International Journal of Arts and Social Science **www.ijassjournal.com**
ISSN: 2581-7922,
Volume 5 Issue 3, March 2022

Development of Six Ware Cyber Defense Framework (SWCDF) Design as a Standardization of Computer Network Protection State Defense Information System

Rudy Agus Gemilang Gultom[1], Ahmad Farid Wajdi[2]
[1](Researcher, Adjunct Professor,Faculty ofDefense Technology, Indonesian DefenseUniversity, Indonesia)
[2](Researcher, Research and Development Agency, Ministry of Defense of the Republic of Indonesia, Indonesia)

ABSTRACT: *Cyber attacks are actions aimed at altering, disrupting, deceiving, degrading, or destroying information technology systems and their networks or existing information and programs (flowing) and stored in the system. Development of a cyber defense system for critical military infrastructure, and building readiness in the face of cyber warfare because the virtual world is a battlefield that will determine victory in war. This study aims to find an effective cyber defense system design to protect the Ministry of Defense's critical infrastructure and state defense information system (Sisinfohanneg) from the threat of cyber attacks and to prepare both cyber warfare capabilities. The results obtained are that the response framework to cyber threats at the Pusdatin and Pushansiber of the Ministry of Defense shows the readiness for development is adequate or good with ICSW >3.5. The proposed measurement concept has been able to formulate the ICSW index through modeling: ICSW = 0.208*BW + 0.228*HW + 0.095*SW + 0.079*IW + 0.305*FW + 0.085*BG. The ideal cyber defense design at the Ministry of Defense is to follow the Sixware Cyber Defense Framework with its six factors (Brainware, Hardware, Software, Infrastructure ware, Firmware and Budgetware) to improve the cyber defense system. For this reason, the availability of the measurement formula makes the Cyber Sixware Defense Framework concept more complete to implement.*

KEYWORDS *- Sixware Cyber Defense Framework, Cyber Attack, Cyber Defense, State Defense Information System*

I. INTRODUCTION

1.1 BACKGROUND

It is undeniable, in the era of the Industrial Revolution 4.0 and the Internet of Things (IoT) and in the midst of the rampant development of the Society 5.0 society, human dependence on information and communication technology is getting bigger. Economic activities, public services, politics, security, and even defense are now increasingly computerized, autonomous, and integrated, making it easier, more effective, and efficient. For the military, information technology significantly increases the effectiveness, efficiency, and lethality of troops in carrying out missions. Information technology and computers create command and control processes; detection system; navigation; target acquisition system; intelligence gathering; information dissemination; and the management of military organization administration is becoming more effective, autonomous, fast, near instantaneous, efficient, and integrated. Ironically, with the increasingly computerized armed forces, it creates a new threat to the system. Cyber attacks can cause disruption and damage to the network system that connects, integrates, synchronizes, and controls the computerized and integrated military equipment and infrastructure.

Cyber attacks are actions aimed at altering, disrupting, deceiving, degrading, or destroying information technology systems and their networks or existing information and programs (flowing). and stored) in the system [1].

Cyber attacks can also arise from non-state actors. Cyber attacks from non-state actors can be in the form of cyber crimes, cyber riots/hacktivists (cyber vandalism), and cyber espionage (Schreier, 2015: 8-9). Cybercrime is a cyber attack that aims to profit from criminal activity in cyberspace. Cyber riots are cyber attacks aimed at conveying certain political messages by damaging or interfering with the performance of the cyber activity being attacked. Cyber espionage is an attack in the form of gathering confidential information belonging to an opponent for his or her benefit. Cybercriminals use cyberspace to earn money through fraud, extortion, account theft, and so on.

It is also possible for cybercriminals to attack important facilities and infrastructure belonging to law enforcement officers to smoothen their actions in the real world, such as hacking surveillance camera systems at police stations and banks to facilitate robberies, or interfering with surface and aerial radars to disguise the process of smuggling illegal goods. in the sea and in the air. Cyber rioters use cyberspace as a way to convey political messages such as environmental and animal protection, rejection of certain government policies, or demands for human rights enforcement such as hacktivist attacks on the Indonesian Ministry of Foreign Affairs website in the late 1990s. Cyber riot attacks have occurred when NATO accidentally dropped a bomb on the Chinese Embassy in Belgrade in May 1999 which led Chinese hacktivists to attack the website of the United States Government (Schreier, 2015: 108). Cyber espionage actors use cyberspace to collect valuable information such as personal data for extortion, intelligence data, troop movement positions, or weapons technology blueprints. One example of a significant case of cyber espionage is the theft of data relating to the blueprint of the F-35 fighter aircraft by Chinese hackers in Canada (vice.com).

The most important cyber attacks to watch out for are the Stuxnet and WannaCry worm attacks. The Stuxnet worm is considered very sophisticated because its features are very complex, difficult to detect, and can even attack specific targets. The Stuxnet worm becomes active and functional if the computer uses the Windows operating system, and it includes the Siemens step7 software which is a program for the Industrial Control System (ICS). The Stuxnet worm was made to be able to take over the entire control system and find out the activities carried out by the program it attacked to the programmer / creator (Rao, 2014: 3). This means that it is not only capable of performing cyber attacks, Stuxnet is also capable of simultaneously conducting cyber espionage so it is very dangerous if this worm is programmed to attack the control system of military defense equipment.

It should be noted that Indonesia is one of the countries affected by the Stuxnet attack (Kerr et al, 2010:1). Stuxnet was first detected by a security company in Belarus in June 2010 and is known to be programmed to specifically attack the ICS controlling the nuclear reactor, which in this case is Iran's nuclear reactor because Iran is the country with the worst Stuxnet attacks. Stuxnet can be spread manually via a thumb drive (flash disk) or via an internet connection (Kerr et al, 2010: 1) and can be easily obtained freely on the internet (Kerr et al, 2010: 2). Stuxnet's sophistication is also enhanced by its ability to automatically update (Mueller and Yadegari, 2012: 3) so that it can be properly set according to the needs of the programmer and potentially more difficult to detect and eliminate. Stuxnet is a real cyber attack threat because of its algorithms set to attack the Windows platform, which is widely used as an ICS operating system and military defense equipment, such as on Britain's newest aircraft carrier Queen Elizabeth.

WannaCry is a ransomware type malware. Ransomware extorts computer users by infecting and locking/encrypting the files it attacks and to open it, you are required to pay a certain amount of money (using digital currency such as bitcoin). Even then it is not guaranteed 100% after the payment is made the file will be immediately decrypted (Mohurle, Savita and Manisha Patil, 2017: 1939). Because WannaCry works by opening a file, reading its contents, encrypting the file, then closing the file (Mohurle& Patil, 2017: 1939), it is very likely that the data and information contained in the infected file will be stolen. This means that if a file belonging to the military is attacked by WannaCry, not only can the file not be opened, but also its contents are stolen by the author so that national security can be threatened.

