Critical Information Infrastructure Cyberspace Situational Awareness: Measure it, Manage it

Njoga A O David[1], Liyala, Samuel[2], Abeka Silvance[3]

[1](School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Kenya)
[2](School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Kenya)
[3](School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Kenya)

DOI: 10.29322/IJSRP.12.04.2022.p12425
http://dx.doi.org/10.29322/IJSRP.12.04.2022.p12425

Paper Received Date: 15th March 2022
Paper Acceptance Date: 1st April 2022
Paper Publication Date: 6th April 2022

Abstract:

Background: The sustainable development goals (SDGs) were designed to serve as a useful guide for focused and coherent action on sustainable development at the global, regional, national and local levels, and also help to mainstream sustainable development into the United Nations system by 2030. Information, a leading factor of production cutting across all sectors lacks the due consideration as a significant enabler of progressive development of infrastructure and e-readiness for improved service delivery. Critical Information Infrastructure (CII) players have set up a local, regional and global collaboration arena which inevitably involves among others intensive information sharing, collaboration, distribution and preservation in the cyberspace, powered by assorted information communication technologies (ICTs). The cyberspace, however, has been targeted by cybercriminals with the view to compromising the confidentiality, integrity and availability of strategic information systems in the CII.

Materials and Methods: With Kenya as a case study, using purposive sampling and qualitative analysis using Cybersecurity Capability Maturity Model (C2M2), this study explores the level of cyberspace situational awareness with a view to leveraging on its maturity level.

Results: It is established that cyberspace situation awareness is an obligatory requisite towards cyberspace security management approaches which is predominantly technical solutions oriented. The study further reveals that a thorough and comprehensive cyberspace incidents' intelligence, surveillance and reconnaissance are vital, but missing components to achieving a mature, measured and managed cyberspace which may guarantee the assurance of CII platforms.

Conclusion: In view of these findings, we demonstrate and create insights into how other non-technical thematic areas are pertinent towards the cyberspace situational awareness. It is recommended that adopting suitable framework encompassing technical, social and political facets would enable a maturity, sustainability and furtherance of CII cyberspace situational awareness, being core ingredient of information governance, thus the achievement of the e-readiness for improved delivery of SDGs.

Key Word: Information; Cyberspace; Situation; Awareness; Governance; Surveillance; Intelligence; Maturity.

I. Introduction

Cyberspace refers to a network that connects various IT infrastructure, such as the Internet, telecommunications networks, sensor networks, internal industrial and military networks, industrial systems with embedded controls, the Internet of Things made up of processing devices, various computers systems, and interactions between virtual space and people constructed by information and data[1]. With the development of emerging technologies such as the Internet, the Internet of Things and mobile communications, cyberspace has become a second space for human production and life[2]. Cyberspace has become a new field of geospatial and geographical expansion in the Information Age[3]. It stands in juxtaposition to the real spaces of land, sea, air and outer space as the fifth largest strategic space[4]. The rapid development and massive incorporation of advanced technologies transform industries, services, conflict, government, leisure and social interaction. In the strive for competitive positioning, developers and users often underestimate safety and security considerations, which in turn provides ample opportunities for exploitation by malicious actors [5].

There exist the cyber and the physical environment which bring a large set of opportunities but also new vulnerabilities and threats that must be keenly managed[6]. Under the two major driving forces of state requirements and discipline integration, research on measuring, understanding and representing cyberspace has emerged[7]. Cyberspace situational awareness refers to knowledge about ongoing events in the cyber ecosystem, making human significantly important in the process of achieving quality[8]. Cyberspace

protection is a computer network protection mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks, thus focusing on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with[9].

Therefore, to achieve an effective defence in this hybrid scenario, where risks and threats have moved to a higher level, new strategies, security tools, and remediation plans must be developed complying with current environment demands to both physical and cyber world [10] in order to achieve the adequate hybrid situational awareness.[11] According to[12], although multiple works focus on the study of the CII's risks and threats in the hybrid environment, it is not easy to find an implemented solution that provides the necessary cyber- physical situational awareness to protect them efficiently from potential cyber-attacks.

