JDST., vol. 2, no. 1, p3-p10, 2020
https://doi.org/10.46713/jdst.002.01

www.jdst.eu, e-ISSN 2534-9813

Research Article

Analysis of definition set formed by given definitions of term cybersecurity

Nikolay Kulev [a]

[a] *NVU Vasil Levski, faculty Artillery, AD and CIS, 1 Karel Shkorpil str., Shumen 9700, Bulgaria*
http://aadcf.nvu.bg

ABSTRACT

This work exposes logical semantics analyses of definitions set of given definitions of the term cybersecurity and its impact on evolution of strategies in the field. With the given formalization of the definitions author suggests an approach of building structured understanding of the term cybersecurity, which could be used toward to build a layered model of the persistent cybersecurity state in digital context. Given that, this could result to gain more efficacy in certain educational process when cybersecurity is in topic.

ARTICLE INFO

RECEIVED: 09 Oct 20xx
REVISED: 10 Nov 20xx
ACCEPTED: 30 Nov 20xx
ONLINE: 12 DEC 20XX

KEYWORDS

learning app, teaching, web based education, ICT approaches, modelling..

Creative Commons BY-NC-SA 4.0

I. OVERVIEW

There are no conclusive evidences when the term “cybersecurity” was first used in the literature but some of the sources tend to accept 1989 as a started point. As for the root of the word “cyber” it can be stated that it is a neologism based on “cybernetics”. In turn “cybernetics” is originated from biblical proverbs text (kubernēsis) till 1948 where the word “cybernetics” appears first time in modern literature[10].

✉ Corresponding Author: Tel.: + Fax: + ; E-mail:

Since then various forms of idioms with prefix “cyber” were coined in the field. But human activity supported by technology has its dark side.

According to [8] there was hackers attack every 39 Seconds in 2017. Impressively, alongside diversity of types of attacks [35], according to [9] the attacks rose to 250 per second in 2020 where WEB objects are scanned for unwanted web content in real-time mode.

In this study it is acceptable that in parallel of outside source of cyber-related occurrences with negative impact there is an internal source of cyber-related occurrence. This internal source could be presented by such types of internal indicators classified as vulnerabilities, characterized as flaws in software that can be directly used by “initiator”(fig.2) to gain access over the object(target) trough subject. It is a notable tendency of growth of such features as shown in fig. 1 [18].

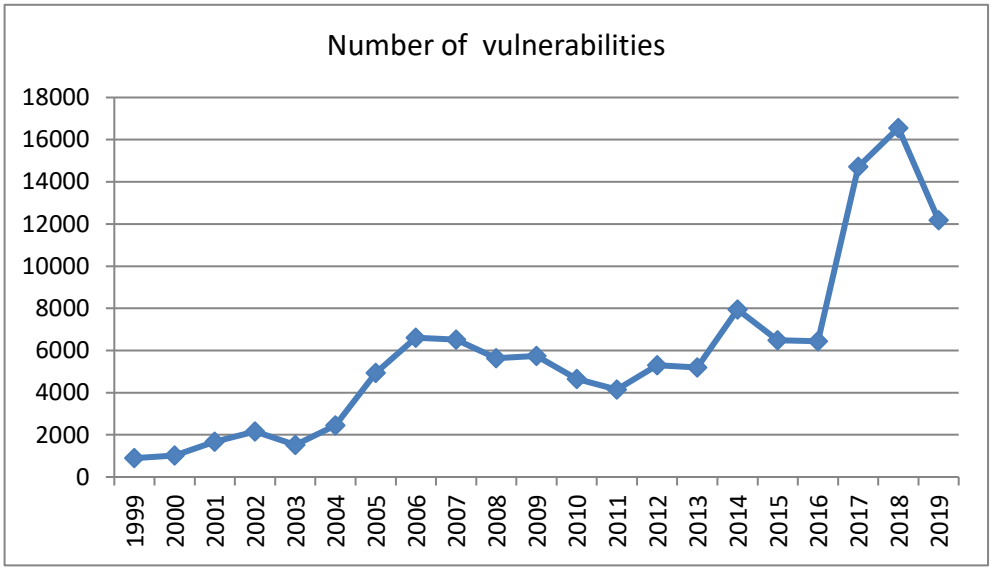

Figure 1: Number of vulnerabilities per year

Such vulnerabilities found in native software can be leveraged as exploits to steal data, hold files for ransom, perform reconnaissance, or to deploy malware [32].

