MAGISTER MANAJEMEN-UNISSULA
SAMaJ
SULTAN AGUNG MANAGEMENT JOURNAL

Baintelkam Polri Leadership Strategy Based on Cognitive Warfare in Strategic Decision-Making in the Framework of Maintaining Security Stability and Public Order in the Digital Era

Anom Setyadji
Faculty of Economic, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: 20402500535@std.unissula.ac.id

Abstract. *This research examines the strategic leadership model of Baintelkam Polri based on cognitive warfare in maintaining national security stability in the digital era. Amidst the shifting landscape of modern threats that target psychological dimensions, public opinion, and collective societal awareness, the role of adaptive leadership serves as the primary key in steering institutional transformation. The findings of this study reveal that a profound understanding of the dynamics of cognitive warfare, coupled with strategic leadership commitment, acts as the core driving force in accelerating doctrinal modernization, enhancing human resource capacity, and leveraging cyber analytical technologies. However, the transformation process in the field still encounters several structural challenges. These challenges include the predominance of conventional investigation methods, rigid standard operating procedures, uneven distribution of digital monitoring infrastructure up to the frontline units, and regulatory ambiguity concerning the operational legal framework. To overcome these obstacles and bridge the gap between leadership vision and empirical field conditions, this study formulates an ideal strategic leadership model anchored on four core pillars: (1) mastery of algorithmic intelligence and the integration of human intelligence; (2) rapid and responsive crisis command agility; (3) doctrinal reform alongside massive specialized education and training in cyber-social domains; and (4) strengthened cross-sector collaboration supported by legal certainty and the protection of human rights.*

Keyword: *Cognitive; Intelligence; Leadership; Strategic; Transformation.*

1. Introduction

The development of globalization and information technology has brought fundamental changes to the strategic environment of people's lives. These changes are occurring in various fields, from social, economic, political, cultural, and security. Advances in communication technology enable information to be produced, distributed, and received quickly without being limited by space and time. This development is intensifying with the Industrial Revolution 4.0, which is characterized by the use of artificial intelligence, big data, cloud computing, the Internet of Things (IoT), robotics, and various other digital technologies.

Technology is no longer merely a means of supporting human activities, but has evolved into a critical infrastructure that influences interaction patterns, economic activities, public services, communication, and even decision-making processes.

Digital transformation is also changing the patterns of relationships between individuals, groups, communities, and institutions. The use of e-commerce, e-money, digital banking services, and various internet-based applications has created an increasingly connected economic and social ecosystem. At the same time, the development of social media and digital platforms is changing the patterns of information distribution. The public is no longer merely a recipient of information from mainstream media, but also plays a role as a producer, disseminator, and shaper of public opinion. Every individual and group can express their views, build narratives, and influence public perception through various digital platforms.

The extent of Indonesian society's connectedness to the digital space can be seen from internet penetration data. The Indonesian Internet Service Providers Association (APJII) recorded that the number of Indonesian internet users in 2024 reached 221,563,479, representing a penetration rate of 79.5% of the total population. Meanwhile, the Central Statistics Agency (BPS), through its publication of the 2024 Indonesian Telecommunications Statistics, recorded that 72.78% of Indonesia's population had access to the internet in the same year. Both figures come from different institutions and measurement methods, but both demonstrate the extent of society's connectedness to the digital space. This situation opens up opportunities to utilize technology for productive activities and public services, while also expanding the scope for the spread of misinformation, opinion manipulation, and various forms of digital crime (APJII, 2024; BPS, 2025).

Behind the benefits of digital transformation, there are increasingly complex risks. Technology can be misused for online fraud, online gambling, illegal investments, financial transaction manipulation, personal data theft, hacking, hate speech, and various forms of cybercrime. The digital space can also be exploited by extremist groups and terrorist networks to spread propaganda, build ideological support, recruit, and coordinate activities through digital communication. The open, fast-paced, and cross-border nature of the digital space makes these threats difficult to identify through conventional surveillance approaches.

