Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

SWOT Analysis in Determining POLRI Organizational Resource Strategies to Anticipate the Development of Cyber Crime in the Framework of Maintaining National Security

Azis Andriansyah[A], Edmon Makarim[B], Yudho Giri Sucahyo[C], Chairul Muriman Setyabudi[D]

Abstract

The purpose of this research is to formulate appropriate alternative organizational resource strategies and policies for the Republic of Indonesia Police to anticipate the development of cyber-crime in order to maintain Kamdagri using the SWOT (Strength, Weakness, Opportunity, Threat) analysis method. The SWOT analysis is carried out using the IFE (Internal Factor Evaluation) matrix which describes the strengths and weaknesses of POLRI and the EFE (External Factor Evaluation) matrix which outlines the opportunity and threat factors and the IE (Internal External) matrix which shows the current position of Indonesian Police Agency. The last is the determination of strategic choices that can be made based on the strategic position of the Republic of Indonesia Police organization. The strategic choices suggested in this study are to make policies at the national strategic level in the short to long term, increase human resource capacity in the short term and form a team of experts and make performance evaluations for handling cyber cases in the medium term.

Keywords: *SWOT, Organizational Resources, Cybercrime.*

INTRODUCTION

The development of cybercrime will become increasingly complex and sophisticated, both those using computers as a tool (computer-related crime) and the primary tool (computer crime), where the impact of this crime can damage the life of society, nation and state. In addition, the character of cybercrime (borderless, anonymous, and organized) makes it difficult for the authorities to solve cases (Monteith et al., 2021; Al-Khater et al., 2020).

According to McGuire, M. and Dowling, S., 2013, the role of digital and information technology in generating national wealth now means that new risks associated with this change require continuous attention on all fronts: national, regional and international. While "globalization" continues to accelerate, a complete global response to security problems in the digital age is yet to emerge, and efforts to secure cyberspace are

[A]*School of Strategic and Global Studies, University of Indonesia, Email: azis.andriansyah01@ui.ac.id*
[B]*School of Strategic and Global Studies, University of Indonesia*
[C]*School of Strategic and Global Studies, University of Indonesia*
[D]*School of Strategic and Global Studies, University of Indonesia*

reactive rather than proactive. Developments in transnational policing in "cyberspace", which is so crucial in tackling cybercrime, is the focus of this paper and outlines what the international community has achieved so far (Cascavilla et al., 2021; Buil et al., 2021).

Crime control involving digital technology and computer networks will also require a variety of new networks: networks between the police and other government agencies, police and private institutions, and police networks across national borders (Bossler & Barenblum, 2019; Kshetri, 2019)). Over the last decade, much progress has been made within and between countries to develop police capacity to respond to cybercrime. Computer users are now increasingly aware of the need for basic security online. Nevertheless, the pace of technological change will continue, and cybercriminals' adaptability will continue to challenge law enforcement (Payne & hadzhidimova, 2020; Fahlevi et al., 2019). Thus, the cliché 'think globally, act locally' is highly relevant in cybercrime control. The extraordinary acceleration of transnational law enforcement cooperation in response to cybercrime and other global threats has radically changed expectations about what can be achieved internationally (Anderson et al., 2019; Hawdon et al., 2020). However, promising these developments may be, what has been achieved can only be considered a start.

According to Wow Essay (2009), cybercrime is "Criminal activity directly related to the use of computers, in particular illegal intrusion into other people's computer systems or databases, manipulation or theft of stored or online data, or sabotage of equipment and data."

One form of cybercrime that worries the public is the spread of hoaxes. Where to data from the Republic of Indonesia Ministry of Communication and Information (2018-2020), there were 5,156 findings on hoax issues, while 304 LPs related to hoaxes received by the Criminal Investigation Unit of the National Police and Regional Police ranks were 304 LP, of which 87 cases (28.62%) can be completed.