It was generally observed that the sole responsibility of cyberspace regulation was undertaken by the state. Even with the most updated laws and regulations aligned with the contemporary technology, the effectiveness of cyberspace regulation will not be adequately achieved[13]. The regulation of the cyberspace is pertinent to the protection of the CII by providing both active and passive reinforcement of the deterrent, preventive, detective and corrective controls. However, dictating cybersecurity policy through traditional top-down approaches has engendered stagnation in network protection as cybersecurity personnel become preoccupied with compliance rather than the intent of the policy[14]. Regulatory approaches may be desired to ensure a common standard is required of all, to promote certain industry practices, where appropriate, and to ensure compliance is not a competitive disadvantage[15].

Ismaili (2017) has presented several views by two divergent scholars: that national laws are best suited to govern the cyberspace, and that international law should be harmonized to regulate the cyberspace. These aforementioned approached by Ismaili (2017) are sanctioned by a state-centric view that transpose a "statal" conceptualization of order onto the cyberspace. The current cyber security frameworks and strategies which are top-bottom government driven and attribution based are deficient to tackle the increasingly sophisticated cyber threats (Shiffman & Ravi, 2013). Some of the goals and mission of a cyber-security regulator according to [16] include ascertaining and agreeing protection goals, setting standards, certifying standards achievement and enforcing compliance, reducing vulnerabilities, reducing compromises and reducing system externalities.

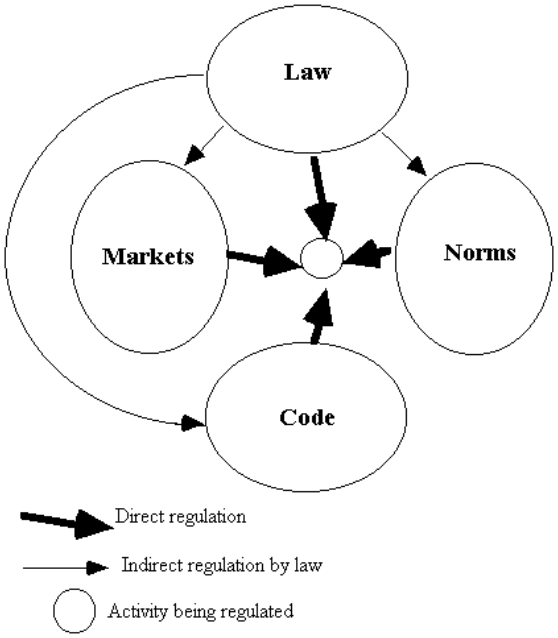

Figure No.1: Four Modalities of Regulation in Real Space and Cyberspace (Lessig, 1999)

According to Lessig (1999), behaviour in the cyberspace is regulated by four kinds of constraints. Firstly, law, which orders people to behave in certain ways and threatens punishment for disobedience. Secondly, norms, which are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate. Thirdly, markets, which operate within the domain permitted by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behaviour. Lastly, the code or architecture, which refers to the software and hardware that make cyberspace the way it is, and constitutes a set of constraints on how one can behave.

II. Material and Methods

The study population was the conglomeration body for cyberspace surveillance and regulation in Kenya, referred to as the National Cyber Security Committee. The committee draws membership from the lead telecommunication regulator (Communications Authority of Kenya); three key government ministries (Ministry of Information Communication Technology,

Ministry of Interior and Coordination of National Government, and the Ministry of Defence); the Information Communication Technology (ICT) Authority and the Central Bank of Kenya. The target population for respondents for the regulatory framework were 42 senior officers handing various portfolio of governance and cyber security at various Regulatory Authorities (Communication Authority and ICT Authority) under the Ministry of ICT, Innovation and Youth Affairs. Census was used to select the sample for regulatory authorities, hence no sample size was estimated.A structured questionnaire was administered as a primary tool for the data collection. Within the questionnaire, which is a set of questions to which respondents recorded their answers within closely defined alternatives Sekaran and Bougie (2010), was close-ended questionnaires as to guarantee uniform responses from the different respondents reached out to.

