Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education

Milos Tisma[131]
Jasmina Andric[132]

Abstract

Everyday use of information and communication technologies by the global society that was accelerated by the virus COVID-19 pandemic has led to a drastic increase in the number of cyber-attacks, frauds and other security threats in cyberspace. Society as a whole has faced lack of cyber security professionals, low knowledge of threats in the cyber spaces and depths of the web with no existence of effective way of gathering cyber security intelligence and informing and warning the public on the threats.

This paper will present the possibilities of boosting information security and cyber security awareness in the education and e-learning that will motivate future cyber security professionals to take their career path. We will also preview how we can use information on cyber-attacks and with machine learning models for security analytics that will contribute to better understanding of threats and threat intelligence. The aim of this paper is to show the possibilities of cyber security education and importance of awareness on the security threats in the process of reshaping the education. Paper should provide an overview of current state in cyber security area and technologies in this area as well as a proposal for the possible development of cyber security educational strategies based on machine learning and security analytics models.

Keywords: Security, cyber security, information security, security analytics, threat intelligence, e-learning, machine learning

1.Introduction

Everyday use of information and communication technologies by the global society that was accelerated by the virus COVID-19 pandemic has led to a drastic increase in the number of cyber-attacks, frauds and other security threats in cyberspace. There are problems that the global community is facing and some of them are:

[131] MSc, milos.tisma@istrazivackicentarob.com, Research Centre for Defence and Security, Republic of Serbia

[132] PhD Candidate, jasmina.andric@istrazivackicentarob.com, Military Academy, University of Defence, Republic of Serbia

- Society as a whole has faced lack of cyber security professionals,
- low knowledge of threats in the cyber spaces and depths of the web,
- no existence of effective way of gathering cyber security intelligence and informing and warning the public on the threats,
- there is a large use of multiple terms related to security in I(C)T that can bring confusion to public as well to the potential candidates that would take career path in these areas.

There is average of 40 000 000 cyber-attacks daily and 82% of employers report a lack of cybersecurity skills, 61% of companies feel that their cybersecurity candidates are not qualified, 66% of cybersecurity professionals struggle to define their career paths, 60% of cybersecurity professionals are dissatisfied with their current job. These data were presented by ISSA17, which conducted this research. In addition, the unemployment rate in cyber security is estimated to be 0% and is projected to remain there until end of 2021 when it is projected that there will be 3.5 million vacancies in cyber security globally [1].

As solution of this problems, we the possibilities of cyber security education and importance of awareness on the security threats in the process of reshaping the education. We will give and brief overview of current state in cyber security area and technologies in this area as well as a proposal for the possible development of cyber security educational strategies based on machine learning and security analytics models.

2. Definition of basic terms

As we need to view current state in the area of cyber security, we need to define some of the basic terms as it follows:

The example of definition that we use for cyber security is IT security that emphasizes on providing computer networks, data, programs, and computers from unauthorized or unwanted variation, loss, changes, or access [2]. The elements that are binding to cyber security are protection, provision of unauthorized entry, loss of assets, changing content, illegal activities, information systems, technology, hardware (machines, computers, media ...) and other systems that depend on information, data and software. What we recognize in these definitions is that the accent of cyber security is placed on cyber space and systems dependent on information, while events and actors in the real world are in another plan.

Information security also has a wide range of understanding, so many theorists start from CIA (confidentiality, integrity, availability) and AA (appropriate access) definition -CIA: some information I am sure if, only if all parts of me keep the confidentiality, integrity properties availability. AA: The facility is safe for the role holder H if and only if: for each agent A and each part of P of O and has only an appropriate approach to preletive H. [3]. Unlike cyber security, the security of information refers to information in any form, treating them as assets, with three pillars related to confidentiality, integrity and availability. So that information is engaged in real world and cyberspace, with an emphasis that they are only available to those who are intended, which is also the main task of information security, to protect information from its creation to its destruction or if become obsolete.

I(C)T security- Security of information and communication technologies are most binding to the safety of critical infrastructures of countries and includes the intersection of information and cyber security. Its definitions are all those used in information security definitions and cyber security with the addition of critical part of the area they protect. For example The Law on Information Security of the Republic of Serbia has been adopted to protect state against security risks in information and communication systems, and under them implies (1) electronic communication networks in terms of law regulating electronic communications; (2) Devices or groups of interconnected devices, such as in the device, ie within at least one from the device group, automatic data processing using a computer program; (3) data that is kept, stored, processed, searching, or transmitted funds from the under case. (1) and (2) of these points, and for the purpose of their work, use, protection or maintenance; (4) organizational structure through the ICT system; (5) all types of systemic and application software and software development tools; [4] We see that ICT security protects the state and its citizens.

