



SPCSJ

**SCIENTIFIC AND PRACTICAL
CYBER SECURITY JOURNAL**

VOL5 No3

September 2021

ISSN 2587-4667

GETTING STARTED WITH ANDROID MOBILE APPLICATIONS SECURITY TESTING

P. Raghu Vamsi, Assistant Professor, Department of Computer Science and Engineering,
Jaypee Institute of Information Technology, Noida, India.
Agrah Jain, Solution Advisor, Delloitte USI, Gurugram, India.

ABSTRACT:The availability of the Internet, cheaper data tariffs, and easy way of using the mobile phones made the effective use of Android mobile phones for availing Electronic Commerce (e-commerce) mobile Applications (Apps) by the people for purchasing the daily needs and regular household items. The success of the e-commerce platforms is based on their availability to public as web and Android mobile Apps. Further, their success is based on the trust and security that they maintain regarding users personal and payment data. But the poor design and development, unnoticed mistakes in coding of the e-commerce Android mobile Apps lead to many vulnerabilities and thereby becomes the simple target for the hackers. Along with conventional security testing methods, application dependent methods need to be applied on the e-commerce android Apps. To this end, this paper presents various possible practical security methods followed by penetration testers along with countermeasures that can be applicable for avoiding vulnerabilities in e-commerce Android Apps.

KEYWORDS:*Android Applications, e-commerce, penetration testing, security, testing, trust, vulnerability.*

1. INTRODUCTION

Nowadays every Electronic Commerce (e-commerce) company, from early stage startups to rising unicorns, has their Android application (Apps). There exists variety of applications like shopping Apps, dating Apps, gaming Apps, educational Apps, medical Apps etc. Only internal applications of the company cannot be found on Google Playstore due to privacy reasons other than this nearly every application can be found on Google Playstore. According to android.com there are around 50 billion android applications on Google Playstore as of December 2020 and the count is increasing day by day. Out of which around 80% of the application owner does not take any measures for the android security. Taking the example of big giants like McDonalds, its android application is so compromised by the attackers which allow anyone to buy burgers and fries for free from the Android App. According to the one of the leading Indian news agency Times of India [27] report, a company named ixigo's data was breached by the attackers and around 18 millions users' personal data was went to dark web. In this way, there are many of such examples [18, 19, 24, 26].

1.1 Contribution and Paper organization

As the number of e-commerce Apps are increasing exponentially their security concerns are also increasing rapidly. Since android penetration testing is the most underrated thing but it is as important as web application penetration testing. Also it is sometimes more important than web application since generally companies have more number of applications than a single main website. Therefore, Android App security must be the prime focus of companies and this is paper will address Android vulnerabilities in practical ways and countermeasures to protect them [7, 8, 11, 12]. An Android App will be designed generally to run on various Android operating system versions such that the presence of bugs in operating system design or patches, and the permissions used by the App may lead to new vulnerabilities and will become exploitable target. This may lead to any of the OWASP top 10 security vulnerabilities of mobile applications [1-6, 17, 18, 19]. To this end, this paper focused on practical Android App security checks to be made to get started with android security testing. This

paper articulates the Google Playstore security and privacy policies, what hackers can do with the presence of vulnerable App, the vulnerabilities hackers try to exploit, sensitive data exposure, static and dynamic analysis etc. In this way, this paper is focusing on important basic bugs that have low to medium impact to check during App security testing.

There exist two ways of analysis during security testing: 1) Static and 2) Dynamic [20-23, 25]. The static security testing is the testing of internal structure of App program and will be performed without running it. This will be done by code inspections, code walkthroughs. On the other hand, dynamic testing is the testing of program during its runtime. This paper focuses more on the static analysis and few concepts of dynamic analysis. In the Section 2, a short description the App structure and the Google security policies for Android Apps are explained. Section 3 focuses on Android Apps security testing. In this section, we present reverse engineering an App, debugging the App apk, stealing information from shared preferences folders, OAuth API call back locking (SDK testing), Hardcoded secrets, and weak logouts. Section 4 concludes the paper with future work. List of abbreviation used in this paper are illustrated in the Table 1.

API	Application programming interface
APK	Android application package
APPS	Applications
Pen-Testing	Penetration testing
POC	Proof of concept
OWASP	Open Web Application Security Project
IDOR	Insecure Direct Object Reference
Burp	Burpsuite
RCE	Remote Code Execution
ADB	Android Debug Bridge
GUI	Graphical User Interface

Table.1. List of abbreviations

2. ANDROID PRILIMINARIES AND GOOGLE PLAYSTORE SECURITY

Before finding vulnerabilities in Android Apps, it is important to understand basic information about its structure. This section presents the preliminaries of Android Application structure and the security scanning method of Google Play store [14, 16].

2.1 Basic structure of the Android Applications

The basic structure of the Android Apps includes the following components:

Activities: It is one of the most important things in an Android App. Since every screen on which the user interacts is an activity, when the user starts an application then the function *onCreate()* is launched and it may also start more than one activity. In other words it is the UI screen with which the user interacts. Security tester main focus should find hidden information and check for the exported status of activity.

Intents: It is a way of telling an activity to perform something or intent is a messaging object that allows communication between different application components such as Activity, Content Providers, Services, etc. It can be used for communication between application components of the same or different applications. Intents contain three items: action, data and category.

Web Views: Android allows developers to display web content directly into their application through Webviews. Security testers can consider Webview as a dedicated web browser of an application. If

the web view is not implemented properly then the attacker can open its URL in the webview of the application. To check for Web Views in application the following sequence to be followed in App: Go to manifest file [search for loadUrl or Webviews] details of webview to view the details.

Broadcast receiver: It helps to send and receive the system's event notification. For example if the battery is low, downloading is complete, no signal then the Android system sends broadcast messages which are received by application for their functioning like during offline the YouTube App shows no internet. The attackers mainly focuses on changing the message and makes the application behaves inappropriately.

2.2 Description of Google Play Protect

Google has developed Artificial Intelligence based systems to detect malicious applications on their platform. It can be on Google Playstore as 'Google Play Protect'. Every application that is downloaded is scanned by the Play Protect, if it is found to be malicious then Google will not allow it to be installed. Also the Play protect scans the installed applications for security threats. Fig. 1 shows the Google Play Protect after scanning Apps for security threats.

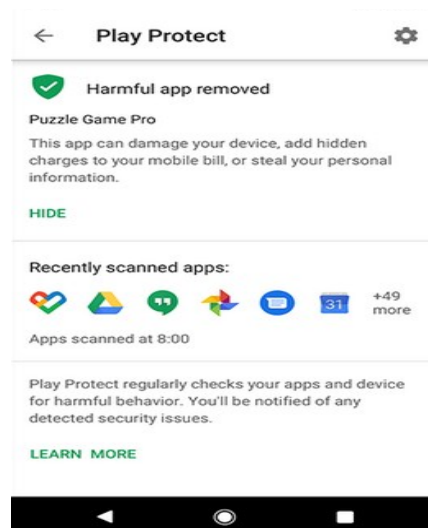


Fig.1. Result after Play Protect scanned the Apps

Play Protect regularly scans Apps for any sign of malware, it also monitors installed applications for any unintended behavior and Google play protect also helps to track the mobile phone when lost and wipe data if needed. Apart from playstore Apps there are non playstore apps i.e., internal Apps of any organization which is not published on playstore. To scan these types of Apps, users should scan it from virustotal.com for any traces of malware or loggers present. The virus total scans the item (Android apk) with 70+ antivirus scanners and also looks for presence of any blacklist URL. Security tester need to do is upload the apk to the virus total before installing and see the score and results of every scanner present as shown in the Fig. 2.

Now the question arises is why the Google play protect or website like virus total is not sufficient for scanning Apps. The answer is that it is because they work on phone security level i.e., scanning the apk for virus, malware, loggers, privacy etc. But to find vulnerabilities like authentication bypass of any application, sensitive data leakage, parameter tampering while payment from any application, code tempering, insecure data storage, insufficient cryptography, reverse engineering etc, and to get application level security proper vulnerability assessment and penetration testing is needed. Further, these tests cannot be performed by either by Google play protect and any other scanning website like virus total.

3. ANDROID APPLICATION SECURITY TESTING

In this section, the basic and medium level vulnerabilities that appear in the Android Apps were explained. For this, the tools we will be using are frida, drozer, jadx-gui, android debugging bridge, mob-sf and the Burpsuite. From which frida and mob-sf is used for automated vulnerability scanning, drozer for interaction analysis, adb is used for debugging, jadx-gui is used for reversing the android app and Burpsuite is used for dynamic analysis [9, 10, 13, 15].

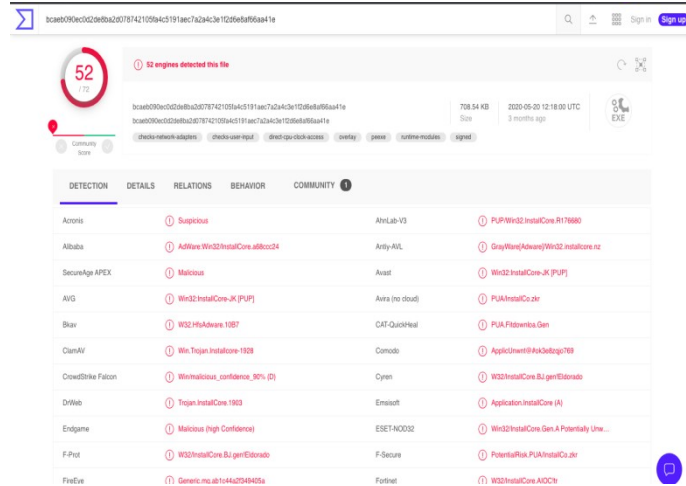


Fig.2. Result after Virus total scan

3.1 Reverse engineering and Debugging Apps

Reverse engineering is one of the important steps in any testing also known as back engineering with the help of it attacker can do source code analysis of android application, manipulate the raw data, reconstruct the application, extract the knowledge from the data, and present this repackaged apk to end user to initiate attacks such as personal information stealing, server side information gathering etc. Now the most important part is how to decompile an android application. To do it, we use the tool named jadx-gui which is graphical user interface tool to decompile android application. Run the jadx tools and load the apk such that it will do rest of the things for analysis of the application. Fig. 3 shows the manifest.xml file generated by jadx-gui after decompiling apk file.

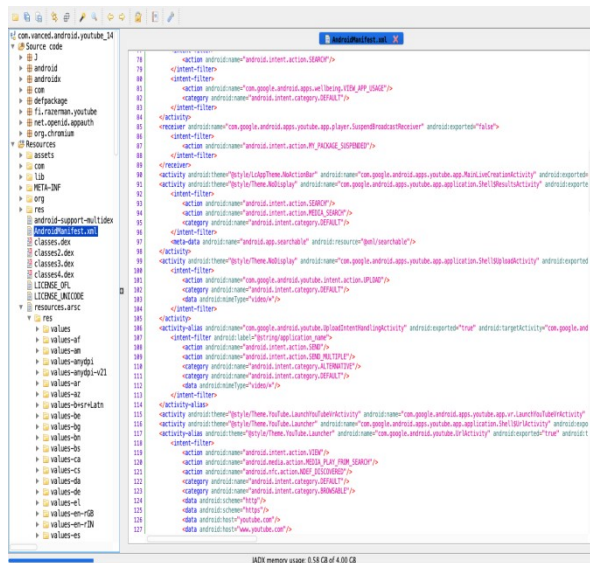


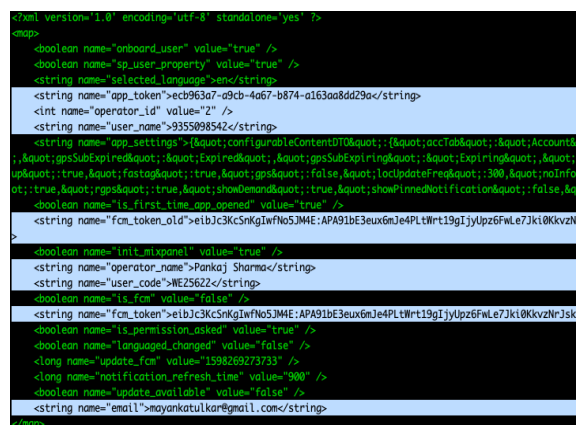
Fig.3. Manifest.xml file in Jadx-gui after decompiling

After the source code analysis, the debugging is done in android studio to analyze the working of functions, intents, actions, data storage details etc. For this first decompile an application using jadx-gui and save it then import this file as grade in android studio and can debug at any specific section of the code. Also the testers need to understand the working of application using debug option in Android studio. As a precautionary step, it is recommended to turn on the anti debugging flag in the code so that the attacker cannot debug it. This anti debugging does not allow injecting garbage data in the communication channel of manually set breakpoints to confuse the debugger.

3.2 Stealing sensitive information from shared preferences

In general, Apps write sensitive information in shared_prefs files which can be anything from access token to some credentials. To this vulnerability, tester need to check MIME type in android manifest file, MIME type must be application/pdf, application/*. Navigate to the activity in which MIME type is defined in the jadx-gui and look for functions named onCreate(), onResume(), onNewIntent(). Remember that whenever tester will trigger these types of exploits using apk it always comes via the intent function. Once it is done, analysis to be conducted in the above mentioned functions which is sending intent with some data as stream and to which destination path and file name is set. For this two types of exploitations are possible: 1) using a rogue app and 2) using adb (Android debugger) to access the shared_Prefs folder. The second method is used for explanation. To do this, try to find the access token in the shared_prefs using ADB for MIME type. Setup adb in the system terminal and use the below commands to access the shared_prefs to see the data as shown Fig. 4.

```
# adb devices
# adb shell
# cd data/data/com.package_name
# cd shared_prefs
# cat prefs.xml
```



```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<map>
  <boolean name="onboard_user" value="true" />
  <boolean name="sp_user_property" value="true" />
  <string name="selected_language"></string>
  <string name="app_token">ecb963a7-a9cb-4a67-b874-a163aa8dd29a</string>
  <int name="operator_id" value="2" />
  <string name="user_name">9355098542</string>
  <string name="app_settings">{&quot;configurableContentDtt0&quot;:{&quot;accTab&quot;:{&quot;Account&quot;:{&quot;gpsSubExpired&quot;:{&quot;Expired&quot;:{&quot;gpsSubExpiring&quot;:{&quot;Expiring&quot;:{&quot;gpsUp&quot;:{&quot;true&quot;,&quot;fastag&quot;:{&quot;true&quot;,&quot;gps&quot;:{&quot;false&quot;,&quot;locUpdateFreq&quot;:{&quot;300&quot;,&quot;noInfoCot;true&quot;,&quot;rgps&quot;:{&quot;true&quot;,&quot;showDemand&quot;:{&quot;true&quot;,&quot;showPinnedNotification&quot;:{&quot;false&quot;,&quot;
  <boolean name="is_first_time_app_opened" value="true" />
  <string name="fcm_token_aId">e1b1c3KcSnKgwNo5JMIE:APA91BE3eux6mJe4PLtWrt19gIjyUpz6FwLe7Jki0KkvzNrJ
  >
  <boolean name="init_mlxpanel" value="true" />
  <string name="operator_name">Pankaj Sharma</string>
  <string name="user_code">WE25622</string>
  <boolean name="is_fcm" value="false" />
  <string name="fcm_token">e1b1c3KcSnKgwNo5JMIE:APA91BE3eux6mJe4PLtWrt19gIjyUpz6FwLe7Jki0KkvzNrJsktt
  <boolean name="is_permission_asking" value="true" />
  <boolean name="language_changed" value="false" />
  <long name="update_fcm" value="15982692733" />
  <long name="notification_refresh_time" value="900" />
  <boolean name="update_available" value="false" />
  <string name="email">mayankatulkar@gmail.com</string>
</map>
```

Fig.4. Secret data and access tokens in shared prefs

From Fig.4 it can be seen that so much sensitive information can be found in shared prefs which includes fcm token, access token, user code, email, phone number etc. To get protected from this never ever store sensitive information in the shared_prefs folder because it is the main target of attackers. Further, it is recommended to place the data in an encrypted format to avoid data theft.

3.3 OAuth API call back Locking (or SDK Testing)

OAuth is token based authorization used commonly by every application to authenticate the user to access their account without entering password using Google, Facebook, Pinterest, Yandex etc. For example, if the user is using an e-commerce App X, and there is a provider which connects with your application say Paypal for payments. Paypal provides a dashboard where user can define redirect uri in android application there is a “scheme” to redirect uri is the url for the web domain similarly scheme is the url for the mobile application. And if user does not define it then the App X become vulnerable and it can be used to hijack the sessions in the App X. To exploit this vulnerability, an attacker needs an rogue apk installed on user device so that it can capture the token and hijack user session. We have made an apk token catcher and defined the scheme name praskhar to capture it as shown in Fig. 5. The countermeasure to get protected from this vulnerability is to define ‘scheme’ in intent filter and filter out the url that is passing any unwanted content.

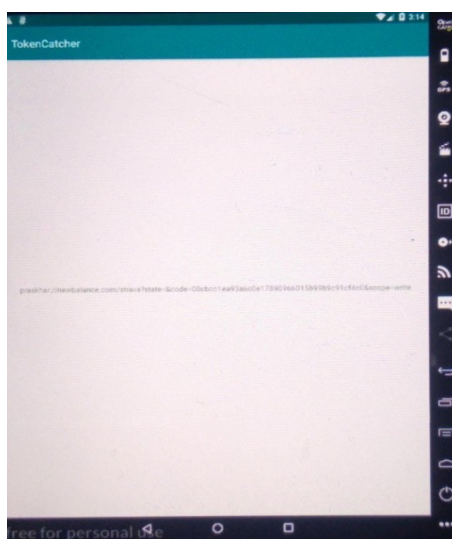


Fig.5. Rogue apk capturing token with scheme praskhar

3.4 Hardcoded Scerates

This section focuses on sensitive data exposure, in which we will look for the hardcoded tokens, api keys, keys, Oauth tokens, jwt tokens, username and passwords etc. There are two types of exploitations one is SDK based, and other is API as a service (mostly Google maps). We focus on API as service and find some secrets and try to exploit them practically. Starting with the point where to find these hard coded secrets, for this need Jadx-gui tool used to decompile application. After decompiling the following three paths for any hardcoded keys with proper filters to be checked as shown in Fig. 6.

1. Resources.asrc [] values [] strings.xml
2. Resources.asrc [] values [] Array.xml
3. Code analysis (also androidManifest)

After obtaining the hardcoded api key (AIzaSyDHfC0q0Ahujq9Pduvjs-757ffUtd), tester need to check whether it is exploitable or not. For Google maps api key, a command line and Python based open source tool called gmapapiscanner is used. To launch this tool use the following command

```
$ python3 maps_api_scanner_python3.py AIzaSyDHfC0q0Ahujq9Pduvjs-757ffUtd
```


Output of the above command is shown in the Fig. 7. From Fig. 7 it can be observed that the API key found is vulnerable to two paid services. To get protected from this, user need to do following things: 1) try not to hardcode any secret keys; 2) if it is necessary to hardcode then always put the url white listing andreferrer check to ensure that only these api keys must be called from App but not by any other anonymous user.

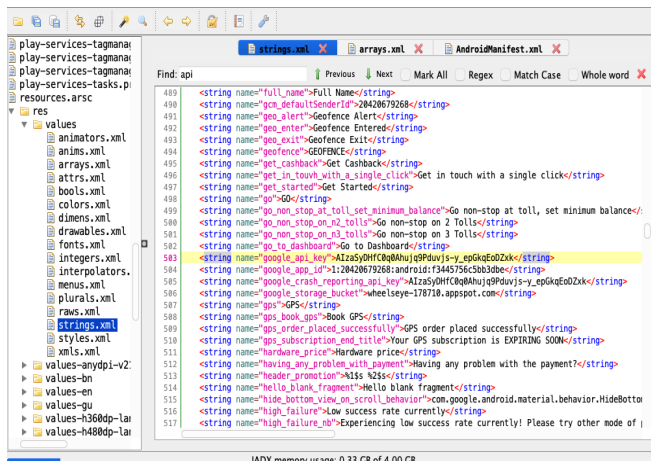


Fig.6. Harcoded google api key in strings.xml

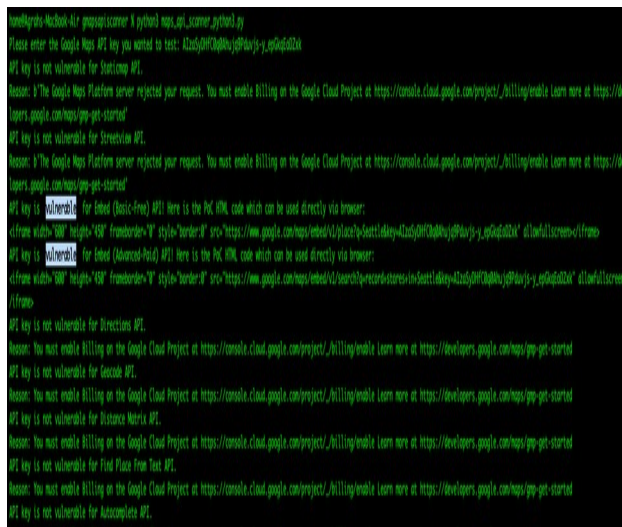


Fig.7. Google api key is vulnerable to two services

3.5 Weak Logouts

This vulnerability is known as authentication bypass which arises due to not implementing proper logout functionality of OAuth clients like login with Google, LinkedIn etc. With this the attacker can login to the victim's account through any of the above client api without entering the login credentials. This vulnerability arises when an application logs out but the application token does not expire or logout the access or session token taking advantage of it. Then the attacker gains unauthorized access to your account.

We present this vulnerability check using Burpsuite. To check this vulnerability, trigger the application login using Google, Facebook or any other client. Turn the intercept on in the Burpsuite and logout the application. Now check for the response at the Burpsuite, if tester observes that there is only app token which is logging out and no session id present then this vulnerability may exist in the application. To have cross verification, logout the application after logging in from third party client then login again. Click on login with Facebook don't put any email and password in the fields as shown in Fig. 8 and press the tiny close button and check for will be logged in automatically in the application or not. It can be observed from Fig.8 that login with Facebook API call is giving success response in the Burpsuite. It is because user was not properly logged out from the application as session id or token is not expired.

As a countermeasure to this vulnerability one must need to properly implement logout functionality both access token and application token must expire after logout. And each new session will be assigned a new session ID which should expire after logging out an application.

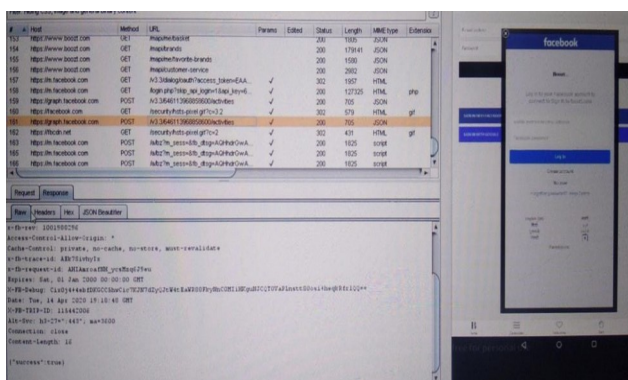


Fig.7. Finding weak logout functionality

4. CONCLUSION AND FUTURE WORK

This paper presented the method of starting with the Android mobile Apps security testing. It covered the topics such as the description of Google play protect, how to perform malware analysis of non play store apps using virus total, static analysis of Apps using reverse engineering, API key exploitation, digging hard coded secrets, weak logout functionality, and sensitive information disclosure. This paper also discussed how to find these vulnerabilities, what attacker can do with these vulnerabilities and countermeasures. In this paper, we have limited our research to basic important vulnerabilities present in android applications which have a severity level of low to medium.

As part of the future work, we attempt to perform dynamic analysis (both manual and automated) with the help of open source tools with main focus on advanced critical bugs related to android applications such as Broadcast receiver exploitation, broadcast sniffing, IDOR in android applications, remote code execution, content provider exploitation using drozer and deep link exploitation and others.

REFERENCES

1. Mahmood, Riyadh, Naeem Esfahani, Thabet Kacem, Nariman Mirzaei, Sam Malek, and Angelos Stavrou. "A whitebox approach for automated security testing of Android applications on the cloud." In 2012 7th International Workshop on Automation of Software Test (AST), pp. 22-28. IEEE, 2012.
2. Rai, Pragati Ogal. Android Application Security Essentials. Packt Publishing Ltd, 2013.

