

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

Agus Ngurah Maha Krisna¹, Nera Marinda Machdar²

^{1,2}Bhayangkara University, Greater Jakarta, Indonesia Address: Jl. Raya Perjuangan No. 81, RT.003/RW.002, Bekasi, West Java 17143

ABSTRACT: This study aims to evaluate the implementation of recruitment systems, competencies, and training programs and their impact on the career advancement of personnel within the Directorate of Cyber Crime (Dittipidsiber), Criminal Investigation Agency (Bareskrim) of the Indonesian National Police (Polri). The rapid evolution of the internet has created a borderless cyberspace where illegal activities often transcend legal boundaries. To address these challenges, Polri has continuously restructured its cyber units since 2002, culminating in the establishment of the dedicated Dittipidsiber in 2017. This research employs a qualitative descriptive method utilizing a "chain of evidence" approach, drawing data from direct interviews with primary informants, focus group discussions (FGD) with 20 personnel, internal documents, and open-source intelligence (OSINT). Findings reveal that recruitment requires specific expertise in cybercrime handling and prioritizes top-tier graduates from police academies. Competency development and training are specialized based on functional roles to enhance professionalism and reliability. However, FGD results indicate inconsistencies in recruitment methods, which vary between formal testing and direct appointment based on organizational needs. A SWOT analysis suggests that while current systems are effective, there is a critical need for standardized recruitment regulations and continuous updates on IT technology to counter organized cybercrime (cyber armies). Furthermore, strengthening collaborations with international partners, ministries, the National Cyber and Crypto Agency (BSSN), and community leaders is essential to enhancing professional cybercrime handling and increasing public trust in the police force.

KEYWORDS: Recruitment System, Competency, Cyber Crime, Dittipidsiber, Career Advancement, Bareskrim Polri.

INTRODUCTION

The emergence and development of various new computer-related technologies have led to new threats and vulnerabilities that must be addressed. Specifically, there is a need to enhance cybersecurity capabilities effectively and efficiently. International cooperation is considered vital in preventing and tackling international or transnational cybercrimes, as well as in developing the capacity of police institutions—particularly in building cyber defense capabilities that will be managed by the Indonesian National Police in collaboration with police forces from other countries. This concept aims to handle cybersecurity threats and establish decision-making mechanisms within a synergistic cooperation between national police forces, acceptable through regional platforms to strengthen cybersecurity. "It is suspected that internet users have crossed boundaries and used the internet to achieve their goals through illegal means. This is known as cybercrime, although the use of this term is still debated given the broad scope of cybersecurity within the development of information flows. The Electronic Information and Transactions (ITE) Law and Telecommunications Law No. 36 of 1999 are considered insufficient to prosecute ITE criminals, prompting the Indonesian House of Representatives (DPR RI) to currently draft the Information Technology Crime Law (UU Tipiti) to provide protection for internet users, credit card holders, and other electronic transaction enthusiasts." As cybercrime increases, the Indonesian National Police (Polri) is expanding its capacity by changing its structure from a Sub-Directorate to a Cybercrime Directorate. This will increase the number of investigations and require additional budgeting at the directorate level. This will allow the police to better anticipate future cybercrime.

METHODS

Research Design

This study uses a qualitative descriptive research method because its purpose is to describe or depict certain symptoms, conditions, or social phenomena. In this case, the data is described in depth and comprehensively, and presents a detailed view of the topic. This study uses a qualitative approach because it defines qualitative methods as research procedures that produce

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

descriptive data in the form of writing or speech from people and observed behavior. This approach is directed at the background and individuals holistically (whole). Therefore, in this case, it cannot isolate individuals or organizations into variables or hypotheses, but must be viewed as part of a goal. The reason this study uses a qualitative approach is because the resulting data is descriptive data obtained from data in the form of writing, words, and documents from reliable sources or informants. This study was conducted with a qualitative descriptive approach, where the data obtained will be analyzed and described qualitatively so that it can be used as an illustration of the implementation process of the recruitment, competency, and training system that is expected to have an impact on improving the career levels of members of the Cyber Crime Directorate of the Criminal Investigation Agency of the Indonesian National Police. So in this study the data collected is in the form of words rather than a series of numbers that explain the process of implementing recruitment, competency and training in the local scope, especially for members of the Cyber Crime Directorate of the Criminal Investigation Agency of the Indonesian National Police.