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 0.852 and 0.659 for Regulatory Framework and Situational-Aware Cyberspace – Regulatory framework 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

Response Rate

The response rate represents the total number of respondents who participated in the study, presented in its percentage form. The researcher shared a link to the questionnaire on google docs to 52 senior officers handling various portfolios of governance and cybersecurity, out of which 47 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 90%. 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.2 below:

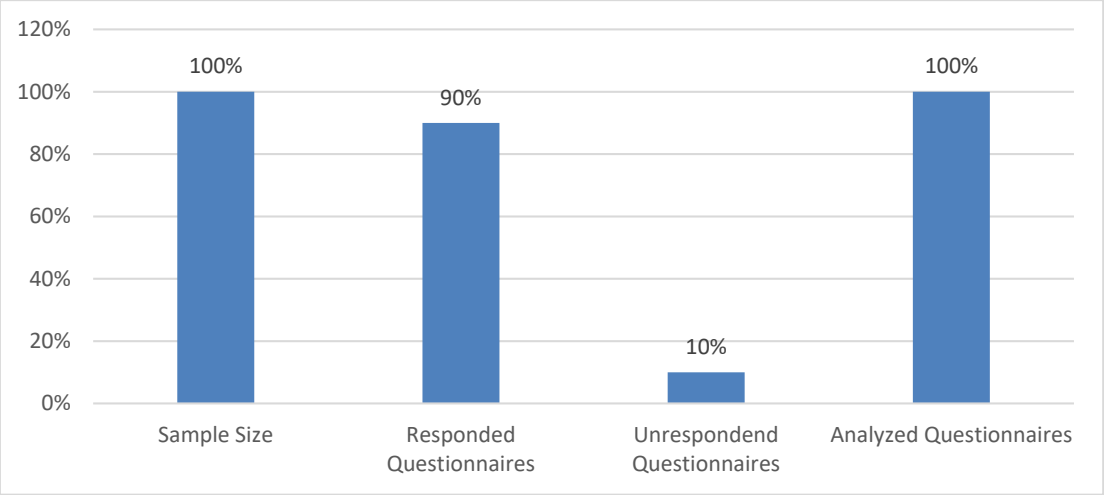

Figure No. 2: Response Rate for Regulatory Framework

Ratings for Situational-Aware

Descriptive statistics in terms of means and standard deviation were used to analyse the ratings for situational-aware variable and the findings are in Table No.1. The findings from Table No.1 indicate that most of the respondents agreed that operational environments are continuously monitored for anomalous behavior that may indicate a cybersecurity event($M = 3.57, SD = 0.773$). This is the variable that stood out across all the variables for situational-aware.

Table No1: Ratings for Situational-Aware

	Statement	Mean	SD
1.	Cybersecurity monitoring activities are performed.	2.83	1.070
2.	Operational environments are continuously monitored for anomalous behavior that may indicate a cybersecurity event.	3.57	0.773
3.	Monitoring and analysis requirements have been defined.	3.43	0.972
4.	Alarms and alerts are configured to aid in the identification of cybersecurity events.	3.55	0.829
5.	Indicators of anomalous activity have been defined.	3.53	0952
6.	Monitoring is integrated with other business and security processes	3.04	0.977

Ratings for Establishment and Maintenance of a Common Operating Picture

Descriptive statistics in terms of means and standard deviation were used to analyse the ratings for establishment and maintenance of a Common Operating Picture (COP) variable and the findings are in Table No.2. The findings from Table No.2 indicate that most of the respondents agreed that information from outside the organization is collected to enhance the COP($M = 3.60, SD = 0.825$). This variable stood out across all the variables under establishment and maintenance of a common operating picture.

Table No.2: Ratings for Establishment and Maintenance of a COP

	Statement	Mean	SD
1.	Methods of communicating the current state of cybersecurity for the organisation are established and maintained.	3.32	0.98
2.	Monitoring data are aggregated to provide an understanding of the operational state of the organisation.	3.09	0.977
3.	Information from across the organization is available to enhance the COP.	3.45	0.928
4.	Information from outside the organization is collected to enhance the COP.	3.60	0.825
5.	Documented practices are followed for logging, monitoring, and COP activities.	3.45	0.855
6.	Stakeholders for logging, monitoring and COP activities are identified and involved.	3.60	0.742
7.	Adequate resources are provided to support logging, monitoring and COP activities.	1.51	0.547
8.	Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy.	2.96	1.021
9.	Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel.	2.62	1.033
10.	Staff performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities.	2.36	0.942

Ratings for Sharing Cybersecurity Information

Descriptive statistics in terms of means and standard deviation were used to analyze the ratings for sharing cybersecurity information variable and the findings are in Table No.3. The findings from Table No.3 indicate that most of the respondents agreed that the organization participates with information sharing and analysis centers ($M = 3.62, SD = 0.848$). This variable that stood out across all the variables for sharing cybersecurity information.