3. Avancini, Andrea, and Mariano Ceccato. "Security testing of the communication among Android applications." In 2013 8th International Workshop on Automation of Software Test (AST), pp. 57-63. IEEE, 2013.
4. Salva, Sébastien, and Stassia R. Zafimiharisoa. "APSET, an Android aPplication SEcurity Testing tool for detecting intent-based vulnerabilities." *International Journal on Software Tools for Technology Transfer* 17, no. 2 (2015): 201-221.
5. Mente, Rajivkumar, and Asha Bagadi. "Android application security." *Advances in Computational Sciences and Technology* 10, no. 5 (2017): 1207-1210.
6. Fischer, Felix, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. "Stack overflow considered harmful? the impact of copy&paste on android application security." In 2017 IEEE Symposium on Security and Privacy (SP), pp. 121-136. IEEE, 2017.
7. Acar, Yasemin, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L. Mazurek, and Sascha Fahl. "Developers need support, too: A survey of security advice for software developers." In 2017 IEEE Cybersecurity Development (SecDev), pp. 22-26. IEEE, 2017.
8. Dashevskiy, Stanislav, Olga Gadyatskaya, Aleksandr Pilgun, and Yury Zhauniarovich. "The influence of code coverage metrics on automated testing efficiency in android." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2216-2218. 2018.
9. Sinaga, Arnaldo Marulitua, P. Adi Wibowo, Ariestoni Silalahi, and Nita Yolanda. "Performance of automation testing tools for android applications." In 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), pp. 534-539. IEEE, 2018.
10. Kulkarni, Keyur, and Ahmad Y. Javaid. "Open source android vulnerability detection tools: a survey." arXiv preprint arXiv:1807.11840 (2018).
11. Montealegre, C., Njuguna, C.R., Malik, M.I., Hannay, P., & McAteer, I.N. (2018). "Security vulnerabilities in android applications", In *proceedings of the 16th Australian Information Security Management Conference* (pp. 14-28). Perth, Australia: Edith Cowan University.
12. Pan, Yuanyuan. "Interactive application security testing." In 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), pp. 558-561. IEEE, 2019.
13. Morgado, Inês Coimbra, and Ana CR Paiva. "The iMPAcT tool for Android testing." *Proceedings of the ACM on Human-Computer Interaction* 3, no. EICS (2019): 1-23.
14. Alkindi, Zainab R., Sultan Qaboos Univresity, Oman Muscat, Mohamed Sarrab, and Nasser Alzidi. "Android Application Permission Model." In 4th FREE & OPEN SOURCE SOFTWARE CONFERENCE (FOSSC'2019-OMAN). 2019.
15. Almeida, Diego R., Patrícia DL Machado, and Wilkerson L. Andrade. "Testing tools for Android context-aware applications: a systematic mapping." *Journal of the Brazilian Computer Society* 25, no. 1 (2019): 1-22.
16. Lai, Duling, and Julia Rubin. "Goal-driven exploration for android applications." In 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 115-127. IEEE, 2019.
17. He, Yongzhong, Xuejun Yang, Binghui Hu, and Wei Wang. "Dynamic privacy leakage analysis of Android third-party libraries." *Journal of Information Security and Applications* 46 (2019): 259-270.
18. Alanda, Aide, Deni Satria, H. A. Mooduto, and Bobby Kurniawan. "Mobile Application Security Penetration Testing Based on OWASP." In *IOP Conference Series: Materials Science and Engineering*, vol. 846, no. 1, p. 012036. IOP Publishing, 2020.
19. Li, Jinfeng. "Vulnerabilities mapping based on OWASP-SANS: a survey for static application security testing (SAST)." *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN (2020): 2516-0281.
20. Xiao, Jianmao, Shizhan Chen, Qiang He, Zhiyong Feng, and Xiao Xue. "An Android application risk evaluation framework based on minimum permission set identification." *Journal of Systems and Software* 163 (2020): 110533.

21. Savola, Reijo M., Markku Kylänpää, and Habtamu Abie. "Risk-driven security metrics for an Android smartphone application." *International Journal of Electronic Business* 15, no. 4 (2020): 297-324.
22. Yasin, Husam N., Siti Hafizah Ab Hamid, Raja Jamilah Raja Yusof, and Muzaffar Hamzah. "An empirical analysis of test input generation tools for android apps through a sequence of events." *Symmetry* 12, no. 11 (2020): 1894.
23. Pecorelli, Fabiano, Gemma Catolino, Filomena Ferrucci, Andrea De Lucia, and Fabio Palomba. "Testing of mobile applications in the wild: A large-scale empirical study on android apps." In *Proceedings of the 28th International Conference on Program Comprehension*, pp. 296-307. 2020.
24. Rani, Sangeeta, and Kanwalvir Singh Dhindsa. "Android application security: detecting Android malware and evaluating anti-malware software." *International Journal of Internet Technology and Secured Transactions* 10, no. 4 (2020): 491-506.
25. Dawoud, Abdallah, and Sven Bugiel. "Bringing balance to the force: Dynamic analysis of the android application framework." *Bringing Balance to the Force: Dynamic Analysis of the Android Application Framework* (2021).
26. Κούκουνας, Άγγελος Παναγιώτης. "Malware analysis, security evaluation for Android application." Master's thesis, Πανεπιστήμιο Πειραιώς, 2021.
27. News Article: <https://timesofindia.indiatimes.com/business/india-business/emails-hashed-passwords-of-18m-ixigo-users-stolen/articleshow/68016866.cms> (Last accessed 15-08-2021)

INFORMATION WAR IN MODERN CONDITIONS PART 2

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine,

Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev, Ukraine,

Lytvynenko Oleksandr, Taras Shevchenko National University of Kyiv, Doctor in Technical Sciences, Professor, Kyiv, Ukraine

Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine,

ABSTRACT: The article is based on the model of information warfare and the methods of psychological influence on the consciousness of people and society are considered. The influence of Russia's aggression on Ukraine through the three-level network concept, which combines all permissible types of influence on the enemy and represents a comprehensive strategy of influence, is proved. The concept of informational and psychological confrontation of society is developed, attention should be paid to the manipulation of information in a society, which aims to change the behavior of the object in the right direction for the subject as well as influence of information and psychological action of mass media on young people, expressed in violence, unmotivated aggression, hostility, cynicism.

KEYWORDS: *information warfare, information influence, aggression, information attack*

Introduction

At all stages of the historical development of human civilization, information has been both the most important object and a means of struggle between peoples, nations, states, military-political blocs and alliances. Some facts of informational influence on a wide audience can be found throughout human history. It is clear that in different periods the intensity of the application of certain methods of influence, as well as the perfection of its organization, differed greatly.

As a result, information and information technology in general have become extremely important for national security and particularly for military security. A number of countries, most notably Russia, have been intensifying the study and resolution of information and information warfare since the 1990s. Thus, the information war has turned from a futurological ghost into a real military discipline, which is being under development and study [1,2,3].

Thus, the geopolitical authority of the state in the international arena and its ability to influence world events today depends not only on economic and military power. Informational factors rather than the power ones are becoming increasingly important, i.e. the ability to effectively influence the intellectual potential of other countries, to disseminate and implement in the public consciousness the relevant spiritual and ideological values, to transform and undermine the traditional foundations of nations and peoples. A new stage is coming in military affairs, which is the transition from a strategy of nuclear deterrence to high-precision counter-force information weapons [4,5].

The role of information struggle are constantly growing in the system of national security of the states. The leading countries of the world, first of all Russia, the USA, France, Germany, Great Britain, Japan, that possess powerful information potential, are constantly increasing it on a scientific basis and at high culture of management.

In these and other countries, the scientific basis for the creation and application of means of information confrontation is the achievement of two main branches of science: cybernetics and computer science, which have been able to integrate many provisions of not only natural but also humanities.

Information is a terrible thing. Now it is indeed the fourth element of state power, which very often comes to the fore in the 21st century. It is enough to take a look at the influence of information on the electorate of such countries as France, Germany, and the United States. And Russia uses it very

well: it creates an artificial world, and if the real world brings it up all the time, it's very soon that the real world begins to believe in the unreal one.

Therefore, information confrontation is the rivalry of social systems (nations, blocs of countries) in the information sphere over the impact on certain areas of social relations and the establishment of control over the sources of strategic resources, as a result of which one group of rivals gets the benefits they need for further development.

According to the intensity, scale and means used, the following stages of information confrontation are distinguished: information expansion, information aggression and information war [6,7].

Information expansion i.e. the activities to achieve national interests by the method of conflict-free penetration into the information sphere in order to:

- carry out gradual and planned change in the system of social relations on the model of the source of expansion invisible to the society;
- displace the provisions of national ideology and national value system and replace them with their own values and ideological attitudes;
- increase the degree of its influence and presence, establish the control over strategic resources, information and telecommunication structure and national mass media (mass media);
- increase the presence of their own media in the information sphere of the object (system), penetration, etc.

Information aggression can be defined as illegal actions of one of the parties in the information sphere, aimed at inflicting specific, tangible damage to the enemy in certain areas of its activities through limited and local use of force.

Information warfare is the highest degree of information confrontation aimed at resolving socio-political, ideological, as well as national, territorial and other conflicts between states, peoples, nations, classes and social groups through the large-scale implementation of means and methods of information violence. (information weapons) [4,5].

Information aggression in the information sphere is assumed to escalate into war if one of the parties to the conflict begins to use information weapons widely against its opponents. This criterion makes it possible to distinguish from all the variety of processes and phenomena occurring in the information society those that pose a danger to its normal (peaceful) development.

In addition, it should be noted that currently there are no international and national legal norms that allow in peacetime (in the absence of an official declaration of war by the aggressor) to legally qualify hostile actions of a foreign state in the information sphere, accompanied by damage to information or other security such, as actions of information aggression or information war of material, moral, other damage. This allows to actively use the most dangerous and aggressive arsenal of forces and means of information warfare as the main means of achieving a political goal in peacetime.

Main part

In information warfare, information weapons are widely used, which represent devices and means designed to inflict maximum damage on the opposing side during the information struggle (through dangerous information influences) [4,5]. For the widespread use of information weapons (as well as any other) it is necessary that it:

- as quickly as possible in comparison with other types of weapons could be applied to the object of influence;
- caused the object of influence the necessary damage in a given time interval;
- was quite simple and cheap to manufacture compared to other weapons of the same class of influence.

At the turn of the XX-XXI centuries. there were conditions that allowed us to speak of information weapons as the most important weapons of the modern era. These include:

- a sharp decline in the cost of data production due to the advent of computer technology. And the production of information is put on the assembly line;
- creation of automated tools for obtaining knowledge from data;
- a sharp reduction in the cost and reduction of time for delivery of messages to almost anywhere in the world due to the development of telecommunications and the Internet;

- a sharp increase in the effectiveness of information impact, due to the emergence of advanced theories in the field of reprogramming of self-learning information systems: the theory of programming for computers and NLP;

- programming for social systems, including a large number of methods and techniques of information and psychological influence.

Objects of influence of information weapons can be:

- information and technical systems;
- information and analytical systems;
- information and technical systems, including service personnel (operator);
- information-analytical systems that include people;
- information resources;
- systems of formation of public consciousness and opinion based on mass media and propaganda;
- human psyche.

In cases where information weapons are not directly or indirectly used against the human psyche (or social group), it is practically possible to name only three objects of influence, each of which belongs to a certain type of information confrontation (in its pure form). These are information-technical and information-analytical systems (which do not include a person) - information-technical confrontation.

Sources of information hazards can be natural (objective) and intentional.

Considering the theory of information confrontation in the political sphere, it should be borne in mind that it occurs at the strategic, operational and tactical levels [1,2].

Basically, the higher political elite should operate at the strategic level, and the information unit of the political clan should operate at the operational and tactical levels.

According to experts, information warfare consists of actions taken to achieve informational advantage in ensuring national, military strategy by influencing the information and information systems of the enemy while strengthening and protecting their own information and information systems and infrastructure.

Information advantage is defined as the ability to collect, process and distribute a continuous flow of information about a situation, preventing the enemy from doing the same. It can also be defined as the ability to assign and maintain a pace of operations that exceeds any possible pace of the enemy, throughout its conduct, while remaining unpredictable, ahead of the enemy in its respective actions.

The information advantage allows you to have a real idea of the combat situation and gives an interactive and highly accurate picture of the actions of the enemy and their troops in real time. The information advantage is a tool that allows the command in critical operations to apply a wide range of different forces, to ensure the protection of troops and the introduction into battle of groups whose composition best meets the task, as well as to provide flexible and targeted logistics.

Previously, information weapons in terms of efficiency / cost were significantly inferior to any other weapon. The value of this parameter (efficiency / cost) in turn depended on the climatic conditions, the development of science, industrial production, the level of relevant technologies.

Currently, a classification is proposed, which has two subgroups of information weapons, the first subgroup includes: mass media; psychotropic generators; psychotropic drugs.

Information weapons of this subgroup are designed to have a negative impact on people. In particular, this influence can be exercised through various media. According to the Law of Ukraine "On Mass Media", these media mean periodicals, radio, television, video programs, newsreels, and other forms of periodic distribution of mass information.

Mass media means printed, audio, audiovisual and other messages and materials intended for an unlimited number of persons. The chronology of many military conflicts in recent years has included, as a rule, at the beginning of their development the stage of psychological treatment of the world community through the media [2, 9].

Psychotropic generators are devices that affect a person by transmitting information through unconscious perception. It has long been established that various human organs have their own resonant frequencies, using which you can influence the mental and physiological state of an

individual or group of people, causing them fear or other feelings. These and other features of the human body are used in the construction and selection of parameters (frequency range, radiation power, duration, etc.) of psychotropic generators.

Psychotropic drugs are drugs that can cause a state of dependence, have a stimulating or depressant effect on the central nervous system, causing hallucinations or impaired motor function of the body, under the influence of which there is a violation of thinking, mood swings, behavior.

The second group includes [7]:

- means of electronic warfare;
- complexes of special software and hardware influence.

Electronic warfare (EW) means systems for detecting and electronically suppressing enemy command and control systems and electronic weapons of the enemy, its reconnaissance and navigation systems, as well as systems for ensuring the stable operation of their systems.

Complexes of special software and hardware (CPT) - software, hardware or software and hardware, which can be used to make unauthorized copying, distortion, destruction of information, its transmission outside the controlled area or blocking access to it.

Currently, in addition to land, sea, air and space, the information sphere has been added to the number of areas of hostilities. According to military experts, the main objects of defeat in the new wars will be the information infrastructure and psychology of the enemy (there was even the term "human network").

The main objects of influence in the information war are [10]:

- communication networks and information and computer networks used by state organizations in performing their management functions;
- military information infrastructure, the crucial task of which is the management of troops;
- information and management structures of banks, transport and industrial enterprises;
- Mass media (primarily electronic).

There are now many definitions of information warfare. Let's focus on one of them. In August 1995, the US National Defense Institute published Martin Libiki's work "What is Information Warfare?" In it, the author identified 7 types of information warfare: command and control, intelligence, psychological, hacking, economic, electronic and cyber warfare. [11].

Command-and-control war as the main object of influence considers the channels of communication between command and executors. By cutting the "neck" (communication channels), the attacker isolates the "head" from the "body". It is said that this is better than just killing the "head". It is believed that the Internet was born as a defensive version of this war ("scattered neck").

Reconnaissance war aims to gather militarily important information and protect one's own.

Electronic warfare is affected by electronic communications networks - radio, radar, computer networks. Its important component is cryptography, which allows you to close and open electronic information.

Psychological warfare is carried out through propaganda, "brainwashing" and other methods of information processing of the population.

M. Libiki identifies 4 components of psychological warfare: undermining the civic spirit; demoralization of the armed forces; disorientation of command; war of cultures.

The purpose of the hacker war is total paralysis of networks, interruptions of communication, introduction of errors in data transmission, theft of information, theft of services due to unauthorized connections to networks, their secret monitoring, unauthorized access to closed data. To achieve these goals, various software tools are used: viruses, "Trojan horses", "logic bombs" sniffers.

Economic information war. Martin Libiki distinguishes two forms of it - information blockade (directed against the United States) and information imperialism (the method of the United States itself).

The world is changing rapidly and raises many new questions for humanity. The capital that plays a major role in the "digital revolution" is intellectual capital, especially in the field of information technology.

Finally, the main product of this sector - information - has unique properties that are not unique to other sectors of the economy. Information, unlike all other resources, is reusable and for

many users, and the more it is used, the more valuable it becomes. The same can be said about networks that connect different sources of information.

This is one of the approaches to determining the nature and content of information warfare. Among the first official documents on this issue is the US Department of Defense Directive T3600.1 of 21.12.1992 entitled "Information Warfare". In 1993, a directive of the Committee of Chiefs of Staff № 30 already set out the basic principles of information warfare. Finally, in 1997, the following definitions of information warfare were given: "Actions taken to achieve information advantage in the national interests of the country and carried out by influencing the information of enemy information systems while protecting their own information and their own information systems."

Since 1994, the United States has held official scientific conferences on "information warfare" with the participation of prominent representatives of the country's military and political leadership [12]. To this end, the Center for Information Strategy and Policy was established in the United States, the task of which is to study the possibilities of using information technology in military conflicts of the XXI century.

In all conflicts involving the United States ("Desert Storm", the operation in Haiti, Panama, against Yugoslavia and others), various types of information weapons were tested. To date, information warfare officer positions have been introduced in the U.S. Army, Navy, and Air Force. One can trace the evolution of the views of the top US leadership on the formation of the concept of "information operations". There are two periods of their origin, formation and development [11,12].

The first period (1950 - 1985) In this period there are two stages: at the first stage (1947 - 1973) the basic approaches to future information operations have arisen. The content of the second stage (1974 - 1985) was a comprehensive study of the experience of information components of hostilities during local wars and armed conflicts.

The second period consists of four stages.

The first stage 1985 - December - 1992 - the use of the latest information technology, psychological operations, electronic warfare at the strategic, operational and tactical levels.

The second stage of December 1992 - February - 1996 - is characterized by active theoretical development (with a great variety of approaches) of a single concept of information warfare on the scale of the armed forces, as well as the corresponding types of their contacts in the land forces, navy and air force.

The third stage, February 1996 - October - 1992 - completion of the development of the theoretical foundations of information warfare, preparation and conduct of information operations. These years clearly showed the limitations of the forms and methods of information warfare used, which prompted the further development of its theory, including in peacetime, as well as in the whole range of hostilities and in so-called military operations other than war.

The fourth stage, October 1998 - to date - the adoption of the view of the information struggle as a strategic means of achieving the goal of the national military strategy and the strategy of national security of the United States through information operations.

Many definitions of information warfare are associated, apparently, with the complexity and versatility of such a phenomenon as information warfare, the difficulty of drawing analogies with traditional wars.

If we try to transform the definition of war into the concept of "information warfare", it is unlikely to be constructive. This is due to a number of features of information warfare. For war in its usual sense, the subjects (different sides) are clearly defined, there are notions of the beginning and end of the war, the front line. Different sides are usually described by the same models. The outcome of the war is largely determined by the ratio of military capabilities of the parties.

For information warfare, defense is usually clearly defined, the concepts of beginning and end can be applied only to individual operations of information warfare, the front line is not defined, defense and offensive are described by different models. The success of the information operations is not directly related to the ratio of military capabilities of the parties. Ensuring information security in the field of state and municipal government (SMU) is based on a detailed analysis of the structure and content of the SMU, as well as information processes and technologies used in management. In this case, the determining factors in the development of information weapons are the individual

characteristics of the elements. It is clear. In order to model the behavior of the basic elements, it is necessary to know the individual characteristics and preferences.

The time interval at which systems try to win the information war, in this case can be compared with the lifetime of the elements (their time in the control system), which means that we are talking about insignificant in terms of generational changes in the time interval. Therefore, for a specific situation for a while it becomes permissible to talk about the victory of a particular algorithm. However, it should be remembered that the lifetime of the system and the training time are constantly changing. New learning technologies appear and the characteristics of the information environment change. This means that comparing the lifetime of the elements with the time interval of active information warfare is not entirely correct. Here it is necessary, first of all, to note the following: the intensity of modification of the surrounding world often does not leave the information system the opportunity to get out of the proposed scenarios of behavior [11]. It should also be noted that in modern models and methods of protection of man and social group from influences are used, as a rule, only the personal characteristics of a particular person, which distinguish him from others. Moreover, it is promising to create such a set of information and psychological characteristics of man, which would be characteristic of a broad and correct definition of the circle of persons. Moreover, it is desirable that such characteristics be objective in nature, that is, describe the real nature of man, rather than his subjective representation.

Based on what is stated about the simulated basic elements, we can formulate a statement: the greater the power of the set of basic elements and their relationships, the more resistant the system to targeted information.

In conditions when the time of information counteraction between the systems is small (for example, does not exceed the average lifetime of the system element) and the enemy system has simulated basic elements, we can offer the following algorithm, which should "always win":

- definition of basic elements of the information space of the enemy system;
- study of individual features and potential capabilities of basic elements;
- modeling of different variants of behavior of basic elements at different input influences;
- selection of the best scenario of basic elements;
- preparation of the environment in which the basic elements (public opinion) function, and themselves;
- implementation.

Given the above, the general scheme of information warfare can look like in Fig.1.

The given scheme, certainly, does not reflect all possible approaches and receptions to the organization and carrying out of operations on information influence. The human mind is more refined than any possible projection of the thoughts generated by it into the plane of practical algorithms.

The typical strategy includes only what is obtained from previously proven theorems, statements and consequences. From here we have: if the information system has influence against itself a complex of receptions of the scheme of fig. 1, it may mean that this information system is in a state of information warfare.

Many methods and techniques have changed, they have received a scientific basis. There are whole scientific disciplines on how to manage human behavior, team, society. These include: sociology, psychoanalysis, advertising theory, suggestology, NLP programming, dianetics, etc.

Hypnosis has been substantiated, attempts have been made to transfer the methods of hypnotic influence from the individual to groups and to entire human societies. Production and dissemination of information is put on the assembly line. All this was not even in the last century - there were not enough effective media, there were no scientifically sound algorithms for managing society, and these algorithms could arise only with the advent of programming theory for today's computer technology. Because to carry out an information operation means to select the input data for the system in order to activate certain algorithms in it, and in their absence to activate the algorithms for generating the necessary algorithms. The current theory of algorithms allows us to explain how automatic writing of programs can be carried out for certain subject areas, which is very important for the management of the individual, group and society as a whole.

In the conditions of information war a special place is occupied by information and psychological influence. It is a type of psychological influence, which is defined as a way to influence

people (individuals and groups), carried out to change ideological and psychological structures, their consciousness and subconscious, emotional transformation, stimulation of certain types of behavior using different ways of explicit and implicit psychological coercion.

Currently, which is characterized by intensive use of various methods of information, psychological pressure, which is especially associated with the development of modern technologies that can affect the consciousness, the psyche of many people simultaneously without influence and direct contact with them. The problem of psychological influence on people's consciousness becomes relevant, especially in the conditions of information warfare in various spheres of society.

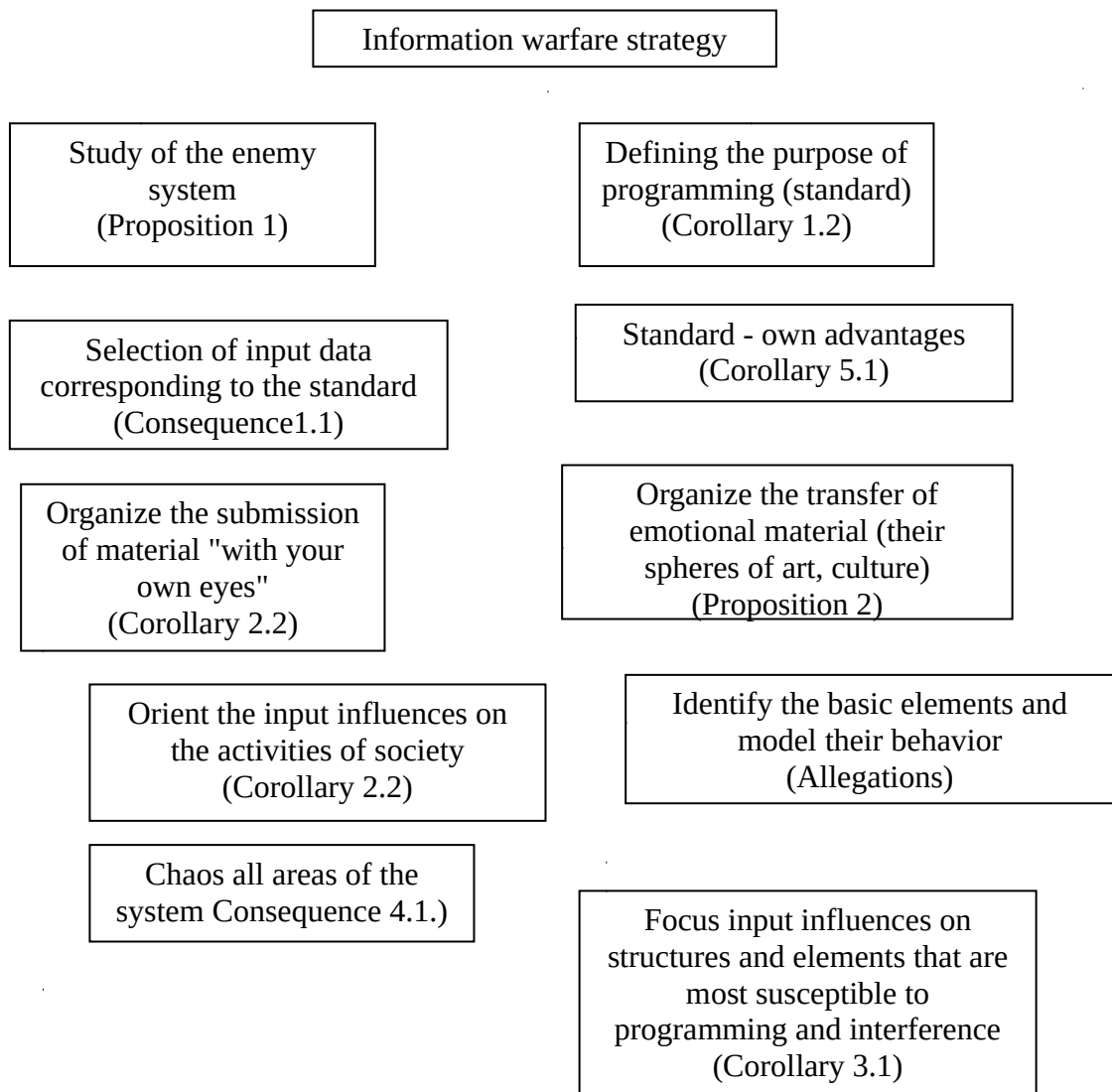


Fig. 1. A typical information warfare strategy

Of particular concern is the impact of information and psychological action of the media on young people, which is expressed in violence, unmotivated aggression, hostility, cynicism, legal negativity, rejection of traditional social values, etc. Information and psychological influence affects the following areas of the psyche of an individual, social group of people and society as a whole [10, 11, 12]: consumer-motivational sphere (values, desires, desires, beliefs, knowledge); intellectual and cognitive sphere (feeling, imagination, thinking and memory); emotional and volitional sphere (moods, emotions, feelings, will); communicative-behavioral sphere (nature and specifics of interpersonal perception and interaction).