The Wanna Cry attack was the largest cyber attack in 2017 and attacked up to 200,000 computer systems (Naidu & Sireesha, 2017:83) in the banking, office, health, automotive industry, to strategic infrastructure such as port terminals worldwide. Given the increasing dependence of the military on the use of information and communication technology, cyber security for the military is very important. Previously, several examples of how cyber attacks could interfere with military performance in carrying out their missions were described, such as sabotage of air threat detection systems, theft of critical data, to "theft" of robotic defense equipment (drones). Even cyberspace or the virtual world is now considered the fifth combat dimension, after the land, sea, air, and outer space dimensions. Countries such as the United States, China, North Korea, Iran, and Russia are also actively developing cyber capabilities as a supporting element in winning wars. In the future, the military will make cyber elements an integrated and crucial part due to increasingly network-centric warfare, as a consequence of the increasing military investment in information and communication technology, nanotechnology, and computers. However, the main concern and concern for cyber defense should be focused on protecting critical military infrastructure. Infrastructure is a system that combines various facilities so that from this combination an activity can be carried out (Tabansky, 2011: 61).

Tabansky added that an infrastructure is declared critical if the disturbance that occurs on it can cause a socio-economic crisis, which can further lead to community instability which has bad political, strategic and security consequences (Tabansky, 2011: 62). According to the USA Patriot Act Session 1016, critical infrastructure is systems and assets, both physical and virtual, whose paralysis and damage will affect national security, the national economy, public safety and health, or a combination of these conditions.

If it is related to the military, critical military infrastructure is military facilities, systems and assets, both physical and virtual, which in the event of a disturbance can have a catastrophic impact in the implementation of a military activity. Radars, satellites, satellite control stations, communications facilities, broadband towers, fuel depots, water management facilities, power plants, power substations, computer control equipment, and servers are some examples of critical military infrastructure. Currently, these critical military infrastructures can become targets for cyber attacks due to computerization and the implementation of information technology. Although the period of cyber attacks tends to be short, if carried out at critical times such as when an invasion is initiated by another country, it can provide an easy victory on the enemy side like Russia's military victory over Georgia in 2008 which took advantage of cyber attacks . If cyber-defense systems are not built effectively, cyber attacks can last as long as the cyber attackin Estonia by Russian hackers.

1.2 RESEARCHQUESTION

Based on this, it is important for the TNI to develop a cyber defense system for critical military infrastructure, and build readiness to face cyber warfare because the virtual world is a battlefield that will determine victory in war. The form of cyber attacks in the future will be more complex and can attack at any time. Cyber attack actors such as hacktivists (cyber activists); hacker (hacker); malware creators, spammers, and private data collectors; botnet herder (botnet herder); hackers from organized criminal organizations; internal employees/traitors of the institution itself; security/intelligence institutions; and terrorist-radical groups (Tabansky, 2011:83-84) can at any time attack the TNI cyber system for their own sake. All of these actors can come from state and non-state actors so that the TNI must be ready to ward off cyber attacks from various actors in accordance with the character of the attacks from these parties.

This research is directed to answer the following research questions. 1) What is the response framework to cyber threats, and work priority options related to other national-level security issues? For example, in the Strategic Plan of the Ministry of Defense, cyber is a priority for the 2020-2024 Strategic Defense and Security work; 2) What is the measurement framework for the cyber defense index where does it fit in this context?

1.3 RESEARCHOBJECTIVES

This study aims to find an effective cyber defense system design to protect the Ministry of Defense's critical infrastructure and state defense information system (Sisinfohanneg) from the threat of cyber attacks and to prepare both cyber warfare capabilities. This design must be made based on the current form and condition of cyber threats and the ability to adapt to the dynamism of future conditions. The hope is that critical infrastructure and information systems of the Sisinfohanneg information system are optimally protected from cyber attacks and are able to carry out cyber warfare effectively.

The urgency of this research is due to the increasing complexity of cyber defense threats and the increasing number of actors involved in the use of cyber media to gain advantages and advantages from other parties. The acquisition of information technology by the Ministry of Defense to facilitate the implementation of tasks and missions is also getting bigger, so that the disruption of their activities by cyber attacks is very possible.

Disruption due to cyber attacks can hinder mission execution, create chaos, and even cause damage to assets and loss of life considering that more work and equipment are integrated with information and communication management tools. In addition, the perception of cyberspace as a new medium of battle shows that war by the military is no longer limited to only occurring on land, sea, air, and outer space, but also in cyberspace.

Warfare in the modern era is increasingly network centric and is largely determined by cyber defense, so building cyber warfare capabilities also needs to be a priority. In the Strategic Plan Of The Ministry Of Defense And The Indonesian National Army for 2020-2024 (Ministry of Defense No. 10 of 2021) it is emphasized the need to strengthen cyber defense and the establishment of a Computer Emergency Response Team (CERT). In this regard, it is important to have an effective cyber defense system design concept in protecting critical infrastructure and national defense information systems from the threat of cyber attacks and to have the concept of developing cyber warfare capabilities.

In addition, this research also has the target of making this application system for finding cyber defense system vulnerabilities easily, quickly, and accurately so that it can be used as a basic reference for building strong cyber defense systems in other agencies.

II. RESEARCHMETHOD

2.1 RESEARCH STEPS

This type of research is exploratory research with a mixed methods design, which is a research framework that combines quantitative and qualitative research methods (Creswell & Clark, 2018:5). With such an approach, the researcher uses two types of data to be analyzed in parallel, namely qualitative data analysis and quantitative data inference in parallel to obtain a convergence of conclusions. To obtain qualitative data, this study conducted interviews with one resource person at Pusadatin and Pushansiber each. For this purpose, structured interview questions based on a cyber-sixware framework were developed.

Meanwhile for quantitative data, the research team explored the elements of the cyber-sixware framework in such a way as to obtain an instrument and confirm it with the results of interviews. Such a research strategy is called a sequential exploratory strategy[49]. In the first stage the researcher collects and analyzes qualitative data then collects quantitative data and analyzes it in the second stage which is based on the results of the first stage. The stages of the research are as shown in Figure 2.1.

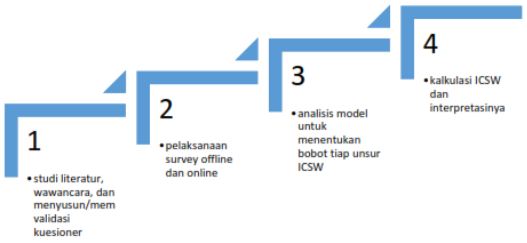

Figure 2.1ResearchSteps

Referring to Figure 2.1, the research design is divided into four stages, namely: First, literature study, interviews, and compiling and validating a questionnaire to ascertain the constructs/variables and indicators in the constructed ICSW model; second, the implementation of offline and online surveys; the third analysis model to determine the weight of each element; and fourth, ICSW calculation and interpretation.

2.2 RESEARCHSTEPS

By considering the background, problem formulation, research questions, literature review, and research framework, this study will examine the effectiveness of the SWCDF framework to understand loci conditions in the context of research questions. It can be interpreted that the role of primary data is very significant in research to determine the condition of the locus in the context of this research question. In addition, respondents and resource persons selected in this study were officials, employees and computer technicians at the research locus object at the PusdatinKemhan and Pushansiber who were assumed to be able to provide a comprehensive explanation of the implementation of cybersecurity systems. Meanwhile, field survey data collection was carried out online due to the Covid-19 pandemic, so there was a "lockdown" policy imposed at the Ministry of Defense which caused most employees to "Work-From-Home (WFH)".

