International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 9 Issue 3, March 2022

ISSN: 2394-4404

Influence Of Cognitive Agility Of Cyber Operators On Situational-Aware Cyberspace Protection

David A.O. Njoga

Samuel Liyala

Silvance Abeka

Jaramogi Oginga Odinga University of Science and Technology

Abstract: ***The effectiveness of the cyberspace protection for the national critical information infrastructure (CII) depends on a dynamically and reliably established cyberspace situational awareness framework. The current attribution based cyberspace protection models and frameworks are characterised by over dominance of government agencies and laws, over-reliance on technology and lack of trust, transparency and goodwill leading to weak protection of critical information infrastructure. The study adopted a descriptive survey research design, in which conveniently sampled participants answered questions administered through Self-Regulation Questionnaires through three stage Delphi-Technique evaluation. Data was then analyzed using mean, standard deviation, frequency distributions, Pearson's correlations and Linear Regression Analysis. The study revealed that there was a statistically significant moderate and positive association /relationship between cognitive agility and situational-awareness. This implies that the cyberspace protection is as strong or as weak as the cyberspace protection operators. The study concluded that a human-factored security endeavour is required that can improve the capabilities of the operational technology human constituents, so that they can appropriately recognise and respond to cyber intrusion events within the CII environment. Amidst evolving security trends that places human industrial actors as prime vectors of CII cyber-attacks, human-factored security efforts are required to manage and control the menace of prevailing attacks. Its invaluable considering that cyber security knowledge and skills capabilities of the CII workforce (people) is crucial and strategic towards building a more effective and cybersecurity-compliant workforce. Cognitive agility is a major contribution to cyberspace's protection since cyberspace is a fluid, technically changing environment, continuously increasing in scale and sophistication that must be constantly supervised and redefined by actors' stable presence. These findings provide a human-centred security capability and resilience building model which can be used to strengthen the security aptitude of human agents within CII. Noting the 'standardization' and 'accountability' common to traditional education models, this study recommends new and likened pedagogical interventions which provide the context for new literacies that include metacognitive strategies such as critical thinking, complex problem solving, expert communication and applied knowledge in real world settings. Inspired by constructivism, and the slow education approach to learning, specific pedagogical interventions designed to improve higher-order thinking and understanding, such as self-directed workshops, flipped classroom, reflection logs, and cognitive task analysis. An outcome of this method is students gaining situational self-efficacy and empowerment as they engage in critical thinking. This is valuable for cyber education as it leads learners to exhibit and contextualize richer relationships and meanings beyond the prescribed lesson content.***

Keywords: Cyberspace, Cognitive, Critical, Human

I. INTRODUCTION

Cognitive agility is defined as a construct made up of three components: Cognitive flexibility (ability to cognitively control and shift mental sets and overcome automatic or dominant responses), Cognitive openness (being receptive to new ideas, experience, and perspectives), and Focused attention (ability to attend to relevant stimuli and ignore distracting one) (Good and Yeganeh, 2012). By turning the lens of behavioural science onto cyber security challenges,

ISSN: 2394-4404

cyber defenders can identify new ways to approach old problems (Maalem Lahcen, Caulkins, Mohapatra, & Kumar, 2020). Many recorded industrial cyber breaches have effectively beaten technological security solutions through exploiting human-factor limitations in knowledge and skills, and these attack patterns have manipulated human elements into unintentionally conveying access to critical industrial assets (Ani, He, & Tiwari, 2019). More contextually, technical security control may well be easily subverted by intelligent adversaries who can easily deceive unaware, unskilled and unsuspecting ICS operators and users into undertaking actions and activities that can grant the attackers easy access and high privilege capacities to execute their malicious intents (Ani et al., 2019).

An earlier study aimed at 'Threat Modelling' by Chopitea (2012) makes a generalisation characterising these hacker groups as having key features including: decentralised hierarchy, leverage "low-hanging fruit" vulnerabilities, instantaneity, extensive use of the social web and cooperation. Whereas the cyberspace is perceived and conceived as an unsecured space, improving protection and resilience is by maintaining a constant presence to anticipate the exploitation of a CII and simultaneously capture the enemy's capabilities (Gaiser, 2018). The full spectrum of the information domain runs from hardware, through software to what has been called 'wetware', the realm of knowledge in the human brain and mind. This expands the understanding of 'cyber' from simply being about technology to having its greatest value in the form of knowledge. It can be noted that currently, industries are turning to humans to mitigate cyber threats, because the promises of automated defenses are not enough; therefore, the human cyber network defenders are being planted between malicious actors and the data being protected within organizations (Gutzwiller, Hunt, & Lange, 2016).