Thus, only taking into account the features inherent in these areas of functioning of individual, group and social consciousness, information and psychological influence gives the most real effect.

It should be noted that any influence that aims to change the behavior of the object in the right direction for the subject, even if this influence is carried out for the benefit of the object, but without his consent, is considered a manipulative effect.

Regarding the consequences of information and psychological impact on objects, there are two types of information and psychological impact: positive and negative. In information warfare or confrontation, negative informational and psychological influence is of paramount importance. Experts distinguish a significant number of types of negative impact: [8,10] falsification (fraud) and misinformation; zombification or targeted programming to perform certain actions, including negative ones; introduction to a hypnotic state; harm to life and health; astro-terfing, which is defined as a deliberate centralized manipulation of public opinion on the Internet for the purpose of misinformation, distortion of statistical information, their use by public opinion; trolling - posting informational messages in order to persuade users to discuss a certain direction or create a conflict situation, etc.

Among the facts that determine the tendency to negative information and psychological influence are psychological factors, which include situational and non-situational [11,12].

Situational factors are due to a specific information and communication situation (psychological state, various stressors, extreme conditions, etc.). Non-situational factors include a person who is exposed to negative information and psychological influence, which affects his propensity to psychological manipulation, etc.

The information environment, acquiring the character of the second, subjective reality, in the part that contains information that adequately reflects the world around us, and its characteristics and processes that complicate or hinder the adequacy of perception and understanding of the world and himself, despite his illusory, becomes a significant external source of threats to information and psychological security of the individual.

The process of bringing a hypnotic state to a particular society in the context of information warfare can, for example, look like this [11]:

1) to relax society - to instill through the media that there are no enemies, while discussing individual historical periods and the interests of individual peoples (the body as a whole must disappear as an object of consciousness);

2) to force society to listen only to the enemy, not paying attention to any other thoughts or feelings, for example, to focus the media exclusively on any one paradigm of social development (eg, Western), excluding any other experience: China, Japan, the Muslim world (goal - the process of loading the public consciousness and the action of the forming forces are weakened);

3) to force the society not to think about what the opponent is saying, for this purpose to exclude from the mass media serious analytical studies of problems (the goal is to help slow down the continuous flow of opinions);

4) to focus society's attention on something other than the incoming information flow, such as internal cataclysms, wars, acts of terror (the goal - the protection subsystem responsible for processing incoming information, is unable to perform its function and as if disconnected);

5) constantly inspire that society itself and everything around it is getting better and better (the goal - such a suggestion weakens the historical memory and sense of self-identification, which characterizes the normal state of society);

6) the media at the same time must convince members of society that caused the state - this is not exactly what it should be (the goal - to create a passive state of consciousness, which retains the possibility of dependence on the informational influence of the enemy).

Today, the number of channels of information influence on people and society is growing. And mostly the number of those channels and factors that affect not only the rational but also the emotional perception of reality by man.

Thus, people and social groups are under increasing informational and psychological influence.

The above algorithm generally reflects the work of the media in Russia from 1990 to 1997. In addition, it should be noted that this algorithm is used in the Ukraine-Russia confrontation.

Management of human behavior is one of the primary tasks of the state. It must be understood that the state is created by its citizens in order to reconcile their own interests, but state or political power finds its own interests and its primary task is to manage those who have chosen and maintained the goal of trivial self-preservation.

If citizens begin to express dissatisfaction with the current policy pursued in the narrow corporate interests of the ruling elite and its proxies, then to avoid violence against the people, this can be countered only through the use of tools used by the media.

Noam Chomsky, a professor at the University of Massachusetts Institute of Technology, identified 10 ways to control the masses in his book, *Silent Weapons for a Peaceful War*.

Method № 1. Distraction.

The main element of public administration is to distract people from important problems and decisions made by political and economic circles of the country, by constantly saturating the information space with insignificant messages. The method of distraction is very important in order not to give the citizens of the country the opportunity to receive important data and knowledge in the field of modern philosophical currents, advanced science, economics, psychology, neurobiology and cybernetics. Instead, the information space is filled with sports news, show business, mysticism, and other informational components based on relict human instincts from eroticism to brutal pornography or from household soap operas to dubious ways to make easy and quick money.

Method № 2. Create problems and then suggest ways to solve them.

This method is also called "problem-response-solution". A problem is created, a kind of "situation" designed to provoke a certain reaction among the population so that it itself would demand the necessary measures to be taken by the ruling circles. That is, to cause some kind of economic, man-made and terrorist crisis in order to force people in their minds to take measures to eliminate its consequences, even in violation of their social rights, as a "necessary evil." But it is necessary to understand that crises are not born by themselves.

Method № 3. Method of gradual application.

To achieve any unpopular event, it is enough to implement it gradually, day after day, month after month, year after year. This is how fundamentally new socio-economic conditions (neoliberalism) are globally imposed. Minimization of state functions, privatization, uncertainty, instability, mass unemployment, wages that no longer provide a decent standard of living. If all this happened at the same time, it would probably lead to a revolution.

Method № 4. Delay execution.

Another way to push through an unpopular solution is to present it as "painful and necessary" and to obtain at the moment the consent of citizens to implement it in the future. It is much easier to accept any sacrifices in the future than at present.

First, because it will not happen immediately. Secondly, because the people in their mass are always inclined to cultivate naive hopes that "tomorrow everything will change for the better", that the sacrifices demanded of them will be avoided. This gives citizens more time to get used to the idea of change and humbly accept it when the time comes.

Method № 5. Address the people as small children.

Most propaganda speeches intended for the general public use arguments, characters, words and intonations, as if they were school-age children with developmental delays or mentally handicapped individuals. With this link, someone is trying to mislead the listeners, that is, to a greater extent he is trying to use infantile language expressions. If a propagandist addresses a person as if he or she were 12 or younger, then due to the suggestion, response, or reaction of that person, there is also a certain degree of probability that there will be no critical appraisal, which is typical for children 12 years or younger. Pre-naive reasoning and capitalized truths embedded in political speeches designed to be perceived by a wide audience, which are already used in the described methods of manipulating consciousness.

Method № 6. Works that focus on emotions to a much greater extent than on reflection.

Influence on emotions is a classic technique of neurolinguistic programming, aimed at blocking the ability of people to rational analysis, and ultimately to the ability to critically comprehend what is happening. On the other hand, the use of the emotional factor allows you to open the door to the subconscious state in order to root there thoughts, desires, fears, fears, coercion or stable patterns

of behavior. Spells are not as brutal a terrorism as an unjust government, as the hungry and humiliated suffer, who bring to the fore, while ignoring the true causes of what is happening. Emotions are the enemy of logic.

Method № 7. Keep people in ignorance by cultivating mediocrity.

To make people unable to understand the techniques and methods used to control and subordinate them to their will. The amount of education provided to the lower social classes should be as meager and mediocre as possible so that the ignorance that separates the lower social classes from the higher ones remains at a level that the lower classes cannot overcome. This includes the promotion of so-called "modern art", which is the arrogance of mediocrity, claiming popularity, which is unable to reflect reality through those works of art that do not require detailed explanation and agitation for their "genius". Those who do not recognize innovation - are declared backward and stupid and their opinion is not widely publicized.

Method №8. Encourage citizens to admire mediocrity.

Introduce into the population the idea that it is fashionable to be stupid, vulgar, and rude.

This method intersects with the №7 method, because everything mediocre in the modern world appears in large numbers in all social spheres - from religion and science to art and politics. Scandals, yellow pages, witchcraft and magic, dubious humor and populist actions - all good to achieve one goal - to prevent people from being able to expand their consciousness to the vast expanses of the real world.

Method № 9. Strengthen guilt.

To make a person believe that he alone is to blame for his own misfortunes, which occur beyond his mental capabilities, abilities or efforts. As a result, instead of rebelling against the economic system, man begins to engage in self-destruction, blaming himself for everything that causes depression, which leads, among other things, to inaction. And without action there can be no talk of any revolution! Both politicians and scientists (especially psychotherapists) and religious figures use fairly effective doctrines to achieve the effect of self-flagellation of patients and "flocks" to manage their life-affirming interests, directing their actions in the right direction.

Method № 10. Find out more about people than they know about themselves.

Over the past 50 years, advances in the development of science have led to the formation of a growing gap between the knowledge of ordinary people and the information possessed and used by the ruling classes.

Thanks to biology, neurobiology and applied psychology, the "system" has received advanced knowledge about man, both in physiology and psychology. The system has managed to learn more about the average person than it knows about itself. This means that in most cases, the system has more power and controls people more than they control themselves and their actions and deeds.

It should be noted that currently there is a strong negative information and psychological influence from Russia. At the same time, the terms "Russian-speaking population", "Russian world" and others are actively used by Russia in order to exert a negative information and psychological impact on people and social groups of Ukraine. These terms are not clearly defined - they are used solely as metaphors or analogues. The purpose of such use is to make a person or social group feel their "unity" with others. Psychologically, it is possible to reject the individual and come into conflict with himself, which dramatically reduces the threshold of suggestiveness and practical perception of information about the surrounding events [13]. It should be noted that the hybrid war was invented by Eugene Messner - a White Guard colonel who was chief of staff of the Kornilov division. He developed the theory of the rebellion of the war in 1967 in Argentina published a book "Theory of the Third World". However, elements of the "hybrid war" were already used during the First World War.

Realizing that fighting on two fronts was extremely exhausting and dangerous, Germany in 1914 turned its back on subversive activities in France, Britain and Russia, funding the so-called fifth column, ie various organizations, political forces and newspapers, campaigning for the defeat of its governments in war. That is, the "hybrid war" that the Kremlin is waging against Ukraine today is far from new. Its elements were used by the German General Staff in the fight against Russia and its allies 100 years ago.

By the way, the German and Austro-Hungarian governments provided material assistance in organizing Ukrainian political emigrants - the Union for the Liberation of Ukraine, whose members

conducted propaganda and agitation in the camps among fellow prisoners of war and tried unsuccessfully to organize resistance to the tsarist army in Galicia. This fact led to the spread of the myth that Germany allegedly financed the Ukrainian People's Republic - to split Russia. The General Staff of the Soviet Union began to develop and implement this concept in the early 1980s. Russia has adopted this concept and is now using it.

This concept is to create three levels of the network [13]. First, the territory of the enemy is covered with a very dense network of Russian broadcasting, the necessary history is introduced (it does not matter whether it is true or false). Then cultural societies and circles are created that support politics and ties with Russia. Organizational moments are superimposed on the cultural basis, ie pro-Russian parties are created.

Building a level 2 matrix are people who sympathize with Russia without recruiting. There are those who studied in Russia. The apologists of the Russian world, those who have come to this themselves and say: "They have a layer of culture more interesting than ours" - they become information nodes. Without realizing it, such a person is already conducting information intelligence. Moreover, all this is open, everything is legal [13].

Then, the so-called combat platform is inserted into this territory - from one person to a division. You are told to create a fighting cell of people who will be ready to side with Russia in case of force majeure. At the same time, they ask to create a combat group that will protect against the fascist coup or Bandera. This is what happened in Ukraine in Donbass. Donbass "feeds all Ukraine and Ukraine lives at its expense".

Any system responsible for processing the input data must be "fed", ie must consume energy in order to activate the algorithms embedded in the processing of input data and generate new ones. The basic elements of each system have a certain physical nature, which largely determines the reaction time, and hence the choice of a particular algorithm for solving a particular problem [8, 11, 14].

When considered as information self-learning systems of the states under "other kinds of influence" in the light of the above it is necessary to understand first of all economic war. But in a narrow sense, related exclusively to economic sanctions such as "it is impossible and it is impossible", and in a broader sense, which includes "economic interventions" in the form of goods and products at dumped prices.

The time of information and economic wars has come also because today's world is no longer characterized by a shortage of information and industrial goods, on the contrary, it is distinguished by their excess. This means that as in the case of information warfare, when the system must think more not about the protection of information, but about protection from information and the promotion of its vision of the world, and in economic warfare should be about protection from other people's goods and news. their own.

Competent combination of all permissible types of influence on the enemy is a comprehensive strategy of influence.

Permissible types of influence here are those actions that "grossly" do not violate the currently accepted norms and rules of conduct in society.

Adherence to the principle of complexity in the formation of a common security strategy to influence the enemy can enhance the effect of the use of information weapons and thus may be another sign of information warfare.

In recent years, the information war has increasingly turned into a geopolitical information confrontation. This is well illustrated by the example of Russia, which is conducting active advocacy activities in the global information space.

Not only ordinary people in Russia and the world are exposed to these propaganda influences, but also many of those who define, create and influence public opinion. Moreover, Russia has in its arsenal many different developments aimed at propaganda and manipulation of public opinion and consciousness.

It should be borne in mind that the purpose of geopolitical information confrontation is to violate the information security of the enemy state, in certain cases - the integrity (stability) of public and military government, effective informational influence on their leadership, political, public

opinion and decision-making, and also providing information security for gaining (providing) information superiority in the world information space

There are two types of information confrontation (struggle): information-technical and information-psychological [15].

In information and technical confrontation, the main objects of influence and protection are information and technical systems (communication systems, telecommunications systems, data transmission systems, electronic means, information protection systems, etc.).

In information and psychological confrontation, the main object of influence and protection are the psyche of the political elite and the population of the opposing parties, the system of formation of public opinion and consciousness, decision-making.

The confrontation includes the following stages:

- forecasting and planning;
- organization and incentives;
- feedback;
- regulation;
- performance control,

as well as the stages of testing decisions during the information confrontation:

1) assessment of the situation:

- determining the composition of indicators and criteria;
- assessment of the reliability of data receipt;
- analysis of the state of the control object;
- analysis of the state of the subject of management;
- analysis of deviations.

2) goal setting;

3) definition of the plan and decision;

4) the formation of solutions (there must be at least three).

Information confrontation (especially in the political sphere) has three components:

- strategic political analysis;
- informational influence;
- information counteraction.

Strategic political analysis is a set of measures to obtain information about the enemy in the conditions of information confrontation; gathering information about their political allies; processing information and exchanging it between members of their political clan in order to organize and conduct information confrontation. The information must be reliable, accurate and complete, and the information must be selective and timely. It is logical to call the solution of the listed tasks information maintenance of management of material and financial resources.

Information impact includes measures to block, retrieve, process and exchange information, and introduce misinformation.

Information counteraction (protection) includes the action of blocking the information needed to solve problems of political process management, and blocking misinformation disseminated and introduced into the system of formation of world public opinion by political competitors (opponents).

Levels of information confrontation are divided into: strategic, operational and tactical.

Basically, at the strategic level of information geopolitical counteraction, the highest state authorities of the country should act, and special services and large capital - at the operational and tactical levels.

The world's leading countries (primarily the United States, Russia, China, Britain, France, Germany, Israel) currently have a powerful information potential that can ensure them achieve political goals, especially since international legal norms of information warfare as such are absent.

Conclusions

At all stages of the historical development of human civilization, information has been both the most important object and the means of confrontation between peoples, nations, states, military-political blocs and alliances. Some facts of information and psychological influence on a wide

audience can be found throughout the history of society. It is clear that in different periods the intensity of the application of certain methods and methods of influence, as well as the perfection of their organization, differed greatly.

At the present stage, science has such theoretical constructions, on the basis of which the technology of information confrontation, ie the relevant governmental and non-governmental structures involved in such activities, develop and test new information technologies, techniques, methods of implementation, information and psychological impact, technical means necessary for such activities. Such changes could not but affect the growth of the effectiveness of information technology, which can lead to radical changes in society, economic, political and other areas of a country, or globally.

The uncontrolled spread of the use of information space, along with the significant benefits of their use, has led to the emergence of fundamentally new, related problems. The main one was the sharp intensification of international competition for ownership of information markets. At the same time, in order to ensure information confrontations and conduct certain operations during local hostilities and armed conflicts - the so-called information confrontation, the countries of the world began to actively use the information space (Internet), a vivid example of this was the events in Iraq, Yugoslavia, Libya, Chechnya, Georgia, Ukraine, etc. This state of affairs, as a consequence, in turn led to the strengthening of integration processes in the infosphere, gave rise to information confrontation, ie information wars.

In today's world, interstate conflicts are fraught with excessive losses for each of the warring parties. Therefore, the technique used is only half-truths, half-cooperation, mutual competition in development, in the pursuit of moral leadership. Activities in information confrontation and information-psychological influence give opportunities for the use of this approach.

It is proved that information war is an element of information confrontation, a political conflict in which political struggle in the form of information-psychological operations with the use of information weapons.

BIBLIOGRAPHY

1. Litvinenko O.V. Information influences and operations. Theoretical and analytical essays / Litvinenko O. V. – Kyiv: National Institute for Strategic Studies, 2003.-240 p.
2. Pirtskhalava L.G. Information confrontation in modern conditions / Pirtskhalava L.G., Khoroshko V.A., Khokhlacheva Y.E., Shelest M.E. - Kyiv: CP "Kompint", 2019.-226 p.
3. Rastorguev S.P. Philosophy of information war / Rastorguev S.P. - Moscow: Moscow Psychological and Social University, 2003. – 496 p.
4. Litvinenko O.V. Special information operations and propaganda companies / Litvinenko O.V. - Kyiv: Satsanga, 2000. - 242 p.
5. Grishchuk R.V. Cyber weapons: classification, basic principles of construction, methods and means of application and protection against it / Grishchuk R.V., Khoroshko V.O. // Modern special equipment, No. 4. 2016. - pp. 30-37.
6. World hybrid war: the Ukrainian front / Edited by V.P. Gorbulina – Kyiv: National Institute for Strategic Studies, 2007.- 496 p.
7. Eremenko V.T. Actual problems of information confrontation in sociotechnical systems / Eremenko V.T., Pershukov V.M., Pikalov B.V., Tretyakov O.V. - Orel: Publishing House "Gosuniversitet" - Prioksky State University, 2015. – 291 p.
8. Prokofiev M.I. The concept of application of information influences and counteraction of information weapons / Prokofiev M.I., Khoroshko V.O., Khokhlacheva Y.E. // Legal, regulatory and logistical support of information security systems in Ukraine, Vol. 1 (31), 2016. – pp. 9-14.
9. Khoroshko V.O. Information war. Mass media as a tool of informational influence on society. Part 1. / Khoroshko V.O., Khokhlacheva Y.E. // Information Security, Volume 22, №3, 2016. - pp. 283-289.
10. Dereko V.N. - Theoretical and methodological principles of classification of threats to the object of information security / Dereko V.N. // Information security of man, society, state, No. 2918), 2015. – pp. 16-23.

11. Khoroshko V.A. Information and analytical security / Khoroshko V.A., Shelest M.E. - Kyiv: Private printing establishment "Zadruha", 2016. - 183 p.
12. Ostapenko G.A. Information operations and attacks of socio-technical systems / Ostapenko G.A. - Moscow: Hotline - Telecom, 2007. -134 p.
13. Messer E.E. If you want peace, win the interwar / Messer E.E. - Moscow: Published by "Russkii Put' " 2005. – 485 p.
14. Artemov V., Khoroshko V., Ivanchenko I., Brailovskyi N. Geopolitics and Information Warfare // SPCSJ, vol. 4, No.1, 2020.- pp. 61-64
15. Prokofiev M.I. Problems of information protection in Ukraine / Prokofiev M.I., Khoroshko V.O. // Legal, regulatory and logistical support of information protection systems in Ukraine, Vol. 2 (30), 2015. - pp. 9-14

О НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ И ТЕХНОЛОГИЯХ ON THE NEED TO ENSURE CYBERSECURITY IN EDUCATIONAL INFORMATION SYSTEMS AND TECHNOLOGIES

д.т.н., профессор Хлапонин Юрий Иванович, Киевский национальный университет строительства и архитектуры,
г. Киев, Украина

Doctor of Technical Sciences, Professor Yuri Khlaponin, Kiev National University of Civil Engineering and
Architecture, Kiev, Ukraine

к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев
Крут, г. Киев, Украина

Ph.D., Lesya Kozbtsova, Military institute of telecommunications and informatization named after Heroes of Krut,
Kiev, Ukraine

д.п.н., профессор РАЕ Козубцов Игорь Николаевич, Научный центр связи и информатизации Военного института
телекоммуникаций и информатизации, г. Киев, Украина

Doctor of Pedagogical Sciences, Professor of RAE, Igor Kozubtsov, Scientific center of communication and
Informatization of the Military Institute of telecommunications and Informatization, Kiev, Ukraine

АННОТАЦИЯ. Актуальность темы исследований о необходимости обеспечения кибербезопасности информационных систем и технологий в образовании обусловлена постоянно возрастающей уязвимостью, а также скрытым риском потери активов учебных заведений.

Основных аспекты работы. В статье поднимается вопрос о необходимости рассмотрения обеспечения кибербезопасности информационных систем и технологий в образовании. Установлено, что в данное время исследователями не приделано надлежащего внимания вопросу обеспечения кибербезопасности в проектируемых информационных системах и технологиях в сфере образования.

Научная новизна. Научная новизна темы заключается в постановке задания о необходимости решение научно-практической задачи обеспечения кибербезопасности информационных систем и технологий в образовании.

КЛЮЧЕВЫЕ СЛОВА: кибербезопасность, образование, информационная система, технология, деструктивное информационное влияние, киберзащитенность, методика.

ABSTRACT. The relevance of the research topic on the need to ensure the cybersecurity of information systems and technologies in education is due to the constantly increasing vulnerability, as well as the hidden risk of losing assets of educational institutions.

The main aspects of the work. The article raises the question of the need to consider the provision of cybersecurity of information systems and technologies in education. It is established that at this time, researchers have not paid proper attention to the issue of ensuring cybersecurity in the projected information systems and technologies in the field of education.

Scientific novelty. The scientific novelty of the topic lies in the formulation of a task about the need to solve the scientific and practical problem of ensuring the cybersecurity of information systems and technologies in education.

KEYWORDS: cybersecurity, education, information system, technology, destructive information influence, cyber security, methodology.

ВВЕДЕНИЕ. В настоящее время наблюдается высокий интерес исследований, который отображен в диссертационных работах ученых по направлению разработки моделей и информационных технологий обеспечения гармонизации высшего образования. Анализируя одну из таких работ, например, [1] на удивление нами не было выявлен актуального аспекта, а именно, каким образом обеспечивается кибербезопасность указанной информационной системы. В связи с этим возникают два очевидных вопроса:

- 1) почему проектанты информационных системы пренебрегают кибербезопасностью?
- 2) осознают ли проектанты информационных системы катастрофической опасности в результате нарушения кибербезопасности?