One of the key issues in the development of the digital space is the increasing spread of false information, or hoaxes. The Ministry of Communication and Digital (Komdigi) identified and clarified 1,923 pieces of hoax content throughout 2024. Of these, the fraud category accounted for the most, with 890 pieces, followed by politics (237 pieces), government (214 pieces), health (163 pieces), and disasters (145 pieces). This data shows that false information has reached various areas of public life, including the political and government sectors, which are related to public trust in state institutions (Ministry of Communication and Digital, 2025).

In terms of law enforcement, the National Criminal Information Center (Pusiknas) of the Indonesian National Police Criminal Investigation Agency (Bareskrim Polri) recorded that throughout 2024, the Indonesian National Police prosecuted 3,331 cybercrime cases. These

cases included fraud, defamation, pornography, fake news or hoaxes, hate speech, illegal access, data theft, and hacking. In the same year, the Indonesian National Police also prosecuted 13,922 cases of data manipulation crimes using the Information and Transactions (ITE), a 23.35% increase compared to 2023's 11,286 cases. This data demonstrates that the digital space has become a breeding ground for various forms of legal violations, requiring adaptive police detection, information processing, analysis, and response capabilities (Pusiknas Bareskrim Polri, 2025).

In addition to the aforementioned data, based on Komdigi's data recapitulation for the period from August 1, 2018, to July 29, 2026, which was used as the initial research material, there were 16,999 hoax content findings from various categories. The fraud category recorded 3,904 contents, government 2,997 contents, health 2,610 contents, politics 2,121 contents, international 842 contents, disaster 833 contents, crime 751 contents, defamation 613 contents, religious 367 contents, myths 236 contents, trade 166 contents, education 85 contents, and other categories totaling 1,474 contents.

Table Summary of Hoax Content Findings by Category for the Period 1 August 2018–29 July 2026

No.	Category	Amount
1	Fraud	3,904
2	Government	2,997
3	Health	2,610
4	Political	2.121
5	International	842
6	Disaster	833
7	Crime	751
8	Defamation	613
9	Religious	367
10	Myth	236
11	Trading	166
12	Education	85
13	Other	1,474
Total		**16,999**

Source: Ministry of Communication and Digital (Komdigi).

The data shows that the spread of hoaxes is not only related to fraud, but also touches on issues of government, health, politics, religion, and various aspects of public life. The spread of false information in these areas has the potential to influence how people understand events, form assessments of institutions, and determine attitudes and behavior. While not all hoax content can be categorized as Cognitive Warfare, the data provides a snapshot of the information environment that is vulnerable to being exploited to influence public perceptions and behavior.

The changing nature of these threats demonstrates that security issues are no longer solely related to threats to territory, infrastructure, or physical safety. The security dimension is also increasingly linked to a party's ability to influence the thoughts, perceptions, beliefs, emotions, and decision-making processes of individuals and groups. Information has become a strategic instrument that can be used to build trust, but it can also be exploited to create

distrust, strengthen polarization, and influence the legitimacy of state institutions. Therefore, the development of digital technology must be understood not only as a change in communication media, but also as a change in the strategic environment that influences the patterns and characteristics of security threats.

One relevant concept for understanding these changes is Cognitive Warfare. Du Cluzel (2020) explains that Cognitive Warfare transforms the human cognitive domain into a strategic competitive space. Threat orientation is not only directed at destroying physical capabilities or controlling territory, but also at influencing how individuals and groups receive information, understand reality, form beliefs, and make decisions. Thus, humans and their cognitive processes become a crucial part of the strategic competitive environment.

Deppe and Schaal (2024) explain that Cognitive Warfare is a concept developing in security and defense studies, focusing on the use of technology and various forms of action to produce cognitive impacts on individuals and groups. They point out that this concept is related to disinformation, hybrid threats, information operations, and perception manipulation, but maintains a particular emphasis on the intended impact on cognitive processes. Within this framework, the primary characteristic of Cognitive Warfare is not simply the presence of false information, but rather the attempt to influence or alter the target's cognitive processes through actions with strategic objectives.