2.3 RESEARCHSTEPS

a. INTERVIEW

The interview technique used in this research is structured interviews online/online through social media networks and the Internet through the interview question guidelines that have been prepared. This is because PPKM is still in effect in Jakarta and its surroundings, due to the Covid-19 pandemic situation, most of the personnel in the three agencies work at home (Work From Home/WFH), so that researchers have difficulty conducting face-to-face interviews. face-to-face). This online interview technique is used as a data collection technique on the grounds that there needs to be a match between the themes of qualitative questions and quantitative questionnaires.

Thus the assumption is that this research requires qualitative data related to the indicators in the questionnaire (quantitative). Therefore, in conducting interviews, the interviewer has prepared research instruments in the form of prepared questions. With this structured interview, each respondent is given the same question by the interviewer and the data collector records it, either online or online.

b. SURVEY

The survey was conducted by compiling a questionnaire in the form of a list of questions which was then distributed to the respondents directly so that the results of the filling would be clearer and more accurate. Researchers distributed questionnaires to respondents using a list of questions related to the knowledge, skills, abilities and performance of employees in the development of cyber defense technology against cyber threats or attacks.

c. SAMPLING

By using a simple random sampling approach, population assumptions, and with two approaches, namely Cochran [50], the data requirements are obtained as shown in the following table.

Table 2.1samplerequirement

Lokus	Populasi (N)	Cochran (moe=5%, conf level=95%)
Pusdatin	100	80
Pus Siberhan	50	45
Total	**150**	**125**

With the Rule of Thumb approach to modeling [51], the sample requirement is 7 x 10 = 70 samples (respondents). Thus, in collecting data in this study, at least 70 samples were obtained and if possible, 125 samples or more were obtained.

III. RESULT

3.1 DESCRIPTIVE DATA RESULTS

The following are the results of data preparation, namely efforts to clean data from Outlier. In this study, the researcher used the Grubb Test [56], [57]. The treatment for outliers is to replace them with MEAN (mean).