To meet the protection objectives, this requires prioritizing five issues, according to Huang & Pai (2019) which include: planning and resource allocation, information sharing, indicators and warnings, human capital and crisis awareness, technology research and development, and simulation and analysis to build infrastructure protection programs. In order to mitigate threats, the analyst needs to develop vast situation awareness capabilities of the CII, referred to as cognitive perspective on situation awareness, in which a human operator in a dynamic environment will seek to perceive the relevant, critical elements of information, attempt to comprehend their meaning and use this knowledge to make predictions in the near future about the state of the environment (Gutzwiller et al., 2016). The process of situational awareness can be viewed as a three-phase process: situation perception, situation comprehension, and situation projection (Sa & Hutchison, 2017).

II. METHODS AND MATERIALS

The study population comprised of the participants of the National Cyber Security Training Programme (NCSTP). Census was also use to select the sample for the 64 participants of NCSTP at eKRAAL Innovation Hub Census due to the convenience and the small size of the population.

The reliability of the instrument was estimated after the pilot study using Cronbach's reliability coefficient (Frankael and Wallen, 2008). Cronbach's reliability coefficient was established at 0.721 and 0.725 for Cognitive Agility and Situational-Aware Cyberspace – Cognitive Agility variables respectively.

Descriptive analysis was used to measure the central tendency such as the frequency, percentages, mean and standard deviation was used to get the mean and standard deviation of the data. For inferential statistics, Pearson's correlation and regression analysis and model as well as linear regressions was used to draw inferences. These were generated to analyze the respondents' measure to the various aspects in the questionnaires.

Correlation analysis was used to describe the strength and direction of relationships among the dependent variables and independent variables for the study (Kothari & Garg, 2014). Linear regression analyses were used to determine the influence of each dynamic on situational-aware cyberspace protection for critical information infrastructure (Saunders, Lewis & Thornhill, 2014). Prior to conducting linear regression, pre-requisite test like tests for normality, heteroscedasticity, multicollinearity and linearity were done. The linear regression model used was:

$$y = \beta_0 + \beta_i X_i + \varepsilon$$

Where

Y =Situational-Aware

If $X_i = X_1$ then we have regulatory framework

β_i is the Coefficients of the independent variables, where i=1,2,3,4

ε is the error term

Stepwise regression analysis was used to determine the optimal model for situational-aware cyberspace protection where all the insignificant factors were dropped. The significance level was at 5%.

III. RESULTS

INFLUENCE OF COGNITIVE AGILITY ON SITUATIONAL-AWARE CYBERSPACE PROTECTION RESPONSE RATE

The researcher shared a link to the questionnaire on google docs to 64 officers at the National Cyber Security Training Programme (NCSTP), out of which 46 responded fully to the questionnaire. Since it was mandatory to complete one question in order to move to the next, no questionnaire was incomplete hence none was disregarded, thus, yielding a response rate of 72%. This was hence considered a reliable response rate for analysis and generalizing from the study findings. The results are represented in percentages as per the Figure No.1 below.

ISSN: 2394-4404

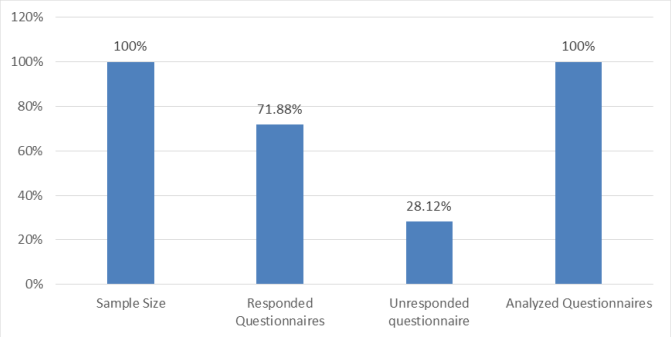

Figure 1: Response Rate for Cognitive Agility

GENERAL INFORMATION

RESPONDENTS GENDER

The respondents were asked to identify their gender and findings are represented in the Table No.1 below shows that majority of the respondents are male (37%) while the female respondents were 63%.