Hung and Hung (2022) also draw attention to the relationship between Cognitive Warfare and non-kinetic forms of warfare. This perspective places influence on mental states and behavior as a crucial component of competitive strategy. Meanwhile, advances in information technology expand actors' capabilities to produce and disseminate messages quickly, precisely, and repeatedly. The use of artificial intelligence, algorithms, behavioral analysis, and user data allows messages to be tailored to specific target groups. This allows the process of opinion formation and perception to be influenced through systematically designed communication and information distribution strategies.

In the digital environment, cognitive threats can develop through various mechanisms, including the spread of misleading narratives, manipulation of information contexts, repetitive perception formation, exploitation of social differences, and the reinforcement of certain sentiments. Ienca (2023) draws attention to the relationship between technological development and human cognitive vulnerabilities. The use of data-based technologies and algorithms can influence the information environment individuals receive, including how information is selected, displayed, and prioritized. In the context of cognitive threats, these mechanisms can be exploited to construct certain narratives, reinforce prejudices, direct attention, and influence decision-making processes.

This issue relates to the concept of information disorder proposed by Wardle and Derakhshan (2017). They differentiate information disorder into three main forms: misinformation, disinformation, and mal information. Misinformation is false information spread without any intention of causing harm, disinformation is false information deliberately produced and

spread to cause harm, and mal information is information based on reality but used to harm a particular party. This distinction is important because not all misinformation has the same motives and impacts. In a security context, the ability to identify the source, motive, distribution pattern, and potential impact of information is a crucial part of the intelligence analysis process.

The organized spread of disinformation can have broader impacts than simply individual misunderstandings. Narratives designed to reinforce certain sentiments can fuel social polarization, exacerbate intergroup tensions, undermine public trust in the government, and undermine the legitimacy of state institutions. When false information is received and disseminated widely, public responses to an event can be formed before verification can be carried out. In certain situations, this can escalate into social unrest, horizontal conflict, and disruptions to security stability.

In the context of police duties, these changes have consequences for the maintenance of public security and order (Kamtibmas). Digital space has become a public space where people express their aspirations, criticisms, complaints, and demands on state institutions. Information about an event can spread rapidly and shape public perception in a short time. The "No Viral, No Justice" phenomenon, for example, demonstrates how public attention in the digital space can influence responses to law enforcement issues. This phenomenon does not always indicate negative issues, as digital media can also be a means of social control. However, this situation demonstrates that the legitimacy of and public trust in the police is increasingly linked to the dynamics of public information and communication.

Peyton et al. (2019) demonstrated the importance of police legitimacy and public trust in building public cooperation in security enforcement. Public trust is formed not only through law enforcement actions but also through perceptions of the fairness, integrity, transparency, and accountability of officers. In a digital environment, these perceptions can be influenced by widely circulated information, including unverified or intentionally manipulated information. Therefore, the police need to be able to understand the dynamics of public opinion and anticipate information that could potentially disrupt public order and security.

Normatively, Law Number 2 of 2002 concerning the Indonesian National Police affirms that the main duties of the Indonesian National Police (Polri) include maintaining public security and order, enforcing the law, and providing protection, guidance, and services to the community. These duties place the Polri as an institution with a crucial responsibility in maintaining domestic security. Changes in the strategic environment in the digital era require that the implementation of these duties be supported by the organization's ability to understand evolving threats, manage information, and make appropriate and proportionate decisions.

These strategic environmental changes require the Indonesian National Police (Polri) to continue organizational transformation and strengthen institutional capacity. Police transformation is not simply achieved through modernizing equipment and utilizing

information technology; it also needs to address aspects of leadership, human resource competency, doctrine, information governance, coordination, and decision-making patterns. Technology will only deliver strategic benefits if supported by leadership capable of directing its use according to organizational needs. Therefore, the Indonesian National Police's digital transformation needs to be positioned as part of the organization's capacity to read, understand, and respond to increasingly complex threats.