a. DATA PREPARATION

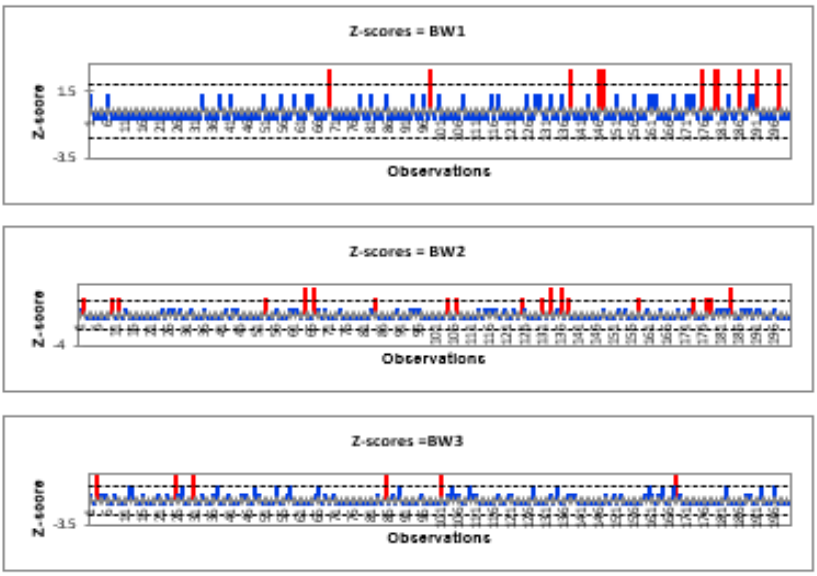

Figure 3.1Outlier Data Brainware

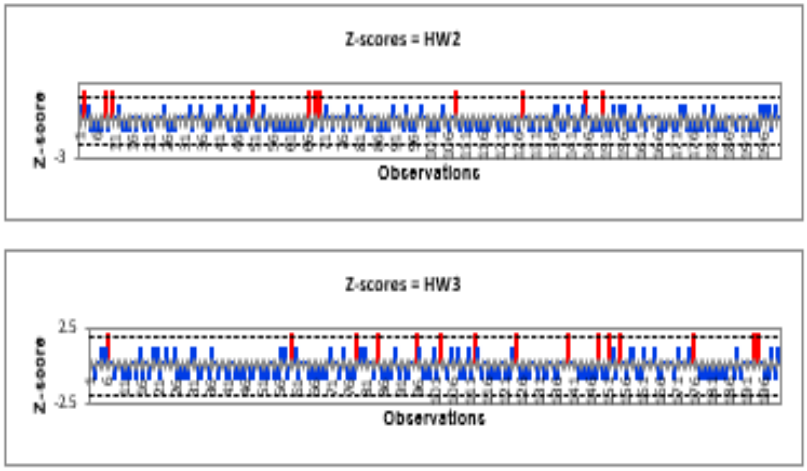

Figure 3.2*Outlier* Data *Hardware*

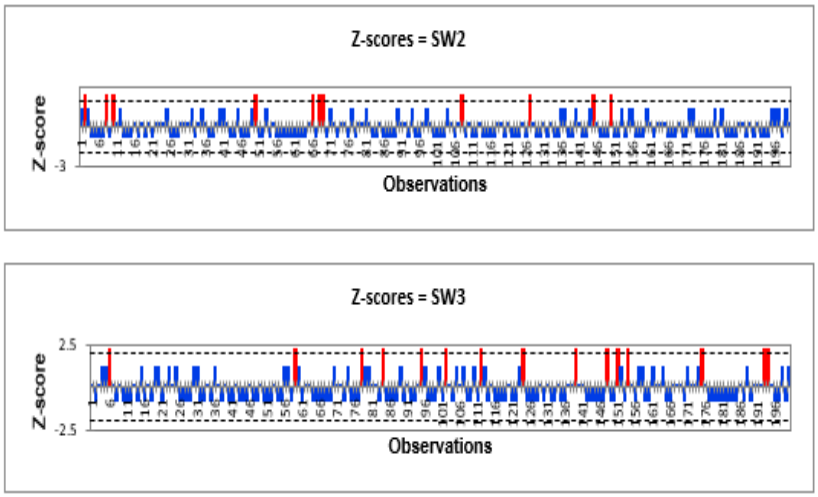

Figure 3.3*Outlier* Data *Software*

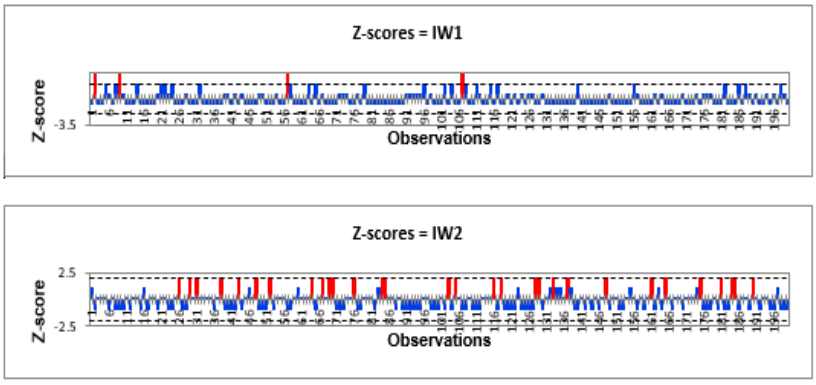

Figure 3.4*Outlier* Data *Infrastructure-ware*

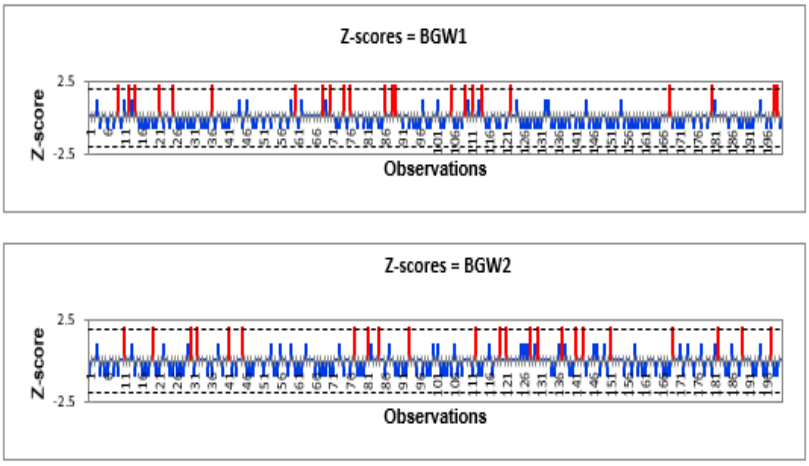

Figure 3.5*Outlier* Data *Budgetware*

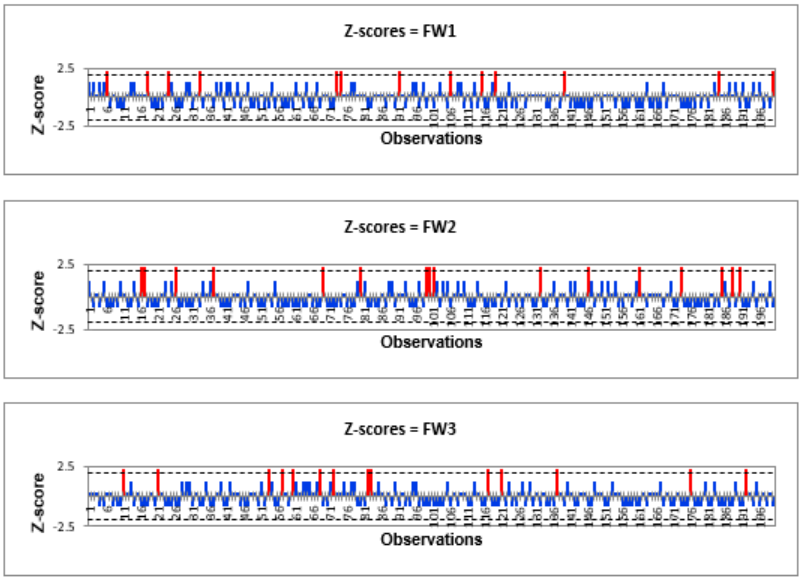

Figure 3.6*Outlier* Data *Firmware*

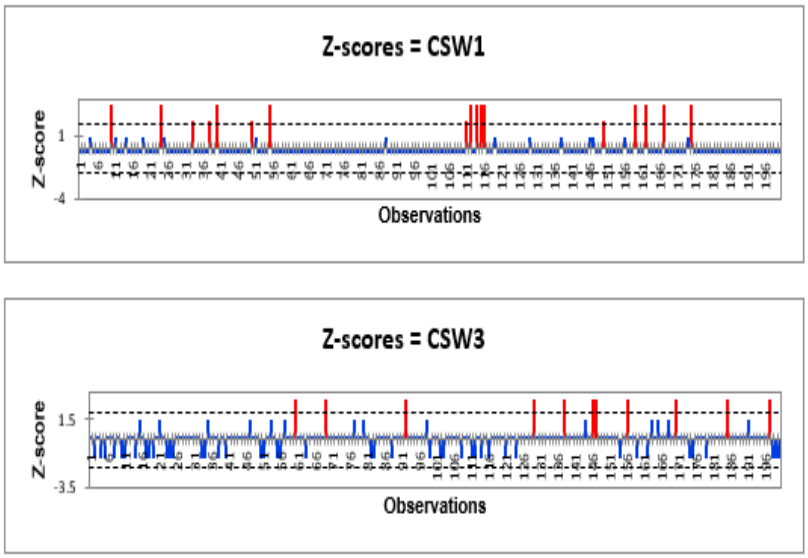

Figure 3.7*Outlier* Data Persepsi Aman

b. DATA DESCRIPTION

Table 3.1DescriptionofQuantitative Data

Statistic	Nbr. of observations	Min	Max	Freq. of minimum	Freq. of maximum	Mean	Standard deviation (n-1)
BR1 WIKI	200	0.000	100.000	7	22	50.625	25.613
BR1 WIKI | LAINNYA	9	0.000	100.000	1	3	66.667	33.333
BR1 WIKI | PUSDATIN	99	0.000	100.000	2	11	50.758	25.116
BR1 WIKI | PUSHANSIBER	92	0.000	100.000	4	11	50.543	26.462
BR1 YT	200	0.000	100.000	38	83	61.250	37.322
BR1 YT | LAINNYA	9	0.000	100.000	3	2	44.444	39.087
BR1 YT | PUSDATIN	99	0.000	100.000	18	37	59.596	36.194
BR1 YT | PUSHANSIBER	92	0.000	100.000	17	44	64.674	38.186
BR1 GS	200	0.000	100.000	30	37	48.375	34.371
BR1 GS | LAINNYA	9	0.000	100.000	4	4	50.000	50.000
BR1 GS | PUSDATIN	99	0.000	100.000	16	13	46.465	32.735
BR1 GS | PUSHANSIBER	92	0.000	100.000	14	24	50.272	36.969
BR2	200	0.000	100.000	6	42	70.875	22.525
BR2 | LAINNYA	9	0.000	100.000	1	4	66.667	35.355
BR2 | PUSDATIN	99	0.000	100.000	3	26	72.727	22.894
BR2 | PUSHANSIBER	92	0.000	100.000	3	12	67.663	22.094
BR3	200	0.000	100.000	15	62	65.875	30.094
BR3 | LAINNYA	9	0.000	100.000	2	5	66.667	44.096
BR3 | PUSDATIN	99	0.000	100.000	8	33	66.667	30.929
BR3 | PUSHANSIBER	92	0.000	100.000	7	24	64.130	29.019
BR4	200	0.000	100.000	41	65	50.375	39.824
BR4 | LAINNYA	9	0.000	100.000	3	2	33.333	39.528
BR4 | PUSDATIN	99	0.000	100.000	19	38	54.040	40.987
BR4 | PUSHANSIBER	92	0.000	100.000	19	25	48.098	38.380
BR5-1	200	0.000	100.000	9	80	70.625	29.275

Table 3. 2DescriptionofQualitative Data

Variable\Statistic	**NumberofObservations**	**Frequency per category**	**Proportion per category**
GROUP	200	179.000	0.895
Online		21.000	0.105
GROUP | LAINNYA	9	6.000	0.667
Online		3.000	0.333
GROUP | PUSDATIN	99	94.000	0.949
Online		5.000	0.051
GROUP | PUSHANSIBER	92	79.000	0.859
Online		13.000	0.141