Threat Intelligence- Cyber threat hunting is the activity of cyber security and active defenses. It is a "process of proactive and iTerative search through networks to detect and isolate advanced threats that avoid existing security solutions"[5]. This is unlike traditional threat management measures, such as fivers, intrusion detection systems, sandy software and Siem systems, which usually include evidence-based data on the potential danger. Intelligence work on threats[6] plays an incredibly important role as a component of cyber security. It provides vital information for use in security analytics, then this information can help identify and determine the priorities of suspicious activity. It also helps security administrators in quality intelligence by providing insight into the history of certain IP addresses, domain names, etc. The same information can be invaluable to respond to the threat management component. Security administrators can use intelligence on threats to learn more about nature and the threat they are investigating. Organizations are increasingly using intelligence on threats from a third party to improve their ability to manage threats as well as other aspects of their security. For example, one of the most common use of performance intelligence sources is improving the accuracy of discovering and determining the priorities of Siem technology. Whether information on threats come into an organization through Siem or other route, it is important that it is connected by automated means with an organizational safety intelligence and analytical platform. Connecting allows you to fully integrate with other related to threats of information that organizations provide better insight into the nature of suspicious activities that include their systems and networks.

Intelligence - The term Intelligence means the entire process of intelligence activity, intelligence, counter-intelligence activities and secret actions, subversive effects. It concludes that in modern intelligence theory, the understanding of the notion of intelligence unites everything that in some other countries calls the forms of intelligence services, i.e. special activities of intelligence services [7]. Intelligence services and their work in the literature would be a "organized activity or organization, at the request and intentional political forces, assesses the leading classes of class or state, protects their own interests from opponents and engages On other activities that contribute to the realization of certain political goals "[8]. As we see intelligence or intelligence, which under the guidance of management-management, attracts, analyzes and interprets the information on the other party's intentions (enemy, competitor, etc.) to prepare the rest of the system to react, increase resilience Resilience), save the answer and protect your interests on time and thus prevented an attack or some other type of malicious activity, plotting the normal functioning and development of the system.

Data Science - Data Science is defined as use of scientific methods to obtain useful information from data, especially large amounts of data set (data set is aggregated data from a particular database that can be used for various purposes, and we will use it for research purposes.)

By defining what is what and how to use state of the art tools is crucial in rising capacities of human resources with non-formal education and e-learning. It will also help in motivating students or junior cyber security officers to take the career path if they better understand the importance of their work. Work in the scientific field is also needed and defining basic terms globally will contribute to development of science. A lot of experience is needed for one to become a cyber security expert and one of the key elements is constant education and learning, of which e-learning is one of the main points where this can be done, especially in the crisis times (Covid, disasters etc.)

3. Cyber security awareness, human resources and education

As we have already mentioned, in a large number of researches, people are marked as the weakest actors of the systems that defends (cyber security) and are used by systems that attack (hackers, states etc.), while in addition the professional staff in cyber security is in absolute deficiency. Demand for cyber security professionals continues to grow together with the attack number (official statistics more companies say that cyber-attack occurs every 39 seconds or 2244 times a day) and by increasing the actor’s budget. The imbalance of the number of qualified workers in cyber security degrades the lack of framework and social security skills. Anyone who wants to hire cyber security professionals is in a problem because their deficit has already given results through the numbers of successful attacks during Covid-19 pandemics. To make a new professional, the strategy and will of all actors for the training of people for cyber security with educational, research and military institutions and professional associations are launched by the sharing practices, training and knowledge transfers to find new talents. A good step and example of this is the launch of a project by several universities in Serbia called, Information Security Services Education in Serbia – ISSES, which with support of the EU needs to develop a Curriculum for Master Studies that needs to deal with cyber-security [9]. Under this program there were competitions, hackathons, e-learning and other activities that were on-line and that engaged students and participants.