The research object in this study is the police personnel who serve in the Directorate of Cyber Crimes of the Criminal Investigation Agency of the Indonesian National Police. Police personnel were chosen as the research object because they are the personnel who carry out investigations and inquiries of special crimes related to cybercrime, information crimes and electronic transactions, telecommunications crimes including transnational crimes related to cybercrime. The variables in this study consist of three independent variables, namely the recruitment system (X1), competence (X2), and training (X3), and one dependent variable, namely career advancement (Y).

Data collection was conducted using interviews, focus group discussions, and questionnaires. The data obtained was then analyzed in detail by analyzing internal factors (strengths and weaknesses) and external factors (opportunities and threats), which are crucial for identifying indicators of the capabilities of the National Police's Cyber Crime Directorate (Ditipidsiber) members, based on the recruitment and training conducted, thus improving their capabilities.

The population in this study was all police personnel assigned to the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency, totaling 160 personnel at the headquarters of the Indonesian National Police. The sample was determined using a purposive sampling technique by considering certain criteria, including: (1) having the status of an active police member; (2) having followed the applied recruitment system; and (3) having followed a series of competency tests and training such as analysis, shooting, intelligence, cybercrime and surveillance training.

The data analysis used is the SWOT analysis model (Strengths, Weakness, Opportunities, Threats). Strengths and weaknesses are both internal factors of the members of the Cyber Crime Directorate of the Indonesian National Police. While Opportunities and Threats are external factors of the members of the Cyber Crime Directorate of the Indonesian National Police. Several internal and external factors related to the recruitment, competence and training of members of the Cyber Crime Directorate of the Indonesian National Police where the Internal Factor Analysis Summary (IFAS) consists of Strengths (S) and Weakness (W) while the External Factor Analysis Summary (EFAS) consists of Opportunities (O) and Threats (T) need to be identified and analyzed to determine a good strategy for the future in recruiting and training members of the Cyber Crime Directorate of the Indonesian National Police in order to achieve good competence in the future for the future of the organization or the Cyber Crime Directorate of the Indonesian National Police.

RESULTS

The next step taken after the process of creating a list of indicators from internal and external environmental variables, and formulating them into S-O, S-T, W-O and W-T strategies is to give weight to each indicator, namely by comparing the role of one particular indicator with other indicators. The maximum weight given to each category is 1 or 100%. Which is obtained from the average score assessment results for each indicator taken from 20 respondents then divided by the number of each indicator so that the total is 1 or 100% with the attached research questionnaire data. Respondents were asked to fill in several indicators on several factors with the following values:

- 1: very weak
- 2: weak
- 3: average
- 4: strong
- 5: very strong

According to (Fredy Rangkuti, 2011: 22-24), the higher the strengths and opportunities, the higher the rating (closer to 5). Conversely, the higher the weaknesses and threats, the lower the rating (closer to 1). The lower the weaknesses and threats, the closer the rating is to 5. Therefore, the maximum weight is then distributed across all indicators presented in Table 1 below.