3.2 INFERENTIALANALYSIS

In the MANOVA approach, the six elements of SWCDF are analyzed according to categories according to a scale. The results are as follows:

Table 3.3Manova: Wilks' test (Rao'sapproximation)

	BW	HW	SW	IW	FW	BGW
Lambda	0.499	0.737	0.582	0.782	0.794	0.936
F (Observed values	92.291	16.394	66.091	17.146	23.827	6.239
DF1	2	4	2	3	2	2
DF2	184	184	184	184	184	184
F (Critical value)	3.045	2.421	3.045	2.654	3.045	3.045
p-value	< 0.0001	< 0.0001	< 0.0001	< 0.0001	< 0.0001	0.002

The table above shows the significance of the Wilk test results where the Budget shows the greatest influence of the observed elements on the CSW security index

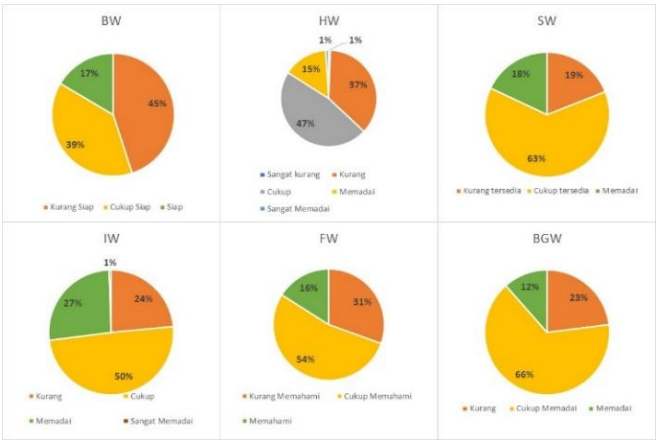

Figure 3.8CWS elementcategorizationbasedon MANOVA

From Figure 3.8 it can be seen that almost all respondents still perceive that the six elements are not optimal in the Ministry of Defense, except for hardware (HW) which is relatively adequate or adequate (>50%). The problem that is seen as the most crucial is the Budget element (BGW) 66%.

To analyze univariately, we use Principal Component Analysis (PCA), which simplifies the data to only F1 (one data) for each element and rotates (Square of Cosin), it is clearly seen that the current Budget Element is not significant. on the measurement of the CWS Index.

Table 3.4 Analisis Anova

Goodness of fit statistics (CSW):	
Observations	200.000
Sum of weights	200.000
DF	194.000
R^2	0.980
Adjusted R^2	0.979
MSE	0.251
RMSE	0.501
MAPE	12.677
DW	1.028
Cp	-180.450
AIC	-270.403
SBC	-250.613
PC	0.021
Press	52.199
Q^2	0.979

Analysis of variance (CSW):

Source	DF	Sum of squares	Mean squares	F	Pr > F
Model	6	2385.270	397.545	1582.664	**< 0.0001**
Error	194	48.730	0.251		
Corrected Total	200	2434.000			

Computed against model Y=0

Table 3.5Tipe Sum of Square I, III and Parametric Test

Type I Sum of Squares analysis (CSW):

Source	DF	Sum of squares	Mean squares	F	Pr > F
BW	1	2316.953	2316.953	9224.011	**< 0.0001**
HW	1	35.182	35.182	140.065	**< 0.0001**
SW	1	14.500	14.500	57.725	**< 0.0001**
IW	1	5.122	5.122	20.390	**< 0.0001**
FW	1	13.096	13.096	52.136	**< 0.0001**
BGW	1	0.417	0.417	1.659	0.199

Type III Sum of Squares analysis (CSW):

Source	DF	Sum of squares	Mean squares	F	Pr > F
BW	1	4.312	4.312	17.165	**< 0.0001**
HW	1	3.747	3.747	14.916	**0.000**
SW	1	0.778	0.778	3.099	0.080
IW	1	1.472	1.472	5.859	**0.016**
FW	1	9.445	9.445	37.600	**< 0.0001**
BGW	1	0.417	0.417	1.659	0.199

Model parameters (CSW):

Source	Value	Standard error	t	Pr > |t|	wer bound (95%)	per bound (95%)
Intercept	0.000					
BW	0.245	0.059	4.143	**< 0.0001**	0.128	0.362
HW	0.192	0.050	3.862	**0.000**	0.094	0.291
SW	0.134	0.076	1.760	0.080	-0.016	0.285
IW	0.152	0.063	2.421	**0.016**	0.028	0.276
FW	0.338	0.055	6.132	**< 0.0001**	0.229	0.446
BGW	0.096	0.075	1.288	0.199	-0.051	0.243

The table above shows that the budget and software for computer and network security of the Ministry of Defense are elements that are less supportive. This can be seen in the context of the negative lowerbound model parameters. Interpretation (ICSW): Given R2, 98% of the variability of the CSW dependent variable is explained by 6 explanatory variables. Based on the Type III quadratic summation, the following variables provide significant information to explain the variability of the CSW dependent variable: BW,HW,IW,FW.

Based on the results of the Type III quadratic summation, the following variables do not provide significant information to explain the variability of the dependent variable CSW: SW and BGW. Among the explanatory variables, based on the sum of the squares of Type III, the variables SW and BGW are the ones that require the most attention. It is therefore reasonable to suspect that due to the small security budget in the institution and the absence of procurement of computer and network security licenses at a significant personal level, CSW was greatly affected.

3.3 MODEL ANALYSIS

The conceptual model in Figure 3.9, was tested according to the model test rules [53] which include:

1) Loading factor >0.7
2) Construct Reliability and Validity, for example Cr-α >0.7
3) Validity (FornellLarcker& HTMT)
4) Statistical collinearity < 5
5) *Fit model, for example SRMR < 0.08*

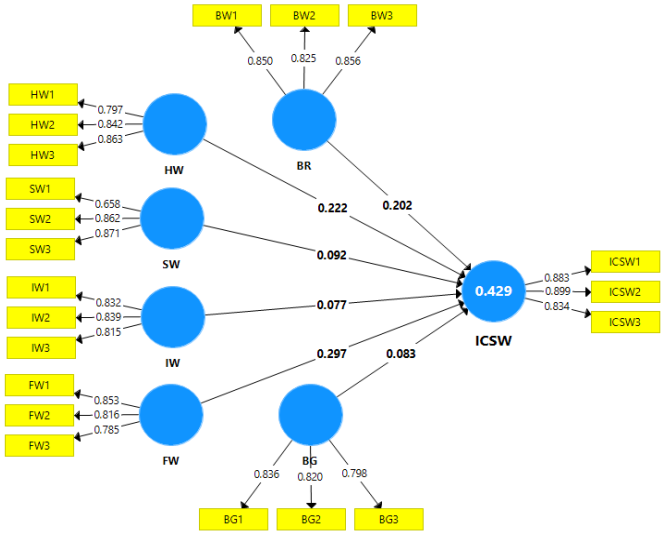

Figure 3.9Cybersix-waresecurity Index Conceptual Model

The conceptual model aboveshowsthattheequationforobtaining ICSW is as follows:

ICSW = 0.202*BW + 0.222*HW + 0.092*SW + 0.077*IW + 0.297*FW + 0.083*BG

In order forthe ICSW formula tobeusefulforconsideration in furtheranalysis, the model testparametersmustbemet. In testing the model parametersusingsmartPLSVersion 3.3, generallytheresultsthatmeetthecriteria as in thefollowingTables are obtained.