In addition, the trend of reporting cyber crimes is increasing yearly, whereas during 2020-2021, the number of reports submitted via patrolsiber.id amounted to 15,816 complaints, with a total loss of IDR 3.89 trillion. At the same time, the trend of cybercrime in Indonesia throughout 2018 -2020 also increased, where there were a total of 13,736 cases with an average trend of increasing cybercrime cases of 193.58%, of which 13 Regional Police experienced an increase above 100%, even 2 (two) Regional Police increased more than 1000%, namely the Regional Police North Kalimantan and Papua. While the settlement of cybercrime cases from 2019 to 2021 at the Dittipidsiber Bareskrim Polri and Polda ranks can be seen in Table 1 below:

Table 1. Data on Settlement of Cyber Crime Cases (2019 to 2021)

No	Task Force	2019			2020			2021		
		CT	CC	%	CT	CC	%	CT	CC	%
1.	Indonesian Cyber Task Force	202	159	78,71	234	94	40,17	147	82	55,78

2.	Regional Police	4.384	2.123	48,43	4.556	1.189	26,10	1.582	764	48,29
Total		**4.586**	**2.282**	**49,76**	**4.790**	**1.283**	**26,78**	**1.729**	**846**	**48,93**

Source: Indonesia Cyber Task Force (Year 2021)

From the data in Table 1 above, it can be seen that from 2019 to 2021, the Dittipisiber Bareskrim Polri received 583 prison cases for various types of cyber-crimes, and 335 cases have been resolved. Meanwhile, the regional police received prison sentences of 10,522 cases and 4,076 cases that could be resolved. Apart from that, it can also be seen that from 2019 to 2021, there were 27,412 reports of the spread of harmful content in the Polda ranks. Then, in 2021, the Dittipidsiber Bareskrim Polri will handle 3,468 contents of radicalism, of which 2,468 contents (71.16%) have been followed up through efforts to monitor, block, and investigate. Based on these various data and facts, the development of cybercrime is very complex and can threaten the life of society, nation and state.

It takes human resources who have the skills to solve cyber-crimes. To realize human resources requires the right strategy. SWOT analysis determines the right human resource strategy according to needs. The condition of Polri's organizational resources, namely in the Dittipidsiber Bareskrim Polri and Polda in its ranks, will have a significant impact in anticipating the development of cybercrime, where the Polri Organizational Resources element currently consists of aspects of human resources (HR), budget, facilities and infrastructure, as well as systems and methods.

In general, the problems to be discussed are 1). Why is a SWOT analysis framework needed in determining the Polri organizational resource strategy? 2). How to utilize the SWOT analysis framework by determining organizational resource strategies to anticipate developments in cybercrime in order to maintain Kamdagri. The research objectives are

1. To identify, obtain, document, and model various SWOT elements in determining the HR strategy of the Polri organization.
2. To develop a methodology that examines problems and challenges that hinder achieving the set goals and seeks solutions. The method can bring all the views and insights about SWOT into the framework.
3. Implement framework solutions in various dimensions that can form and strengthen organizational resources by minimizing external weaknesses and threats

LITERATURE REVIEW

Cybercrime

Digital technology and cybercrime are images of modern life that have become widespread in human life. About 60% of the world's population are internet users, and global adoption of digital technologies is increasing rapidly; global internet penetration increased by approximately 7% over one year (from January 2020 to January 2021) [Kemp, S. Digital 2021]. The increasing adoption of digital technologies has led to the evolution of criminal behaviour, increasing the incidence

of 'cybercrime'. However, there still needs to be more clarity about what constitutes cybercrime.