Поэтому, учитывая выше изложенного, по нашему мнению, возникла необходимость в данной работе рассмотреть отдельные аспекты, которые связаны с необходимостью обеспечения кибербезопасности в

информационных системах и технологиях, что предлагаются в образовании.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Автор работы [2] приводит перечень проблем, возникающих при использовании информационных технологий в образовательном контексте. Также он даёт характеристику потенциальным угрозам кибербезопасности: несанкционированный доступ к данным, фильтрация нежелательной информации, кибертерроризм. Но к сожалению, не рассматривается такой важный и актуальный аспект, как кибербезопасность информационной технологий в образовании. Но в отличие от этой работы в статье [3] затрагивается проблема обеспечения кибербезопасности систем дистанционного обучения образовательных учреждений. Результатом работы стало известно об наличии основных факторов риска безопасности, а также виды и источники угроз систем дистанционного обучения образовательных учреждений. Полученные новые знания подводят на мысль о необходимости обеспечения кибербезопасности в образовательных информационных системах и технологиях, объектом исследования которая выступают в данном исследовании.

ЦЕЛЬ СТАТЬИ

Рассмотрение вопроса о необходимости обеспечения кибербезопасности в существующих и проектируемых информационных системах и технологиях в образовании.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Для понимания вопроса о необходимости решения проблемы обеспечения кибербезопасности информационных систем и технологий в образовании, обусловлено рассмотрение сущности с методологической точки зрения толкование дефиниции “информационных систем” и “информационной технологии”. Затем изучить источники возможных киберугроз, а также возможные уязвимости информационных систем и технологий в образовании.

Поскольку дефиницию “информационных систем” мы подробно рассматривали в публикации [4], где сделаны соответствующие выводы, поэтому с точки зрения понимания уязвимости к киберугрозам будут интересны следующие два определения:

согласно ДСТУ 2392-94 [5] «информационная система» – это коммуникационная система, обеспечивает сбор, поиск, обработку и пересылку информации;

ISO/IEC 2382:2015 [6] «информационная система» – система, предназначенная для сбора, хранения, обработки, передачи и использования информации”.

Исходя из этих определений резюмируя понятия «информационная система» – это совокупность технических, вычислительных средств, которые обеспечивают сбор, поиск, обработку и пересылку информации. Как показывает современная практика они в большей степени подвержены киберугрозам.

Целесообразная необходимость обеспечения киберзащищенности информационных систем и технологий основывается на следующих постулатах:

1. Не существует абсолютной киберзащищенности систем управления.
2. Чем более сложная система, чем больше задач она выполняет, тем ниже ее киберзащищенность.
3. Необходимым условием повышения киберзащищенности системы является введение избыточности в сочетании с организацией эффективного контроля.
4. Киберзащищенность системы управления должна обеспечиваться на всех этапах жизненного цикла.
5. Уровень киберзащищенности системы ограничен экономическими рисками заказчика и эксплуатирующей организации.

Таким образом, абсолютной киберзащищенности невозможно достичь, поскольку устранение одних уязвимостей в системе не исключает возможности появления новых, что свидетельствует современная практика.

Целью применения деструктивных информационных влияний (кибератаки) на информационную систему является нарушение одного или комплекса перечислений, а именно: конфиденциальности и целостности информации, доступности информационной системы или содержащихся в ней данных (рис. 1).

С учетом этого, категорию кибербезопасности информации, которая циркулирует в информационной системе образования $K_{KB}(S)$, можно представить следующим выражением (1):

$$K_{KB}(S) = \left[\begin{matrix} K \\ Ц \\ Д \end{matrix} \right] \quad (1)$$

где K – конфиденциальность;

$Ц$ – целостность;

$Д$ – доступность.

Учитывая выражение (1) кибербезопасность системы $K_{KB}(S)$ можно представить через потерю конфиденциальности, целостности или доступности данных [7, с. 36] (2):

$$K_{KB}(S) = 1 - (1 - P_K)(1 - P_{Ц})(1 - P_{Д}) \quad (2)$$

где $P_K, P_{Ц}, P_{Д}$ – соответствующие вероятности нарушения конфиденциальности, целостности и доступности

информации в информационной системе образования.

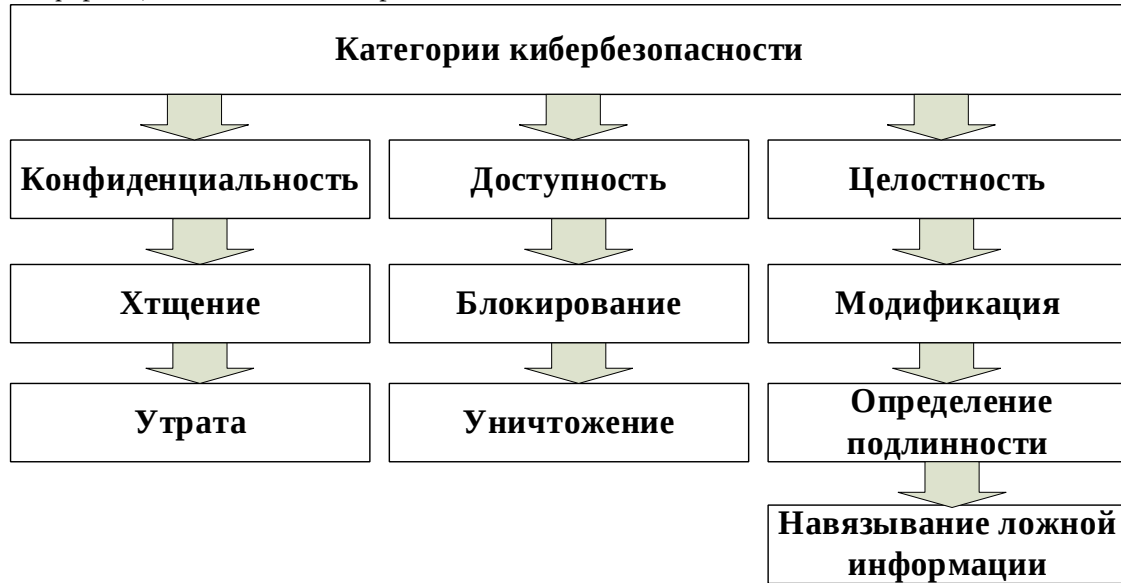


Рис. 1 Категории кибербезопасности

Нарушения кибербезопасности, то есть потери конфиденциальности, целостности или доступности, подробно рассматривается в работе [8, с. 110 – 112] через механизм способов их реализации. Поэтому нет смысла повторного рассмотрения.

Перейдем к рассмотрению дефиниции “информационной технологии”. Информационная технология – это совокупность методов, производственных процессов, программно-технических и лингвистических средств, интегрируемых с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей. [9, с. 61]. Более в упрощённом случая информационная технология – это совокупность методов, средств, приемов, обеспечивают поиск, сбор, хранение, обработки, представления, передачи информации между людьми. Как видим, в основу информационной системы закладывается информационная технология. Другими словами, функционирование информационной системы, которая обеспечивает сбор, поиск, обработку и пересылку информации осуществляется по разработанной информационной технологии, которая и определяет какие именно применять методы, средства, приемы, обеспечивают поиск, сбор, хранение, обработки, представления, передачи информации. Исходя из этого и свидетельства современной практики информационные системы уязвимы к деструктивным информационным воздействиям (кибервлияниям).

Рассмотрим режимы работы информационных систем: автономный (закрытый); общедоступный (открытый). Исходя из режимов работы информационных систем вытекают возможны варианты кибервлияний (табл. 1).

Таблица 1 – Возможные варианты кибервлияния с учетом режимов работы информационных систем

№ п/п	Источники кибервлияния	режимы работы системы	
		автономный	открытый (общедоступный)
1	внутренние	+	+
2	внешние	–	+

Если мы рассматриваем закрытую от внешнего мира информационную систему, то источником нарушения кибербезопасности, как правило, является только человек-инсайдер этой системы, поскольку влияний с внешней не будет.

В открытом режиме использования информационная система в образовании к существующим внутренним источникам кибервлияниям могут присоединяться и внешние. Источником внешних кибервоздействий на образовательную систему может стать кто-либо угодно имеющий достаточный опыт в применении средств кибервлияний и соответствующую мотивацию.

Рассмотрим классификацию нарушений кибербезопасности связанной с человеческим фактором, которую представлено в табл. 2.

При комбинированном случае источниками являются нарушители выше рассмотренных случаев.

Учитывая данные критерии (конфиденциальность, цельность и доступность) необходимо осуществить декомпозицию информационной системе образования S, то есть разложить ее на составляющие – средства и компоненты, которые уязвимы к воздействию деструктивным информационным воздействиям.

После этого, необходимо осуществить мониторинг киберзащищенности компонентов информационной системе образования на предмет их уязвимости. Для этого достаточно воспользоваться ранее предложенным методом мониторинга киберзащищенности информационной системы, предложенный в работе [10].

Таблица 2 – Классификация нарушений кибербезопасности связанной с человеческим фактором

№ п/п	Человеческий фактор	Уровень пользователей системы	
		Пользователь (обучаемый)	Администратор (обучающий)
1	недовольные сотрудники	+	+
2	шпионаж	+	+
3	халатность	+	+
4	низкая квалификация	+	+
5	шантаж	+	+

По его итоге киберзащищенности информационной системы необходимо оценить уровень защищенности и за необходимости осуществить соответствующую корректировку киберзащищенности.

Технические сбой мы опускаем с рассмотрение, поскольку он больше связан с технической надежностью технических средств, реализовывает информационную систему. Практика показывает, что уже через 5 лет эксплуатации компьютеров, в следствие морального старения, целесообразно заменять их на новые, хотя физическое старения или износ их далекие от предельного состояния. Это связано с тем, что кривая морального старения объекта пересекает и превышает предельно допустимый уровень показателя цена/качество и, следовательно, дальнейшая его эксплуатация нерентабельна [11].

О грядущей проблеме кибербезопасности в образовательных информационных системах и технологиях всеобщая идеология максимального внедрения дистанционных форм обучения. В данном случай используется только общедоступный режимы работы информационной системы дистанционного обучения транспортной системой которой выступает Интернет. Прошло то время, когда обучение происходило посредством выполнения домашних контрольных заданий с последующей их отправкой по почте.

Рассмотрим наиболее уязвимые сточки зрения кибербезопасности части информационной технологии. Для этого представим процесс, который протекает в информационной технологии в виде этапов следующего алгоритма:

- этап 1 поиск информации;
- этап 2 сбор информации;
- этап 3 хранение информации;
- этап 4 обработка информации;
- этап 5 представление информации;
- этап 6 передачи информации.

Каждый этап процесса информационной технологии важен для правильности функциональной работы проектируемой информационной системы. Если нарушить доступность к информационной системе образования, то очевидно, что и нарушатся (приостановятся) протекающие в ней процессы информационной технологии.

ВЫВОДЫ

Таким образом, строить полноценную комплексную систему защиты информации (КСЗИ) в проектируемых информационных системах образования возможно не стоит, но необходимо соблюдать (обеспечивать) превентивную кибербезопасность (кибергигиену) не только когда она соприкасается с внешним киберпространством, но, когда находится в автономном режиме.

Для понимания взаимосвязей очень удобно пользоваться моделью основных понятий безопасности и характер связей между ними разработанный в DUS ISO/IEC 27032: 2012 [12]. Эта модель позволяет наглядно представить для понимания взаимосвязи между кибербезопасностью и источниками угроз для дальнейшего моделирования мероприятий по предотвращению киберугроз.

Необходимо рекомендовать исследователям в предлагаемых ими информационных системах и технологиях описывать меры обеспечения кибербезопасности.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Разработка методики планирования кибербезопасности информационных системах и технологиях в образовании.

СПИСОК ЛІТЕРАТУРЫ

1. Цюцюра М.І. Інформаційні технології гармонізації зрівноваженого освітнього простору: автореф. дис. ... д-ра техн. наук: 05.13.06; Київ. нац. ун-т буд-ва і архітектури. Київ, 2020. 44, с.
2. Зубалова О.А. Проблемы информационной безопасности образовательной среды в современных условиях // Мир науки, культуры, образования. 2018. № 3 (70). С. 36 – 38. ISSN 1991-5497.
3. Оладько В.С. Риски кибербезопасности систем дистанционного обучения // Международный научно-исследовательский журнал. 2019. № 10 (88). С. 31 – 34.
4. Козубцова Л.М., Кіт Г.В., Ліщина В.О., Козубцов І.М. Аналіз змісту поняття інформаційна системи спеціального призначення // Materials of the XVI International scientific and practical Conference Cutting-edge science – 2020, April 30 – May 7, 2020 Construction and architecture. Mathematics. Modern information technology. Technical science: Sheffield. Science and education LTD, 2020. Volume 8. Pp. 56 – 58.
5. ДСТУ 2392-94 “Інформація та документація. Базові поняття”. К.: УкрНДІССТ, 1994. 25 с.
6. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ).
7. Тутубалин П.И., Моисеев В.С. Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления: монография. Казань: РИЦ «Школа», 2008. 144 с. (Серия «Современная прикладная математика и информатика»).
8. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. СПб.: Научное издание «Наукоёмкие технологии», 2017. 120 с.
9. Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. – М.: Институт развития информационного общества, 2009. 160 с.
10. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2020. Випуск № 39. С. 127 – 135.
11. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.
12. DUS ISO/IEC 27032: 2012. Information technology – Security techniques – Guidelines for cybersecurity. 61 p.

SYNTHESIS OF QUANTUM KEY DISTRIBUTION AND LIGHTWEIGHT ENCRYPTION FOR DATA PRIVACY IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab <http://cyberlab.fccpi.nau.edu.ua/>
National Aviation University, Kyiv, Ukraine

Rat Berdibayev, Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan

Yuliia Burmak, NAU Cybersecurity R&D Lab <http://cyberlab.fccpi.nau.edu.ua/>
National Aviation University, Kyiv, Ukraine

Dinara Ospanova, Kazakh Humanitarian Juridical Innovative University, Semey, Kazakhstan

Yuliia Polishchuk1, NAU Cybersecurity R&D Lab <http://cyberlab.fccpi.nau.edu.ua/>
National Aviation University, Kyiv, Ukraine

ABSTRACT: Key distribution is one of the most important problems of cryptography. This problem can be solved by different approaches – QKD is one of these methods. Today there are many QKD methods and systems, most of them is used in complex with traditional cryptography. In this paper the analysis of quantum technologies was carried out. It was declared that QKD is most implemented quantum technology in both laboratory (experimental) and commercial sector. Modern QKD protocols were analyzed as well as advantages / disadvantages were defined. Also it was declared, that QKD protocols can be used in complex with lightweight encryption for data privacy in modern information and communication systems (for example, IoT). To provide high security level lightweight algorithms can be changed on secure post-quantum algorithms.

KEYWORDS: *ICT, cybersecurity, QKD, data privacy, encryption, IoT, lightweight cryptography.*

1. Introduction

The main features of information security are confidentiality, integrity and availability (CIA-Triad, Fig. 1). Only providing these all gives availability for development secure ICT[1]:

- *Confidentiality* is the basic feature of information security, which ensures that information is accessible only to authorized users who have an access.
- *Integrity* is the basic feature of information security indicating its property to resist unauthorized modification.
- *Availability* is the basic feature of information security that indicates accessible and usable upon demand by an authorized entity.

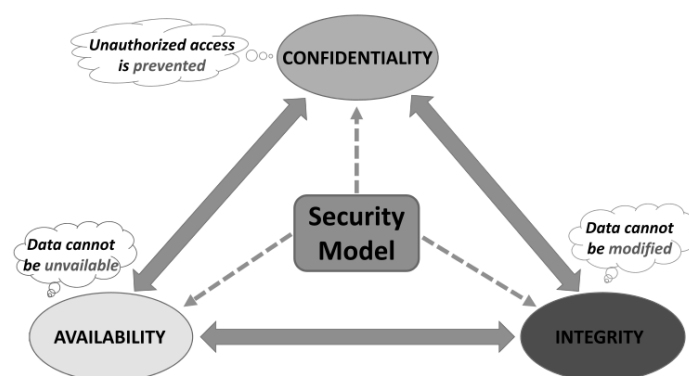


Figure 1. CIA-Triad

One of the most effective ways to ensure confidentiality and data integrity during transmission is cryptographic systems. The purpose of such systems is to provide key distribution, authentication, legitimate users authorisation, and encryption. *Key distribution is one of the most important problems of cryptography.* This problem can be solved with the help of the following approaches [2]:

- *Classical information-theoretic schemes* (requires channel with noise; efficiency is very low, 1-5%).

- *Classical public-key cryptography schemes* (Diffie-Hellman scheme, digital envelope scheme; it has computational security).
- *Classical computationally secure symmetric-key cryptographic schemes* (requires a pre-installed key on both sides and can be used only as scheme for increase in key size but not as key distribution scheme).
- *Quantum key distribution* (provides information-theoretic security; it can also be used as a scheme for increase in key length).
- *Trusted Couriers Key Distribution* (it has a high price and is dependent on the human factor).

In recent years, quantum cryptography (QC) has attracted considerable interest. Quantum key distribution (QKD) plays a dominant role in QC. The overwhelming majority of theoretic and practical research projects in QC are related to the development of QKD protocols. The number of different quantum technologies is increasing.

The first of all *quantum technologies of information security* consist of [2]:

- Quantum key distribution.
- Quantum secure direct communication.
- Quantum steganography.
- Quantum secret sharing.
- Quantum stream cipher.
- Quantum digital signature etc.

<i>QUANTUM DIGITAL SIGNATURE</i>		<i>QUANTUM KEY DISTRIBUTION</i>		<i>QUANTUM STREAM CIPHER</i>	<i>QUANTUM SECRET SHARING</i>		<i>QUANTUM SECURE DIRECT COMMUNICATION</i>		
QDS using single qubits	QDS using entangled states	QKD using single qubits and qudits	QKD using entangled states	Yuen 2000 protocol (Y-00, crj-scheme)	QSS using single qubits	QSS using entangled states	Ping-pong protocol	QSDC using single qubits	QSDC with block transfer

Figure 2. Quantum technologies of information security

The main task of this study is...

2. QKD protocols

2.1. Review of the modern QKD protocols

QKD includes the following protocols:

- protocols using single (non-entangled) qubits (two-level quantum systems) and qudits (d -level quantum systems, $d > 2$);
- protocols using phase coding;
- protocols using entangled states;
- decoy states protocols and some other protocols.

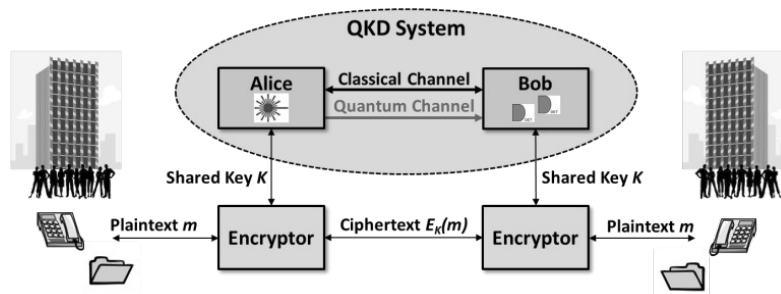


Figure 3. Scheme of QKD system implementation

The main task of QKD protocols is encryption key generation and distribution between two users connecting via quantum and classical channels (Fig. 3). In 1984 Ch. Bennett from IBM and G. Brassard from Montreal University introduced the first QKD protocol, which has become an

alternative solution for the problem of key distribution. This protocol is called *BB84* and it refers to QKD protocols using single qubits. The states of these qubits are the polarisation states of single photons. The BB84 protocol (Fig. 4) uses four polarisation states of photons (0° , 45° , 90° , 135°). These states refer to two mutually unbiased bases. Error searching and correcting is performed using classical public channel, which need not be confidential but only authenticated. For the detection of intruder actions in the BB84 protocol, an error control procedure is used, and for providing unconditionally security a privacy amplification procedure is used. The efficiency of the BB84 protocol equals 50%. Efficiency means the ratio of the photons number which are used for key generation to the general number of transmitted photons.

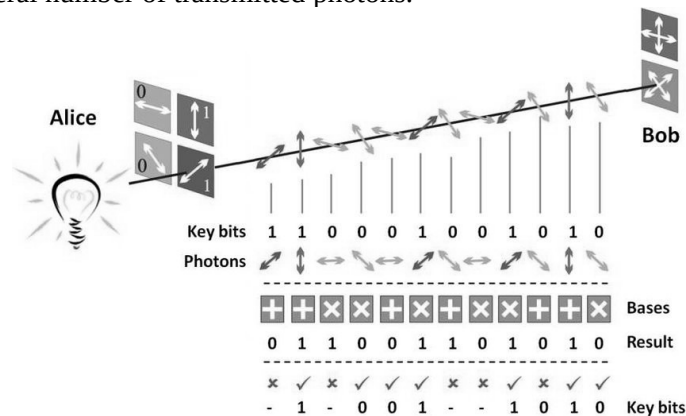


Figure 4. Scheme of BB84 protocol realization

Six-state protocol requires the usage of four states, which are the same as in the BB84 protocol, and two additional directions of polarization: right circular and left circular. Such changes decrease the amount of information, which can be intercepted. But on the other hand, the efficiency of the protocol decreases to 33%.

Next, the *4+2 protocol* is intermediate between the BB84 and B92 protocol. There are four different states used in this protocol for encryption: “0” and “1” in two bases. States in each base are selected non-orthogonal. Moreover, states in different bases must also be pairwise non-orthogonal. This protocol has a higher information security level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender. But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol.

In the *Goldenberg-Vaidman protocol*, encryption of “0” and “1” is performed using two orthogonal states. Each of these two states is the superposition of two localised normalised wave packets. For protection against intercept-resend attack, packets are sent at random times.

A modified type of Goldenberg-Vaidman protocol is called the *Koashi-Imoto protocol*. This protocol does not use a random time for sending packets, but it uses an interferometer’s non-symmetrisation (the light is broken in equal proportions between both long and short interferometer arms).

Another type of QKD protocol is a protocol using phase coding: for example, the B92 protocol using strong reference pulses. An eavesdropper can obtain more information about the encryption key in the B92 protocol than in the BB84 protocol for the given error level, however. Thus, the security of the B92 protocol is lower than the security of the BB84 protocol. The efficiency of the B92 protocol is 25%.

The *Ekert protocol (E91)* (Ekert, 1991) refers to QKD protocols using entangled states.

Entangled pairs of qubits that are in a singlet state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ are used in this protocol. Qubit interception between Alice to Bob does not give Eve any information because no coded information is there. Information appears only after legitimate users make measurements and communicate via classical public authenticated channel. But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol.

The *SARG04 protocol* does not differ much from the original BB84 protocol (Fig. 5). The main difference does not refer to the ‘quantum’ part of the protocol; it refers to the “classical” procedure of key sifting, which goes after quantum transfer. Such improvement allows increasing security against photon number splitting attack. The SARG04 protocol in practice has a higher key rate than the BB84 protocol.

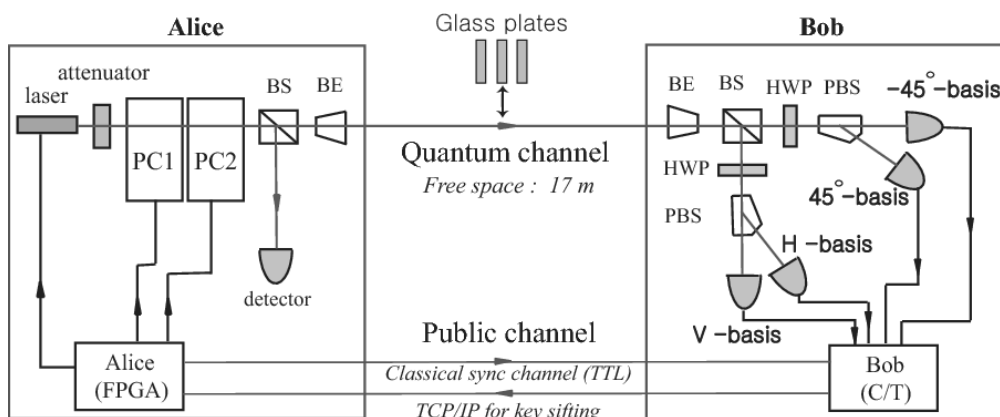


Figure 5. Scheme of SARG04 protocol implementation

Another way of protecting against photon number splitting attack is the use of *decoy states QKD protocols* (Fig. 6), which are also advanced types of BB84 protocol. In such protocols, besides information signals Alice's source also emits additional pulses (decoys) in which the average photon number differs from the average photon number in the information signal. Eve's attack will modify the statistical characteristics of the decoy states and/or signal state and will be detected. As practical experiments have shown for these protocols (as for the SARG04 protocol), the key rate and practical length of the channel is bigger than for BB84 protocols. Nevertheless, it is necessary to notice that using these protocols, as well as the others considered above, it is also impossible without users pre-authentication to construct the complete high-grade solution of the problem of key distribution.

