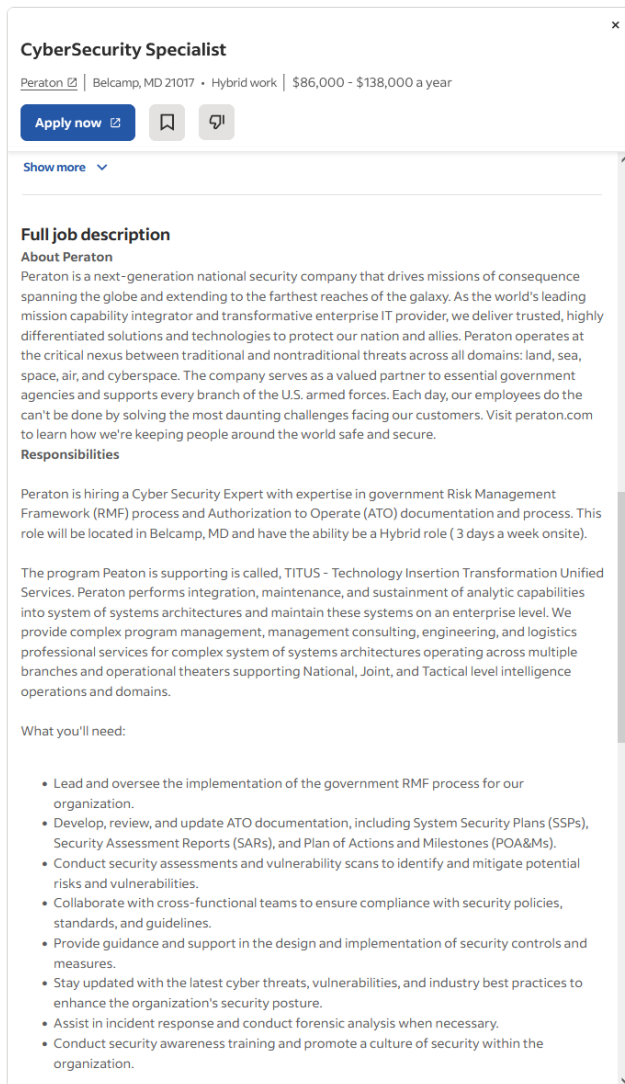
This position is responsible for assisting in the ongoing support and administration of the Department's information security program. The incumbent in this position will focus on areas relating to risk management, continuity of operations, and disaster recovery in support of the information security program. This individual will also have a secondary focus in areas of governance and compliance for information security regulations. The incumbent will also assist in formulation and maintenance of information security policies in conjunction with the FDLE Information Security Manager relating to these areas.

#### DUTIES & RESPONSIBILITIES:

Specific duties include:

- Establishing and continuously enhancing the Continuity of Operations (COOP) programs, plans and processes for FDLE in conjunction with the Information Security Manager;
- Establishing and continuously enhancing the Disaster programs (DR), plans and processes for FDLE in conjunction with the Information Security Manager;
- Establishing and continuously enhancing the Risk Management programs, plans, and processes in conjunction with the Information Security Manager;
- Researching mandates, regulations and rules for Information Security requirements for the agency;
- Conducting interviews and information gathering meetings;
- Leading tabletop exercises relating to COOP, Risk Management and DR in conjunction with the Information Security Manager; and
- Establishing applicable security policies and best practices.

**Fig.1** ინფორმაციული უსაფრთხოების დარგის სპეციალისტის ვაკანსია, (https://www.indeed.com n.d.) დამსაქმებელი: ფლორიდის შტატის სამართალდამცავი დეპარტამენტი



**Fig.2** კიბერუსაფრთხოების მეცნიერების სპეციალისტის ვაკანსია დამსაქმებელი: კომპანია „Peraton“, გახლავთ აშშ-ს სამთავრობო სააგენტოებისა და აშშ-ს შეიარაღებული ძალების მომსახურე კომპანია. (https://www.indeed.com n.d.)

აშკარაა, რომ ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული და პრაქტიკული მიმართულებების, ანუ ინფორმაციული უსაფრთხოების დარგის სპეციალისტისა და კიბერუსაფრთხოების მეცნიერების სპეციალისტის წინაშე წაყენებული მოთხოვნები და პასუხისმგებლობები სპეციფიურად აქცენტირებულია,

კონკრეტული მიმართულებისთვის დამახასიათებელი, შესაბამისი ცოდნისა და გამოცდილების ჭრილში.

აქვე, შემაჯამებელი სახით, გთავაზობთ მოკლე განმარტებას ინფორმაციული უსაფრთხოების სფეროს ზემოთხსენებული ორი მიმართულების ძირითად ფუნქცია - მოვალეობებზე.

ინფორმაციული უსაფრთხოების დარგის პროფესიონალების ძირითადი ამოცანებია, რომ, პირობითად, კომპანიაში დოკუმენტირებული და დანერგილი იყოს სხვადასხვა პოლიტიკები და პროცედურები, რომლებიც შესაბამისობაში იქნება სახელმწიფო კანონებთან და საერთაშორისოდ აღიარებულ სტანდარტებთან. ასევე, პრაქტიკულ ნაწილში, პირობითად, ხდებოდეს ბიზნეს უწყვეტობის პროცედურის პერიოდული ტესტირება, ბიზნეს პროცესების კომპანიაში დანერგილ პოლიტიკებთან თავსებადობის აუდიტი და ასევე სხვა, ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული მიმართულების აქცენტის მქონე ფუნქცია-მოვალეობები, რაც თავისთავად არ გამორიცხავს ტექნიკურ ცოდნასა და ტექნიკური კონტროლების დანერგვა / კონფიგურაციაში ჩართულობას.