Table No.3: Ratings for Sharing Cybersecurity Information

	Statement	Mean	SD
1.	Information is collected from and provided to selected individuals and/or organizations.	1.91	0.654
2.	Responsibility for cybersecurity reporting obligations are assigned to personnel.	1.70	0.507
3.	Information-sharing stakeholders are identified based on their relevance to the continued operation of the organisation.	1.83	0.601
4.	Information is collected from and provided to identified information-sharing stakeholders.	3.40	0.925
5.	Technical sources are identified that can be consulted on cybersecurity issues.	2.72	1.015
6.	Provisions are established and maintained to enable secure sharing of sensitive information.	2.79	0.977
7.	Information-sharing practices address both standard operations and emergency operations.	3.49	0.906
8.	Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure.	3.45	0.88
9.	The organization participates with information sharing and analysis centers.	3.62	0.848
10.	Information-sharing requirements have been defined for the organisation.	3.34	0.984
11.	Procedures are in place to analyze and de-conflict received information.	2.77	1.047
12.	A network of internal and external trust relationships has been established to vet and validate information about cyber events	3.34	0.891

Ratings for Management Activities

Descriptive statistics in terms of means and standard deviation were used to analyse the ratings for management activities variable and the findings are in Table No.4. The findings from Table No.4 indicate that most of the respondents agreed that the Responsibility and authority for the performance of information-sharing activities are assigned to personnel ($M = 3.55, SD = 0.855$). This variable that stood out across all the variables for management activities.

Table No.4: Ratings for Management Activities

	Statement	Mean	SD
1.	Documented practices are followed for information-sharing activities.	3.43	0.878
2.	Adequate resources are provided to support information-sharing activities.	3.40	0.876
3.	Information-sharing activities are periodically reviewed to ensure conformance with policy.	3.34	0.814
4.	Responsibility and authority for the performance of information-sharing activities are assigned to personnel.	3.55	0.855
5.	Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities.	3.51	0.856
6.	Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate.	3.04	0.977

Correlation Analysis

To determine the strength and direction of the relationship/association between maturity of cyberspace regulatory frameworks and situational-aware, correlational analysis was done. The results are presented in Table No.5. Findings in Table No.5 indicate that there was a statistically significant weak and positive association /relationship between maturity of cyberspace regulatory frameworks and situational-aware, $r\ (47) = 0.414, p < .05$.

Table No.5: Correlation between Maturity of Regulatory Frameworks on Situational-Aware

		Situational-Aware Cyberspace Protection	Regulatory Framework
Situational-Aware Cyberspace Protection	Pearson Correlation	1	.414**
	Sig. (2-tailed)		.004
	N	47	47

Regulatory Framework	Pearson Correlation	.414**	1
	Sig. (2-tailed)	.004	
	N	47	47
**. Correlation is significant at the 0.01 level (2-tailed).			

Tests for assumptions of Linear Regression Analysis

Prior to linear regression analysis, tests 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 regulatory framework variable has a normal distribution, the study used Shapiro-Wilk test. The findings in Table No.6 indicate that data for regulatory framework variable is approximately normal.

Table No.6: Test for Normality for Regulatory Framework Variable

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.
Regulatory Framework	.165	47	.003	.962	47	.129
a. Lilliefors Significance Correction						

Test for Linearity

To determine if the relationship between maturity of cyberspace regulatory frameworks 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 maturity of cyberspace regulatory frameworks and situational-aware, $F\ (1, 25) = 1.808, p > .05$).

Table No.7: Test for Linearity between Regulatory Framework and Situational-Aware

			Sum of Squares	Df	Mean Square	F	Sig.
Situational-Aware Cyberspace * Regulatory Framework	Between Groups	(Combined)	9.361	26	.360	2.256	.033
		Linearity	2.149	1	2.149	13.463	.002
		Deviation from Linearity	7.212	25	.288	1.808	.090
	Within Groups		3.192	20	.160		
	Total		12.553	46			

4.2.7.3 Test for Multicollinearity

To determine the assumption of no multicollinearity between regulatory framework and situational-aware variables, the study used variance inflation factor (VIF) values. Table No.8 presents the VIF values, which indicated that there is no multicollinearity since the VIF value was between 1 and 10.