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

Table 1. Weighting Indicators of the 4 Quadrants of SWOT Analysis

NO	INDICATOR	VALUE
1	STRENGTH	1.00
	a. Good capabilities, experienced in handling cyber crimes b. Trained members/personnel c. Members are equipped with sophisticated IT technology d. Complete weaponry e. Proven and professional capabilities f. Extensive networking skills and relationships g. Solid and responsible personnel h. High level of confidentiality i. Possess extensive information on cybercrime networks j. Possess greater authority than other units in handling cybercrime k. High member morale and a never-give-up spirit that is the hallmark of the Special Directorate	0,10 0,08 0,08 0,08 0,08 0,08 0,08 0,10 0,10 0,10 0,12
2	WEAKNESS	1.00
	a. A constantly changing recruitment system b. Lack of advanced training for members c. Training is somewhat out of sync with member duties d. Budget constraints e. Less than optimal empowerment of existing members' potential f. Dittipidsiber members living in Jakarta lack housing, making mobility difficult g. Limited Personnel/Membership	0,26 0,20 0,06 0,16 0,20 0,06 0,06
3	OPPORTUNITY	1.00
	a. Maintaining good cooperation with foreign police forces b. Exchanging information regarding extensive cybercrime networks worldwide c. Collaborating with the ministries of domestic affairs and foreign affairs, the Ministry of Communication and Information Technology, and the National Cyber and Crypto Agency (BSSN), which allows members to have an extensive network d. Members of the Cyber Crimes Directorate of the Indonesian National Police Criminal Investigation Agency (Bareskrim Polri) still have a good image compared to other National Police units e. Members of the Cyber Crimes Directorate of the Indonesian National Police Criminal Investigation Agency (Bareskrim Polri) are considered the best elite/special forces in the world in handling cybercrime	0,26 0,20 0,14 0,20 0,20
4	THREAT	1.00
	a. The high level of heterogeneity in Indonesian society increases the threat of cybercrime. b. Cybercriminals continue to train to seek out or attack members of the National Police's Cyber Crime Directorate (Dittipidsiber) due to a shift in targets, with police officers, police headquarters, or members of the Dittipidsiber (Dittipidsiber) themselves becoming the primary targets. c. Rapid technological developments require the skills of Bareskrim Polri's Cyber Crime Directorate (Dittipidsiber) members to keep pace with this technology, as cybercrime often utilizes the latest technology, particularly organized cybercrime attacks (cyberarmies).	0,25 0,25 0,50

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

After each indicator is determined, the next step is to assess the contribution or obstacles provided by each indicator to the achievement of the weighted objectives, especially for one period of strategic planning. This assessment is carried out by giving a score from 1 to 5 sourced from (Fredy Rangkuti, 2019: 22-24) where 1 means very weak, 2 means weak, 3 means average, 4 means strong and 5 is very strong. The total score results for each indicator are from the average results of 20 respondents through the SWOT research questionnaire that has been distributed to members of the Dittipidsiber Bareskrim Polri to provide a value for each indicator with the attached data presented in Table 2 below.

Table 2. Total Score of Each Indicator

NO	INDICATOR	SCORE
1	Strength	
	a. Capability	5
	b. Trained	4
	c. IT Technology	4
	d. Weaponry	4
	e. Professionalism	4
	f. Networking Skills	4
	g. Solidity and Responsibility	4
	h. Confidentiality	5
	i. Extensive Information	3
	j. Greater Authority	3
	k. Enthusiasm	5
2	Weakness	
	a. Changed recruitment system	5
	b. Lack of advanced training	4
	c. Slight lack of synchronization of training with duties	2
	d. Budget constraints	3
	e. Less than optimal empowerment of potential	4
	f. Members of the Cyber Crimes Directorate of the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri) lack housing	2
	g. Limited number of members	2
3	Opportunity	
	a. Good cooperation with foreign police forces	5
	b. Extensive information exchange on cybercrime networks	4
	c. Cooperation with other agencies	3
	d. Good image	4
	e. The best elite/special forces in Southeast Asia in handling cybercrime	4
4	Threat	
	a. The high heterogeneity of Indonesian society	4
	b. Cybercriminals continue to practice	4
	c. Rapid technology / cyber army	3