A clear conceptualization of cybercrime is essential because even minor variations in the conceptualization of cybercrime can affect the measurement of and responses to cybercrime behaviour [Leukfeldt et al., 2020]. Barn and Barn [Barn, R, 2016] argue that one of the factors that may contribute to difficulties in estimating cybercrime is the need for a good definition and classification system capable of taking into account various cybercrimes. This problem is further exacerbated by the fact that cybercrime laws across jurisdictions are neither systematic nor uniform; moreover, the laws themselves are often scattered across multiple criminal and civil laws, which in turn results in fragmented international efforts to tackle cybercrime as well as cybercrimes that are weighted and perceived differently across jurisdictions [Black, A et al., 2019, Viano, E.C, 2016]. Additionally, this is further complicated by the fact that for many individual cybercrimes, there is variability across jurisdictions as to what constitutes a felony. For example, see ICMEC's global legislative review of 'Online Care' [ICMEC, 2017].

The problem with defining cybercrime begins with the terminology itself: "The myriad of terminologies used, sometimes combined with the prefix cyber, computer, e-, internet, digital or information. Terms are disseminated, applied randomly, reflect overlap in content or reflect important gaps" (quote from Van der Hulst and Neve, 2008, cited in Paoli et al., 2018). Alternative terminology for cybercrime includes, for example, 'cybercrime'; 'computer crime, ' computer-related crimes'; 'electronic crime'; 'electronic crime'; 'technology-enabled crime'; 'high-tech crime' [Chang, L.Y, 2012, Sarre, R, et al., 2018]. The variability in cybercrime terms and language highlights thneed forof a shared lexicon among professionals working in the field.

SWOT Anaysis

SWOT stands for Strengths, Weaknesses, Opportunities and Threats, and can be analyzed as a process, in which the management team identifies the internal and external factors that affect the performance of the company and business. Strengths in SWOT analysis are internal capabilities and positive factors of business establishment, which are relevant for companies to achieve their goals and serve their customers, efficiently (Eastwood et al, 2016, Frada et, al, 2008).

Weaknesses are internal factors or constraints that may impede or hinder organizational performance. Therefore, the strengths and weaknesses of the company are internal elements.

Opportunities in a SWOT analysis are factors or features that can support or facilitate the establishment of a business with links outside the organization. They are external factors where companies can exploit their advantages (Eastwood et al, 2016). Threats related to negative factors outside the company, which can hinder or delay the goals that can be achieved. Thus, opportunities and threats are seen as environmental factors. Examples of elements when conducting a SWOT analysis are

related to attribute dimensions such as competitors, raw material prices, and optimal supply chain management systems. New insights are made on resource SWOT analysis, making business competitive and strategic with the template toolkit (Sammut, 2015).

SWOT analysis was conducted to analyze strategic planning and evaluation through case studies of Higher Education Institutions in Thailand (Phaderrod, 2016). The SWOT analysis model was articulated for wheat farming, incorporating a number of strategic dimensions in the modeling process (Ommani, A. R. (2011). A review was conducted of SWOT in a qualitative and quantitative perspective (Gurel, M and TAT, M. (2017). SWOT analysis was carried out in various corporate strategic planning scenarios using empirical studies (Jeyaraj, et al, 2012).

METHOD

The research method using descriptive qualitative is the term used in qualitative research for a descriptive study. This type of research is generally used in social phenomenology (Polit & Beck, 2014). The social phenomenon under study is related to resource management in the face of changes in crimes that are now being carried out in the online realm. This change forced human resources in the Indonesian National Police to adapt to this new type of crime.

To conduct this research, the data used is secondary data originating from the Republic of Indonesia Police Cyber Crime Unit both at the central level and at the regional level, namely at the provincial level. This data consists of data on the number of cyber-crimes that have occurred, data on resolved cases, existing human resources both in quantity and quality.

Furthermore, with this data an analysis is carried out using the Strength, Weakness, Opportunity and Threat framework. This framework is useful for looking at the current strengths and weaknesses of the Indonesian National Police organization as well as external threats and opportunities that can be seized in the cyber era. The SWOT framework can then help the Indonesian National Police organization to see the current position of its human resources by using a matrix of external and internal factors. The EFAS and IFAS matrices are used to determine the strategic position quadrants. Based on this strategic position, a strategy was then chosen to direct the Indonesian National Police organization.