Table 3.6LoadingFactor

Indikator	Faktor Loading
BW1	0.850
BW2	0.825
BW3	0.856
HW1	0.797
HW2	0.842
HW3	0.863
SW1	0.658
SW2	0.862
SW3	0.871
IW1	0.832
IW2	0.839
IW3	0.815
FW1	0.853
FW2	0.816
FW3	0.785
BG1	0.836
BG2	0.820
BG3	0.798
ICSW1	0.883
ICSW2	0.899
ICSW3	0.834

Table 3.7ConstructReliabilityandValidity

Indikator	Cronbach's Alpha	rho_A	*Composite Reliability*	*Average Variance Extracted* (AVE)
BG	**0.755**	**0.764**	**0.859**	**0.669**
BR	**0.798**	**0.803**	**0.881**	**0.712**
FW	**0.755**	**0.761**	**0.859**	**0.670**
HW	**0.782**	**0.787**	**0.873**	**0.696**
ICSW	**0.844**	**0.857**	**0.905**	**0.761**
IW	**0.772**	**0.775**	**0.868**	**0.687**
SW	**0.715**	**0.732**	**0.843**	**0.645**

Table 3.8Fornell-LarckerDiscriminantValidity

	BG	BR	FW	HW	ICSW	IW	SW
BG	0.818						
BR	0.273	0.844					
FW	0.236	0.305	0.819				
HW	0.399	0.499	0.067	0.835			
ICSW	0.373	0.479	0.448	0.445	0.872		
IW	0.473	0.453	0.356	0.475	0.462	0.829	
SW	0.429	0.197	0.303	0.353	0.372	0.471	0.803

Table 3.9StatisticalCollinearity

Indikator	VIF	Indikator	VIF	Indikator	VIF	Indikator	VIF
BG1	1.465	FW1	1.678	IW1	1.621	ICSW1	2.009
BG2	1.566	FW2	1.447	IW2	1.568	ICSW2	2.292
BG3	1.531	FW3	1.506	IW3	1.564	ICSW3	1.880
BW1	1.724	HW1	1.539	SW1	1.154		
BW2	1.678	HW2	1.614	SW2	1.994		
BW3	1.700	HW3	1.844	SW3	2.066		

Table 3.10Fit Model

Parameter Fit Model	Saturated Model	Estimated Model
SRMR	**0.074**	**0.074**
d_ULS	1.256	1.256
d_G	0.5	0.5
Chi-Square	611.019	611.019
NFI	0.687	0.687

Table 3.11T testonPathCoefficient

Path	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
BR -> ICSW	**0.202**	0.193	0.077	2.617	**0.0090**
HW -> ICSW	**0.222**	0.224	0.074	2.996	**0.0030**
SW -> ICSW	**0.092**	0.099	0.048	1.977	**0.0494**
IW -> ICSW	**0.077**	0.077	0.001	2.897	**0.0042**
FW -> ICSW	**0.297**	0.303	0.066	4.516	**0.0000**
BG -> ICSW	**0.083**	0.085	0.079	2.899	**0.0042**

Table 3.12T teston R Square Model

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
ICSW- RSquare	0.430	0.455	0.054	7.901	**0.0000**
ICSW- RSquare Adjusted	0.412	0.438	0.056	7.350	**0.0000**

3.4 CYBERSIX-WARE INDEKS MEASUREMENTRESULTS (ICSW)

In the formulation of ICSW, the weights obtained on the conceptual model are proposed using a normalization approach, taking into account Rsquare (Rs) as a model representation indicator by each element, as follows:

$$\mathbf{ICSW} = \mathbf{0.202} * \mathbf{BW} + \mathbf{0.222} * \mathbf{HW} + \mathbf{0.092} * \mathbf{SW} + \mathbf{0.077} * \mathbf{IW} + \mathbf{0.297} * \mathbf{FW} + \mathbf{0.083} * \mathbf{BG}$$

By maximizing the normal scale, ICSW max = 1, then with the number of constants = 0.973 transformed to ICSW max, the formula becomes

$$\mathbf{ICSW} = \mathbf{0.208} * \mathbf{BW} + \mathbf{0.228} * \mathbf{HW} + \mathbf{0.095} * \mathbf{SW} + \mathbf{0.079} * \mathbf{IW} + \mathbf{0.305} * \mathbf{FW} + \mathbf{0.085} * \mathbf{BG}$$

By entering the results of the data obtained from the PCA, the following are the results of ICSW.

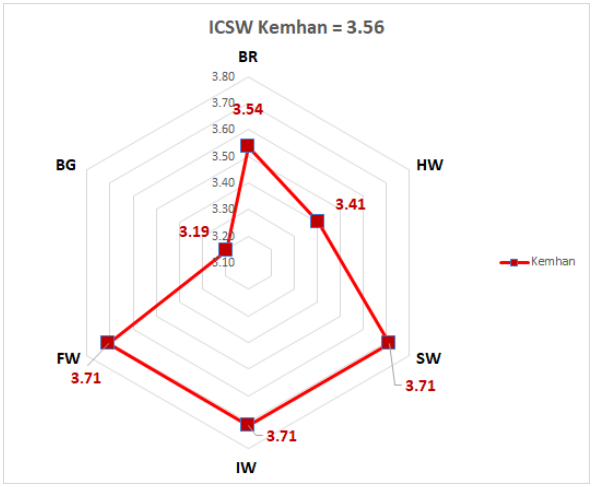

Figure 3.10ICSW Results

By referring to the interpretation of the scale where the ICSW measured 3.56 indicates that the research subject's Readiness Level is Fairly Ready. However, if you look at the elements of the Budget (BG) that are close to the threshold value (3.0), it is very worrying. It is clear that the main problem with setting up cyber defenses is Budgetware.

3.5 RESULTOFMEASUREMENTOFCYBERSIX-WARE INDEKS (ICSW)CYBERSIX-WARE INDEKS MEASUREMENTRESULTS (ICSW)

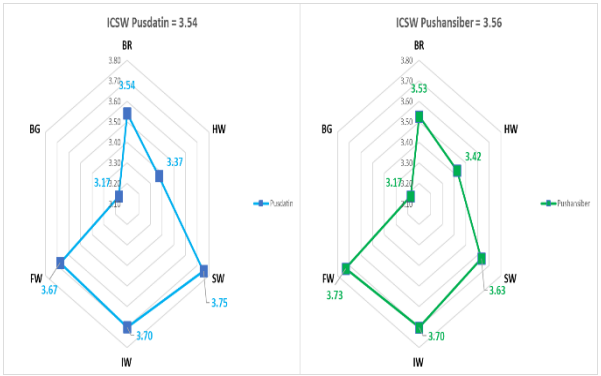

Figure 3.11ICSW PusdatinandPushansiber

PusdatinKemhan, especially the IT Center division in supporting its main task, has adequate personnel education qualifications (>3.5), as is Pushansiber. Personnel who are in the IT Center section, have an Information Technology educational background and there are several different educational qualifications. Officials and technical teams have special qualifications and experience in the field of Information and Communication Technology.