Table No.8: Test for Multicollinearity between Regulatory Framework and Situational-Aware

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.674	.546		3.065	.004		
	Regulatory Framework	.547	.179	.414	3.049	.004	1.000	1.000
a. Dependent Variable: Situational-Aware Cyberspace								

Linear Regression Analysis Test

The study null hypothesis 1 was formulated from the study specific objective: "To evaluate how maturity of cyberspace regulatory frameworks influences situational-aware cyberspace protection for critical information infrastructure."

Null hypothesis 1(H_0): of maturity of cyberspace regulatory frameworks 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 maturity of cyberspace regulatory frameworks as tested predictor factor. The results are exemplified in Table No.9.

Table No.9: Linear Relationship between Regulatory Framework and Situational-Aware

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.674	.546		3.065	.004	.574	2.775
	Regulatory Framework	.547	.179	.414	3.049	.004	.186	.908
a. Dependent Variable: Situational-Aware Cyberspace Protection								

F (1, 45) = 9.294, P-value <0.05, R-squared = 0.171, Adj R-squared = 0.153

The value of R^2 = 0.171, shows that 17.1% of the situational-aware cyberspace protection is explained by maturity of cyberspace regulatory frameworks (regression line). The value of F (1, 45) = 9.294, P-value < 0.05, shows that maturity of cyberspace regulatory frameworks 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 maturity of cyberspace regulatory frameworks is statistically significant and it significantly influences situational-aware cyberspace protection (t=3.049, $p < .05$). The regression model which explains the results in Table 4.24 is given by:

$$Situational - Aware = 1.674 + 0.547 \times Maturity\ of\ cyberspace\ regulatory\ framework$$

The model shows that maturity of cyberspace regulatory frameworks positively influences situational-aware cyberspace protection, i.e. an increase in maturity of cyberspace regulatory frameworks increases the situational-aware cyberspace protection for critical information infrastructure by a positive unit mean index value of 0.547.

The model shows that regulatory framework is a significant dynamic with fundamental positive effect on situational-aware cyberspace protection i.e. an increase in the variables increases the situational-aware cyberspace protection by a positive unit mean index value. Regulatory Framework is the factor which increases situational-aware cyberspace protection by 0.185. Thus, the constructs derived from the study are illustrated by Figure No**. 3** below.

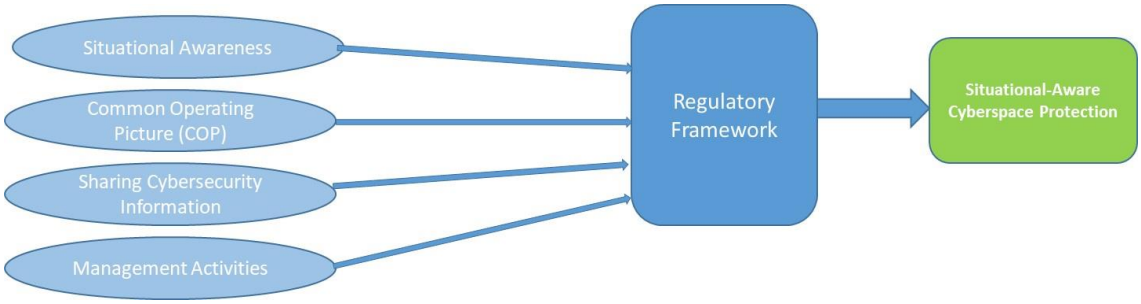

Figure No.3: Constructs Derived from Regulatory Framework Variable

IV. Discussions

In terms of evaluating how maturity of cyberspace regulatory frameworks influences situational-aware cyberspace protection for critical information infrastructure, the study found that there was a statistically significant weak and positive association /relationship between maturity of cyberspace regulatory frameworks and situational-aware, $r\ (47) = 0.414, p < .05$. Maturity of cyberspace regulatory frameworks positively influences situational-aware cyberspace protection (t=3.049, $p < .05$). This implies that the significant role of regulatory provisions embedded in laws, statutes, policies, standards, guidelines amongst others fortify the cyberspace protection's framework. The controls framework stratified as deterrent, preventive, detective and corrective are more likely to be fulfilled.

This means that the availability of effective regulatory bodies to champion and govern the cyberspace has a positive impact towards the realisation of the desired cyberspace protection objectives. This is consistent with the theory of the public interest, also known as the functionalist theory which asserts that regulation exists to promote the public good and increase social welfare [17].