RESULT AND DISCUSSION

Current Condidition in Indonesian National Police

Based on data, facts, observations, interviews, and the author's empirical experience, the factual conditions of Polri's human resources in strengthening the capacity of Polri's SDO are considered to be still not ideal, where these conditions can be described as follows:

1. Quantity

Based on the data at hand, an overview of the quantity of Polri human resources at the Dittipidsiber Bareskrim Polri and Polda ranks can be observed in Table 2 below:

Table 2. Readiness of Human Resources for Dittipidsiber Bareskrim Polri and Polda Ranks (Year 2021)

No.	SATKER	DSP	RIIL	KET.	% RIIL
1.	Cyber Task Force	90	142	+ 52	157,78%
2.	Regional	1.076	732	(-) 344	68,03%
Total		**1.166**	**874**	**(-) 292**	**74,96%**

Source: Dittipidsiber Bareskrim Polri (2021)

Based on the data from Table 2 above, it can be seen that the quantity of Polri personnel in the Dittipidsiber Bareskrim Polri and the Polda ranks is 874 personnel (74.96%) of the total DSP, where in general there is a shortage of Polri members as many as 292 of the total DSP. apply. As a result, this shortage of personnel can affect the implementation of tasks and functions in the field, including anticipating developments in cyber-crime.

2. Quality

One of the parameters of the quality of human resources in an organization can be observed from educational background to the participation of members of the organization in various types of training so that it will have an impact on aspects of knowledge, skills and work attitudes, which is in accordance with Article 1 of RI Law No. 13/2003 concerning Manpower. From the conditions above, it can be seen that the quality of Polri human resources at the Dittipidsiber Bareskrim Polri and Polda ranks cannot be said to be qualified, which will have an impact on aspects of knowledge, skills and attitudes/behavior of personnel.

3. Knowledge

There are still members of the National Police who are still lacking in mastery of legal instruments in efforts to deal with cyber-crimes, such as RI Law No. 19/2016 concerning ITE and other related rules, to the extent that they do not understand IT literacy, as a result there are still members who are not optimal in handling cases, including in anticipating the dynamics of cyber-crime consistently.

4. Skill

There are still members who are not proficient in filing and resolving cases to accurate analysis techniques related to the development of cybercrime, as a result the process of handling cybercrime is often not thorough and professional and not optimal in analysis and tactics to anticipate developments in cybercrime.

5. Attitude

There are still members who lack integrity, low professionalism, lack motivation to cooperate, and lack determination to study the dynamics/developments of cybercrime, as a result they are less effective when dealing with cybercrime, less integrated in working together, so they are less innovative and creative in anticipating cybercrime developments.

6. Budget

Budget support received and managed by the Dittipidsiber Bareskrim Polri and the Polda ranks currently comes from the DIPA Polri, where the budget for the program at the Dittipidsiber Bareskrim Polri in 2020 is Rp. 18.012.198.000, and Rp. 43.633.102.000,- for Regional

Police-, but this budget amount is deemed to still need to be increased, because it is still not comparable to the complexity and number of cybercrime cases, as a result effort to anticipate the development of cybercrime are often not optimal and are often tactically constrained in the field.

7. Facilities and infrastructure

The condition of Polri's institutional facilities and infrastructure in anticipating the development of cyber crime still needs to be improved, one of which can be seen from the condition of Alsus at the Dittipidsiber Bareskrim Polri, namely the existence of Alsus whose license has expired. such as cyber campaigns (education), PVP (virtual police alerts), cyber patrols, and law enforcement, as well as other activities that are not running optimally and effectively, even personnel often experience technical problems in the field.