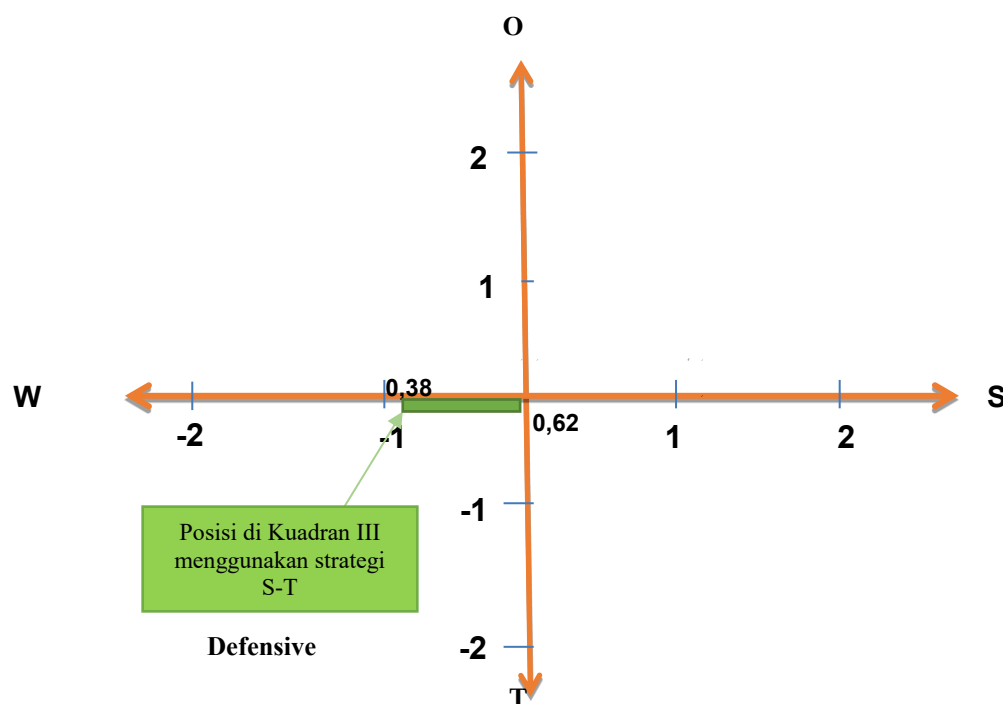
The next step after determining the score or value of each indicator is to calculate the weighted value of each indicator by multiplying the weight by the score per indicator. Once the weighted value for each indicator is found, the weighted values are then added together. The final result of these four steps is the total weighted value for all variable categories, as presented in Table 3 below.

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

Table 3. Total Weighted Value

No	Indikator	Value	Score	Weighted Value
1.	Strength	1.00		
	a. Capability	0,10	5	0,5
	b. Trained	0,08	4	0,32
	c. IT Technology	0,08	4	0,32
	d. Weaponry	0,08	4	0,32
	e. Professionalism	0,08	4	0,32
	f. Networking Skills	0,08	4	0,32
	g. Solidity and Responsibility	0,08	4	0,32
	h. Confidentiality	0,10	5	0,5
	i. Extensive Information	0,10	3	0,3
	j. Greater Authority	0,10	3	0,3
	k. Enthusiasm	0,12	5	0,6
	Total Strength		45	4,12
2.	Weakness	1.00		
	a. Changed recruitment system	0,26	5	1,3
	b. Lack of advanced training	0,20	4	0,8
	c. Slight lack of synchronization of training with duties	0,06	2	0,12
	d. Budget constraints	0,16	3	0,48
	e. Less than optimal empowerment of potential	0,20	4	0,8
	f. Members of the Cyber Crimes Directorate of the Criminal Investigation Agency of the Indonesian National Police (Bareskrim Polri) lack housing	0,06	2	0,12
	g. Limited number of members	0,06	2	0,12
	Total Weakness		22	3,74
	NUMBER OF INTERNAL FACTORS		67	7,86