It is assumed that about 500,000 data protection officers were employed only in the EU since the implementation of GDPR. For example, this is an excellent opportunity that Serbia is currently using to build a new generation of specialist in cyber security. There are master programs developed specifically for the industry needs, that were initiated by the government of Serbia and started the project Master 4.0[10]. This programs also showed how people are easily engaged with e-learning and can boost their knowledge, and many people used this opportunity due to COVID-19 pandemic and restrictions imposed for health reasons.

Research Centre for Defence and Security [11] also had experience with raising awareness on cyber and information security through trainings and practice that was organized on faculties. Students tended to be very active and engaging in practical workshops and using tools over distance learning platforms.

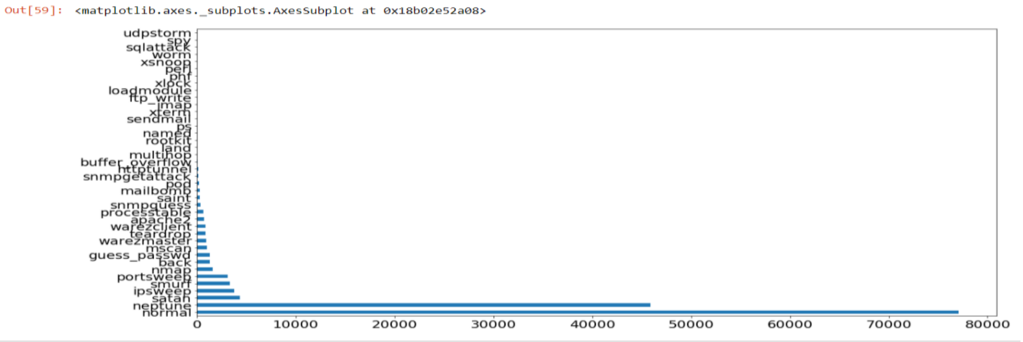
One of the key elements in developing good education and curricula is hands on materials and practical tools, code, practice, competitions, and simulations. With ENISA and other international bodies that work on cyber security it is crucial to invest in educational strategies connected to cyber security that are reshaped by today's needs.

4. Data gathering and machine learning in cyber security

Threat hunting, unlike traditional threat management measures, such as fivers, intrusion detection systems, sandy software and Siem systems, which usually include evidence-based data on the potential danger. Intelligence work on threats [12] plays an incredibly important role as a component of cyber security. It provides vital information for use in security analytics, then this information can help identify and determine the priorities of suspicious activity. It also helps security administrators in quality intelligence by providing insight into the history of certain IP addresses, domain names, etc. The same information can be invaluable to respond to the threat management component. Security administrators can use intelligence on threats to learn more about nature and the threat they are investigating. Organizations are increasingly using intelligence on threats from a third party to improve their ability to manage threats as well as other aspects of their security. For example, one of the most common use of performance intelligence sources is improving the accuracy of discovering and determining the priorities of Siem technology. Whether information on threats come into an organization through Siem or other route, it is important that it is connected by automated means with an organizational safety intelligence and analytical platform. Connecting allows you to fully integrate with other related to threats of information that organizations provide better insight into the nature of suspicious activities that include their systems and networks. For example, gathering the information from open sources, intelligence services, networks, media and other sources and gathering data for data sets for testing machine learning models. Intelligence can be gathered on multiple levels (national, international, local, CERT) for reports and gathering code data for developing recommendation systems. Although very vulnerable, cyber security experts point out the need for opening of data sources for the simple fact that machine learning models can be used for better understanding of cyber threat landscape, and also help in the intelligence work. Knowledge of data science and machine learning can raise the capacities of cyber and information security experts, given them an opportunity to have early warning systems, to gather information on cyber threats, to learn machines in recognizing most of the malicious software and social engineering attacks or to develop code.