8. System and Methods

The condition of Polri's institutional facilities and infrastructure in anticipating the development of cyber crime still needs to be improved, one of which can be seen from the condition of Alsus at the Dittipidsiber Bareskrim Polri, namely the existence of Alsus whose license has expired. such as cyber campaigns (education), PVP (virtual police alerts), cyber patrols, and law enforcement, as well as other activities that are not running optimally and effectively, even personnel often experience technical problems in the field.

Strategy Analysis

External Factor Analysis Summary (EFAS)

EFAS aims to identify external factors (opportunities and threats) of the organization through weights and ratings. This EFAS method produces a total EFAS score and obtains the weight, rating, and external factor scores, where the results of these calculations can be seen in Table 3 below:

Table 3. EFAS Analysis

No.	External Factors	Weight	Rating	Score
	I. OPPORTUNITIES			
1.	Support from the Republic of Indonesia Ministry of Communication and Information, BSSN, and related.	0.121	8	0.968
2.	Experts, practitioners, and academics in the field of IT	0.102	7	0.714
3.	Advances in information and communication technology (ICT)	0.111	8	0.888
4.	Government and DPR RI support for Polri	0.085	6	0.510
5.	Training institutions from within and outside the country	0.081	6	0.486
Total		**0.500**		**3.566**
	II. THREATS			
1.	Low public digital literacy related to cyber crime	0.078	4	0.312
2.	Cybercrime is increasing and complex	0.070	4	0.280
3.	Mainstream and online media are often disinformation	0.142	2	0.284

4.	Sectoral ego attitudes among government agency personnel	0.084	4	0.336
5.	The role of external oversight institutions is not yet optimal	0.126	3	0.378
Total		**0.500**		**1.590**
IFAS Total Score		**1.000**		**5.156**

From Table 3 above, it can be seen that the total score for the opportunity factor is 3.566, while the threat factor is 1.590, so the total EFAS score is 5.156.

Internal Factor Analysis Summary (IFAS)

IFAS aims to identify internal factors (strengths and weaknesses) of the organization through weights and ratings. This IFAS method produces a total IFAS score and obtains weight, rating, and internal factor scores, where the results of these calculations can be seen in Table 4 below:

Table 4. IFAS Analysis

No.	Internal Factor	Weight	Rating	Score
	I. STRENGTH			
1.	Police leadership policy related to strengthening SDO	0.117	8	0.936
2.	The police synergy system can strengthen cooperation	0.083	6	0.498
3.	Performance appraisal system in the Polri organization	0.111	8	0.888
4.	Existence of internal control function	0.103	7	0.721
5.	The Polri organization already has work relationship guidance between Task Force	0.086	6	0.516
Total		**0.500**		**3.559**
	II. WEAKNESS			
1.	The application of the management function is less systematic	0.078	4	0.312
2.	The quality of Polri personnel is uneven and reliable	0.151	2	0.302
3.	The availability of facilities and infrastructure is relatively limited	0.081	4	0.324
4.	There are no specific blueprints, SOPs, operational guidelines and technical guidelines	0.128	3	0.384
5.	Budget support is seen as inadequate.	0.062	4	0.248
Total		**0.500**		**1.570**
IFAS Total Score		**1.000**		**5.129**

From Table 4 above, it can be seen that the total score for the strength factor is 3.559, while the weakness factor is 1.570, so the total IFAS score is 5.129.

Strategic Position Viewed from the EFAS and IFAS Matrix

After calculating the EFAS and IFAS, the next step is to map the position of the Polri organization with regard to strengthening the human resources capacity of the Polri organization, namely:

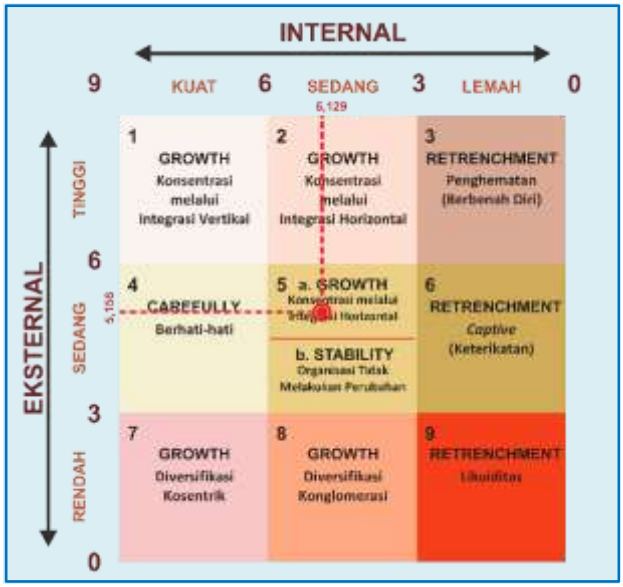

Figure 1. EFAS and IFAS Matrix (Organizational Position)

The figure above shows that the total EFAS score is 5.156 and the total IFAS score is 5.129, so the confluence of the two points is in Quadrant 5a growth (growth), namely Concentration through Horizontal Integration. This can mean that with external opportunities and internal strengths, Polri is in a position to effectively strengthen the Polri organizational resource capacity in order to be able to anticipate progressive and massive developments in cybercrime.

Strategic Position Viewed from the SWOT Matrix

After calculating EFAS and IFAS and understanding the organizational position, the next stage is to map out the strategic position to show the Polri's strategic position regarding strengthening the capacity of Polri's organizational resources, where this condition can be observed as follows:

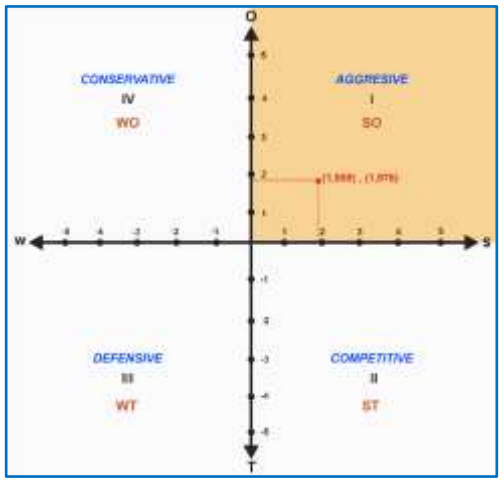

Figure 2. SWOT Matrix (Strategic Position)

The figure above shows the value of the IFAS analysis of 1.989, namely the reduction of the value of the strength factor (3.559) by the weakness factor (1.570), while the value of the EFAS analysis is 1.976, which is the reduction of the value of the opportunity factor (3.566) by

the threat factor (1.590). From the results of this analysis, Polri's strategic position is in the aggressive quadrant.

Strategy Choice

Based on the strategic position analysis in terms of the EFAS and IFAS matrices, it means that the Polri organization has moderate conditions, where opportunity factors (external) and strength factors (internal) are moderate. The response from the Polri organization in order to be able to deal with this condition (Horizontal Integration Strategy) is to increase (generic strategy) coordination (grand strategy) with parties (stakeholders) who have the resources to be able to support efforts to strengthen the capacity of the Polri organizational resources so that they are able to anticipate developments. cyber crime effectively and comprehensively. Key words: coordination. For this reason, there are several general strategies that must be carried out by the Polri organization, including by increasing the readiness of elements of the SDO Polri, in this case the Dittipidsiber Bareskrim Polri and Polda ranks, including elements of human resources, budget, facilities and infrastructure, as well as systems and methods, through training, improving the implementation of management functions, consisting of planning, organizing, implementing, and supervising functions, to support strengthening the capacity of SDO Polri, in this case Dittipidsiber; improve the performance achievements of SDO Polri, in this regard at the Dittipidsiber Bareskrim Polri and Polda ranks, through efforts to internalize, socialize, mentorship, control/supervise performance, assess performance targets, monitor/supervise, empower external oversight institutions, Jukrah leadership, to integrated studies with Related Ministries/Institutions..