As growing the area of human activity in digital environment this imminently affects also educational process and as inevitable imperative postulate many of our academics leverage the traditional learning into digital learning process through WEB access [1][3]-[6] either with the usage of new technology approaches[2]. At the same time all of the computer systems in the labs, including various types of digital devices, are interconnected. Learning platforms and learning resources are WEB based also broad spectrum of university services are WEB oriented.

In such digital transformation of the real life activities here takes place exploration of the set of definitions of the term “cybersecurity”.

As [11] argues there is evidence of “paucity” of literature (2014) according to what term “cybersecurity” actually means and how it is correlated with various contexts which is a notable weakness in the existing understanding of the term “cybersecurity”.

The existence of many terms in conjunction with “cybersecurity” and how these terms are interpreted differently in many cases was noted in 2018[15]. However, having a common understanding of the terms and how they relate to one another is more than essential [15]. In [12] is argued that “cybersecurity” is one of the poorly understood terms of our time(2020). Also, as noted [7] the need was to construct a conceptualization of security which in present days is imperative.

In 2019 there is still ambiguity about the clear definition of the term “cybersecurity”[17], which could cause confusion in certain institutions, organizations, social groups, etc. The discussions about the definition of “cybersecurity” are still in under consideration (2020) [11].

From other side governments, international institutions, companies and social organizations are developing their own approaches for “cybersecurity” implementations in digital environment in response of digital threats.

II. Logical Semantics Analysis

In this study under analysis were put three common sections:

- Commercials;
- Institutions;
- Researchers.

With subject “cybersecurity definition” a research in literature and official sources[11]-[34] was conducted and collected data of definitions were put into analysis and then structured. In this study an approach of formulating a common definition, proposed by [7],[11] is adopted as initial prerequisite. In the construction of the definition of “cybersecurity” certain key comprising terms should be encompassed:

- *feature* (main feature of “cybersecurity” domain)
- *initiator (*of the “cybersecurity” event*)*
- *subject (*of the “cybersecurity” event*)*
- *object (*of the “cybersecurity” event*)*
- *goal (*of the “cybersecurity” occurrence of consequence*)*
- *consequence (*as a result of “cybersecurity” occurrence*)*

These terms build hierarchical logical structure with specific logical-semantics relations between the subset of terms of given above definition “cybersecurity”. Given that a test to determine the relationship between two

categorical variables, representing subset, was made. For the test procedure were selected as follow:

1. Principal – a group of sources by their subtypes – commercials, institutions and academics who have been made definition of the term "cybersecurity".
2. Subject – mapped as subject of the "cybersecurity" and it is presented as single word in definition or definition-related content.

The null hypothesis states: *There is no dependence between type(class) of the creator(principal) of the definition and its subject*. A *Pearson Chi-square* test is calculated with value = 6.617647 and with a *p*-value = 0.03656. Because the *p*-value is less than *alpha* = 0.05, the null hypothesis was rejected. This could be interpreted as existence a relationship between the actual creator(*principal*) type(class) of the definition and the given subject. The result is presented in Table1.

Table 1: Pearson Chi-square test result

	Chi-square	df	P
Pearson Chi-square	6.617647	df=2	p=.03656
M-L Chi-square	9.162763	df=2	p=.01024

As some of subset of data in this structure are expressed with number of terms and with argumentations of [7][11] a conceptualization was made as presented in the fig2.