In this study, this perspective was derived from the public sector regulators which seem to domineering the regulation and governance space implying that cyberspace protection frameworks are developed and /or based on securitization of cyber governance. This is consistent with the narrative of [18] that the regulatory tools used to manage cyberspace risks generally involve legislation, binding state guidelines issued by the state regulatory agencies, and self-regulation by conforming to recommended standards. In the perspective of [19], there should be normalisation of a rationale according to which the private sector should be also, and further involved in the regulatory process, as it is associated, not only to a higher degree of efficiency, but also to a greater level

of expertise and knowledge. This would create a shift of the private sector from a victim of cyber-attacks to be protected by national legislation, to a self-regulator with an imposed duty to ensure that it responds effectively to identified security threats, and thereafter to an active participant in shaping regulations applicable to the sector[20]. A collaboration of various sectors within and outside the state helps to achieve these goals since CII sustainability is related to the need to maintain the viability of the environment and society, starting with administration, economic and financial institutions, those of social welfare and health, the military, and civil protection, and ending with supplies of food, water, and energy, transport, communications, amongst others[21]. Similarly, when developing the country's critical infrastructures cyber security model it is also recommended to involve public institutions, national regulators and the private sector[22].

Regulating the cyberspace however, faces some challenges including conflicts between state institutions, tensions between competing/conflicting interests, costs for regulatory compliance, attempts to find the right balance between transparency and secrecy, as well as between centralization and decentralization[23]. [24] holds that whereas escalating enforcement practices should be considered as a way to individualize the regulatory activity's intensity in relation to the regulated actors' behaviour, the default strategy in this context is non-intrusive and delegated regulation, which is more likely to generate cooperation among private actors by allowing them discretion in deciding how best to achieve regulatory goals.

[25] asserts whereas the traditional Command and Control systems-based security tools still do not efficiently integrate the situational awareness of the cyber domain, the most extended cybersecurity solutions do not still provide a single and intuitive visualization space of the whole cyber-physical situation for an adequate decision-making support.

The strength of an effective situational-aware model resides in its three main capabilities: data gathering, data analysis, and data visualization[26].

Assertions of [27] are that for cyber information sharing and situational awareness, the benefits and challenges of emerging technologies, such as artificial intelligence, the human factor, education and training for cyber security and resilience, the need to incorporate the cybersecurity efforts into the search for effective and efficient exploitation of information technologies, policies and solutions for security and resilience of Industry 4.0 and critical infrastructures.

V. Conclusion

The significant role of regulatory provisions embedded in laws, statutes, policies, standards, guidelines amongst others fortify the cyberspace protection's framework. The controls framework stratified as deterrent, preventive, detective and corrective are more likely to be fulfilled. This means that the availability of effective regulatory bodies to champion and govern the cyberspace has a positive impact towards the realisation of the desired cyberspace protection objectives. This is consistent with the theory of the public interest, also known as the functionalist theory which asserts that regulation exists to promote the public good and increase social welfare [23].

Notes

[1] Gao et al., "Theoretical Basis and Technical Methods of Cyberspace Geography."
[2] Gao et al.
[3] Tagarev, "DIGILIENCE - A Platform for Digital Transformation, Cyber Security and Resilience."
[4] Gao et al., "Theoretical Basis and Technical Methods of Cyberspace Geography."
[5] Tagarev, "DIGILIENCE - A Platform for Digital Transformation, Cyber Security and Resilience."
[6] Hingant et al., "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection."
[7] Gao et al., "Theoretical Basis and Technical Methods of Cyberspace Geography."
[8] Al-Shamisi et al., "Towards a Theoretical Framework for an Active Cyber Situational Awareness Model."
[9] Galinec, Moznik, and Guberina, "Cybersecurity and Cyber Defence: National Level Strategic Approach."
[10] Hingant et al., "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection."
[11] Sager and Security, "The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense."
[12] Hingant et al., (2018)
[13] Chang and Grabosky, "The Governance of Cyberspace."
[14] (Wehner, Rowell, Langley, & Mathews, 2017.)
[15] Department of Homeland Security, "A Guide to a Critical Infrastructure Security and Resilience - November 2019."
[16] Clayton and Anderson (2017)
[17] (Siboni & Sivan-sevilla, 2017)
[18] Siboni & Sivan-sevilla (2017)
[19] Carrapico & Farrand (2017)
[20] Carrapico and Farrand.
[21] Turskis et al., "A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development."