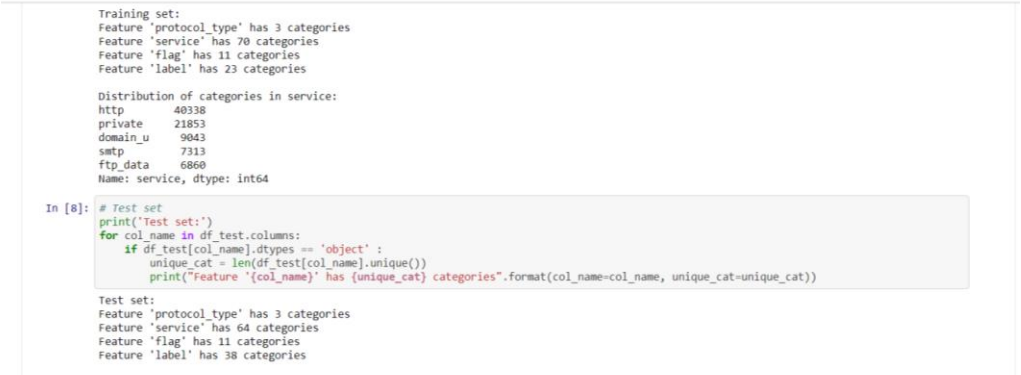
We will examine simple experiment with basic NSL KDD [13] data set example. We will use Anaconda platform and Jupiter Notebook to write Python code and examine data.

We first use the instructions from the data set and after basic data processing using plotting and other methods, we got results of identified threats that are shown on picture 1. and that are usage of Neptune, Satan, Nmap, buffer overflow etc.



```
Out[59]: <matplotlib.axes._subplots.AxesSubplot at 0x18b02e52a08>
```

Figure 1 Most common threats in NSL KDD



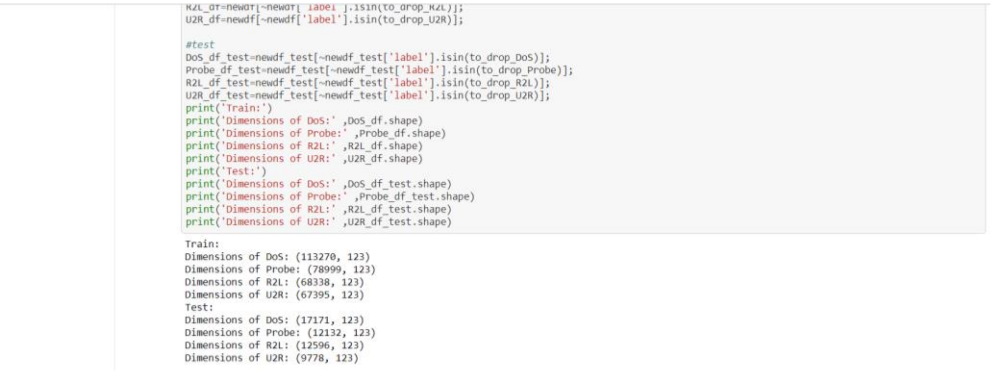
```
Training set:
Feature 'protocol_type' has 3 categories
Feature 'service' has 70 categories
Feature 'flag' has 11 categories
Feature 'label' has 23 categories

Distribution of categories in service:
http        40338
private     21853
domain_u     9043
smtp         7313
ftp_data     6860
Name: service, dtype: int64
```

```
In [8]: # Test set
        print('Test set:')
        for col_name in df_test.columns:
            if df_test[col_name].dtypes == 'object' :
                unique_cat = len(df_test[col_name].unique())
                print("Feature '{col_name}' has {unique_cat} categories".format(col_name=col_name, unique_cat=unique_cat))
```

```
Test set:
Feature 'protocol_type' has 3 categories
Feature 'service' has 64 categories
Feature 'flag' has 11 categories
Feature 'label' has 38 categories
```

Figure 2 Categories

After this step, a preprocessing was performed, and then we examined correlations among attributes and removed the weakest correlations. After that, selecting an attribute that has four categories (Figure 2) using the Dummy coding (entered these four categories through the labeling turn into numbers 1 to 4, with the following values



```
R2L_df=newdf[~newdf['label'].isin(to_drop_R2L)];
U2R_df=newdf[~newdf['label'].isin(to_drop_U2R)];

#test
DoS_df_test=newdf_test[~newdf_test['label'].isin(to_drop_DoS)];
Probe_df_test=newdf_test[~newdf_test['label'].isin(to_drop_Probe)];
R2L_df_test=newdf_test[~newdf_test['label'].isin(to_drop_R2L)];
U2R_df_test=newdf_test[~newdf_test['label'].isin(to_drop_U2R)];
print('Train:')
print('Dimensions of DoS:' ,DoS_df.shape)
print('Dimensions of Probe:' ,Probe_df.shape)
print('Dimensions of R2L:' ,R2L_df.shape)
print('Dimensions of U2R:' ,U2R_df.shape)
print('Test:')
print('Dimensions of DoS:' ,DoS_df_test.shape)
print('Dimensions of Probe:' ,Probe_df_test.shape)
print('Dimensions of R2L:' ,R2L_df_test.shape)
print('Dimensions of U2R:' ,U2R_df_test.shape)
```

```
Train:
Dimensions of DoS: (113270, 123)
Dimensions of Probe: (78999, 123)
Dimensions of R2L: (68338, 123)
Dimensions of U2R: (67395, 123)
Test:
Dimensions of DoS: (17171, 123)
Dimensions of Probe: (12132, 123)
Dimensions of R2L: (12596, 123)
Dimensions of U2R: (9778, 123)
```