Both Pusdatin and Pushansiber have competent personnel in the field of cyber security. Personnel who are in this position are well responsible. Operations manager has responsibilities as data center maintenance, physical security management, information security, and protection of Information and Communication Technology Center facilities, management of system services, applications, information technology platforms, information technology infrastructure, information and data center services, and central services. data recovery.

Overall, the results of the analysis at the Pusdatin show that ICSW Index = 3.54 (> 3.5) and Qualitative Coding = "Ready" can be interpreted that the Center for Defense of the Ministry of Defense has adequate technology and capability to develop cyber defense technology. Likewise with Pushansiber with ICSW Index = 3.56 (> 3.5) and Qualitative Coding = "Ready".Meanwhile, the crucial problem in these two satkers is the Budget Element, which is slightly above the 3.0 threshold, which is a worrying thing.

IV. CONCLUSION

The response framework for cyber threats at the Pusdatin and Pushansiber of the Ministry of Defense shows adequate or good development readiness with ICSW >3.5. The priority options for cyber defense development work at the Ministry of Defense are as follows from the ICSW elements in the following order: **Budgetware** (index 3.19) needs to be prioritized to be realized; **Hardware** (index 3.37) however complained as seen from the index numbers so that it requires serious attention; **Brainware** (index 3.54) needs improvement because the human factor is the difference if you want to continue to strengthen cyber security at the Ministry of Defense.

Other elements **(Software, Infrastructure, and Firmware)** even though the ICSW number is >3.5. They still need to be improved to become stronger. However, it is impossible for the increase to run well if there are elements that are still minimal (in this case budget realization).

The research shows that the proposed measurement concept has been able to formulate the ICSW index through modeling:

$$\mathbf{ICSW} = \mathbf{0.208} * \mathbf{BW} + \mathbf{0.228} * \mathbf{HW} + \mathbf{0.095} * \mathbf{SW} + \mathbf{0.079} * \mathbf{IW} + \mathbf{0.305} * \mathbf{FW} + \mathbf{0.085} * \mathbf{BG}$$

The ideal cyber defense design at the Ministry of Defense is to follow the SixwareCyber Defense Framework with its six factors (Brainware, Hardware, Software, Infrastructureware, Firmware and Budgetware) to improve cyber defense systems. For this reason, the availability of the measurement formula makes the Six Ware Cyber Defense Framework concept more complete to implement.

REFERENCES

[1] F. Schreier, "On Cyberwarfare," 2015. [Online]. Available: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

[2] P. Chen, J. Xu, Z. Lin, D. Xu, B. Mao, and P. Liu, "A practical approach for adaptive data structure layout randomization," 2015, doi: 10.1007/978-3-319-24174-6_4.

[3] M. Taddeo, "An analysis for a just cyber warfare," 2012.

[4] S. Adepu, S. Shrivastava, and A. Mathur, "Argus: An Orthogonal Defense Framework to Protect Public Infrastructure against Cyber-Physical Attacks," IEEE Internet Comput., 2016, doi: 10.1109/MIC.2016.104.

[5] I. Burke and R. P. Van Heerden, "Automating cyber offensive operations for cyber challenges," 2016.

[6] R. A. GemilangGultom, T. Kustana, and R. Oktovianus Bura, "ENHANCING COMPUTER NETWORK SECURITY ENVIRONMENT BY IMPLEMENTING THE SIX-WARE NETWORK SECURITY FRAMEWORK (SWNSF)," 2018, pp. 153–166, doi: 10.5121/csit.2018.81714.

[7] A. Capatina, A. Olaru, and C. B. Balan, "The Impact of the Brainware Intelligence on the Intellectual Capital of the Romanian IT Companies," Proc. 4Th Eur. Conf. Intellect. Cap., no. Ic, pp. 127–135, 2012.

[8] D. Antoni, F. Jie, and A. Abareshi, "Critical factors in information technology capability for enhancing firm's environmental performance: Case of Indonesian ict sector," Int. J. Agil. Syst. Manag., 2020, doi: 10.1504/IJASM.2020.107907.

[9] J. Barney, "Special Theory Forum the Resource-Based Model of the Firm: Origins, Implications, and Prospects," J. Manage., 1991, doi: 10.1177/014920639101700107.

[10] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, and N. Samarakoon, "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience," IEEE Trans. Eng. Manag., 2021, doi: 10.1109/TEM.2019.2909909.

[11] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," J. Syst. Inf. Technol., 2019, doi: 10.1108/JSIT-02-2018-0028.

[12] M. G. Samaila et al., "A Preliminary Evaluation of the SRE and SBPG Components of the IoT-HarPSecA Framework," 2020, doi: 10.1109/GIOTS49054.2020.9119590.

[13] J. Mignone and J. O'Neil, "Social Capital as a Health Determinant in First Nations: An Exploratory Study in Three Communities," J. Aborig. Heal., 2005.

[14] J. D. F. Vidotto, H. A. Ferenhof, P. M. Selig, and R. C. Bastos, "A human capital measurement scale," J. Intellect. Cap., 2017, doi: 10.1108/JIC-08-2016-0085.

[15] S. H. Lee, P. H. Phan, and T. Yoshikawa, "The Role of the Board and Its Interaction with the Successor's Human Capital in the Asian Family Enterprise," Multinational Business Review. 2008, doi: 10.1108/1525383X200800008.

[16] P. Sharma and C. Salvato, "Commentary: Exploiting and exploring new opportunities over life cycle stages of family firms," Entrepreneurship: Theory and Practice. 2011, doi: 10.1111/j.1540-6520.2011.00498.x.

[17] G. H. Mardini and F. E. Lahyani, "Impact of firm performance and corporate governance mechanisms on intellectual capital disclosures in CEO statements," J. Intellect. Cap., 2020, doi: 10.1108/JIC-02-2020-0053.

[18] R. Hejazi, M. Ghanbari, and M. Alipour, "Intellectual, Human and Structural Capital Effects on Firm Performance as Measured by Tobin's Q," Knowl. Process Manag., 2016, doi: 10.1002/kpm.1529.

[19] C. P. Lin, "Modeling job effectiveness and its antecedents from a social capital perspective: A survey of virtual teams within business organizations," Comput. Human Behav., 2011, doi: 10.1016/j.chb.2010.11.017.

[20] A. Usman, H. Wirawan, and Zulkifli, "The effect of human capital and physical capital on regional financial condition: the moderating effect of management control system," Heliyon, 2021, doi: 10.1016/j.heliyon.2021.e06945.

[21] G. Cybenko and J. Hughes, "No free lunch in cyber security," 2014, doi: 10.1145/2663474.2663475.

[22] M. G. Samaila, J. B. F. Sequeiros, T. Simoes, M. M. Freire, and P. R. M. Inacio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2965925.

[23] R. Colomo-Palacios, E. Fernandes, P. Soto-Acosta, and M. Sabbagh, "Software product evolution for Intellectual Capital Management: The case of Meta4 PeopleNet," Int. J. Inf. Manage., 2011, doi: 10.1016/j.ijinfomgt.2011.04.001.