[22] Limba et al., "Cyber Security Management Model for Critical Infrastructure."
[23] (Siboni & Sivan-sevilla, 2017)
[24] Dupont (2019)
[25] Hingant et al., (2018)
[26] Hingant et al.
[27] Tagarev, "DIGILIENCE - A Platform for Digital Transformation, Cyber Security and Resilience."

Bibliography

Al-Shamisi, Ahmed, Panos Louvieris, Mohammed Al-Mualla, and Martin Mihajlov. "Towards a Theoretical Framework for an Active Cyber Situational Awareness Model." *International Conference on Systems, Signals, and Image Processing* 2016-June, no. May (2016). https://doi.org/10.1109/IWSSIP.2016.7502753.

Carrapico, Helena, and Benjamin Farrand. "'Dialogue, Partnership and Empowerment for Network and Information Security': The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers." *Crime, Law and Social Change* 67, no. 3 (2017): 245–63. https://doi.org/10.1007/s10611-016-9652-4.

Chang, Lennon YC, and Peter Grabosky. "The Governance of Cyberspace." *Regulatory Theory*, no. April (2017): 533–51. https://doi.org/10.22459/rt.02.2017.31.

Clayton, Richard, and Ross Anderson. *Standardisation and Certification of Safety , Security and Privacy in the ' Internet of Things ,'* 2017. https://doi.org/10.2760/25200.

Department of Homeland Security. "A Guide to a Critical Infrastructure Security and Resilience - November 2019," no. November (2019).

Dupont, Benoît. "The Cyber-Resilience of Financial Institutions: Significance and Applicability." *Journal of Cybersecurity*, 2019. https://doi.org/10.1093/cybsec/tyz013.

Galinec, Darko, Darko Moznik, and Boris Guberina. "Cybersecurity and Cyber Defence: National Level Strategic Approach." *Automatika* 58, no. 3 (2017): 273–86. https://doi.org/10.1080/00051144.2017.1407022.

Gao, Chundong, Qiquan Guo, Dong Jiang, Zhenbo Wang, Chuanglin Fang, and Mengmeng Hao. "Theoretical Basis and Technical Methods of Cyberspace Geography." *Journal of Geographical Sciences* 29, no. 12 (2019): 1949–64. https://doi.org/10.1007/s11442-019-1698-7.

Hingant, Javier, Marcelo Zambrano, Francisco J. Pérez, Israel Pérez, and Manuel Esteve. "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection." *Security and Communication Networks* 2018 (2018). https://doi.org/10.1155/2018/5625860.

Limba, Tadas, Tomas Plėta, Konstantin Agafonov, and Martynas Damkus. "Cyber Security Management Model for Critical Infrastructure." *Entrepreneurship and Sustainability Issues* 4, no. 4 (2017): 559–73. https://doi.org/10.9770/jesi.2017.4.4(12).

Sager, Tony, and Internet Security. "The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense," n.d.

Siboni, Gabi, and Ido Sivan-sevilla. "Israeli Cyberspace Regulation : A Conceptual Framework , Inherent Challenges , and Normative Recommendations" 1, no. 1 (n.d.): 83–102.

Tagarev, Todor. "DIGILIENCE - A Platform for Digital Transformation, Cyber Security and Resilience." *Information & Security: An International Journal* 43, no. 1 (2019): 7–10. https://doi.org/10.11610/isij.4300.

Turskis, Zenonas, Nikolaj Goranin, Assel Nurusheva, and Seilkhan Boranbayev. "A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development." *Sustainability (Switzerland)* 11, no. 2 (2019). https://doi.org/10.3390/su11020424.

Wehner, Gregory, James Rowell, Joseph Langley, and Joseph Mathews. "Federated Cybersecurity Policy Arbitration," n.d., 1–3.

Ismaili, M. A. (2017). *The cyber ungovernmentality hypothesis*. *10*(1), 17–30. https://doi.org/10.7903/ijcse.1510

Saunders, M., Lewis, P., & Thornhill, A. (2006). Understanding research philosophies and approaches. *Reserach Methods for Business Students*, 127–148.

Shiffman, G. M., & Gupta, R. (2013). Crowdsourcing cyber security: A property rights view of exclusion and theft on the information commons. *International Journal of the Commons*, *7*(1), 92–112.