Figure 3 Test, train sets

From this, a new set of data was created, which we compose from categorical and numerical data from which we then share on four train and test splits and determine X and Y for each data frame for each attack category. Using SCALER-scaling for the new data frames.

The K-Means algorithm collects data trying to separate samples in N groups of equal variances, minimizing criterion known as inertia or "Within Cluster of Squares". This algorithm requires a number of clusters. It is well measured on a large number of samples and is used in a large number of areas of application in many different fields. The K-Means algorithm divides the NI samples X in K "discs" described through "Mean" samples in the cluster. These are usually called Cluster Centroids. K-Means algorithm aims to choose centroids that reduce the inertia or sum of square criteria within the cluster. Clustered four groups of attacks, and the results for DOS attack are shown.

The clusters on the plate (Figure 4) show, in order to see the "elbow" in the graph. Point of fracture:

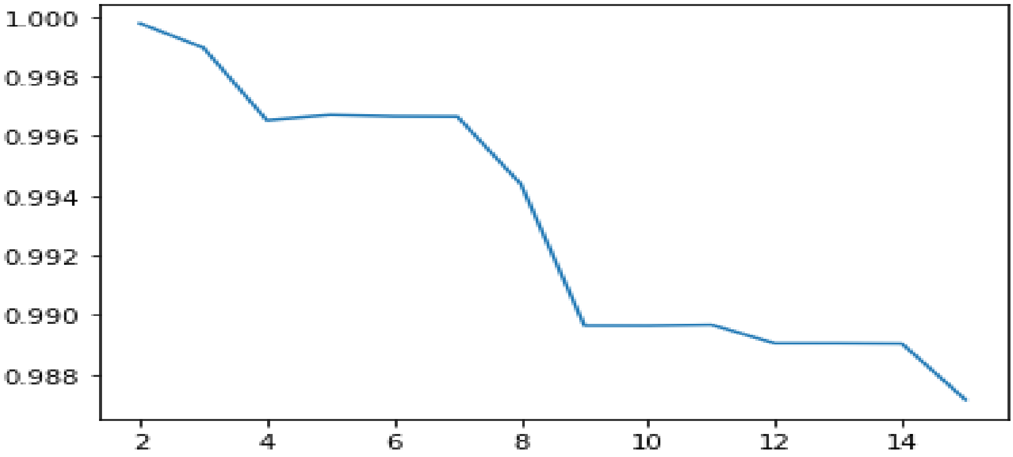


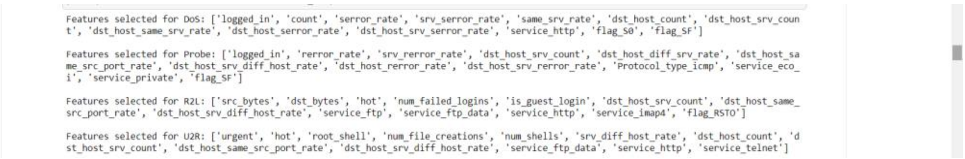
Figure 4 K-means iterations

In this graphic, it is seen that "elbow" is at the 7th cluster, so it can be concluded that the optimal number of clusters 7.

Then the univariate selection of attributes that separates the best attributes for each of the four categories separates.