[24] Kementerian PendayagunaanAparatur Negara Dan Reformasi Birokrasi, PedomanEvaluasiSistemPemerintahanBerbasisElektronikInstansi Pusat Dan Pemerintah Daerah. 2018.

[25] J. R. Lewis, "Psychometric Evaluation of the PSSUQ Using Data from Five Years of Usability Studies," Int. J. Hum. Comput. Interact., 2002, doi: 10.1080/10447318.2002.9669130.

[26] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," Heliyon, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[27] G. Tilei, L. Tong, Y. Ming, and J. Rong, "Research on a trustworthiness measurement method of cloud service construction processes based on information entropy," Entropy, 2019, doi: 10.3390/e21050462.

[28] G. H. Shen et al., "Survey on software trustworthiness evaluation: standards, models and tools," Ruan Jian Xue Bao/Journal of Software. 2016, doi: 10.13328/j.cnki.jos.005024.

[29] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," Comput. Secur., 2017, doi: 10.1016/j.cose.2017.01.004.

[30] J. Wynn et al., "Threat Assessment & Remediation Analysis (TARA)," MITRE Tech. Rep., 2011.

[31] M. Alaeddini, H. Asgari, A. Gharibi, and M. Rashidi Rad, "Leveraging business-IT alignment through enterprise architecture—an empirical study to estimate the extents," Inf. Technol. Manag., vol. 18, no. 1, pp. 55–82, Mar. 2017, doi: 10.1007/s10799-016-0256-6.

[32] U. C. Schroeder, Measuring Security Sector Governance. A Guide to Relevant Indicators, vol. 20. 2010.

[33] M. Mazziotta and A. Pareto, "Use and Misuse of PCA for Measuring Well-Being," Soc. Indic. Res., vol. 142, no. 2, pp. 451–476, 2019, doi: 10.1007/s11205-018-1933-0.

[34] R. A. G. Gultom, A. Farid, A. A. Lestari, C. A. S. Lahallo, and R. N. Akbar, "Cyber-Based Defense Technology Development of the Six-ware Cyber Framework to Enhance the Implementation of the National Defense System in the City of Batam," Int. J. Adv. Sci. Technol., vol. 29, no. 7, pp. 3431–3436, 2020, [Online]. Available: http://sersc.org/journals/index.php/IJAST/article/view/17631.

[35] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. 2018.

[36] WaterISAC, "15 Cybersecurity Fundamentals for Water and Wastewater Utilities," 2019. [Online]. Available: www.waterisac.org.

[37] S. J. Park, Y. Yi, and Y. R. Lee, "Heterogeneous dimensions of SERVQUAL," Total Qual. Manag. Bus. Excell., vol. 32, no. 1–2, pp. 92–118, 2021, doi: 10.1080/14783363.2018.1531700.

[38] M. K. Al-Kofahi, H. Hassan, and R. Mohamad, "Information systems success model: A review of literature," International Journal of Innovation, Creativity and Change, vol. 12, no. 10. pp. 104–128, 2020.

[39] L. N. Amali, M. R. Katili, S. Suhada, and L. Hadjaratie, "The measurement of maturity level of information technology service based on COBIT 5 framework," Telkomnika (Telecommunication Comput. Electron. Control., vol. 18, no. 1, pp. 133–139, 2020, doi: 10.12928/TELKOMNIKA.V18I1.10582.

[40] D. Maheshwari, M. Janssen, and A. F. Van Veenstra, "A multi-level framework for measuring and benchmarking public service organizations: Connecting stages-of-growth models and enterprise architecture," in ACM International Conference Proceeding Series, 2011, pp. 73–80, doi: 10.1145/2072069.2072083.

[41] M. Mazziotta and A. Pareto, "A Non-compensatory Approach for the Measurement of the Quality of Life," 2012, pp. 27–40.

[42] J. Salzman, "Methodological Choices Encountered in the Construction of Composite Indices of Economic and Social Well-Being," 2003.

[43] Addinsoft, "{XLSTAT} statistical and data analysis solution. {Paris}, {France}.," XLSTAT, Your data analysis solution. 2021.

[44] K. Shi, Y. Liu, Z. Zhang, Q. Yu, and Q. Zhang, "Constructing a method for an evaluation index system based on graph distance classification and principal component analysis," Adv. Mater. Sci. Eng., 2019, doi: 10.1155/2019/6015754.

[45] M. Mazziotta and A. Pareto, "Use and Misuse of PCA for Measuring Well-Being," Soc. Indic. Res., 2019, doi: 10.1007/s11205-018-1933-0.

[46] M. Mazziotta and A. Pareto, "Methods for constructing composite indicators: one for all or all for one?," Riv. Ital. di Econ. Demogr. e Stat., vol. LXVII, no. Aprile-Giugno, pp. 67–80, 2013, [Online]. Available: http://www.sieds.it/listing/RePEc/journl/2013LXVII_N2_10_Mazziotta_Pareto.pdf.

[47] R. Gultom, W. Midhio, T. Silitonga, and S. Pudjiatmoko, "Introducing the six-ware cyber security framework concept to enhancing cyber security environment," Proc. 13th Int. Conf. Cyber Warf. Secur. ICCWS 2018, vol. 2018-March, pp. 262–271, 2018.

[48] R. Gultom, W. Midhio, T. Silitonga, and S. Pudjiatmoko, "Introducing the six-ware cyber security framework concept to enhancing cyber security environment," 2018.

[49] J. W. Creswell, "Steps in Conducting a Scholarly Mixed Methods Study," Univ. Nebraska - Lincoln, p. 54, 2013, [Online]. Available: http://digitalcommons.unl.edu/dberspeakers/48.

[50] K. Joshi and M. B. Rajarshi, "Modified probability proportional to size sampling," Commun. Stat. - Theory Methods, vol. 47, no. 4, pp. 805–815, Feb. 2018, doi: 10.1080/03610926.2016.1139131.

[51] J. F. Hair, C. M. Ringle, and M. Sarstedt, "Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance," Long Range Planning, vol. 46, no. 1–2, pp. 1–12, 2013.

[52] R. Heale and A. Twycross, "Validity and reliability in quantitative studies," Evidence-Based Nursing. 2015, doi: 10.1136/eb-2015-102129.

[53] M. Sarstedt et al., "Partial Least Squares Structural Equation Modeling," in Handbook of Market Research, no. September, 2017, pp. 1–40.

[54] M. Sarstedt et al., "Partial Least Squares Structural Equation Modeling," in Handbook of Market Research, no. September, Cham: Springer International Publishing, 2017, pp. 1–40.

[55] M. Mazziotta and A. Pareto, "Composite Indices Construction: The Performance Interval Approach," Soc. Indic. Res., no. 0123456789, 2020, doi: 10.1007/s11205-020-02336-5.

[56] M. Solak, "Detection of multiple outliers in univariate data sets," Schering, 2009.

[57] K.-C. Sohn and I.-H. Shin, "Outlier detection using Grubb test and Cochran test in clinical data," J. Korean Data Inf. Sci. Soc., 2012, doi: 10.7465/jkdi.2012.23.4.657.