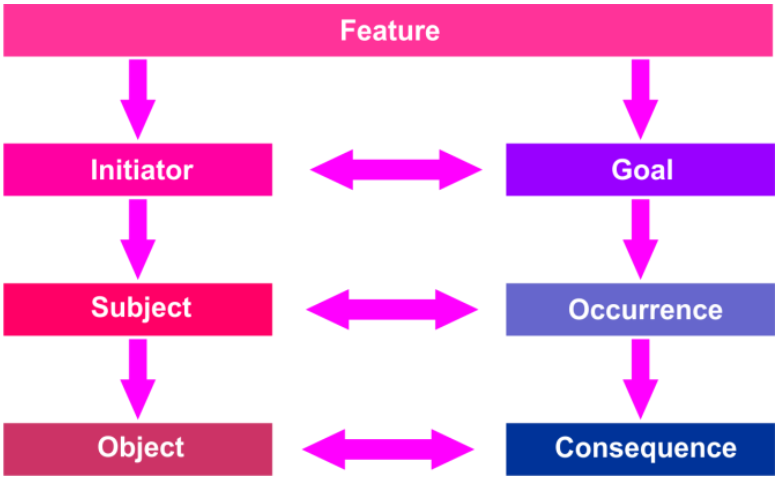

Figure 2: Conceptualization of definition of term "cybersecurity"

We accept that term “cybersecurity” form a time-related domain of events in certain state of stability. And every occurrence of consequence in this domain would change the state. Based on the above a formalization for definition of “cybersecurity” is proposed in (1):

$$\exists\, Q(D(i,l,s,o,)) \;\rightarrow P(c)\; \forall g \in G \tag{1}$$

and

$$\forall i[i \neq \{\}] \rightarrow \{i: i = g_1 \;\vee i = g_2 \ldots \vee i = g_n\} \quad for\ (\forall g \;\in G) \wedge (G \subset A) \tag{2}$$

$$\forall l[l \neq \{\}] \rightarrow \{l: l = m_1 \;\vee l = m_2 \ldots \vee l = m_n\} \quad for\ (\forall m \;\in M) \wedge (M \subset A) \tag{3}$$

$$\forall s[s \neq \{\}] \rightarrow \{s: s = r_1 \;\vee s = r_2 \ldots \vee s = r_n\} \quad for\ (\forall r \;\in R) \wedge (R \subset A) \tag{4}$$

$$\forall o[o \neq \{\}] \rightarrow \{o: o = k_1 \;\vee o = k_2 \ldots \vee o = k_n\} \quad for\ (\forall k \;\in K) \wedge (K \subset A) \tag{5}$$

$$G \neq M \neq R \neq K \tag{6}$$

Where

G, M, R, K – subsets of terms

A – an alphabet

Q – a possibility of definition of term “cybersecurity”

D – a model of definition of term “cybersecurity”

i – initiator of “cybersecurity” event

l – feature of “cybersecurity”

s – subject of “cybersecurity”

o – object of “cybersecurity”

$P(c)$ – possibility of consequence occurrence of “cybersecurity” event

c – consequence of occurrence in “cybersecurity” domain

g – *specific* goal consequence to be truth in “cybersecurity” domain

G – *set of goals* consequence to be truth in “cybersecurity” domain

III. Conclusions

As a result of findings above there is still a lack of coherence in major three areas of stakeholders - academics, business and institutions toward to definition of the term "cybersecurity". The approach in this paper could serve as common

directions when definition of “cybersecurity” is needed. Author intentions are to extend testing cases toward to presented in literature definitions of "cybersecurity" in order to form more comprehensive logical semantics and to set up a meaningful and consistent definition form.

REFERENCES

[1] V. Atanasov, K. Kalev, “Some aspects in the design and development of learning applications for engineering specialties”, Proceedings on: 62nd International scientific conference’2019, Publishing house of University of Mining and Geology “St. Ivan Rilski”, Sofia, Bulgaria, pp.126-129, 2019, ISSN 2682-9525.

[2] K.O. Slavyanov, “Fuzzy logic procedure for drawing up a psychological profile of learners for better perception in courses“, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 12th International Scientific and Practical Conference. vol. II, pp.136-140, 2019, ISSN 1691-5402, doi: http://dx.doi.org/10.17770/etr2019vol2.4073.

[3] V. T. Atanasov and A. S. Ivanova, "A Framework for Measurement of Interactivity of Digital Learning Resources," 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, pp. 649-654, 2019, doi: 10.23919/MIPRO.2019.8757052.

[4] V. Atanasov, “Smart Educational Cluster Conceptualization”, Annual, Vasil Levski National Military University Publishing House, vol. 1, pp.173-181, 2018, ISSN 2367-7902.