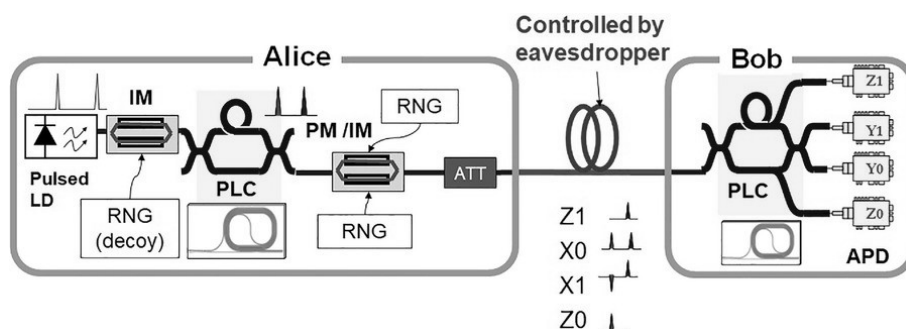


Figure 6. Scheme of decoy states QKD protocols

2.2. Advantages and disadvantages of QKD protocols

As a conclusion, after the analysis of the first and scale quantum method, we must sum up and highlight the following *advantages of QKD protocols* [2-4]:

1) These protocols always allow eavesdropping to be detected because Eve's connection brings much more error level (compared with natural error level) to the quantum channel. The laws of quantum mechanics allow eavesdropping to be detected and the dependence between error level and intercepted information to be set. This allows applying privacy amplification procedure, which decreases the quantity of information about the key, which can be intercepted by Eve. Thus, QKD protocols have unconditional (information-theoretic) security.

2) The information-theoretic security of QKD allows using an absolutely secret key for further encryption using well-known classical symmetrical algorithms. Thus, the entire information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (one-time pad) which in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of quantum key distribution protocols are following [2-4]:

1) A system based only on QKD protocols cannot serve as a complete solution for key distribution in open networks (additional tools for authentication are needed).

2) The limitation of quantum channel length which is caused by the fact that there is no possibility of amplification without quantum properties being lost. However, the technology of quantum repeaters could overcome this limitation in the near future.

3) Need for using weak coherent pulses instead of single photon pulses. This decreases the efficiency of protocol in practice. But this technology limitation might be defeated in the nearest future.

4) The data transfer rate decreases rapidly with the increase in the channel length.

5) Photon registration problem which leads to key rate decreasing in practice.

6) Photon depolarization in the quantum channel. This leads to errors during data transfer. Now the typical error level equals a few percent, which is much greater than the error level in classical ICT and systems.

7) Difficulty of the practical realisation of QKD protocols for *d*-level quantum systems.

8) The high price of commercial QKD systems (€ 120K +).

3. IoT Cybersecurity and Lightweight Cryptography

It was defined a lot of QKD challenges as well as many advantages for modern ICT. Most of all advantages relate to the only key distribution part and the security of encryption process is open question that depends on encryption algorithm [5]. Up to date secret key ciphers have key length of 256 bit (min) and cannot be implemented effective for example in IoT systems to ensure its security and privacy (Fig. 7).

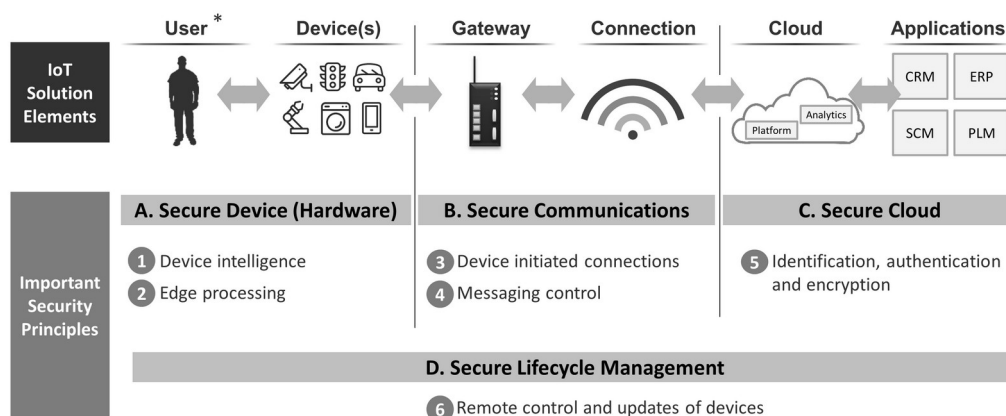


Figure 7. Principles of IoT cybersecurity

Encryption is an effective countermeasure, and the IoT is now required to apply encryption to sensor devices in environments with various restrictions that have not previously been subject to encryption (Fig. 8). Lightweight cryptography is a technology researched and developed to respond to this issue. The biggest security-related threat of IoT systems from the traditional IT systems is that even using devices for data collection from the real world can become a target of cyberattacks. For example, the purpose of applying IoT to a plant is to significantly improve the productivity and maintainability by collecting data from a large number of sensors installed in production equipment, by analyzing it and performing autonomous control in real time. If sensor data should be falsified during this process, incorrect analysis results would be induced and erroneous control would result due to such an occurrence having the potential of leading to major damage. Moreover, since measurement data and control commands are trade secrets associated with the know-how of production and management, preventing leakages is also important from the viewpoint of competitiveness. Even if there is no problem at present, it is necessary to consider the effect of threats that might become evident in the future. Applying encryption to sensor devices means the implementation of data protection for confidentiality and integrity, which can be an effective countermeasure against the threats. Lightweight cryptography has the function of enabling the application of secure encryption, even for devices with limited resources [6].

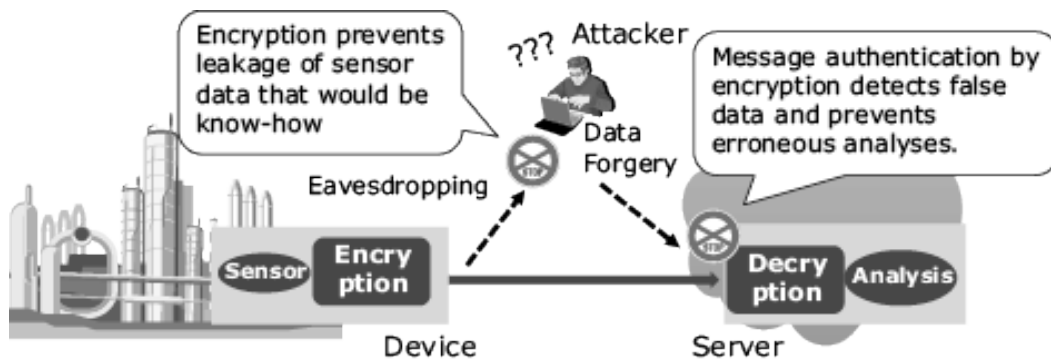


Figure 8. Encryption in IoT

Encryption is already applied as standard on the data link layer of communication systems such as the cellphone. Even in such a case, encryption in the application layer is effective in providing end-to-end data protection from the device to the server and to ensure security independently from the communication system. Then encryption must be applied at the processor processing the application and on unused resources and hence should desirably be as lightweight as possible (Fig. 9).

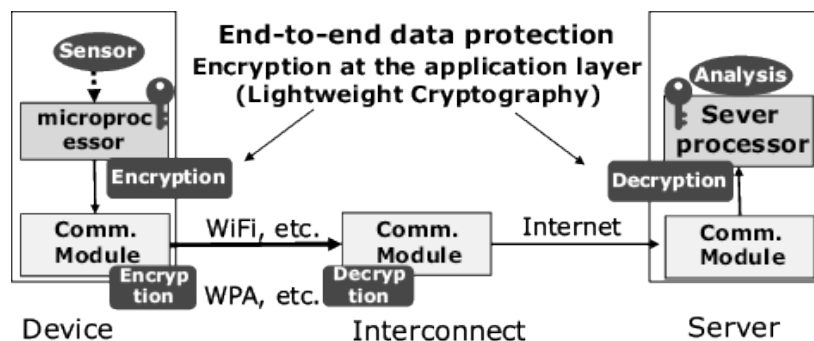


Figure 9. Lightweight encryption in IoT

The symmetric key cryptography uses the same secret key for encryption and decryption. With the processing that is relatively lightweight, it is used in data encryption and authentication. On the other hand, public key cryptography uses a secret key in decryption and a public key different from the secret key in encryption, and it is quite difficult to guess the secret key from the public key. The computational complexity of the public key cryptography is typically as high as more than 1,000 times that of the symmetric key cryptography, but this technology is used in sharing the secret key used in symmetric key cryptography and the digital signature, thanks to the asymmetrical property. With a system such as a plant or car- control system, it may be possible to embed the secret keys shared by the devices in advance. In such a case, secure and efficient data protection can be implemented using symmetric key cryptography alone. On the other hand, with a system that performs encrypted communications dynamically with unspecified parties such as an inter-vehicle communication system, the use of public key cryptography is effective. Symmetric key cryptography can be widely applied to devices that are subject to severe resource restrictions. The symmetric key cryptography consists of core functions such as block or stream ciphers (cryptographic primitives) and methods to apply the core function to a packet called the block cipher mode of operation for encryption and/or authentication.

Today there are many standardized algorithms of lightweight cryptography:

- ISO/IEC 29192-1:2012 Information technology — Security techniques — Lightweight cryptography — Part 1: General
- ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers
- ISO/IEC 29192-3:2012 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers
- ISO/IEC 29192-4:2013 Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques

- ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions
- ISO/IEC 29192-6:2019 Information technology — Lightweight cryptography — Part 6: Message authentication codes (MACs)
- ISO/IEC 29192-7:2019 Information security — Lightweight cryptography — Part 7: Broadcast authentication protocols

4. Conclusions

In this paper the analysis of quantum technologies was carried out. It was declared that QKD is most implemented quantum technology in both laboratory (experimental) and commercial sector. Modern QKD protocols were analyzed as well as advantages / disadvantages were defined.

Also it was declared, that QKD protocols can be used in complex with lightweight encryption for data privacy in modern information and communication systems (for example, IoT). To provide high security level lightweight algorithms can be changed on secure post-quantum algorithms [7,8].

REFERENCES

1. Gnatyuk S. Advanced Technologies of Quantum Key Distribution, Monograph, London, Great Britain : InTech, 2018, 227 p. DOI: 10.5772/65232
2. Korchenko O., Vorobiyenko P., Vasiliu Ye., Gnatyuk S. telecommunications Networks: Current Status and Future Trends, Monograph [edited by Jesus Hamilton Ortiz], Rijeka, Croatia : InTech, 2012, 446 p.
3. Z. Hu, S. Gnatyuk, T. Okhrimenko, V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.
4. Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. Experimental Study of Secure PRNG for Q-trits Quantum Cryptography Protocols, Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.
5. Labadze G., Iavich M., Iashvili G., Gagnidze A., Gnatyuk S. Post-quantum digital signature scheme with BB84 protocol, CEUR Workshop Proceedings, Vol. 2915, pp. 35-44, 2021.
6. Iavich M., Kuchukhidze T., Gnatyuk S., Fesenko A. Novel certification method for quantum random number generators, International Journal of Computer Network and Information Security, Volume 13, Issue 3, pp. 28-38, 2021.
7. Iavich M., Gnatyuk S., Arakelian A., Iashvili G., Polishchuk Y., Prysiazhnyy D., Improved Post-quantum Merkle Algorithm Based on Threads, Advances in Intelligent Systems and Computing, Vol. 1247 AISC, pp. 454-464, 2021.
8. M. Iavich, S. Gnatyuk, G. Iashvili, A. Fesenko. Cyber security European standards in business. Scientific and Practical Cyber Security Journal (SPCSJ), 3(2):36-39, 2019

USING SNA VISUALIZATIONS TO DEPICT SUSPICIOUS SOCIAL MEDIA USERS: A FORAGE FOR LAW ENFORCERS

Dr. Lamek Kiprutto Ronoh, Rongo University, School of information, communication and media studies
Department of Information Science and Informatics

ABSTRACT: The evident increase in the sophistication of cyber criminals has a significant impact that can threaten the national security if it goes unabated. Presently, use of social media in mining crucial digital or forensic evidence by law enforcement bodies in Kenya is a novel idea that needs to be explored and implemented. The study's objective was to demonstrate how Social Network Analysis (SNA) can be used as an investigative tool to mine, analyse data from selected online social media users and present digital forensic evidence to aid law enforcement in Kenya. Particularly, the study aimed at identifying high degree nodes in the network and profiling them using visualizations. NodeXL software was used to mine and analyse data. Computation of centrality measures, network clusters, cliques were presented using both infographic visualizations and centrality metrics of the respondents on egocentric networks focal communication paths through which information flows in the network were also depicted. The discoveries of this study indicated that Social Network Analysis is an essential and supplementary tool that can be employed by law enforcement agencies and related stakeholders to mine, analyse and present court accepted digital forensic evidence. The findings presented in this research illustrates how social network analysis can be used to determine the interpersonal connections, importance of actors in a given social network and detect communities of people and principally how law enforcement agencies can utilize this technique in identifying and tracking suspicious characters and ultimately help in maintaining law and order. SNA ought to be embraced as a supplement of conventional investigation, not necessarily replacing it.

KEYWORDS: *Social Media, visualizations Social Network Analysis, actor(s), node(s)*

Background of the study

Social network analysis regards social interactions from the perspective of network theory comprising of nodes and links (also called ties, edges, or connections). Nodes in this case are the persons within the social networks, whereas the ties are the associations between these persons. The resultant graphical structures are mostly quite intricate (Passmore, 2011)

The increasing availability of large-scale, real-world sociographic data derived from social media, web pages and datasets has led, among other things, to a renaissance of Social Network Analysis and its

application in new fields of enquiry. Social network analysis allows one to measure, map and explain everything pertaining social network and its elements (Gupta & Brooks, 2015).

According to a report by PewResearch Center (2014), social media include the various ways and means people hook with one another through online interactions. Mobile devices, social networks, email, texting, micro-blogging and location sharing are just a few of the many ways people engage in computer-mediated collective action. As people connect, like, follow, friend, reply, retweet, comment, tag, rate, review, edit, update, and text one another they form collections of connections. These set of connections develops into network formations that can be mined, investigated and the results depicted using various ways and techniques. The result can give a new understanding of into the structure, size, and key positions in these networks.

Latent Social Security Information

Nouh and Nurse (2015) corroborated these findings by observing that not only does social media platforms provide a new unexploited fountain of mining intelligence for law enforcement community, but it also gives an insight of understanding behavioural patterns of covert groups.

According to Global Justice Initiative report (2013), various social network platforms are progressively exploited to initiate or carry out unlawful acts and therefore law enforcement agencies ought to comprehend the idea and purpose of these platforms. They also need to understand the way social media forensic apparatus and resources can be used to thwart, lessen, act in response to, and probe illegal actions. Although the advent of social media has created new investigatory opportunities for law enforcement, it also presents ethical, legal, and technical challenges. Depending on the country in which the investigation takes place, it may be illegal to gather information on social media if a user's profile is not public (Rice & Parkin, 2016).

Social Network analysis in law enforcement

In his quest to find out how law enforcers utilize social media platforms to covertly examine unlawful movements, Wyllie (2015) established that law enforcement agencies are employing the use of popular social media platforms such as Facebook and Twitter in various ways to assist in combating offences and give services to their societies. More significantly is the fast growing application of social media investigating means to uncover evidence of criminal activity which the lawless individuals on their own volition frequently place to the online network habitually paving way for swift apprehension of themselves and impending likely sentence. Detectives can use social media platforms as an investigative tool by creating undercover pseudo accounts in order to use to harvest intelligence on crimes and suspects or get the identity and movements of suspects (Murphy & Fontecilla, 2013).

Statement of the Problem

This paper revolved around an ego. The egocentric analysis entails the examination of a single node within a given social network platform including all the actors the node is linked to. Social theorist postulates that influence between social network friends goes up to three degrees or three intermediary levels. In criminology and law enforcement, Social network analysis has been proved to be a powerful tool to learn the structure of a criminal network notably in social media platforms. It allows researchers to understand the structural relevance of single actor and his/her connections amongst members of a given social network by defining the key concepts to characterize network structure and roles.

Purpose of the Study

To perform experiments on real life social networks available in commonly used types of popular social services such as Facebook and Twitter in quest to demonstrate how Social Network Analysis as an invaluable tool can be employed to extract latent knowledge or information from networks encountered in nature, especially networks formed by people.

Specific Objective of the Study

The objective of the paper was to visualize social networks and clusters to uncover the patterns of the social relationships of people in investigating crimes committed over selected popular social media platforms in Kenya.

Research Design and Methodology

Social Network Analysis experimental research design was employed in this study. Initially, selected respondents treated as focus groups were subjected to a brief interview and thereafter persuaded to create pseudo-online accounts in specified social media platforms which were used to perform online mining of the selected respondents to obtain data that ultimately aided in social network analysis.

Discussion and Evaluation

From the initial seed of 94 respondents selected for the study, the social network expanded exponentially to 29295 over the three months of study.

Unearthing Key Social Network Actors Using Visualizations and Clusters

NodeXL was employed by the researcher in the analysis to visualize and identify subgroups (clusters), generate set of graph metrics using various actors' interactions using either force directed algorithms such as Harel- Koren fast multiscale or Fruchterman –Reingold or using geometrical algorithms such as spiral, vertical, grid, horizontal or circle. Therefore, social networks was depicted differently over time due to structural changes as a result of increase or decrease of network membership

In essence, ties between actors was analysed and visualized using various social network analysis metrics.

The researcher employed the use of visualization and clusters so as to aid in focusing and identifying individual nodes that exhibit important network properties to the rest of the network. Use of network visualizations is crucial because it reveals patterns that are otherwise invisible by other means of analysis or investigations of a network setup.

Egocentric Seed Network

Figure 1 depicts the egocentric network of the seed actor whose pseudo-name was “samsonpeter9252” (this name has been by truncated as “sams~” in this study) is visualized and positioned at the epicentre of the social network. The seed actor’s initial connections to the selected respondents are illustrated by the arrows pointing outwards and inwards the main or seed node. Hence it is a directed graph. The graph's vertices were grouped by cluster using the Clauset-Newman-Moore cluster algorithm while the graph was laid out using the Harel-Koren Fast Multiscale layout algorithm. The findings illustrates that at a 1-degree egocentric network comprising of the initial 55 seed correspondences out of the targeted study sample size of 94.

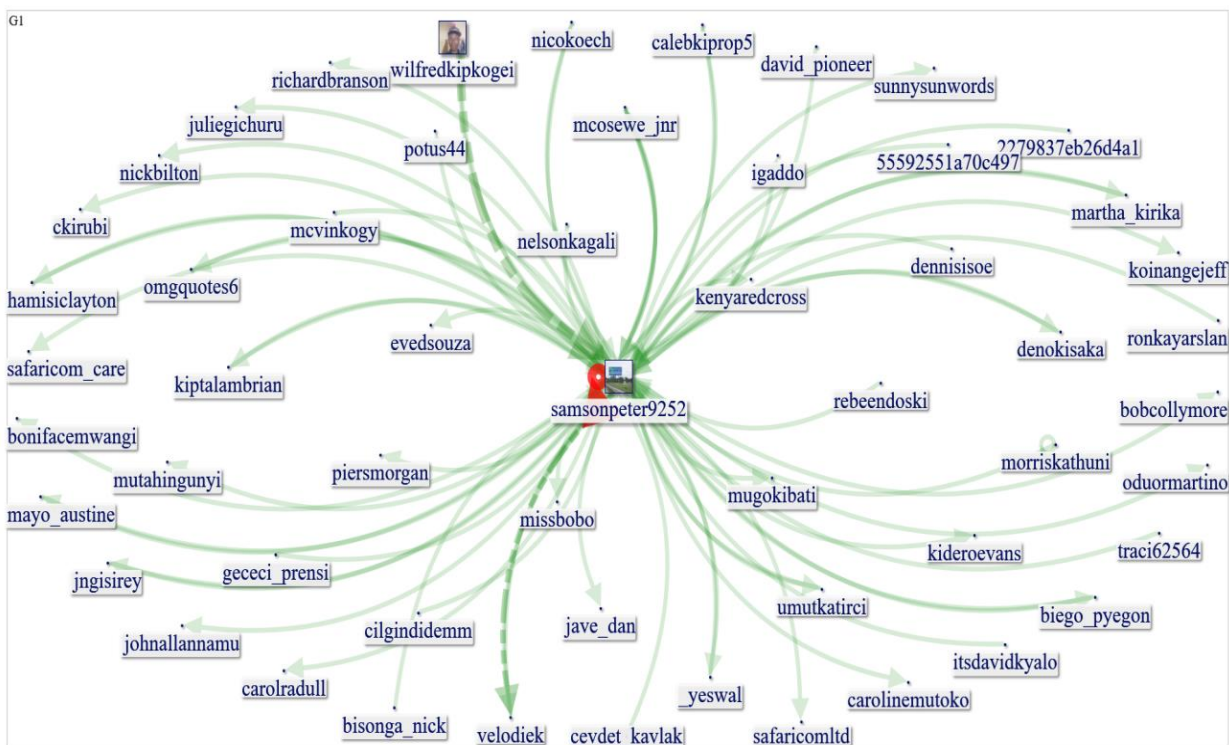


Figure 1: Initial Seed 1-Degree Egocentric Directed Network

Source: Researcher

Identifying Communities

The visualizations result in Figure 2 shows how respondents have regrouped themselves into three distinct communities (labelled C1, C2 and C3). This is an important findings which was achieved by employing the force directed algorithm in the visualization so that the connected actors draw to every other while non-connected actors are separated. This means that the highly linked actors are drawn towards the epicentre of the graph. Evidentially, the findings clearly portrays that in the three communities detected, there is one main influential node in each community. Their pseudo-names are velo~(*velodiek*), wilf~(*wilfredkipkos*) and deno~(*denokisaka*). The results are closely related to study done by Staudt, Marrakchi and Meyerhenke (2014) on detecting communities. In each community, the primary distributors of information were identified. In conformity, Yang, Liu and Sageman (2006) underscores that identifying groups such as this assists a detective to quickly unearth the associated criminals when a small number of suspicious characters are known.

Markedly, in these aforementioned detected communities, respondent velo~ has the highest degree centrality, followed by respondents wilf~ and deno~ in that order. This means that the three actors are not only powerful in the network, but it also shows that have great access to information in their respective communities. These findings are in conformity with that of Wu, Carleton and Davies (2014) which advises that in a terror network, investigators usually go for actors with the highest degree centrality scores because they are the most connected and possibly the most influential nodes in the entire network and that one can easily identify a subgroup of a network communities that particular nodes belongs to by visually assessing the links amongst network actors. In a rejoinder, Perliger and Pedahzur (2011) stressed that discovering the communities enables the investigators to identify the various roles of the nodes in the network such as leadership or brokers and how information flows in the entire network.

Besides examining the roles of several members of the network, investigators ought to concentrate on specific subgroups in order tell their particular duty. Usually, network members come together with an obligation of accomplishing their heinous acts and therefore identifying the subgroups who are interconnected could enhance the chance of detectives comprehending the intention of the entire network. In an investigation scenario, the objective of identifying communities in a suspicious network is to detect their groups and social structures they belong. In Faustand Fitzhugh (2012) Social Network Analysis techniques helps to comprehend network communities by mapping the relations that link them as a network and thereafter determine key players or groups and ties between the nodes.