Gender	Frequency	Percent
Male	17	37.0
Female	29	63.0
Total	46	100.0

Table 1: Respondents Gender

RATINGS FOR COGNITIVE AGILITY

Descriptive statistics in terms of means and standard deviation were used to analyse the ratings for cognitive agility variable and the findings are in Table No.2. The findings from Table No.2 indicate that most of the respondents agreed that if they wanted to change then they were confident that they could do it $(M = 4.52, SD = 0.658)$. This variable that stood out across all the variables for cognitive agility.

	Statement describing Cognitive Agility	M	SD
1.	I usually keep track of my progress toward my goals.	4.04	0.698
2.	My behavior is not that different from other people.	2.76	0.947
3.	Others tell me that I keep on with things too long.	3.02	1.022
4.	I doubt I could change even if I wanted to.	1.87	1.185
5.	I have trouble making up my mind about things.	2.20	1.003
6.	I get easily distracted from my plans.	2.35	1.016
7.	I reward myself for progress toward my goals.	3.91	0.939
8.	I don't notice the effects of my actions until it's too late.	2.30	0.813
9.	My behavior is similar to that of my friends.	2.52	1.070
10.	It's hard for me to see anything helpful about changing my ways.	1.89	0.795
11.	I am able to accomplish goals I set for myself.	4.07	0.611
12.	I put off making decisions.	2.33	0.944
13.	I have so many plans that it's hard for me to focus on any one of them.	2.76	0.993
14.	I change the way I do things when I see a problem with how things are going.	3.96	0.868
15.	It's hard for me to notice when I've "had enough" (alcohol, food, sweets).	1.93	0.827
16.	I think a lot about what other people think of me.	2.72	1.089
17.	I am willing to consider other ways of doing things.	4.28	0.655
18.	If I wanted to change, I am confident that I could do it.	4.52	0.658
19.	When it comes to deciding about a change, I feel overwhelmed by the choices.	2.98	0.954
20.	I have trouble following through with things once I've made up my mind to do something.	2.70	0.963
21.	I don't seem to learn from my mistakes.	1.78	0.593
22.	I'm usually careful not to overdo it when working, eating, and drinking.	3.72	0.807
23.	I tend to compare myself with other people.	2.98	1.043
24.	I enjoy a routine, and like things to stay the same.	2.78	1.134
25.	I have sought out advice or information about changing.	3.52	1.005
26.	I can come up with lots of ways to change, but it's hard for me to decide which one to use.	2.85	0.965
27.	I can stick to a plan that's working well.	4.28	0.584
28.	I usually only have to make a mistake one time in order to learn from it.	3.04	1.192
29.	I don't learn well from punishment.	2.52	1.049
30.	I have personal standards, and try to live up to them.	4.28	0.750
31.	I am set in my ways.	3.87	0.687
32.	As soon as I see a problem or challenge, I start looking for possible solutions.	4.20	0.582
33.	I have a hard time setting goals for myself.	2.09	0.812
34.	I have a lot of willpower.	4.04	0.815
35.	When I'm trying to change something, I pay a lot of attention to how I'm doing.	3.87	0.806
36.	I usually judge what I'm doing by the consequences of my actions.	3.93	0.800
37.	I don't care if I'm different from most people.	3.78	0.917
38.	As soon as I see things aren't going right I want to do something about it.	4.28	0.544
39.	There is usually more than one way to accomplish something.	4.46	0.657
40.	I have trouble making plans to help me reach my goals.	2.37	0.928
41.	I am able to resist temptation.	3.59	0.805
42.	I set goals for myself and keep track of my progress.	3.87	0.542

43.	Most of the time I don't pay attention to what I'm doing.	1.96	0.515
44.	I try to be like people around me.	2.48	0.888
45.	I tend to keep doing the same thing, even when it doesn't work.	1.93	0.712
46.	I can usually find several different possibilities when I want to change something.	4.09	0.509
47.	Once I have a goal, I can usually plan how to reach it.	4.13	0.453
48.	I have rules that I stick by no matter what.	3.67	0.762
49.	If I make a resolution to change something, I pay a lot of attention to how I'm doing.	3.96	0.595
50.	Often I don't notice what I'm doing until someone calls it to my attention.	2.15	0.816
51.	I think a lot about how I'm doing.	4.00	0.730
52.	Usually I see the need to change before others do.	3.87	0.778
53.	I'm good at finding different ways to get what I want.	3.93	0.574
54.	I usually think before I act.	3.96	0.788
55.	Little problems or distractions throw me off course.	2.76	0.947
56.	I feel bad when I don't meet my goals.	4.33	0.560
57.	I learn from my mistakes.	4.17	0.643
58.	I know how I want to be.	4.04	0.842
59.	It bothers me when things aren't the way I want them.	4.24	0.524
60.	I call in others for help when I need it.	4.22	0.696
61.	Before making a decision, I consider what is likely to happen if I do one thing or another.	4.04	0.595
62.	I give up quickly.	2.11	0.900
63.	I usually decide to change and hope for the best.	4.11	0.434