[5] M. Lambeva, M. Vasileva “An approach to the integration of information systems in education”, Proceedings of the second conference on innovative teaching methods (ITM 2017), 28-29 june 2017, pp. 110-116, Publishing house “Science and economics”, Varna, 2017, ISBN 978-954-21-0930-3.

[6] Valentin T. Atanasov, “Intelligent Educational Structure Model”, Annual, Konstantin Preslavsky University Press, Shumen, Bulgaria, vol. IX E, pp. 190-196, 2019, ISSN 1311-834X.

[7] B.Buzzan, O.Weaver,J., Wilde, Security: A new framework for analysis, Lynne Rienner Publishers, 1998, ISBN 1-55587-603-X.

[8] M. Cukier, Hackers Attack Every 39 Seconds , A Study, A. James Clark School of Engineering, University of Maryland, USA, 2017, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

[9] Cyberthreat Real-time Map, https://cybermap.kaspersky.com/stats/.

[10] N. Wiener, Cybernertics or control and communication in the animal and machine, MIT Press, Second edition,1985, ISBN 0-262-73009-X.

[11] D. Craigen, N. Diakun-Thibault,R., Purse, "Defining Cybersecurity", Technology Innovation Management Review, 2014 , url: https://timreview.ca/article/835 (visited at 13.06.2020).
[12] W. G. Urgessa, "Multilateral cybersecurity governance: Divergent conceptualizations and its origin", Computer Law & Security Review, vol. 36, article: 105368, 2020, https://doi.org/10.1016/j.clsr.2019.105368.
[13] R. Hoffmann, J. Napiórkowskia, T. Protasowickia, J. Stanika, "Risk based approach in scope of cybersecurity threats and requirements", Procedia Manufacturing, Elsevier B.V , vol 44. pp.655–662, 2020, ISSN 2351-9789, doi: 10.1016/j.promfg.2020.02.24.
[14] V. G. Promyslov, K. V. Semenkov, A. S. Shumov, "A Clustering Method of Asset Cybersecurity Classification", IFAC PapersOnLine , vol.52(13), pp. 928–933, 2019, ISSN: 2405-8963, https://doi.org/10.1016/j.ifacol.2019.11.313.
[15] K. Ciglic, Cybersecurity Policy Framework: "A practical guide to the development of national cybersecurity policy", https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-framework.
[16] O. Szumski , Cybersecurity best practices among Polish students, Procedia Computer Science, Elsevier Ltd, vol. 126, pp. 1271–1280, 2018, ISSN: 1877-0509, doi: 10.1016/j.procs.2018.08.07.
[17] Challenges to effective EU cybersecurity policy, Briefing Paper, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.
[18] Vulnerabilities By Type, https://www.cvedetails.com/vulnerabilities-by-types.php
[19] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.htm!
[20] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
[21] https://www.microsoft.com/en-s/cybersecurity?activetab=cyber%3aprimaryr2.
[22] https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
[23] https://www.fortinet.com/resources/cyberglossary/cybersecurity
[24] https://www.splunk.com/pdfs/technical-briefs/splunk-cybersecurity-framework.pdf
[25] https://www.paloaltonetworks.com/cyberpedia/cyber-security
[26] https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity.html
[27] https://securitybrief.com.au/story/interview-rsa-explains-security-in-the-epoch-of-it-disruption

[28] https://www.infoblox.com/solutions/network-security/cybersecurity-frameworks/
[29] https://www.checkpoint.com/definitions/what-is-cybersecurity/
[30] https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-wp-cybersecurity-in-modern-era.pdf
[31] https://www.imperva.com/resources/datasheets/Imperva_CorporateOverview_Datasheet_20200219_Web.pd
[32] https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-cybersecurity-fit-for-the-future-wp.pdf
[33] https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C
[34] https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf
[35] Dimo Dimov, Yulian Tsonev, Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse, CompSysTech'17: Proceedings of the 18th International Conference on Computer Systems and Technologies, 2017, pp. 149–154, ISBN: 9781450352345, https://doi.org/10.1145/3134302.3134338