After this step, we apply the recursive feature elimination technique of attributes to which of four categories of attack we want to extract the best. We got the following information here:

[(1, 'same_srv_rate'), (2, 'count'), (3, 'flag_SF'), (4, 'dst_host_serror_rate'), (5, 'dst_host_same_srv_rate'), (6, 'dst_host_srv_count'), (7, 'dst_host_count'), (8, 'logged_in'), (9, 'serror_rate'), (10, 'dst_host_srv_serror_rate'), (11, 'srv_serror_rate'), (12, 'service_http'), (13, 'flag_S0')]

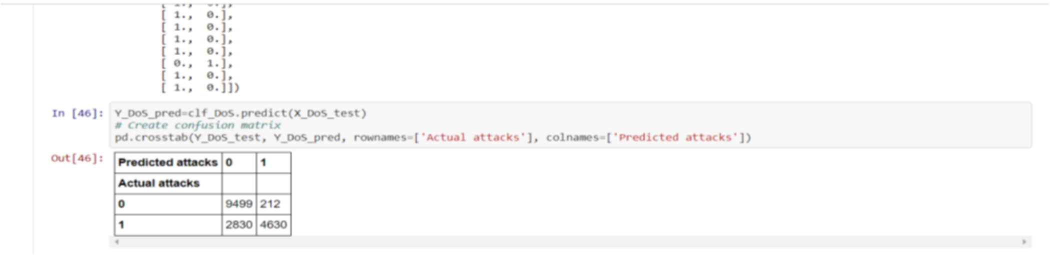


```
Features selected for DoS: ['logged_in', 'count', 'serror_rate', 'srv_serror_rate', 'same_srv_rate', 'dst_host_count', 'dst_host_srv_coun
t', 'dst_host_same_srv_rate', 'dst_host_serror_rate', 'dst_host_srv_serror_rate', 'service_http', 'flag_S0', 'flag_SF']

Features selected for Probe: ['logged_in', 'rerror_rate', 'srv_rerror_rate', 'dst_host_srv_count', 'dst_host_diff_srv_rate', 'dst_host_sa
me_src_port_rate', 'dst_host_srv_diff_host_rate', 'dst_host_rerror_rate', 'dst_host_srv_rerror_rate', 'Protocol_type_icmp', 'service_eco_
i', 'service_private', 'flag_SF']

Features selected for R2L: ['src_bytes', 'dst_bytes', 'hot', 'num_failed_logins', 'is_guest_login', 'dst_host_srv_count', 'dst_host_same_
src_port_rate', 'dst_host_srv_diff_host_rate', 'service_ftp', 'service_ftp_data', 'service_http', 'service_imap4', 'flag_RSTO']

Features selected for U2R: ['urgent', 'hot', 'root_shell', 'num_file_creations', 'num_shells', 'srv_diff_host_rate', 'dst_host_count', 'd
st_host_srv_count', 'dst_host_same_src_port_rate', 'dst_host_srv_diff_host_rate', 'service_ftp_data', 'service_http', 'service_telnet']
```

Figure 5 Recursive features

Now that we have a separate best attribute, we prepare them to build a model.

By further working on the NSL KDD set, a model that leads to this is to be exerted to recognize these attacks and thus make models for attack recognition models. We will first for each category of attacks from which we single out attributes do a classification using decision tree. Then we will apply the classifier over the data not seen from the test set and then make a mixture of confusion and so for all four types of attacks. Here we get a confusion matrix and we see the sole of the envisaged attacks and real attacks by looking at the true positive, false negative, falsely positive and true negative.



```
       [ 1.,  0.],
       [ 1.,  0.],
       [ 1.,  0.],
       [ 1.,  0.],
       [ 0.,  1.],
       [ 1.,  0.],
       [ 1.,  0.]])

In [46]: Y_DoS_pred=clf_DoS.predict(X_DoS_test)
         # Create confusion matrix
         pd.crosstab(Y_DoS_test, Y_DoS_pred, rownames=['Actual attacks'], colnames=['Predicted attacks'])

Out[46]:
```

Predicted attacks	0	1
Actual attacks		
0	9499	212
1	2830	4630

Figure 6 Confusion matrix

From the algorithms of machine learning to which the model will be prepared, decision trees are selected as the most important algorithm and after naive bayes.