Strategic Factor Analysis Summary (SFAS).

The SFAS method/technique aims to summarize the strategic factors of the organization by combining various internal and external strategic factors in a summary analysis of key strategic factors, where the results of this calculation can be shown in Table 5 below:

Table 5. SFAS Analysis

No.	Key Strategic Factor	Weight	Rating	Score	Timeline		
					short	Medium	Long term
1.	Improving the quality of Polri personnel	0.092	2	0.184			
2.	Empower mainstream and online media	0.084	2	0.168			
3.	Develop blueprints, SOPs, operational guidelines and special technical guidelines.	0.090	3	0.270			
4.	Empowering external oversight agencies.	0.122	3	0.366			
5.	Utilizing the support of the RI Ministry of Communication and Informatics, BSSN, and related Ministries/Institutions	0.116	8	0.928			
6.	Realizing police leadership policies.	0.121	8	0.968			
7.	Take advantage of ICT advances	0.101	8	0.808			

8.	Develop a performance appraisal system	0.082	8	0.656			
9.	Empowering the internal control function	0.099	7	0.693			
10.	Utilizing experts, practitioners, and academics	0.093	7	0.651			
Amount		**1.000**					

Through the Strategic Factor Analysis Summary (SFAS) method/technique, the lowest weighted score is obtained, which is 0.168, and the highest weighted score is 0.968. Then the time period/interval will be determined as follows:

For short term the first step is to calculate the median value, by subtracting the highest value from the lowest value, and dividing the result by 3. After that, this lowest value is added to the results of calculating the median value, then the value for the short term is obtained, namely: = (0.968 – 0.168): 3 = 0.267 (median value calculation), so = 0.168 + 0.267 = 0.435; then the value for the short term is from 0.168 to 0.435. = (0.968 – 0.168): 3 = 0.267 (median value calculation), so = 0.168 + 0.267 = 0.435; then the value for the short term is from 0.168 to 0.435.

Second steps are to find out the long-term value, it is obtained from the highest value minus the median value calculation results, then the long-term value is obtained, namely: = 0.968 – 0.267 = 0.701; then the value for the long term is from 0.701 to 0.968.

The third step is to find the medium-term value is the value that is between the upper limit of the short-term value and the lower limit of the long-term value, so the value for this medium term is a value from 0.436 to 0.700.

CONCLUSION

The readiness of elements of the National Police SDO so that the development of cybercrime can be anticipated is still not optimal. This condition can be seen from the human resources (HR) elements Dittipidsiber Bareskrim Polri and Polda ranks, budget, facilities and infrastructure, and systems and methods. For this reason, there need to be strategic efforts on an ongoing basis, including training, discussions, coaching clinics, research, collaborative governance, seminars, governance modernization, and others, so that the readiness of the elements of SDO Dittipidsiber Bareskrim Polri and Polda ranks are in ideal conditions and are increasingly qualified so that it will be able to fully and comprehensively anticipate developments in cybercrime;

Implementing the management function in strengthening the capacity of the National Police's SDO so that the development of cybercrime can be anticipated still needs to be systematic. This condition can be observed in planning, organizing, implementing, and supervising functions. For this reason, there is a need for progressive strategic efforts, namely socialization, internalization, FGDs, information systems, reward and punishment patterns, and others, so that the implementation of the management function at Dittipidsiber Bareskrim Polri and Polda ranks

can run consistently and effectively and can support efforts anticipating the progressive development of cybercrime;

The performance achievements of SDO Polri so that the development of cybercrime can be anticipated still need to be improved. This condition can be seen from the percentage of issuance of SP2HP and the disclosure and resolution of cases related to cybercrime at the Dittipidsiber Bareskrim Polri and Polda in the ranks. For this reason, there is a need for comprehensive strategic efforts, namely coaching clinics, updating performance appraisal systems, collaborative studies, forming desks, and others, so that the performance achievements of the Dittipidsiber Bareskrim Polri and Polda ranks will increase and will be able to anticipate cybercrime developments effectively and completely.