Based on Table 3, the Weighted Value of the Strengths of the Dittipidsiber Members is 4.12. While the Weighted Value of the Weaknesses of the Dittipidsiber Members is 3.74. From the calculation of these two values, a positive difference of 0.38 is obtained. Then for the Weighted Value of the Opportunities of the Dittipidsiber Members is 4.12. While the Weighted Value of the Threats of the Dittipidsiber Members is 3.5. From the calculation of these two values, a positive difference of 0.62 is obtained. For the Number of Internal Factors is 7.86. While for the Number of External Factors is 7.62. From the calculation of these two values, a negative difference of 0.24 is obtained. From the calculation of these weighted values, the position of the implementation of the recruitment, competency and training system to improve the career level of the Dittipidsiber Members of the Criminal Investigation Agency of the Indonesian National Police in the 4-quadrant SWOT matrix can be described as in Figure 1 below.



DISCUSSION

With a weighted value of positive strengths and weaknesses factors of (0.38) while the weighted value of positive opportunities and threats factors of (0.62) then the position of recruitment and training in improving competency in the Four Quadrant SWOT matrix is located in Quadrant III or defensive with a W-T strategy where there are still many shortcomings that need to be fixed in the recruitment and training process to achieve better competency by members of the Dittipidsiber Bareskrim Polri. In addition, a negative difference (0.24) was also found between internal factors and external factors in members of the Dittipidsiber Bareskrim Polri so that it is necessary to work harder to reduce the number of external factors that can affect the performance of members of the Dittipidsiber Bareskrim Polri by adding strength factors in members of the Dittipidsiber Bareskrim Polri through a better recruitment and training process in the future.

Therefore, members of the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri) are required to continuously undergo training by updating their IT knowledge, particularly on the increasingly prevalent cybercrime, to keep pace with cybercriminals who use increasingly sophisticated technological tools. Members of the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri) are also expected to carry out their duties professionally and maintain solidarity among members, while maintaining the confidentiality of data and the members themselves, both in the field and in their daily lives. The following are findings from research on recruitment and training for members of the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri) based on direct observations of the activities of members of the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri), interviews with sources directly involved in recruitment, competency, and training, and focus group discussions with numerous members of the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri).

First, recruitment of members of the Dittipidsiber Bareskrim Polri must continue to be carried out as a regeneration and sustainability of the Dittipidsiber Bareskrim Polri organization itself, even though the recruitment has a changing pattern, the recruitment of the Dittipidsiber Bareskrim Polri has a high standard for entering as a member of the Dittipidsiber Bareskrim Polri compared to other agencies within the Polri itself.

Second, the competence of the members of the Dittipidsiber Bareskrim Polri is very good and diverse, and has even been recognized by the people of the Southeast Asia region. This can be seen from the results of discussions with several members of the Dittipidsiber Bareskrim Polri who underwent training for up to 6 months, which has resulted in members gaining more skills and expertise.

Third, training for members of the Criminal Investigation Agency's Cyber Crime Directorate is urgently needed, especially for newly recruited members, as they offer added value and enhanced skills, particularly in handling cybercrime. For example, members who were initially inexperienced in shooting can become proficient. Members with investigative talents can become investigators.

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

CONCLUSION AND RECOMMENDATIONS

Based on the results of research and detailed discussions and supported by theoretical reviews, documents, data, observation results, interviews, focus group discussions and questionnaire distribution with several members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency, which were then analyzed using the SWOT analysis method which can support researchers in drawing several conclusions as follows. First, the implementation of the recruitment system for members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency is carried out with a very strict process through selection from active or serving Indonesian National Police members with several specific criteria according to the needs of the organization. However, the recruitment process is carried out in different ways every year and there is no standard regarding the recruitment of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency so that the recruitment system is still changing. Second, training for members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency is very much needed by personnel or members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency by looking at the functions and duties of members so that they gain new skills. In addition, the members' abilities have also increased from the results of the training they have received for 3 weeks to 6 months so that they can be directly applied in carrying out their duties in the field professionally. However, there are still trainings conducted by members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency that are not in accordance with the functions of the members on duty and this makes the training inefficient or even wasted because it is not directly used by members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency in carrying out their daily duties. Third, recruitment and training play a very important role in improving the competence of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency. This is proven from the results of observations, direct interviews with the leadership of the Directorate of Cyber Crimes of the Indonesian National Police Criminal Investigation Agency, discussions with members of the Directorate of Cyber Crimes of the Indonesian National Police Criminal Investigation Agency, data and documents as well as SWOT analysis that the competence of members of the Directorate of Cyber Crimes of the Indonesian National Police Criminal Investigation Agency is getting better and increasing after members were recruited through a very selective process and then given very good training by working directly with various parties, especially other national police forces to make members of the Directorate of Cyber Crimes of the Indonesian National Police Criminal Investigation Agency more professional, modern and trustworthy and focused on a data analysis approach (predictive), performance responsibility (responsibility), and fair transparency.