Table 2: Ratings for Cognitive Agility

RATINGS FOR SITUATIONAL-AWARE CYBERSPACE PROTECTION

Descriptive statistics in terms of means and standard deviation were used to analyze the ratings for situational-aware variable and the findings are in Table No.3. The findings from Table No.3 indicate that most of the respondents agreed that having a comprehensive understanding of the adversary was critical $(M = 4.33, SD = 0.560)$. This variable that stood out across all the variables for situational-aware.

	Statement describing Situational-Aware Cyberspace Protection	**M**	**SD**
1.	It's easy for me to be always aware of the current situation (identifying types of attack, the source and the target.	3.93	0.574
2.	I am able to do an assessment of both current and future impact of cyber incident.	3.96	0.788
3.	I am aware that understanding how cyber incidents evolve is important.	2.76	0.947
4.	Having a comprehensive understanding of the adversary is critical.	4.33	0.560
5.	Most of the time, I consider root cause analysis of cyber incidents a priority.	4.17	0.643
6.	Verifying the quality metrics of situational awareness information items such as authenticity, completeness and currency is mandatory.	4.04	0.842
7.	Understanding the future attack is significant to appreciating the current situation.	4.24	0.524

Table 3: Ratings for Situational-Aware

CORRELATION ANALYSIS

To determine the strength and direction of the relationship/association between cognitive agility and situational-aware, correlational analysis was done. The results are presented in Table No.4. Findings in Table NO.4 indicate that there was a statistically significant moderate and positive association /relationship between cognitive agility and situational-aware, $r\ (170) = 0.474, p < .05$.

		Cognitive Agility	Situational-Aware Cyber Protection
Cognitive Agility	Pearson Correlation	1	.474**
	Sig. (2-tailed)		.001
	N	46	46
Situational-Aware Cyber Protection	Pearson Correlation	.474**	1
	Sig. (2-tailed)	.001	
	N	46	46
**. Correlation is significant at the 0.01 level (2-tailed).			

Table 4: Correlation between Cognitive Agility and Situational-Aware

TESTS FOR ASSUMPTIONS FOR LINEAR REGRESSION ANALYSIS

Prior to linear regression analysis, test for the assumptions for linear regression analysis were done. Tests for Normality, Linearity and Multi-collinearity were done to ascertain the assumption of linear regression analysis.

TEST FOR NORMALITY

To determine if the cognitive agility variable has a normal distribution, the study used shapiro-wilk test. The findings in Table No.5 indicate that data for cognitive agility variable is approximately normal $(p > 0.05)$.

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Cognitive Agility	.118	46	.117	.961	46	.124
a. Lilliefors Significance Correction						

Table 5: Test for Normality for Cognitive Agility Variable

TEST FOR LINEARITY

To determine if the relationship between cognitive agility and situational-aware variables are linear in nature, the study used deviation from linearity test. Table No.6 presents the deviation from linearity test results which indicate that there is a linear relationship between cognitive agility and situational-aware, $F\ (1,25) = 1.208, p > .05)$.

			Sum of Squares	df	Mean Square	F	Sig.
Situational-Aware Cyber Protection * Cognitive Agility	Between Groups	(Combined)	2.563	26	.099	1.709	.116
		Linearity	.822	1	.822	14.253	.001
		Deviation from Linearity	1.741	25	.070	1.208	.340
	Within Groups		1.096	19	.058		
	Total		3.659	45			

Table 6: Test for Linearity between Cognitive Agility and Situational-Aware

TEST FOR MULTICOLLINEARITY

To determine if the relationship between cognitive agility and situational-aware variables are linear in nature, the study used deviation from linearity test. Table No.7 presents the deviation from linearity test results which indicate that there is a linear relationship between cognitive agility and situational-aware, $F\ (1,150) = 1.564, p > .05)$.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.249	.749		1.668	.102		
	Cognitive Agility	.806	.226	.474	3.571	.001	1.000	1.000
a. Dependent Variable: Situational-Aware Cyber Protection								

Table 7: Test for Multicollinearity between Cognitive Agility and Situational-Aware

LINEAR REGRESSION ANALYSIS TESTS

The study null hypothesis was formulated from the study specific objective: "To establish how of cognitive agility of cyber protection operators influences situational-aware cyberspace protection for critical information infrastructure."