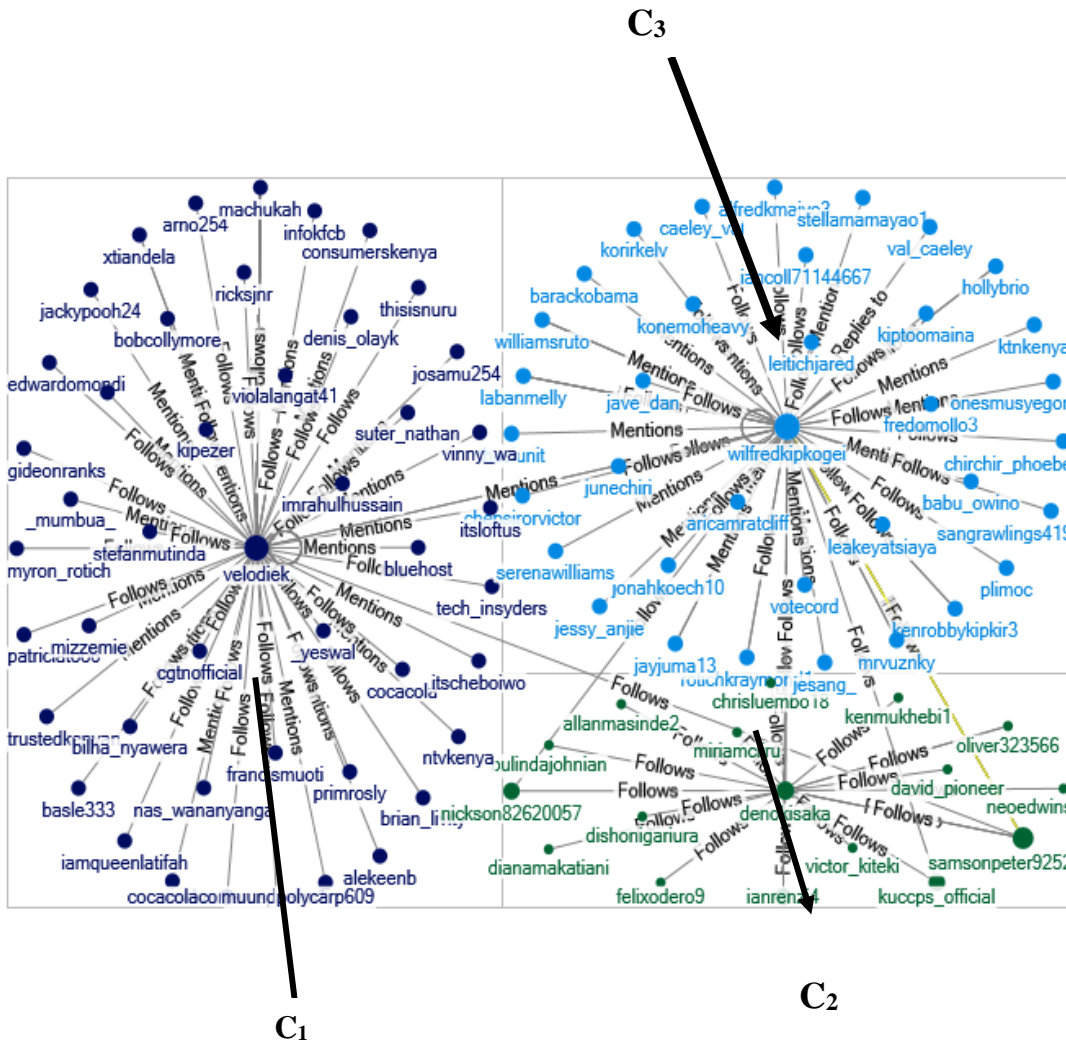


Figure 2: Identifying Communities and their Main Actors

Source: Researcher

Community Densities

The findings in Figure 3 shows varying densities of six communities or subgroups densely connected in one network, each identified by label codings D₁ to D₆. Necessitated by the need to portray the insight phenomenal of how information visually diffuses amongst the actors in the network, researcher employed the Wakita-Tsurumi algorithm to generate the network densities of the detected communities. A similar approach was employed by Waskiewicz (2012). The research findings indicates that as the size of the network exponentially increased over time, the density of the network expanded but not uniformly for each community.

More specifically, the study results in Figure 3 revealed that relationship or links exist between the detected communities. Notably, the densities of D₂, D₃ and D₆ communities are visually more or less

equal which implies that members of these three aforementioned communities communicate more frequently about an issue(s) they are all familiar with and probably know one another most. However, the density is slightly higher for the D1 community in the entire network and visibly has a node with the high degree centrality score.

Borrowing from Krebs (2002), a dense cluster having numerous interactions is suspicious and warrants investigations to unearth or discover more information about the group. Last but not least, the D4 and D5 community members are scattered and also depicted the least density in the whole network. These results closely relates to the study done by Staudt, Marrakchi and Meyerhenke (2014) on community detection in quest of revealing structures or patterns of interactions between nodes in a network. Furthermore, the findings conforms with (Hansen, Shneiderman & Smith, 2011) comparative analysis on determining communities that are highly related or sparsely connected. Density metrics helps to predict the flow of information between nodes of a given network and it indicates homogeneousness of a community and nodes' interactions with one another (Martino & Spoto, 2006). By employ the density measure, detectives are able to a holistic understanding structure of the entire network under scrutiny.

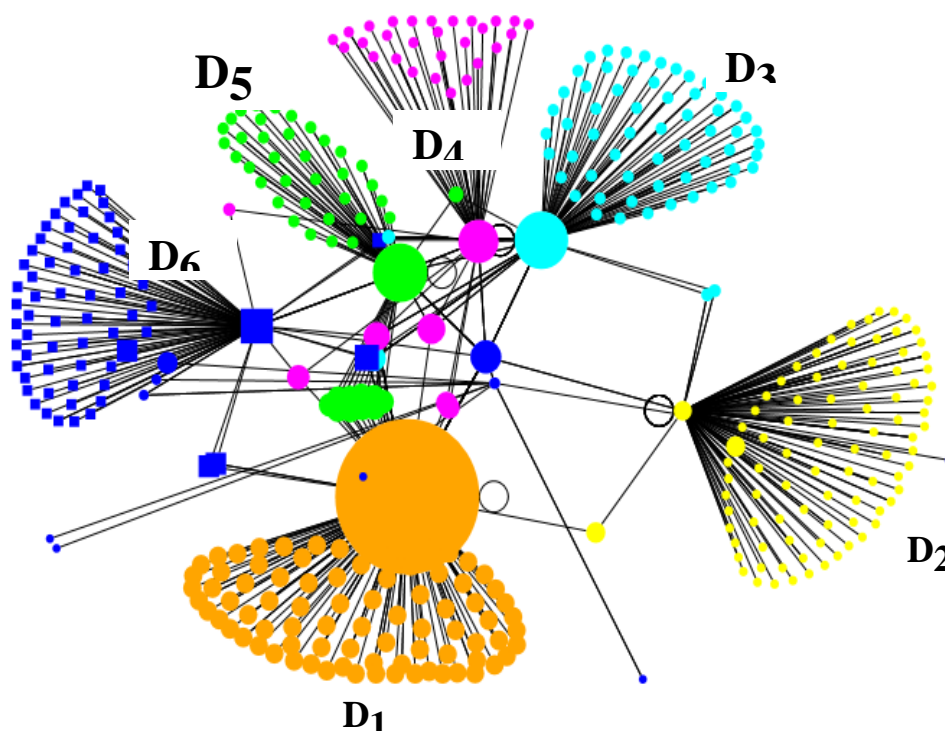


Figure 3: Network Density Isolation
Source: *Researcher*

Therefore, the visualization of network community densities has not only helped to portray the interconnections of individuals and subgroups in a social network, but also it has also aided to expose communities who possibly dominate several ranks in the network are likely to be influential or close and bonded than others in the network. These illustrations concurs with Mulazzani, Huber and Weippl (2012)

that visualizations can be a very effective tool in law enforcement agencies investigating social networks because it enables them understand the behaviour of social media users and they can predict criminal activities by monitoring connections between suspects, understand the dynamics such as discovering the leaders, followers and new individuals being integrated into a group. The techniques of detecting and identifying communities helps to know groups of nodes densely connected than other in the entire network (Tayebi & Glässer, 2016). In a rejoinder, Faust (2006) outlined that the density of a network is proportional to the probable number of connections in that network. A conspicuously dense community is susceptible and exposed to law enforcement officers for further scrutiny and identification of the main actors who are most likely to be the leaders of a particular cohort of felons (Xu, Marshall, Kaza & Chen, 2004).

Detecting Clusters of Communities

Figure 4 shows the generated visualizations results of six distinct interconnected clusters equivalent to the number of network communities (*the clusters are labelled S1 to S6*). The size of the visuals indicates how active a node is in the cluster or the entire network. Evidently, S4 community cluster density is the highest and its members are seemingly well connected and active too, hence the tight bonding visuals. Voigt, Hinz and Jansen (2013) outlined that the characteristics of clusters presenting high density scores are usually attributed to few interrelated or connected nodes. The cluster labelled S6 is the second highly active group in the network although it slightly scattered to vaguely overlap S5 cluster in the network. Except for one isolated member, all members of S3 cluster are dependent on one actor who connects them to the rest of others in the network. By employing such Social Network Analysis visualization techniques, there is a possibility to detect clusters, identify the most important actors and their roles and unveil interactions between nodes (Mena, 2003). The findings can be related to Hoppe and Reinelt (2010) observation that clustering helps to unearth important communities of a network that were not known previously. This was corroborated by Xu *et al* (2004) in cluster analysis as a way of detecting not only network subgroups but also the central actors and how they interact with other communities.

If a network community depicts a strong connection between its members, then it can aid to know the associates that belong to that network community Krebs (2002). This way, detectives can narrow down the list of suspicious characters under investigation. Moreover, identification of gatekeepers connecting to a particular subgroup (community) is also important in unearthing specific dubious characters. In Zhu, Watts and Chen (2010), network clustering helps detectives to narrow down their investigations to a specific subgroup or community.

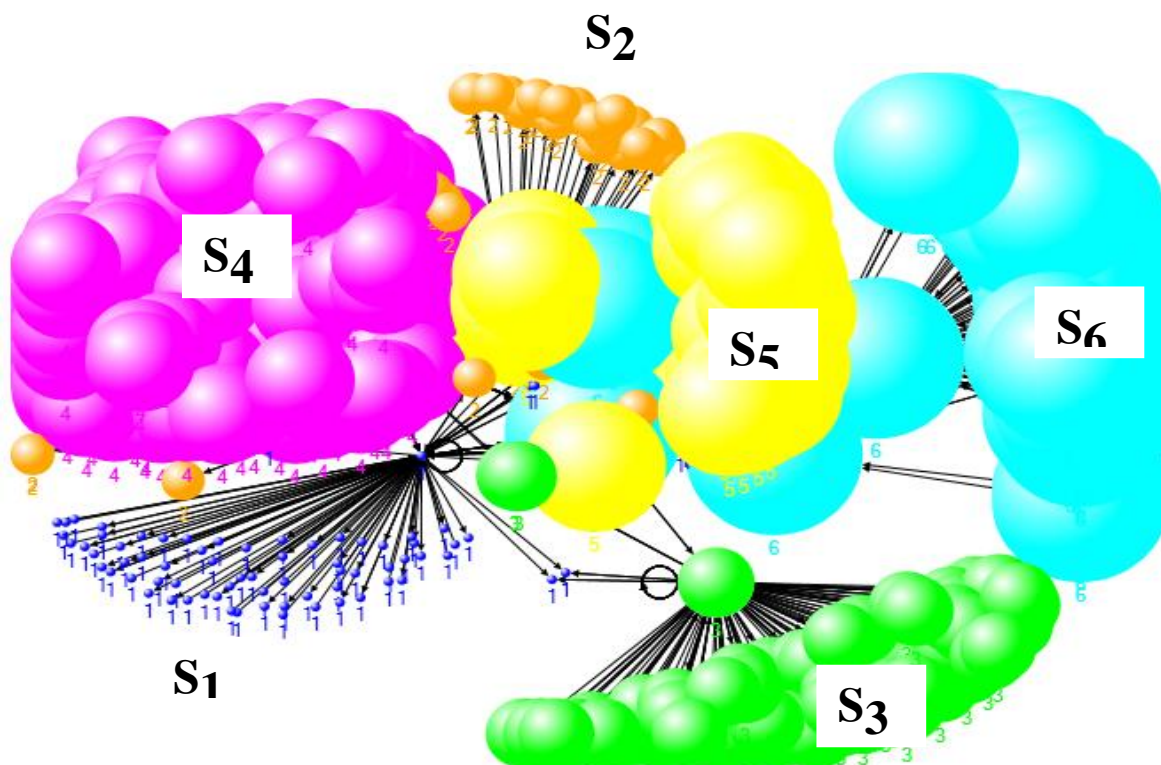


Figure 4: Clustering Network Communities

Source: *Researcher*

Degree Centrality Distributions

Betweenness Centrality Visualizations

Figure 5 shows the corresponding degree distributions of the network actors under study. It clearly illustrates that actor wilf~ has highest degree and betweenness centrality and therefore is the most influential person in the entire network. This implies that respondent wilf~ probably knows what is going on in multiples social clusters of the entire network. Identifying the actors with the highest betweenness centrality in a suspicious network helps detectives to focus their attention and resources in profoundly investigating those nodes in the entire network (Kirchner & Gade, 2011).

The research findings further portrays that respondent wilf~ act as gatekeeper by connecting the cluster that he belongs to the entire network because communications emanating from other clusters from the rest of entire network must pass through him. This means that actor wilf~ is capable of influencing the entire network but he is more susceptible to detection. Besides node wilf~ other actors namely 2279837eb26d4a1, velo~, nico~, deno~ and kiptal~ scored considerably higher degree and betweenness centralities after wilf~ from second to sixth positions respectively in the entire network but first in their clusters. This implies that these main actors are leaders or hubs of their respective subgroups in the social network. Intuitively therefore, the six actors act as intermediaries in their network subgroups because information must flow through them. The findings concurs with advice of Xu, Marshall, Kaza and Chen

(2004) that while carrying out an investigation, one needs to know which nodes other actors have to connect to in order to link to the entire network and gather other valuable leading information. Nodes acting as bridges to their subgroups create structural holes which help investigators to easily detect friends of the influential nodes (Hanneman & Riddle, 2005).

Boundary Spanners Visualizations

It was also necessary to establish the boundary spanners in the network. By doing so, the researcher was able to know the actors that connect several other clusters as this will imply that they are more central in the entire network. Accordingly, Figure 5 further reveals the boundary spanners as actors wilf~, 2279837eb26d4a1, velo~, nico~, deno~ and kiptal~ who bridge their respective clusters and therefore are strategically placed to get information from other clusters. Furthermore, these actors are able to integrate concepts and information from other clusters. The results are closely consistent with Long, Cunningham and Braithwaite (2013) that the boundary spanners act as conduit of information flow between network nodes or individuals who cannot communicate directly or have no or little trust to each other.

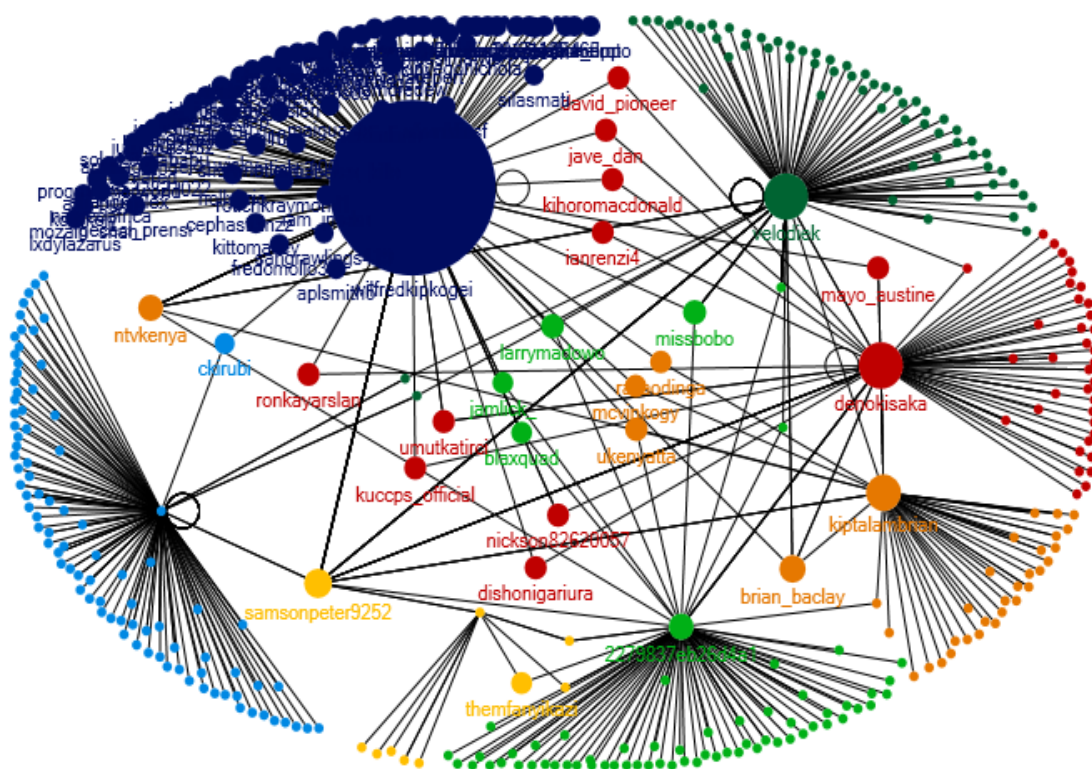


Figure 5: Degree Distributions

Source: *Researcher*

Closeness Centrality Visualizations

Figure 5 visualization results also indicates that actors sams~,wilf~, deno~, velo~, kipatal~, ntvk~ and 2279837eb26d4a1 had almost equal and similar pattern of closeness centrality measures in the entire network. Connections with nodes having high closeness scores when put together with nodes having low degree centrality values can have indirectly impact on the behaviour of the other nodes in that network (Wasserman & Faust, 1994). This implies that the aforementioned respondents were highly connected to other individuals in the network. It is important to note that the thicker the edge the higher the frequency interaction between any given actors in a network.

Regarding structural similarity, the researcher attempted to depict and find actors who are linked to more other nodes connected to the influential actor in the network. This implies that if two or more actors have similar friends, then this implies that all of them are friends in real world. Actors 2279837eb26d4a1, velo~, nico~, deno~ and kipatal~ was found to have structural similarity because they largely share a number of friends as shown by the edges in the diagram and also they are leaders of their respective clusters too. This agrees with McPherson, Smith-Lovin & Cook (2001) similarity yields interconnections between nodes with structural similarity.

Information Flow between Network Actors

It was also imperative for the researcher to visually depict how information flows in a network between actors/respondents under study.

Figure 6 was generated using geometric spiral algorithm. It clearly illustrates the flow of information in the entire network between actors. At the epicentre of the information flow is the subgroup members labelled A_3 , spreading to the second layer. It is densely surrounded by the A_1 subgroup members. This implication here is that the network members of both A_1 and A_3 could be sharing similar information or have same interests with each other. The A_2 subgroup members are somewhat spreading to the hub of the communication flow of the network and also found at the periphery of the communication labyrinth. The results resonates with Nagl, Amos, Sewall and Petraeus (2008) reasoning that nodes on the periphery receive very low centrality scores and are often connected to networks that are not currently mapped but they are important links since they may be resource gatherers or individuals with their own network outside their isolated group. These characteristics make them very important resources for fresh information not available inside their isolated group.

Equally significant is the A_6 and A_4 subgroups, though a little blurred, they are also similarly positioned at the hub of the communication flow and spread heavily to the second layer after epicentre to the periphery. Cluster A_3 is diminutively encircled halfway by subgroup A_6 which spreads heavily to periphery. This conforms with Arnaboldi, Conti, Passarella and Pezzoni(2013) observation that the innermost circle signifies a more stronger social relations of the ego while the outermost circle are typified by fluctuating level of friendliness (also called sympathy or active network groups).

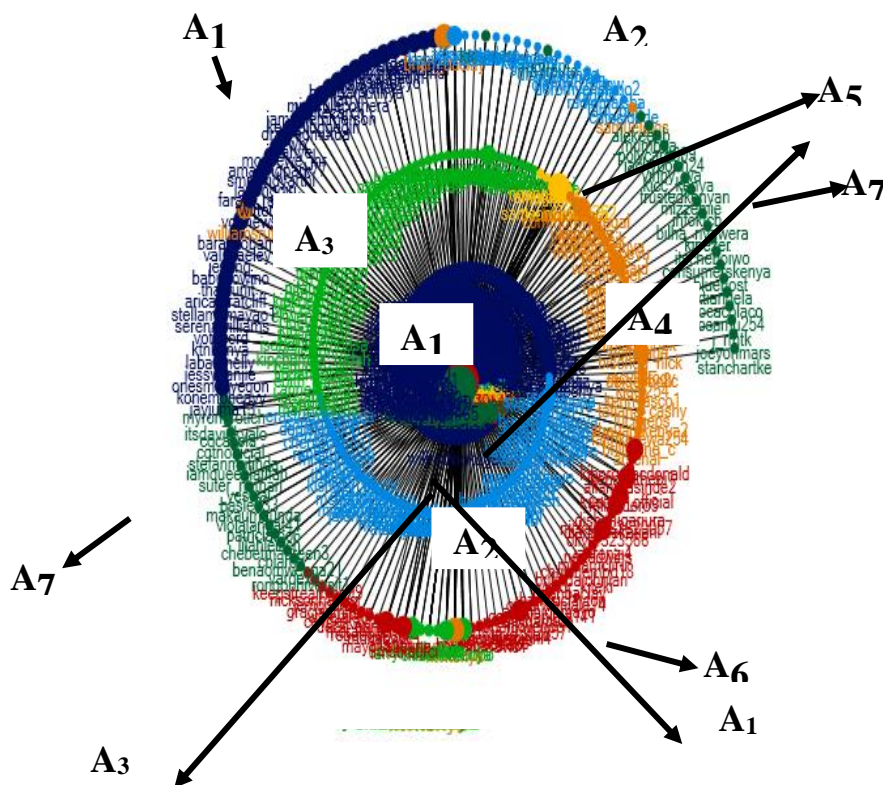


Figure 6: Network Concentric Information Flow

Source: *Researcher*

The A₇ clusters, on the periphery of these visualisations are the isolates in the communication flow. Heeding the advice of Granovetter (1973), that the important channels of communication to be closely monitored are the ones that are rarely utilized and usually located at the network's periphery, cluster A₇ members elicits more scrutiny.

They seem to be recipient of the information from the entire network or they only share information specific to themselves and their interests. This visualization results correlate with Sharma and Strategy (2008) that although nodes at the periphery have less interactions with the entire network, they may be having links beyond the network and as result they can be a reservoir of new information.

Drawing and concluding from Figure 7 therefore, it is apparently evident that A₁, A₃, A₆ and A₅ subgroups are the most influential actors over others in this network. This concurs with Ferrara, De Meo, Catanese and Fiumara (2014) that by analysing the flow of information pattern in a given network, one can unearth actors that play key role in a criminal network or have connections to different clusters. Visualizing and identifying subgroups of a network enables investigators to unravel rich information pertaining the nodes, network recruitments paths, operational characteristics and patterns of flow of information (Bonacich, 1972). Hence, an investigator can narrow down his/he probe to those aforementioned subgroups to gather more valuable information and reveal their activities.

Network Communication Channels

The visualization results in Figure 8 shows the channels of communication between the various subgroups of the entire network under study. Notice that group one (denoted G1) and some members of group 4 (G4) have two major common communication links between themselves. This implies that some members in G4 who may not be prominent in that cluster knows each with the most influential member of G1. The two groups (G1 and G4) also share some influential or common actor in cluster G5. However, the influential node in G1 is conspicuously in touch with periphery members of cluster G6. Noticeably, G1 has the most members while G6 has the least. Nodes that are located at the terminals of the communication channels are likely to influence others whereas those found in-between the channels of communication paths are likely to be information conveyance belts (Waskiewicz, 2012).

In Figure 7 the findings also showed that nodes in various clusters frequently communicate with actors within their clusters than with those outside their clusters. By deriving such information, investigators can easily identify cohesive clusters and ultimately establish part of the network where information moves faster and also which cluster(s) closely keeps information to themselves.