The decision tree for each of the four categories of attack we get the following results

ДОС-Accuracy: 0.99732 (+/- 0.00251) Precision: 0.99679 (+/- 0.00464)

Recall: 0.99705 (+/- 0.00356) F-measure: 0.99692 (+/- 0.00288) Проб-Accuracy: 0.99085 (+/- 0.00559) Precision: 0.98674 (+/- 0.01180) Recall: 0.98467 (+/- 0.01027) F-measure: 0.98565 (+/- 0.00872)

Р2Л-Accuracy: 0.97451 (+/- 0.00906) Precision: 0.96683 (+/- 0.01316)

Recall: 0.96069 (+/- 0.01547) F-measure: 0.96367 (+/- 0.01300)

У2р- Accuracy: 0.99652 (+/- 0.00319) Precision: 0.87747 (+/- 0.15709)

Recall: 0.89183 (+/- 0.17196) F-measure: 0.87497 (+/- 0.11358)

Naive Bayes gave poorer results:

ДОС-Accuracy: 0.9032515636783037, Recall: 0.959167770591444, Precision: 0.88135471860232, F1: 0.918616366282324

Проб- Detection Rate: 0.939235201676270, Recall: 0.9785898855666297, Precision: 0.9701492537313433, F1: 0.898696366282324

This short experiment was prepared so it can show how easily we can prepare and recognize threats if we have intelligence and data, the next step is to use security analytics to better understand given data. Machine learning models can also be used for recommendation of cyber/information security education pathways that could reach potential candidates and it can also be used to learn code or social engineering attacks and prevent breaches/cyber-attacks. Also, little experiments like these can be motivating for the students or participants, as they will get a new interesting view on cyber security.

5. Security analytics

Analytics is a multidimensional discipline that has found its application in a significant number of sciences. Today it is used equally in the social and natural sciences. Thus, for example, due to the constant discovery of new knowledge in the field of physiology, pathophysiology, biochemistry and molecular biology, new analytical methods and techniques are being developed that enable monitoring of physiological and biochemical changes in patients - biochemical analytics or market analytics that studies the attractiveness and dynamics of a particular market in a particular industry [14].

However, given the global trends of challenges, risks and threats, security analytics as a special type of analytics has become increasingly important. In fact, it may be more correct to state that this significance is more and more recognized and acknowledged today, and that it has always existed. Considering that every state tries to cover up its own, and finds out other people's secret intentions [15], it is not questionable that analytical skills have been important for its survival and development since the creation of the state.

This special type of analytics refers to a narrow circle of state authorities: diplomacy, army, police, intelligence and security services, civil protection in which the analytical service is organized and analytical work. In all these state bodies, analytical processes are determined by their activities, so it is the source of its specificity, which is reflected in the following:

- First, security analytics has its strictly legal, illegal or semi-illegal work.

- Second, security analytics is closely linked to politics and political action.

- Third, security analysts are dealt with by specially trained and trained personnel, selected according to strict criteria and a complex procedure.

- Fourth, the results of the work of security analytics are a secret for the external and internal public, which is often mystified.

- Fifth, security analytics uses a specific set of working methods that are special and characteristic of this type of special analytics. [16]

Due to the frequent overlap of analytical and intelligence work, not much data can be found in the literature on how analytical services function. However, what is noticeable is that the authors singled out the basic phases of security analytics within different classifications. By crossing different classifications, these phases can be roughly defined as follows:

- setting (defining) an analytical task,

- data collection,

- processing of collected data and preparation of reports (answers) to the analytical task,

- dissemination (delivery) of the answer to the analytical task.

Data can be classified in various ways and by various criteria, and it is common to classify them according to the criteria of the subject, role, function, usability, truthfulness (reliability), confidentiality and sufficiency. [17] In the data processing phase, those data that are not directly related to the analytical task and which cannot contribute to the solution of the set task are rejected. Although there are different understandings of this phase of intelligence analytics, it is usually realized through three steps: (1) assessment of source reliability and accuracy, (2) classification and comparison of data and (3) stacking in databases. [18]

Today, analytics is often linked to information technology, where it relies on the application of statistics, computer programming and operational research, which are processed quantitatively. Increasingly, analytical processes take place with the use of certain software, which are suitable when it is necessary to process a large amount of data (so-called Big Data). Large amounts of data can be a problem for many companies that work through the transaction system "online" and as a negative result, large amounts of data are obtained in a very short time interval. [19] Then software takes over the role of analyst and in that context advanced analytics is mentioned.

In addition to advanced safety analytics, the term predictive analytics is also associated. Predictive analytics is a set of advanced tools and techniques used in the analysis of large series of past and present data to predict future events based on identified patterns of behavior. [20] This type of security analytics makes it easier to prevent future events that could jeopardize the security of citizens.