The suggestions that can be given for the implementation of the recruitment, competency and training system to improve the career level of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency are as follows. First, create a regulation regarding standard standards related to the recruitment of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency who are truly selected and the best members of the Indonesian National Police who are tasked with eradicating cybercrime in Indonesia properly so that they have a fixed and good standardization every time they are recruited. Second, continue to provide the best training on an ongoing basis so that members increasingly master their skills by looking at the functions or duties of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency so that the training material can be absorbed directly and not wasted, especially providing more training on information technology / IT or cyber army which is currently increasingly prevalent in order to keep up with the increasingly rapid technological developments. In addition, members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency are expected to always add and update their competencies so as not to be left behind by technological developments. Third, members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency are expected to collaborate with relevant parties such as the Ministry of Communication and Information Technology of the Republic of Indonesia, which has also played an active role in the supervision and implementation of technical guidance on policies in the field of communication and informatics on a national scale. Furthermore, the leadership of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency needs to pay attention to the welfare of members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Agency so that they are more active and serious in participating in training and on duty so that they can foster enthusiasm in carrying out their work to combat cybercrime in Indonesia more optimally and professionally, modernly and reliably.

REFERENCES

- 1) Afrizal, 2016, *Metode Penelitian Kualitatif*, Raja Grafindo Persada, Jakarta.
- 2) Basri, Hasan dan Rusdiana, 2015, *Manajemen Pendidikan & Pelatihan*, CV Pustaka Setia, Bandung.
- 3) Hasibuan, Malayu, S.P, 2017, *Manajemen Sumber Daya Manusia edisi revisi*. Bumi Aksara, Jakarta.
- 4) Himpunan, Peraturan Perundang - undangan, 2012, *Undang - Undang Informasi dan Transaksi Elektronik*, Fokus media,Bandung.
- 5) Jeremy M. Wilson, 2015, *Police Recruitment and Retention for the New Millennium*,Journal,US

Implementation of Recruitment, Competency and Training Systems to Improve the Career Levels of Members of the Cyber Crime Directorate of the Indonesian National Police Criminal Investigation Unit

- 6) Kelana, Momo, 2002, *Memahami Undang – Undang Kepolisian Pada Undang – Undang Nomor 2 Tahun 2002*, Grafira Indonesia, Jakarta.
- 7) Mario S. Staller, 2017, *Weapon System Selection in Police Use of Force*, Journal, US
- 8) Michael D. White and Gipsy Escobar, 2008, *International Review of Law, Emerging issues for the effective recruitment, selection and training of police in the United States and abroad*, Journal, US
- 9) Prathiana, I, Wayan, 2015, *Hukum Pidana Internasional*, Yrama Widya, Bandung
- 10) Redaksi Sinar Grafika, 2009, *Undang - Undang Kepolisian Negara (UU RI No.3 Th. 2002)*, Sinar Grafika, Jakarta.
- 11) Sutanto, 2005, *POLRI Menuju Era Baru Pacu Kinerja Tingkatkan Citra*, Yayasan Pengembangan Kajian Ilmu Kepolisian, Jakarta.



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.