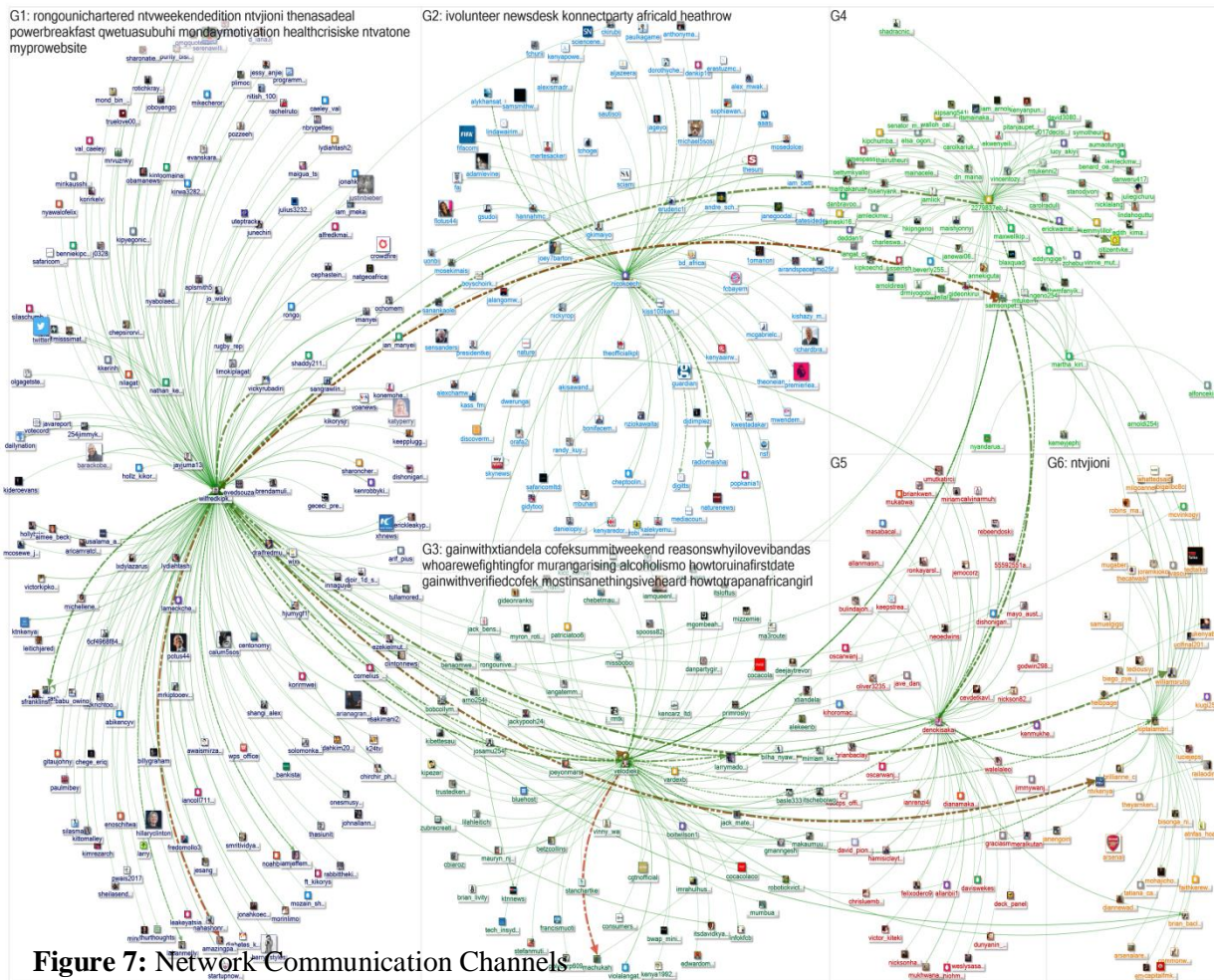


Figure 7: Network Communication Channels

Source: Researcher

Network Cliques

In quest of gaining deeper insight into the network, the researcher generated a complex network visualization shown in Figure 8 depicting how actors of a network over time, can ultimately fragment into interesting groups called cliques. Thus Figure 8 shows the visualization findings of network cliques generated from the now complex network. Notice that the network has now fragmented into subgroups of cliques (denoted as G1, G2, G3,.....up to G23) and each clique is labelled with the topics they frequently discuss. The Clauset-Newman-Moore grouping algorithm identified 23 cliques within this network. However, some cliques such as G1, G2, G3, G4 and G19 have further but minute fragments within the respective cliques. These findings indicate the nodes in the entire network are highly diverse. This implies that as time elapses, network users tend to slowly degenerate into fragmented interactions and eventually form their own cliques according the nature of information exchanged between themselves as well as interests.

Stemming from these findings, the results are consistent with Bonacich (1972) on the painstaking examination of characteristics of such cliques for homogeneous ideologies and the strength of their cohesion with that network, as well as how this influences the activities and development of the

unlawful network. This way, such information can assist an investigator to tell if they are still an healthy communication or leadership roles have been changed and splinter groups emerged. Thus, the graph was generated not only to depict the number of cliques in the network but also to utilize the visual properties to map the attributes of the network showing the interaction of the actors.

The network visualizations depicted in the findings so far discussed above, underscored how important Social Network Analysis visualizations is to law enforcement agencies in unearthing leading information from a large set of data, which could otherwise been difficult or impossible to tell using conventional methods of investigations. While backing up the use of Social Network Analysis, Rahim, Amalina and Sulaiman (2015) emphasized that visualisation methods are crucial because it helps scholars to comprehend social interaction or patterns of online relations and who communicates with who more or less frequently. Hence cannot comprehend the trends and concepts of social networks without employing the use of computerized visualizations as presented in this thesis.

In an investigation scenario, the detectives ought to concentrate their probe efforts to specific actor under scrutiny then traverse the network as they examine for crucial leads. Visualizations makes this investigation process much forthright because it enables the discovery of unknown interactions and relationships that exists between actors.

Social media network connections among Twitter users

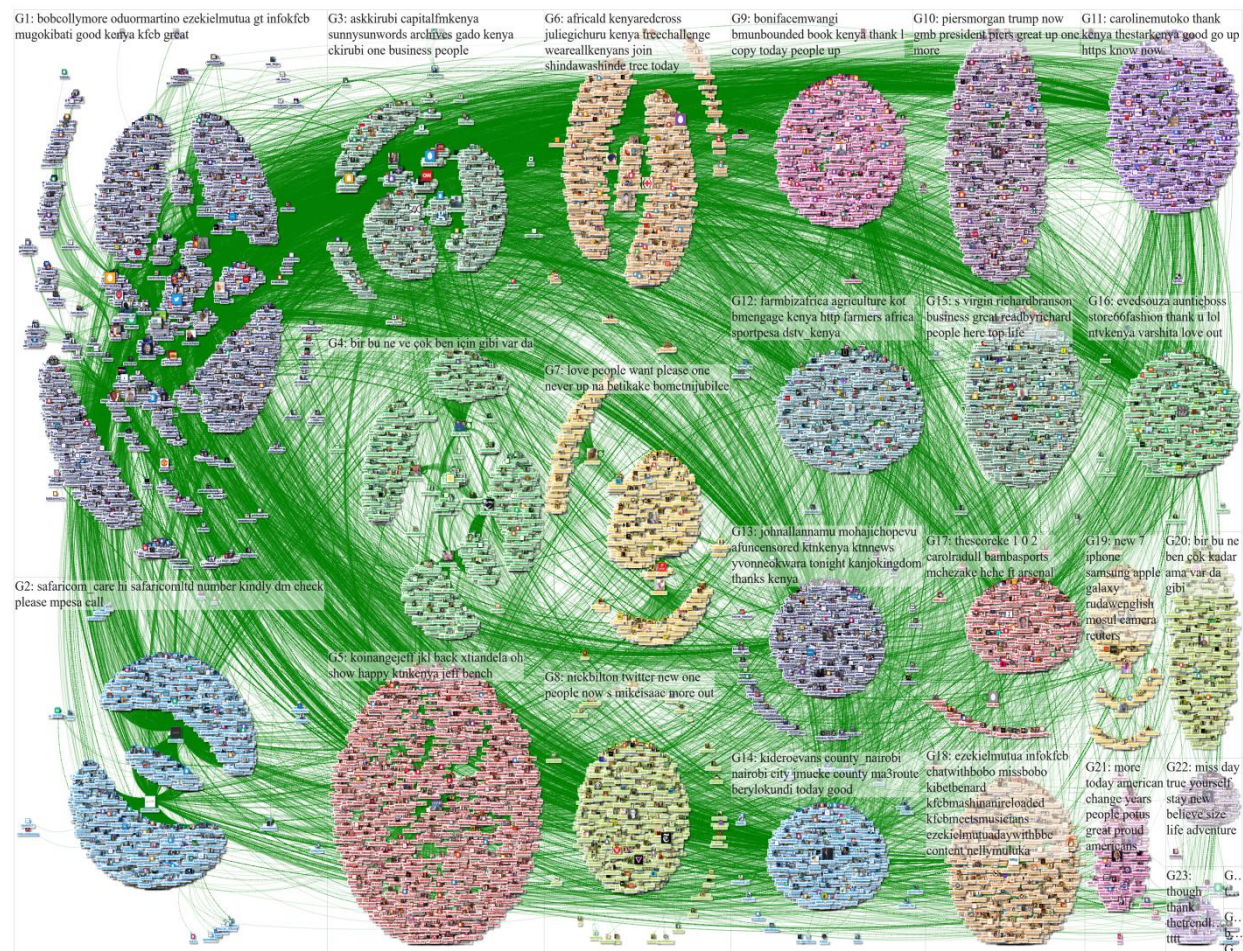


Figure 8: A 2.5 - degree Network Cliques

Source: *Researcher*

Identifying Significant Actors in a Network Using Centrality Metrics

Besides using visualisations to depict interesting patterns of interactions between respondents (actors) of the study, the researcher also employed use Social Network Analysis metrics as buttress of visualizations findings. In this section therefore, centrality measures which are be used to identify crucial actors with the values of closeness, betweenness, degree and eigenvector centralities were computed and tabulated. The network metrics generated has been used to describe either whole network or specific nodes within the network. It is also important to note that the number of vertices and edges kept on growing over time.

Conclusions

The study sought to answer and demonstrate how data obtained from individuals from specific social media can visualized or graph metrics computed as well as harvesting their demographic and related information can aid law enforcement agencies in mining forensic evidence that ultimately lead to arrest of the suspects or arraigning them before a court of law. Through analysis, study noted that there exist numerous ways and measures of determining people that have particular online prominence or influence. Visualizations and graph metric scores supplement one another in the study findings.

The visualizations were used to show fluid relations between nodes in the network and establish the structures of social network connections that exist instead of depending on theoretic or numeric values only. The use visual displays also aided in knowing that a community or network breaks into subgroups based on their interests and other information that captivates specific cohort(s). Thus, Social Network Analysis helps not only to investigate the suspicious characters, but also assist to unearth other dubious nodes that not under probe.

The findings of the study have indicated that the visualizations employed by social network analysis alongside its appropriate software can depict interesting information about the social media users interaction. It is believed that ways and means in which patterns of particular nodes were discovered using visualization will aid the law enforcement officers with ways and techniques of investigating and possibly apprehending online criminal.

Thus, when law enforcement officers employ Social Network Analysis automated tools or techniques to visualize and expose the nature of interactions or structures of suspected criminals using reliable online

information, they can remarkably help to stop them from unleashing their heinous acts to the unsuspecting populace. Thus, graph properties of the visualizations employed in this study helped the researcher to know not only the most central nodes in the network but also nodes that were most influential, popular and those who acted as bridges between subgroups of a network.

Recommendations made in the study are hoped to be of great help to the law enforcement agencies in understanding how to can mine, analyse and unearth concealed network elements and patterns between individuals in question. The study has broadened the knowledge on how to apply some Social Network Analysis techniques that is hoped to be of great help to the law enforcement agencies. Kenya's law enforcement community ought to be challenged to keep abreast both procedurally and legally by the findings of this study. Advanced degree of mining or harvesting data is significant with regards to the forensics evidence from social media users

In Kenya, the majority of members of law enforcement seems to unfamiliar with Social Network Analysis techniques and its associated tools for investigating online suspects. Kenya's law enforcement agencies should embrace the use of social media and social networking in various ways or applications, including recovering evidence, locating and apprehending suspects, conducting intelligence collections using social networking to conduct crime analysis and intelligence trend analysis. Hence, an enabling technology and trained law enforcement officers will help mitigate or thwart crimes about to be committed in real world. The outcomes of this thesis could influence law enforcement community by providing them with a new insight of investigation and analysing crimes from a large dataset.

The study also established the limitations of Social network Analysis which comprised of incomplete datasets, not knowing in advance whom to include or exclude and the fact that social network is dynamic and transcends geographical boundaries.

REFERENCES

1. Acquisti, A., Gross, R., & Stutzman, F. (2011). Faces of facebook: Privacy in the age of augmented reality.
2. Arnaboldi, V., Conti, M., Passarella, A., & Pezzoni, F. (2013, April). Ego networks intwitter: an experimental analysis. In *Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on* (pp. 229-234). IEEE.
3. Bonacich, P. (1972). Factoring and weighting approaches to status scores and clique identification. *Journal of Mathematical Sociology*, 2(1), 113-120.
4. Faust, K. (2006). Comparing social networks: size, density, and local structure. *Metodoloski zvezki*, 3(2), 185.
5. Faust, K., & Fitzhugh, S. (2012). Social Network Analysis: An Introduction. *Recuperado de: <https://www.icpsr.umich.edu/icpsrweb/sumprog/syllabi/97573> [Consulta: 2014, 12 de agosto]*.
6. Ferrara, E., De Meo, P., Catanese, S., & Fiumara, G. (2014). Visualizing criminal networks reconstructed from mobile phone records. *arXiv preprint arXiv:1407.2837*.

7. Global Justice Information Sharing Initiative.(2013).*Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities*. Guidance and Recommendations.
8. Granovetter, M. S. (1973). The strength of weak ties. *American journal of sociology*, 73 (6), 1360-1380.
9. Gupta, R., & Brooks, H. (2015).*Using Social media for global Security*. John Wiley & Sons Inc., Indianapolis.
10. Hanneman, R. A., & Riddle, M. (2005). Ego networks. *Introduction to Social Network Methods*. CA: Riverside. Analytictech. com.
11. Hansen, D., Shneiderman, B. & Smith, A.M. (2011). *Analyzing Social Media Networks With Nodexl: Insights From A Connected World*. Elsevier Inc., Massachusetts.
12. Hoppe, B., & Reinelt, C. (2010). Social network analysis and the evaluation of leadership networks. *The Leadership Quarterly*, 21(4), 600-619.
13. Kirchner, C., & Gade, J. (2011). Implementing social network analysis for fraud prevention. *CGI Group Ind*.
14. Long, J. C., Cunningham, F. C., & Braithwaite, J. (2013). Bridges, brokers and boundary spanners in collaborative networks: a systematic review. *BMC health services research*, 13(1), 158.
15. Passmore, D. L. (2011). Social network analysis: Theory and applications. *Institute for Research in Training & Development–IRTD*.
16. Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections*, 24(3), 43-52.
17. Martino, F., & Spoto, A. (2006). Social network analysis: A brief theoretical review and further perspectives in the study of information technology. *PsychNology Journal*, 4(1), 53-86.
18. Mena, J. (2003). *Investigative data mining for security and criminal detection*. Butterworth-Heinemann.
19. McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1), 415-444.
20. Mulazzani, M., Huber, M., & Weippl, E. (2012, January). Data visualization for social network forensics. In *IFIP International Conference on Digital Forensics* (pp. 115-126). Springer Berlin Heidelberg.
21. Murphy, J. P., & Fontecilla, A. (2013). Social media evidence in government investigations and criminal proceedings: A frontier of new legal issues. *Rich. JL & Tech.*, 19, 11-14.
22. Nagl, J. A., Amos, J. F., Sewall, S., & Petraeus, D. H. (2008). *The US Army/Marine Corps Counterinsurgency Field Manual*. University of Chicago Press.

კიბერუსაფრთხოების საერთაშორისო ინდექსები და საქართველო

INTERNATIONAL INDEXES OF CYBERSECURITY AND GEORGIA

ვლადიმერ სვანაძე საქართველოს ტექნიკური უნივერსიტეტის დოქტორანტი, საქართველოსტექნოლოგიური ინოვაციების აკადემიის დირექტორი

Vladimer Svanadze, Georgian Technical University PhD Candidate. Director of Georgian Academy of Technological Innovations

რეზიუმე: კიბერუსაფრთხოებამ მიუხედავად თავისი განვითარების მოკლე პერიოდისა, შეიძლება ითქვას დაიკავა ერთერთი მთავარი ადგილი როგორც საერთაშორისო, ისე ეროვნულ უსაფრთხოებაში, გახდა ჩვენი ცხოვრების განუყოფელი ნაწილი, და მნიშვნელოვანი კომპონენტი. ფაქტიურად, ყოველივე ეს განაპირობა ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფმა განვითარებამ, პანდემიის ფონზე ელექტრონული სერვისების მიმართ გლობალურად მზარდმა მოთხოვნილებამ. ყოველივე ეს კი ითხოვს ინტერნეტის სტაბილურობისა და უსაფრთხოების დაცვის აუცილებლობას, რაშიც ჩართული არის როგორც ცალკეული ქვეყნები, ისე საერთაშორისო და რეგიონალური ორგანიზაციები. შეიძლება ითქვას, რომ ცალკეული ქვეყნების კიბერსივრცის უსაფრთხოება ისეთივე მნიშვნელოვანი გახდა, როგორც ქვეყნის სახმელეთო, საჰაერო, თუ საზღვაო ტერიტორიების დაცვა, და რაც თავის მხრივ ხდება საერთაშორისო და რეგიონალური უსაფრთხოების შემადგენელი ნაწილი. ფაქტიურად, რაც უფრო დამოკიდებულია საზოგადოება თანამედროვე ტექნოლოგიებზე, მით უფრო მოწყვლადია კიბერ თავდასხმების მიმართ.

მსოფლიო ეკონომიკური ფორუმის 2021 წლის გლობალური რისკების ანგარიშის მიხედვით, კიბერსივრცეში არსებული რისკები კვლავ შედიან გლობალური რისკების რიცხვში. პანდემიამ COVID – 19 დააჩქარა ტექნოლოგიების დანერგვის პროცესი, თუმცა, გამოავლინა კიბერ სისუსტეები და არამზაობა. ამდროულად, გაამწვავა ტექნიკური უთანასწორობა როგორც საზოგადოებებს შორის გარედან, ისე მათ შიგნითაც.

იგივე ანგარიშის მიხედვით „მომავალ წელს ძალზედ მნიშვნელოვანია კიბერუსაფრთხოება განხილულ იქნეს, როგორც სტრატეგიული ბიზნეს - საკითხი და განვითარდეს მჭიდრო საპარტნიორო ურთიერთობები ინდუსტრიებს, ბიზნესის ლიდერებს, მარეგულირებელ ორგანოებსა და პოლიტიკოსებს შორის. ისევე, როგორც ნებისმიერი სხვა სტრატეგიული საზოგადოებრივი გამოწვევა, კიბერუსაფრთხოებაც ვერ მოგვარდება იზოლირებულად“.

საკვანძო სიტყვები: კიბერუსაფრთხოება, გლობალური ინდექსი, ეროვნული ინდექსი, განათლება, საერთაშორისო სატელეკომუნიკაციო კავშირი, ელექტრონული მმართველობის აკადემია, კიბერსივრცე

ABSTRACT: Despite its short period of development, cybersecurity has occupied one of the vital places in both international and national security; it has become an influential component and integral part of our lives. In fact, all these circumstances have been driven by the rapid evolvement of the Internet and Internet technologies, as well as the increasing global demand for e-services in the face of the pandemic. All above-mentioned determines the necessity for Internet stability and security with involvement of individual countries as well as international and regional organizations. It can be said that the cybersecurity of individual countries has become as important as the protection of the country land, air and sea and in turn it becomes an

integralTimes New Roman part of international and regional security. In fact, the more society relies on modern technology, the more vulnerable it is to cyber-attacks. According to the World Economic Forum 2021 Global Risks Report, cyber risks are still among the global risks. The COVID-19 pandemic has accelerated the implementation of technology, however, it revealed cyber vulnerabilities and unpreparedness. At the same time, it has exacerbated technical inequalities between societies both externally and internally. According to the same report, "next year, it is influential to consider cybersecurity as a strategic business issue and to develop close partnerships between industries, business leaders, regulators and politicians. Like any other strategic societal challenge, cybersecurity can't be solved separately in isolation." The paper offers the analysis of international indexes of cybersecurity and analyzes their correlation to Georgian ones.

KEYWORDS: *Cybersecurity, Global Index, National Index, Education, International Telecommunication Union, e – Governance Academy, Cyberspace*

კიბერუსაფრთხოების საკითხის აქტუალობისა და მისი მნიშვნელობიდან გამომდინარე უამრავი საერთაშორისო თუ რეგიონალური ორგანიზაცია ატარებს ერთმანეთისგან დამოუკიდებელ კვლევებს, რითაც აფასებენ კიბერუსაფრთხოების სფეროს მისი ცალკეული კომპონენტის მიხედვით. თუმცა უნდა აღინიშნოს, რომ მათ შორის ყველაზე რეიტინგულად, სანდოდ და კომპეტენტურად აღიარებული არის ორი ორგანიზაციის მიერ წარმოდგენილი კვლევები, კერძოდ:

- 1) გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის „საერთაშორისო სატელეკომუნიკაციო კავშირი/International Telecommunication Union (ITU)“, რომელიც ყოველწლიურად ატარებს გლობალურ კვლევას კიბერუსაფრთხოების განვითარების შესახებ, რაც შემდეგ აისახება ნაშრომში „კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index (GCI)“. ITU თავის კვლევას აწარმოებს უკვე თერთმეტი წელია და ყოველი წლის ივნისის თვეში აქვეყნებს წინა წლის კვლევის შედეგებს;
- 2) ესტონური ორგანიზაცია „ელექტრონული მმართველობის აკადემია/e – Governance Academy (eGA)“ ITU - ს მსგავსად eGA თავის კვლევას „ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)“ აწარმოებს კიბერუსაფრთხოების მიმართულებით, თუმცა არა გლობალურად არამედ ეროვნულ დონეზე ევროპის რეგიონის ქვეყნების მიხედვით და კვლევის შედეგებს აქვეყნებს ყოველი წლის სექტემბრის თვეში, ITU – „გლობალური კიბერუსაფრთხოების ინდექსის“ გამოქვეყნების შემდეგ.

მიუხედავად იმისა, რომ ITU - ს და eGA - ს მიერ კიბერუსაფრთხოების გლობალური ინდექსის შესაფასებლად განსხვავებული მეთოდოლოგიები იყო გამოყენებული, კვლევის შედეგები ძალიან ახლოს არის ერთმანეთთან. ორივე ორგანიზაციის კვლევის ფოკუსი, მიმართულია სახელმწიფოს კიბერუსაფრთხოების გაზომვად ასპექტებზე და კონცენტრირდება სახელმწიფოში არსებული საკანონმდებლო ბაზაზე, სტრატეგიაზე, სამთავრობო უწყებებზე და ა.შ. კვლევებში არ არის მოყვანილი ქვეყნებზე განხორციელებული და წარმატებით მოგერიებული კიბერ თავდასხმების მაგალითები, აქედან გამომდინარე, გარკვეულწილად კითხვის ნიშნის ქვეშ დგას სახელმწიფოს რეალური კიბერ თავდაცვითი პოტენციალი, თუმცა მოცემული ნაშრომის ფარგლებში, კიბერ უსაფრთხოების ასპექტების განხილვა ელექტრონული მმართველობის პერსპექტივიდან ხდება.

კიბერუსაფრთხოების გლობალური ინდექსი (GCI)

როგორც ზემოთ არის აღნიშნული „კიბერუსაფრთხოების გლობალური ინდექსი“ არის გაერო - ს ქვემდებარე სტრუქტურული ინსტიტუტის „საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU)“, უფრო კონკრეტულად, ინფორმაციულ და კომუნიკაციების ტექნოლოგიების სპეციალიზირებული სააგენტოს ინიციატივა. მოცემული პროექტი პირველად გაეშვა 2015 წელს, და მისი მიზანი არის გლობალურად შეაფასოს კიბერუსაფრთხოების მდგომარეობა. ის აჩვენებს აგრეთვე თუ რა მდგომარეობაა კიბერუსაფრთხოების მიმართულებით ცალკეულ ქვეყანაში, კიბერუსაფრთხოების კომპონენტებში თუ სად არიან წარმოდგენილი ძლიერად, სად უჭირთ, და სად შეიძლება მოხდეს კიბერშესაძლებლობების გაძლიერება. აგრეთვე, GCI - ით ხდება თითოეული ქვეყნის კიბერუსაფრთხოების მდგომარეობის ერთმანეთთან შედარება.

მიმდინარე წლის 29 ივნისს „საერთაშორისო სატელეკომუნიკაციო გაერთიანებამ (ITU)“ გამოაქვეყნა 2020 წლის „კიბერუსაფრთხოების გლობალური ინდექსი (GCI)“, რომელიც მოიცავს 194 სახელმწიფოს და კვლევა ტრადიციულად ხორციელდება ხუთი მიმართულებით, რაც მთლიანად აერთიანებს 20 კომპონენტს 82 კითხვით, კერძოდ:

- 1) **საკანონმდებლო ჩარჩოს მიმართულება** - კიბერკრიმინალის რეგულაცია; კიბერუსაფრთხოების რეგულაცია; ტრენინგები კიბერუსაფრთხოების სფეროში;
- 2) **ტექნიკური მიმართულება** - ეროვნული, სამთავრობო და სექტორული CERTები; სტანდარტები და სერტიფიკატები ორგანიზაციებისა და პროფესიონალებისთვის; ბავშვთა ონლაინ დაცულობა;
- 3) **ორგანიზაციული მიმართულება** - სტრატეგია; შესაბამისი სააგენტოები; კიბერუსაფრთხოების შეფასება;
- 4) **შესაძლებლობების განვითარება** - სტანდარტიზაციის ორგანოები; საუკეთესო პრაქტიკის კვლევის და განვითარების პროგრამები; საზოგადოების ცნობიერების ამაღლების კამპანიები; პროფესიონალთა ტრენინგ მოდულები; ეროვნული საგანმანათლებლო პროგრამები და აკადემიური სილაბუსები; წამახალისებელი მექანიზმები; კიბერუსაფრთხოების ადგილობრივი ინდუსტრია;
- 5) **თანამშრომლობის მიმართულება** - შიდა სახელმწიფოებრივი თანამშრომლობა; მრავალმხრივი შეთანხმებები; საერთაშორისო ხელშეკრულებებში მონაწილეობა; კერძო-საჯარო პარტნიორობა; უწყებათაშორისი თანამშრომლობა.