During the analytical processing, the analyst uses all his / her available knowledge and skills as well as the new data he / she came to in the data collection phase in order to reach the analytical conclusions. The choice of the type of conclusions in security analytics is influenced by several properties, among which the two are the most important. First, it is available data on socially deviant phenomena and second, it is the purpose, meaning and goals of security reports. [21]

Using security analytics in processing information from data sets and after data science analysis can give more meaning to data and ability to learn and counter threats. Thus, incorporating security analytics into curricula and e-learning in the areas connected to security can imbue the ability to counter threats.

6. Conclusion

Examining all presented, education is the only way, being formal or non-formal in developing a secure cyber space. Multi sectoral approach is very much needed especially coming from IT and Security sciences. Developing strategies on international (EU, UN etc.) and national levels for development of diversified human resources that can use e-learning to imbue their knowledge daily, but also to give them a scientific basic which they can use for the development of future practitioners and curricula. In the fast passed and everchanging environment pushed by geopolitical earthquakes that shake the multipolar world of today education must become a foundation that will withstand modern security threats, risks and challenges and create new professionals that primary purpose will be to protect the citizens and counter threats lurking in the cyberspace and reality.

Planning of development of cyber security programs has to be an imperative, but also to coordinate and to add security analytics aspect to curricula. As threats are diverse, so it should be education and counter actions. For example, well-educated security analyst with humanities background can be much efficient in countering social engineering attacks and in management of information. For example, if you examine ISO 27000 or other information security standards, you can easily see the security services background in the procedures, controls etc. Sometimes IT professionals can oversee security flaws coming from these areas, but with additional education from humanities, they will develop their abilities and improve resilience of systems they work in.

Motivating current junior, intermediate and senior developers for continuation of their career in cyber security in the state and business environments can contribute in raising the capabilities of personnel. It can be done with benefits, high salaries, but also giving them a perspective trough constant education.

Possibility of individuals with higher education to prequalify to information security, cyber security, not just from computer, information and other hard sciences, but also can come from humanities with basic knowledge of ICT systems (economy, security etc.) can have a good result, as there are such examples in some national programs in Europe.

There is no absolute security and threats are multiplying everyday, especially in cyber and information security. Thus, only multisectoral approach and education can counter them.

References

1. Cyber security ventures, https://cybersecurityventures.com/jobs/, accessed 03.05.2021
2. Sana Gupta, Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, Information Resources management association USA, (2018)
3. Bjorn Lundgren, Defining information security, Sci Eng ethics, (2017)
4. ZAKON O INFORMACIONOJ BEZBEDNOSTI REPUBLIKE SRBIJE ("Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019)
5. Clarence Chio, David Freeman, Machine Learning and Security OReilly Media 2018
6. Karen Scarfone, Definite guide to security intelligence and analytics, (2016)
7. Bajagić. (2004). Bajagic M. Obaveštajna aktivnosti i spoljna politika – studija slučaja SAD, VŠUP, Serbia, 2004
8. Đorđevic O. Osnovi državne bezbednosti, Beograd: VŠUP 1987
9. https://isses.etf.bg.ac.rs/ accessed 05.05.2021
10. https://www.dsi.rs/master-40-it-biznis/programi/ accessed 05.05.2021
11. https://istrazivackicentarob.com/ accessed 05.05.2021
12. Karen Scarfone, Definite guide to security intelligence and analytics, (2016)
13. https://www.unb.ca/cic/datasets/nsl.html accessed 05.05.2021
14. R.UIllerup, R. Stoi, Basic managment. München: Vahlen, 2006.

15. Stajić LJ., Osnovi sistema bezbednosti, Pravni fakultet Novi Sad, Serbia 2008. str 223.
16. Danilović N., Milosavljević S., Osnove bezbednosne analitike, JP „Službeni glasnik", 2008, Serbia str 37.
17. Danilović N., Milosavljević S., Osnove bezbednosne analitike, JP „Službeni glasnik", 2008.str 152
18. Forca B., Anočić B., Bezbednosna analitika, FPSP, Uiverzitet Union-Nikola Tesla u Beogradu, 2018. str 173. 2
19. Naone E., "The New Big Data". Technology Review, MIT. 2011.
20. Lazarević I., Big data u medicini i farmaciji, BB-INFORMATOR, jul 2015/ 242, BB-Soft, str 40.
21. Danilović N., Milosavljević S., Osnove bezbednosne analitike, JP „Službeni glasnik", 2008.str 199.