REFERENSCES

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293-137311.

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime.

Barn, R., & Barn, B. (2016). An Ontological Representation of a Taxonomy for cybercrime. In Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey, 12–15 June 2016.

Black, A., Lumsden, K., & Hadlington, L. (2019). 'Why Don't You Block Them?'Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime. *Online Othering: Exploring Digital Violence and Discrimination on the Web*, 355-378.

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258.

Chang, Y. C. (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Edward Elgar Publishing.

Culp III, K., Eastwood, C., Turner, S., Goodman, M., & Ricketts, K. G. (2016). Using a SWOT analysis: Taking a look at your organization [2016].

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime business digital in Indonesia. In *E3S Web of Conferences* (Vol. 125, p. 21001). EDP Sciences.

Gurel, M., & TAT, M. (2017) SWOT Analysis: A Theoretical Review. *The Journal of International Social Research, 10*(1).

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.

ICMEC. (2017). Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review; International Centre for Missing & Exploited Children: Alexandria, VA, USA,

Jeyaraj, K. L., Muralidharan, C., Senthilvelan, T., & Deshmukh, S. G. (2012). Application of SWOT and Principal Component Analysis in a Textile Company-A Case Study. *International Journal of Engineering Research and Development*, *1*(9), 46-54.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81.

McGuire, M. (2019). It Ain't What It Is, It's the Way That They Do It? Why We Still Don't Understand Cybercrime. In *The Human Factor of Cybercrime* (pp. 3-28). Routledge.

McGuire, M., & Dowling, S. (2013). Cyber Crime: A Review of the Evidence. *Summary of key Findings and Implications. Home Office Research report*, *75*, 1-35.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current psychiatry reports*, *23*, 1-9.

Namugenyi, C., Nimmagadda, S. L., & Reiners, T. (2019). Design of a SWOT Analysis Model and Its Evaluation in Diverse Digital Business Ecosystem Contexts. *Procedia Computer Science*, *159*, 1145-1154.

Nichifor, E., Lixăndroiu, R. C., Sumedrea, S., Chițu, I. B., & Brătucu, G. (2021). How can SMEs Become More Sustainable? Modelling the M-Commerce Consumer Behaviour with Contingent Free Shipping and Customer Journey's Touchpoints Optimisation. *Sustainability*, *13*(12), 6845.

Ommani, A. R. (2011). Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis for Farming System Businesses Management: Case of Wheat Farmers of Shadervan District, Shoushtar Township, Iran. *African Journal of Business Management*, *5*(22), 9448.

Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2018). *The impact of cybercrime on Belgian businesses*. Intersentia.

PAYNe, B. K., & Hadzhidimova, L. (2020). Disciplinary and Interdisciplinary Trends in Cybercrime Research: An Examination. *International Journal of Cyber Criminology*, *14*(1), 81-105.

Phadermrod, B., Crowder, R. M., & Wills, G. B. (2019). Importance-performance analysis based SWOT analysis. *International Journal of Information Management*, *44*, 194-203.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379-398.

Polit, D. F., & Beck, C. T. (2004). *Nursing Research: Principles and Methods*. Lippincott Williams & Wilkins.

Sammut-Bonnici, T., & Galea, D. (2015) SWOT Analysis, Chapter Published in: Wiley Encyclopedia of Management, John Wiley & Sons Ltd. DOI: 10.1002/9781118785317.WEOM120103.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research*, *19*(6), 515-518.

Viano, E. C. (2017). Cybercrime, Organized Crime, and Societal Responses. *Int. approaches, Basel*, 1103.

Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/dbase/ab2/nyr90.shtml