Null hypothesis (H_0): of cognitive agility of cyber protection operators does not have a significant influence on situational-aware cyberspace protection for critical information infrastructure.

The regression analysis ($y = \beta_0 + \beta_1 X_1 + \varepsilon$) was done with situational-aware cyberspace protection as the dependent factor and of cognitive agility of cyber protection operators as tested predictor factor. The results are exemplified in Table No.8.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.249	.749		1.668	.102	-.260	2.758
	Cognitive Agility	.806	.226	.474	3.571	.001	.351	1.262
a. Dependent Variable: Situational-Aware Cyberspace Protection								

F (1, 44) = 12.750, P-value <0.05, R-squared = 0.225, Adj R-squared = 0.207

Table 8: Linear Relationship between Crowdsourcing and Situational-Aware

The value of R^2 = 0.225, shows that 22.5% of the situational-aware cyberspace protection is explained by cognitive agility (regression line). The value of F (1, 44) = 12.750, P-value < 0.05, shows that cognitive agility statistically significantly influences situational-aware cyberspace protection (i.e., the regression model is a good fit of the data). The null hypothesis is consequently rejected and the alternative hypothesis accepted. The cognitive agility is statistically significant and it significantly influences situational-aware cyberspace protection (t=3.571, p < .05). The regression model which explains the results in Table No.8 is given by:

$$Situational - Aware = 1.249 + 0.806 \times Cognitive\ Agility$$

The model shows that cognitive agility positively influences situational-aware cyberspace protection, i.e. an increase in cognitive agility increases the situational-aware cyberspace protection for critical information infrastructure by a positive unit mean index value of 0.806.

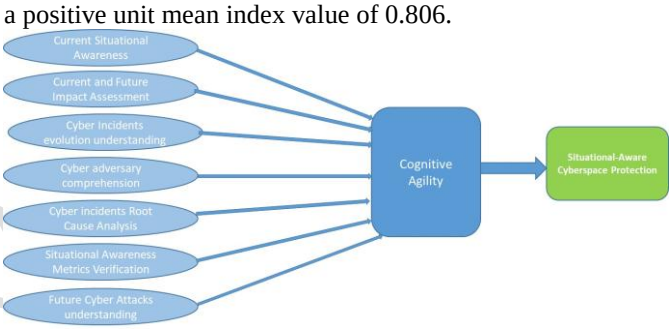

Figure 2: Constructs Derived from Cognitive Agility Variable

IV. DISCUSSIONS

These new constructs in the framework in Figure No.2 contribute directly towards enhanced Dynamic Decision Making (DDM) which is a significant derivative of C4I enabled cyberspace situational awareness. It can be recollected from the Effective Cyber Situational Awareness model (ECSA) analysed by Pahi et al., (2017) as focusing on a particular type of CSA: a holistic view of SA within a computer network applying network monitoring. The ECSA model analysed by Pahi et al., (2017) included three main phases:

- ✓ *Network Awareness* which includes the analysis and enumeration of assets and of defense capabilities.
- ✓ *Threat or Attack Awareness* which establishes a current situation picture of possible attacks and vectors against the network in question.
- ✓ *Operational or Mission Awareness* which establishes SA of the operation e.g., how decreased or degraded network operations will affect the mission of the network.

Operations staff need accurate cyber situational awareness, as they have to be ready to intervene in the face of cyber threats for being able to rapidly adapt security measures(Eckhart, Ekelhart, & Weippl, 2019). It should be noted that the mere technological issues and solutions do not

solve all the problems as a cyber security management model of critical infrastructure should be constantly improved along with the rapidly evolving technology (Limba, Plėta, Agafonov, & Damkus, 2017). People-centric security (PCS) is a strategy that represents an alternative to conventional information security practice. According to Galinec et al., (2017), PCS aims to strike a balance between risk reduction and employee agility; it is a strategic approach to information security that emphasizes individual accountability and trust and de-emphasizes restrictive, preventative security controls.