მეორეს მხრივ, კიბერუსაფრთხოების მეცნიერების პროფესიონალების ძირითადი ამოცანებია, რომ, პირობითად, რეგულარულად ხდებოდეს კომპანიის ინფორმაციული სისტემებსა და მათ შემადგენელ კომპონენტებში არსებული პოტენციური უსაფრთხოების სისუსტეების იდენტიფიცირება, ვალიდაცია და მიტიგაცია - უსაფრთხოების სისუსტეების სკანირებისა (Center, <https://csrc.nist.gov> თ. გ.) და შეღწევადობის ტესტირების გზით (Center, <https://csrc.nist.gov> თ. გ.). რეგულარულად მოწმდებოდეს თანამშრომლების კიბერუსაფრთხოების ცნობიერების დონისა და კომპანიის თანამშრომლების მედეგობის განსაზღვა ე.წ. „ფიშინგ სიმულაციის“ (Phishing Simulation) გზით (IBM, <https://www.ibm.com> n.d.). გარდა ამისა, პირობითად, დოკუმენტირებული იყოს სხვადასხვა ტიპის კიბერ საფრთხეების წინააღმდეგ რეაგირების გეგმები. ეს ყველაფერი თავისთავად არ გამორიცხავს სახელმწიფო კანონებისა და საერთაშორისოდ აღიარებული სტანდარტების ან/და საუკეთესო პრაქტიკების ცოდნას, კომპანიაში დანერგილ უსაფრთხოების პოლიტიკებთან შესაბამისობას და ა.შ.

შემაჯამებელი სახით უნდა აღინიშნოს, რომ ინფორმაციული უსაფრთხოების დარგსა და კიბერუსაფრთხოების მეცნიერებას შორის არსებითი განსხვავება ის გახლავთ, რომ ინფორმაციული უსაფრთხოების დარგი იცავს ინფორმაციასა და მის ატრიბუტებს, ხოლო კიბერუსაფრთხოების მეცნიერება კი ორიენტირებულია ინფორმაციისა და ინფორმაციული აქტივების სხვადასხვა ტიპის კიბერ საფრთხეებისგან დაცვის პრაქტიკაზე.

საბოლოოდ, აშკარად იკვეთება, რომ ინფორმაციული უსაფრთხოების სფეროს როგორც ადმინისტრაციული, ასევე პრაქტიკული მიმართულების პროფესიონალს სჭირდება მედლის მეორე მხარეს მდგომი მეცნიერებისა თუ დარგისათვის დამახასიათებელი სპეციფიკის საფუძვლების ცოდნა, თუმცა ცალკეულად აღებულ მიმართულებათა ჭრილში, მათთვის დამახასიათებელი სპეციფიკა მკვეთრად განსხვავებულია და საჭიროებს შესაბამის სიღრმისეულ ცოდნასა და გამოცდილებას იმისათვის, რომ საერთო ჯამში, ორივე ზემოთხსენებული პროფილის მქონე პროფესიონალების გაერთიანებით შეიკრას ის ძალა, რომელიც ცნობილია ინფორმაციული უსაფრთხოების სფეროს სახელით და რომელიც დღემდე წინ უდგათ კიბერ კრიმინალებს.

## Bibliography

- Center, Computer Security Resource. n.d. <https://csrc.nist.gov>.  
[https://csrc.nist.gov/glossary/term/vulnerability\\_assessment](https://csrc.nist.gov/glossary/term/vulnerability_assessment).
- . n.d. <https://csrc.nist.gov>. [https://csrc.nist.gov/glossary/term/penetration\\_testing](https://csrc.nist.gov/glossary/term/penetration_testing).
- cisa. 2021. <https://www.cisa.gov>. February 1. Accessed February. <https://www.cisa.gov/news-events/news/what-cybersecurity> .
- cisco. n.d. <https://www.cisco.com>. <https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-business-continuity.html>.
- eccouncil. 2024. <https://www.eccouncil.org>. <https://www.eccouncil.org/train-certify/certified-cybersecurity-technician-certification/>.
- Gill, Ritu. 2023. "<https://www.sans.org/blog/what-is-open-source-intelligence/>."  
<https://www.sans.org>. February 23. <https://www.sans.org/blog/what-is-open-source-intelligence/>.
2024. <https://www.eccouncil.org>. <https://www.eccouncil.org/train-certify/certified-chief-information-security-officer-cciso/> .
- n.d. "<https://www.indeed.com>." <https://www.indeed.com/jobs>.  
<https://www.indeed.com/jobs?q=information+security+specialist&sc=0bf%3Aexrec%28%29%3B&start=30&vjk=0355d1840893a397>.
- n.d. "<https://www.indeed.com>." <https://www.indeed.com/jobs>.  
<https://www.indeed.com/jobs?q=cybersecurity+specialist&start=C30&vjk=66a83adb9abe8030>.
- IBM. n.d. "<https://www.ibm.com>." <https://www.ibm.com/topics/threat-intelligence>.  
<https://www.ibm.com/topics/threat-intelligence>.
- . n.d. <https://www.ibm.com>. <https://www.ibm.com/think/topics/phishing-simulation>.
- . n.d. <https://www.ibm.com>. <https://www.ibm.com/topics/internet-of-things>.
- ISO. n.d. <https://www.iso.org>. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en> .
- ISO/IEC. 2022. "Information security, cybersecurity and privacy protection — Information security management systems — Requirements". <https://www.iso.org>.  
<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>.
- nist. n.d. <https://csrc.nist.gov>. [https://csrc.nist.gov/glossary/term/information\\_security](https://csrc.nist.gov/glossary/term/information_security) .
- NIST. n.d. <https://csrc.nist.gov>. [https://csrc.nist.gov/glossary/term/operational\\_technology](https://csrc.nist.gov/glossary/term/operational_technology).