2020 წლის GCI - ში კვლევაში ჩართული იყო 169 მკვლევარი და ის მიმდინარეობდა, როგორც გლობალური გამოწვევების კუთხით, ისე რეგიონებისა და ქვეყნების მიხედვით. ITU - ს სტანდარტებით, რეგიონალური დაყოფა წარმოდგენილია შემდეგნაირად - აფრიკის რეგიონი, ამერიკის რეგიონი, არაბეთის სახელმწიფოების რეგიონი, აზია - ოკეანეთის რეგიონი, ევროპა და დსთ - ს ქვეყნები.

ბოლო ინდექსის ფარგლებში ჩატარებული კვლევის შედეგების მიხედვით, კვლევაში მონაწილე პირველი 25 ქვეყნის ქულები და რეიტინგი მოცემული არის ქვემოთ მოყვანილ ცხრილში

ქვეყანა	ქულა	რეიტინგი
შერთებული შტატები	100	1
დიდი ბრიტანეთი	99.54	2
საუდის არაბეთი	99.54	2
ესტონეთი	99.48	3
სამხრეთ კორეის რესპუბლიკა	98.52	4

სინგაპური	98.52	4
ესპანეთი	98.52	4
რუსეთის ფედერაცია	98.06	5
არაბეთის გაერთიანებული საემიროები	98.06	5
მალაზია	98.06	5
ლიეტუვა	97.93	6
იაპონია	97.82	7
კანადა	97.67	8
საფრანგეთი	97.6	9
ინდოეთი	97.5	10
თურქეთი	97.49	11
ავსტრალია	97.47	12
ლუქსემბურგი	97.41	13
გერმანია	97.41	13
პორტუგალია	97.32	14
ლატვია	97.28	15
ნიდერლანდები	97.05	16
ნორვეგია	96.89	17
მავრიკის რესპუბლიკა	96.89	17
ბრაზილია	96.6	18

წყარო: კიბერუსაფრთხოების გლობალური ინდექსი GCI 2020

კიბერუსაფრთხოების ეროვნული ინდექსი (NCSI)

როგორც აღინიშნა, კიბერუსაფრთხოების გლობალური კვლევის მეორე მნიშვნელოვან დოკუმენტსწარმოადგენს ესტონური ორგანიზაცია „ელექტრონული მმართველობის აკადემიის (eGA)“ მიერჩატარებული კვლევა „კიბერუსაფრთხოების ეროვნული ინდექსი“ (National CyberSecurity Index- NCSI), რომელიც ზომავს ქვეყნების მზაობას კიბერ საფრთხეების დაინციდენტების წინაშე. მოცემული კვლევა ფარავს შემდეგიმართულეებს:

- 1) **კანონმდებლობა** - საკანონმდებლო აქტები; რეგულაციები; განკარგულებები;
- 2) **ორგანიზაციული** - არსებული სააგენტოები; ორგანიზაციები; CERT;
- 3) **თანამშრომლობა** - კომიტეტები; საბჭოები; სამუშაო ჯგუფები;
- 4) **შედეგები/პროდუქტები** - სამთავრობო პოლიტიკა; ტექნოლოგიები; ვებგვერდები; პროგრამები; აპლიკაციები.

მთლიანობაში, კვლევის ფარგლებში სახელმწიფოში არსებული კიბერთავდაცვითი პოტენციალი, 46 ინდიკატორის მიხედვით, 12 განზომილებაში იზომება და შედეგების მიხედვით დგინდება სახელმწიფოს კიბერუსაფრთხოების ინდექსი, კერძოდ:

- ელ - იდენტიფიკაცია და სერვისების;
- პერსონალურ მონაცემთა დაცვა;
- კიბერ ინციდენტებზე რეაგირება;
- კიბერ კრიზისების მართვა;
- კიბერ დანაშაულთან ბრძოლა;
- სამსხდრო კიბერ ოპერაციები;

- კიბერუსაფრთხოების პოლიტიკის განვითარება;
- კიბერ საფრთხეების ანალიზი ;
- განათლება და პროფესიული განვითარება;
- წვლილი გლობალურ კიბერ უსაფრთხოებაში;
- ელ - სერვისების დაცვა;
- კრიტიკული ინფორმაციული ობიექტების დაცვა.

განათლება და კიბერუსაფრთხოება

აღსანიშნავია ის გარემოება, რომ კიბერუსაფრთხოების ორივე ინდექსში, გლობალურშიც და ეროვნულშიც, მოყვანილი კიბერშესაძლებლობების განვითარება თავის თავში მოიცავს ისეთ მნიშვნელოვან კომპონენტს როგორც არის განათლება და პროფესიული განვითარება. ფაქტიურად, განათლება და პროფესიული განვითარება არის ის აუცილებელი მიმართულება, რომლის განვითარებაზეც ზრუნავს ყველა ქვეყანა. კერძოდ, კიბერუსაფრთხოების შესახებ განათლების ზრდის ხელშეწყობა და ცნობიერების გაზრდა ქვეყნებისთვის იმდენად პრიორიტეტულ და მნიშვნელოვან მიმართულებას წარმოადგენს, რომ ის შეყვანილი არის თითოეული ქვეყნის კიბერუსაფრთხოების ეროვნულ სტრატეგიებში. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2017 – 2018 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა“ არის გამონაკლისი, სადაც მოცემული მიმართულება მოხსენიებულია როგორც ერთ - ერთი ძირითადი მიმართულება, კერძოდ:

1. კვლევა და ანალიზი;
2. სამართლებრივი ბაზის შემუშავება და სრულყოფა;
3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება;
4. საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის შექმნა;
5. საერთაშორისო თანამშრომლობა.

უნდა ითქვას, რომ სტრატეგიებში განათლების სფეროს ასახვა ნათლად აჩვენებს ქვეყნების დიდ ინტერესს განავითარონ თავიანთი კიბერუსაფრთხოებითი შესაძლებლობა, რაც პირდაპირ კავშირშია პროფესიული და კვალიფიციური ადამიანური რესურსის არსებობასთან. აქვე ცალკე აღსანიშნავია ის გარემოებაც, რომ სტრატეგიებში მოცემული კიბერუსაფრთხოების ძირითადი მიმართულებები, იქნება ეს კვლევა და ანალიზი, საერთაშორისო თანამშრომლობა, სამართლებრივ ბაზებზე მუშაობა და მისი განვითარება, თუ თავად კიბერუსაფრთხოების სფეროს შესაძლებლობების განვითარება და საზოგადოებრივი ცნობიერების ამაღლება, პირდაპირ კავშირშია სწორად დაგეგმილი და ძლიერი საგანმანათლებლო ბაზის განვითარებასთან, რადგან სტრატეგიის ყველა ჩამოთვლილი მიმართულება მოითხოვს კვალიფიციურ კადრს.

როცა ვსაუბრობთ კვალიფიციურ კადრზე იგულისხმება აკადემიური განათლების მქონე პირები, რომლებსაც მიღებული აქვთ სულ ცოტა ბაკალავრის აკადემიური ხარისხი. გარდა ამისა, არსებობს საერთაშორისო დონეზე აღიარებული სერტიფიცირებული კურსები, თუმცა მათი უმრავლესობა კონკრეტული მიმართულებით ითხოვს საბაზისო ცოდნას, რაც შესაბამისობაშია ბაკალავრის დონესთან. ასევე დამსაქმებელთა დიდი ნაწილი ვაკანტური ადგილის დასაკავებელი კონკურსის მოთხოვნების განათლების სექციაში პირდაპირ უთითებენ მინიმუმ ბაკალავრის დონეს. შესაძლებელია კიდევ ბევრი მაგალითის მოყვანა, თუმცა ეს ორი ერთმანეთისგან განსხვავებული მაგალითი პირდაპირ მიუთითებს კიბერუსაფრთხოების სფეროში აკადემიური განათლების მნიშვნელობაზე. აქვე თუ

დავამატებთ იმ ფაქტს, რომ გლობალურად კიბერუსაფრთხოების სპეციალისტთა აშკარა დეფიციტია, ხოლო მათზე მოთხოვნილება სულ უფრო იზრდება, მაშინ შეიძლება ითქვას, რომ ეს იქნება უახლესი მომავლის ერთ - ერთი მოთხოვნადი სპეციალობა. აგრეთვე, თუ გავითვალისწინებთ ასეთ მზარდ მოთხოვნილებას, თავისუფლად შეიძლება ითქვას, რომ მოცემული მიმართულების სპეციალისტების შრომითი ანაზღაურება არის საკმაოდ მაღალი. კერძოდ, მაგალითისთვის, <https://www.payscale.com/> - ის მიხედვით, უსაფრთხოების ოპერაციების ცენტრის (Security Operations Center SOC) დამწყები ანალიტიკოსის წლიური ხელფასი 81,351 აშშ დოლარს შეადგენს. იგივე წყაროს ინფორმაციით, საკმაოდ მაღალანაზღაურებადი არის ისეთი სპეციალობები როგორებიც არის:

- Penetration Tester;
- Information Security Analyst;
- Security Analyst;
- Ethical Hacker.

ჩამოთვლილი სპეციალობების საშუალო წლიური ანაზღაურება დაახლოებით 83,968 აშშ დოლარს შეადგენს. ალბათ ყველაზე უფრო გასათვალისწინებელი ფაქტი არის ის, რომ მოცემული სპეციალობების ხალხის დასაქმება სირთულეს არ წარმოადგენს და საერთაშორისო და ადგილობრივ ბაზარზე ძნელად თუ მოიძებნება მოცემული სპეციალობების კარგი და კვალიფიციური კადრები. ამიტომ, შეიძლება ითქვას, რომ კიბერუსაფრთხოების მიმართულებით მაღალი დონის განათლების მიღებაში ფინანსური საშუალებების „დაბანდება“ საკმაოდ წარმატებულ ინვესტირებას უნდა წარმოადგენდეს.

განვითარებად ქვეყნებში კიბერუსაფრთხოების მიმართულებით განათლების განვითარების პროცესი არათანმიმდევრულად და რთულად მიმდინარეობს, ხოლო ხშირ შემთხვევაში ეს პროცესი საერთოდ არ არსებობს, ან თუ არსებობს საერთოდ არის მოწყვეტილი დარგის განვითარებისა და მისი მდგრადობის შენარჩუნებასთან. გამონაკლისს არ წარმოადგენს არც საქართველო. შეიძლება თამამად ითქვას, რომ საქართველოში კიბერუსაფრთხოების მიმართულებით აკადემიურ დონეზე განათლება საერთოდ არ არსებობს, არის მხოლოდ სხვადასხვა უნივერსიტეტებში არსებული ცალკეული მოდულები. ქვეყანაში არ არის საბაკალავრო და სამაგისტრო პროგრამები, როცა საქართველოს კიბერსივრცე, კრიტიკული ინფრასტრუქტურა დგას გლობალურად არსებული სულ უფრო ახალი გამოწვევების წინაშე.

ფაქტიურად, შეიძლება ითქვას, რომ კიბერუსაფრთხოების განვითარებისა და მდგრადობის შენარჩუნებისთვის მის ყველა ცალკეულ მიმართულებაზე, აუცილებელი არის შესაბამისი განათლებული და კვალიფიციური კადრების არსებობა, რაც თავის მხრივ უზრუნველყოფს კრიტიკული ინფრასტრუქტურის დაცულობის გაზრდას როგორც გლობალურ, ისე ეროვნულ დონეზე.

საქართველო და კიბერუსაფრთხოების საერთაშორისო ინდექსები

ზემოთ წარმოდგენილი ორგანიზაციების მიერ ყოველწლიურად ხდება საქართველოს კიბერშესაძლებლობების შეფასება. შეიძლება ითქვას, რომ საქართველოსთვის კიბერუსაფრთხოების სფეროში ყველაზე წარმატებული იყო 2017 წელი, როცა ITU - ს „გლობალური კიბერუსაფრთხოების ინდექსის (GCI)“ მიხედვით, ქვეყანამ გლობალურ რეიტინგში დაიკავა მე - 8 ადგილი, ევროპის რეგიონში ასევე მე - 8 ადგილი, ხოლო დსთ - ს ქვეყნებს შორის პირველი ადგილი. ქვემოთ ცხრილში მოცემულია საქართველოს შეფასებები კვლევითი კომპონენტების მიხედვით -

Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 56-66 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

სამართლებრივი, ტექნიკური, ორგანიზაციული, შესაძლებლობებისა და თანამშრომლობის განვითარება.

ქვეყანა	GCI ქულა	სამართლებრივი	ტექნიკური	ორგანიზაციული	შესაძლებლობების განვითარება	თანამშრომლობა
სინგაპური	0.92	0.95	0.96	0.88	0.97	0.87
შვედეთული შტატები	0.91	1	0.96	0.92	1	0.73
მაღაზია	0.89	0.87	0.96	0.77	1	0.87
ომანი	0.87	0.98	0.82	0.85	0.95	0.75
ესტონეთი	0.84	0.99	0.82	0.85	0.94	0.64
მავრიკის რესპუბლიკა	0.82	0.85	0.96	0.74	0.91	0.70
ავსტრალია	0.82	0.94	0.96	0.86	0.94	0.44
საქართველო	0.81	0.91	0.77	0.82	0.90	0.70
საფრანგეთი	0.81	0.94	0.96	0.60	1	0.61
კანადა	0.81	0.94	0.93	0.71	0.82	0.70

წყარო: კიბერუსაფრთხოების გლობალური ინდექსი GCI 2017

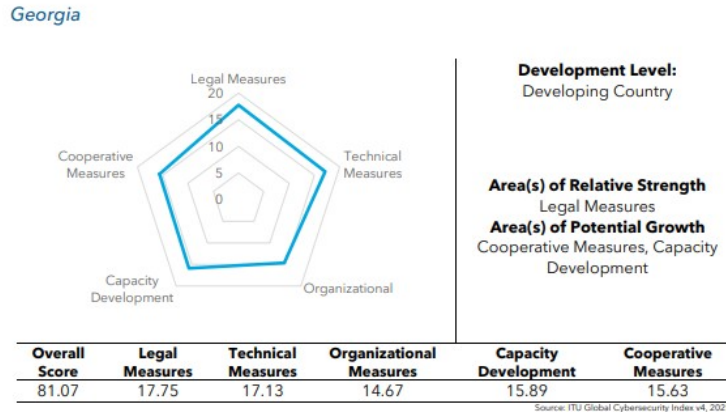
იმავე წელს eGA - ს მიერ გამოქვეყნებული კვლევის შედეგების მიხედვით საქართველომ ევროპის რეგიონში დაიკავა მეორე ადგილი, რაც ქვეყნისთვის საკმაოდ დიდი მიღწევა იყო (იხ. ქვემოთ მოყვანილი ცხრილი).

ქვეყანა	ქულა	რეიტინგი
ჩეხეთის რესპუბლიკა	72.73	1
საქართველო	65.66	2
ლიეტუვა	65.15	3

ბელორუსია	59.09	4
უკრაინა	56.06	5
მოლდოვა	42.42	6
ლატვია	41.92	7

წყარო: კიბერუსაფრთხოების ეროვნული ინდექსი *NCSI 2017*

აღსანიშნავია, რომ 2019 წელს ITU - მ გამოაქვეყნა კიბერუსაფრთხოებისგანახლებული კვლევა, რომლის მიხედვითაც ადგილობრივი ექსპერტები, 153კითხვის ნაცვლად, 50 ასპექტის მიხედვით აფასებდნენ ქვეყანაში არსებულ კიბერუსაფრთხოების გარემოს. აღნიშნული დოკუმენტის მიხედვით, 0.85 ქულით, საქართველომ ევროპაში მეცხრე, ხოლო მსოფლიოში 18 - ადგილი დაიკავა. თავის მხრივ, 2018 წელს eGA - ს მიერ ჩატარებული კვლევის შედეგების მიხედვით თანახმად, საქართველომ 64.9 ქულით, სიაში 19 - ე ადგილი დაიკავა. 2020 წლის GCI - ის მიხედვით, საქართველოს კიბერშესაძლებლობები კიდევ უფრო გაუარესდა, კერძოდ, ქვეყანამ 81.06 ქულით გლობალურ რეიტინგში დაიკავა 55 - ე ადგილი, ხოლო 81.07 ქულით ევროპის რეგიონის რეიტინგში 30 - ე ადგილი. ქვემოთ ნახატზე მოცემულია GCI - ის მიერ შეფასებული საქართველოს კიბერშესაძლებლობა 2020 წლისთვის თავისი ყველა ხუთი მიმართულებითა და შემადგენელი კომპონენტებით.



წყარო: კიბერუსაფრთხოების გლობალური ინდექსი *GCI 2020*

მოცემულ ნახატზე ნათლად ჩანს, რომ საქართველოს კიბერუსაფრთხოების კომპონენტები და ქულები ხუთივე მიმართულებით შემცირებულია, კერძოდ:

1. იურიდიულ - სამართლებრივი - 17.75
2. ტექნიკური შესაძლებლობები - 17.13
3. ორგანიზაციული განვითარება - 14.67
4. შესაძლებლობების განვითარება - 15.89
5. თანამშრომლობის განვითარება - 15.63

ფაქტიურად, საქართველოს კიბერუსაფრთხოება 2017 წლიდან ნაცვლად გაუმჯობესებისა, წავიდა გაუარესებისკენ, რისი მიზეზიც არის ამჟამად დარგის ყველა მიმართულებით არსებული სტაგნაციური მდგომარეობა. ქვეყნის წარმატების

მიზეზად, რამაც 2017 წელს ასახვა ჰპოვა საერთაშორისო კიბერუსაფრთხოების ინდექსებში, შეიძლება მოვიყვანოთ ის ფაქტები, რომ საქართველომ მოკლე დროში შეძლო:

1. იურიდიულ - სამართლებრივი და ნორმატიული ბაზის მოწყობა, კერძოდ:
 - მიიღეს „კანონი ინფორმაციული უსაფრთხოების შესახებ“ (2012);
 - დაიწერა კიბერუსაფრთხოების ორი სტრატეგია და სამოქმედო გეგმა (2013 – 2015 და 2017 - 2018);
 - განისაზღვრა კრიტიკული ინფრასტრუქტურის სუბიექტები (2013);
 - მიიღეს კანონი „პერსონალური მონაცემების შესახებ“ (2013);
2. ქვეყანა შეუერთდა ბუდაპეშტის კიბერდანაშაულის კონვენციას (2012);
3. შსს - შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო (2012);
4. შეიქმნა პერსონალური მონაცემების დაცვის ინსპექტორის ოფისი (2013);
5. თავდაცვის სფერო საერთოდ გამოეყო სამოქალაქო სფეროს და თავდაცვის სამინისტროში შეიქმნა „სსიპ - კიბერუსაფრთხოების ბიურო“ (2014), რაც იყო დიდი წარმატება და აუცილებელი მოვლენა ქვეყნის კიბერუსაფრთხოების მიმართულებით.

დასკვნა

ბოლოში დასკვნის სახით შეიძლება ითქვას, რომ სახელმწიფოებში და ზოგადად გლობალურად კიბერუსაფრთხოების მდგომარეობის შეფასება ხდება ისეთი ორგანიზაციების მიერ, რომელთა სანდოობა და რეპუტაცია არის მაღალი. ჩვენს შემთხვევაში საუბარია მაღალი დონის ისეთ სანდო და რეპუტაციულ ორგანიზაციებზე, როგორებიცაა:

- 1) გაეროს ქვემდებარესტრუქტურული ინსტიტუტის „საერთაშორისო სატელეკომუნიკაციო კავშირი/International Telecommunication Union (ITU)“, რომელიც ყოველწლიურად ატარებს გლობალურ კვლევას კიბერუსაფრთხოების განვითარების შესახებ, რაც შემდეგ იხსნება ანაშრომში „კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index (GCI)“. ITU თავის კვლევას აწარმოებს უკვე თერთმეტი წელია და ყოველწლიურ ინსტიტუტის თვეში აქვეყნებს წინაწლის კვლევის შედეგებს;
- 2) ესტონური ორგანიზაცია „ელექტრონული მმართველობის აკადემია/e – Governance Academy (eGA)“ ITU - ს მსგავსად eGA თავის კვლევას „ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)“ აწარმოებს კიბერუსაფრთხოების მიმართულებით, თუმცა არა გლობალურად არამედ ეროვნულ დონეზე ევროპის რეგიონის ქვეყნების მიხედვით და კვლევის შედეგებს აქვეყნებს ყოველწლიურ სექტემბრის სთვეში, ITU – „გლობალური კიბერუსაფრთხოების ინდექსის“ გამოქვეყნების შემდეგ.

უნდა ითქვას, რომ ორივე ინდექსი ასახავს კიბერუსაფრთხოების მიმართულებით არსებულ მაქსიმალურად რეალურ სურათს, რომლის შეფასება მოიცავს დარგის ყველა მიმართულებასა და მის შემადგენელ კომპონენტებს, კერძოდ:

1. **საკანონმდებლო ჩარჩოს მიმართულება** -
კიბერკრიმინალის რეგულაცია; კიბერუსაფრთხოების რეგულაცია;
ტრენინგები კიბერუსაფრთხოების სფეროში;

2. **ტექნიკური მიმართულება** - ეროვნული, სამთავრობო და სექტორული CERTები;
სტანდარტები და სერტიფიკატები ორგანიზაციებისა და პროფესიონალებისთვის; ბავშვთა ონლაინ დაცულობა;
3. **ორგანიზაციული მიმართულება** - სტრატეგია; შესაბამისი სააგენტოები; კიბერუსაფრთხოების შეფასება;
4. **შესაძლებლობების განვითარება** - სტანდარტიზაციის ორგანოები; საუკეთესო პრაქტიკის კვლევის და განვითარების პროგრამები; საზოგადოების ცნობიერების სამალღობის კამპანიები; პროფესიონალთა ტრენინგ მოდულები; ეროვნული საგანმანათლებლო პროგრამები და აკადემიური სილაბუსები; წამახალისებელი მექანიზმები; კიბერუსაფრთხოების სადგილობრივი ინდუსტრია;
5. **თანამშრომლობის მიმართულება** -
შიდასახელმწიფოებრივი თანამშრომლობა; მრავალმხრივი შეთანხმებები; საერთაშორისო ხელშეკრულებებში მონაწილეობა; კერძო-საჯარო პარტნიორობა; უწყებათაშორისი თანამშრომლობა.

წინამდებარე ნაშრომში ცალკე არის გამოყოფილი განათლების მნიშვნელობა კიბერუსაფრთხოების სფეროში, რადგან ეს არის ის შემადგენელი კომპონენტი, რომლის მიხედვითაც ახდენს შეფასებას ორივე გლობალური და ეროვნული ინდექსი. ამის მთავარი მიზეზი არის ის გარემოება, რომ კიბერუსაფრთხოების დარგი მოითხოვს მაღალკვალიფიციურ აკადემიური დონის კადრებს და ამიტომაც ხდება მოცემული მიმართულებით საგანმანათლებლო პროგრამების განვითარება საბაკალავრო და სამაგისტრო დონეებზე. გარდა ამისა, ხდება აკადემიური კვლევების კომპონენტების განვითარება. ამ კუთხით სავალალო მდგომარეობაა საქართველოში, სადაც არ არსებობს არც ბაკალავრიატი და არც მაგისტრატურა, არ ტარდება კვლევები და ფაქტიურად, მოცემული მიმართულებით დარღვეული არის კავშირი საჯარო სექტორსა და აკადემიურ წრეებს შორის, როცა ამ უკანასკნელისთვის შეიძლება თავად სახელმწიფო ყოფილიყო დამკვეთი მისთვის აუცილებელი კადრების მომზადებასა და გადაამზადებაში. არ შეიძლება არ აღინიშნოს ასევე თანამშრომლობის აუცილებლობა სამეცნიერო კვლევების ჩატარების მიმართულებითაც, რაც დღეს ფაქტიურად საერთოდ მოშლილია და არ ტარდება აკადემიური დონის სამეცნიერო კვლევითი საქმიანობა.

ბიბლიოგრაფია

1. The Global Risks Report 2021, 16th Edition of the World Economic Forum, In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 19 January, 2021 <https://www.weforum.org/reports/the-global-risks-report-2021>;
2. ვლადიმერ ნაფეტვარიძე, ელექტრონული მმართველობის დანერგვა საქართველოში: პრობლემები და პერსპექტივები, 2020;
3. ვლადიმერ სვანაძე „განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში“, 2021;
4. e – Governance Academy <https://ega.ee/projects/?programme=cyber-security>;
5. ვლადიმერ სვანაძე, ანდრია გოცირიძე "კიბერ თავდაცვა: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული)", 2016;

Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 56-66 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

6. GUIDE TO GOOD GOVERNANCE IN CYBERSECURITY, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 January, 2021 https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf;
7. <https://www.cybrary.it/>.
8. M. Iavich, S. Gnatyuk, G. Iashvili, A. Fesenko. Cyber security European standards in business. Scientific and Practical Cyber Security Journal (SPCSJ), 3(2):36-39, 2019