Pahi, Leitner, & Skopik (2017) also explored the widely-known and applicable general definition and theoretical model for SA by Endsley as a cognitive SA model of divided in six components or levels: Perception, Comprehension, Projection, Decision, Performance of Actions and Feedback. The results suggest that security perceptions and general external factors affect individual cyber security adoptive behaviour, and those factors are regulated by users traits (gender, age) and working environment (Maalem Lahcen et al., 2020). In the study of Pahi et al., (2017), SA presents a level of focus that goes beyond traditional information processing approaches in attempting to explain human behaviour in operating complex systems. This implies that the cyberspace protection is as strong or as weak as the cyberspace protection operators. In the study of Self-Regulation and Cognitive Agility in Cyber Operations, Cognitive agility within The Hybrid Space Conceptual Framework was linked to performance in defensive cyber operations (Jøsok, Lugo, Knox, Sütterlin, & Helkala, 2019). The implication of this finding is further asserted by Jøsok et al., (2019) that while technical cyber competence is paramount to operate in the cyber domain, the soft skills and cognitive competencies have started to gain significant contribution towards cyberspace protection.

V. CONCLUSION

Human-factor is as important as technical factors in CII security. Maalem Lahcen et al., (2020) concurs that behavioural science approach can determine the factors shaping cybersecurity behavioural decisions of users, implying that security perceptions and general external factors affect individual cybersecurity adoptive behaviour, and those factors are regulated by users traits (gender, age) and working environment. The target state can be achieved with an efficient process that includes a three-level strategic, operational and technical/tactical operating model to support decision-making and utilizing national and international strengths to provide the strategic agility and speed which are needed to prepare for incidents in dynamic cyber environments (Pöyhönen, Rajamäki, Ruoslahti, & Lehto, 2020). Cognitive agility should comprise of Cognitive flexibility (ability to cognitively control and shift mental sets and overcome automatic or dominant responses), Cognitive openness (being receptive to new ideas, experience, and perspectives) and focused attention (ability to attend to relevant stimuli and ignore distracting ones). Dupont (2019) observes that it is not the lack of resources and time that are the only barriers to cyber-resilience, but psychological factors and cognitive biases also play an important role. It is therefore imperative and important that cyber protection operators are capable of analysing, evaluating, synthesizing, interpreting and lastly articulating cyberpower effects in relation to wider geopolitical conditions, as well as relating to its application in multi-domain cyberspace contexts as depicted by this study. Cognitive agility is a major contribution to cyberspace's protection since cyberspace is a fluid, technically changing environment, continuously increasing in scale and sophistication that must be constantly supervised and redefined by actors' stable presence (Gaiser, 2018). These findings provide a human-centred security capability and resilience building model which can be used to strengthen the security aptitude of human agents within CII.

REFERENCES

[1] Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

[2] Chopitea, T. (2012). Threat modelling of hacktivist groups. Threat Modelling of Hacktivist Groups, (Organization, chain of command, and attack methods), 62.

[3] Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, Vol. 5, pp. 1–17. https://doi.org/10.1093/cybsec/tyz013

[4] Eckhart, M., Ekelhart, A., & Weippl, E. (2019). Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, 2019-Septe, 1222–1225. https://doi.org/10.1109/ETFA.2019.8869197

[5] Gaiser, L. (2018). European critical infrastructure protection: The need for a regional approach and a cyber constant contact strategy. National Security and the Future, 19(1–2), 45–63.

[6] Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. Automatika, 58(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

[7] Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016, (92106), 14–20. https://doi.org/10.1109/COGSIMA.2016.7497780

[8] Huang, K.-H., & Pai, J.-T. (2019). A Study of Disaster Risk Communication and Adaptive Behaviour based on Rail Station Protection. International Review for Spatial Planning and Sustainable Development, 7(3), 4–16. https://doi.org/10.14246/irspsd.7.3_4

[9] Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., & Helkala, K. (2019). Self-Regulation and Cognitive Agility in Cyber Operations. Frontiers in Psychology, 10(APR), 875. https://doi.org/10.3389/fpsyg.2019.00875

[10] Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)
[11] Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00050-w
[12] Pahi, T., Leitner, M., & Skopik, F. (2017). Analysis and assessment of situational awareness models for national cyber security centers. ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017-Janua(Icissp), 334–345. https://doi.org/10.5220/0006149703340345
[13] Pöyhönen, J., Rajamäki, J., Ruoslahti, H., & Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. Annals of Disaster Risk Sciences, 3(1), 1–10. https://doi.org/10.51381/adrs.v3i1.36
[14] Sa, C., & Hutchison, D. (2017). Theory and Models for Cyber Situation Awareness State-of-the-Art. 4, 3–25. https://doi.org/10.1007/978-3-319-61152-5