More specifically, this research aims to examine how the Cognitive Warfare-based leadership strategy of the Indonesian National Police's Intelligence and Security Agency (Baintelkam Polri) is applied in the strategic decision-making process. These issues include how leaders understand the changing nature of threats, determine intelligence information needs, integrate technology and data, direct predictive analysis, consider various alternative courses of action, and make decisions oriented towards maintaining public order and security. This research also needs to explain the factors that support and hinder the implementation of this leadership strategy.

An empirical gap that requires attention is the lack of an integrated picture of the alignment between the complexity of cognitive threats and leadership strategies, the quality of intelligence information, human resource capacity, technological support, coordination mechanisms, and strategic decision-making processes within the Indonesian National Police's Intelligence and Security Agency (Baintelkam Polri). This gap needs to be explored through organizational documents, performance reports, internal policies, and information obtained from relevant stakeholders and personnel. Therefore, this study does not start from the assumption that Baintelkam Polri lacks the capacity to deal with digital threats, but rather from the need to identify the actual conditions, challenges, and scope for developing leadership strategies in response to the changing nature of threats.

2. Research Methods

Based on the formulation of the problem, objectives, and characteristics of the data studied, this type of research is classified into several main methodological dimensions as follows: Based on Approach: Mixed-Methods Research, this study uses a mixed approach, combining quantitative and qualitative approaches sequentially (Sequential Explanatory Strategy). (Creswell, JW, & Creswell, JD, 2018). Quantitative Approach (Dominant): Used to test associative hypotheses, regression, and structural relationships between variables using a Likert-scale questionnaire instrument (scale 1–5) with a sample of n=240 respondents from a total population of N=602 Baintelkam Polri personnel. (Sugiyono. 2022. Quantitative, Qualitative, and R&D Research Methods. Alfabeta). Aims to measurably measure the influence of understanding Cognitive Warfare (X1) and strategic leadership (X2) on operational transformation (Y1) and its impact on national security stability (Y2). Qualitative Approach (Supporting): Used to explore and deepen quantitative data findings, particularly related to inhibiting factors (inhibitors) and strategic ideas (enablers) through text analysis of open-ended questionnaire questions.

3. Results and Discussion

3.1. Sample Structure Description

The population in this study ispersonnel with various ranks and positions in various levels at the Baintelkam Headquarters of the Republic of Indonesia National Police totaling 602 people. This data refers to the Regulation of the Chief of the Republic of Indonesia National Police Number 6 of 2017 concerning the Organizational Structure and Work Procedures of Organizational Units at the Headquarters Level of the Republic of Indonesia National Police.The data for this research was collected by distributing questionnaires to a random sample of 240 people to personnel ranging from the highest to the lowest ranks and positions at the National Police Headquarters' Intelligence and Security Agency.

Within the framework of quantitative research methodology, the availability of samples that meet the criteria and a high response rate are the main prerequisites for ensuring the feasibility of statistical testing, external validity, and representativeness of the sample to the target population. Based on the recapitulation data of instrument collection, the allocation details and eligibility status of the questionnaire are presented in the following table:

Table Questionnaire allocation details

No	Information	Amount
1	The questionnaire was distributed	240
2	Unreturned questionnaires	0
3	The questionnaire does not meet the requirements	0
4	Questionnaires that are returned and can be processed	240

Source: Data Processed by Researchers 2026

Based on the questionnaire recapitulation table, it can be analyzed with the following description:

1) Complete Response Rate (Response Rate = 100.00%):

a) All 240 questionnaire files distributed to the target respondent sample within the Baintelkam Polri environment and related ranks were successfully collected back in full (100.00%).

b) This perfect response rate reflects the high level of commitment, discipline, and active participation of officers, non-commissioned officers, civil servants, and related experts in supporting strategic research on intelligence leadership development.

2) Response Quality and Data Processing Level (Usable Response Rate = 100.00%):

a) No instruments were eliminated (zero incomplete responses). All statement items from Part I (Characteristics), Part III (Likert Indicators P1 to P15), and Part IV (Open/Qualitative Questions) were completed completely without any missing values.

b) This condition indicates that the questionnaire instrument has clear instructions (user-friendly) and very high substance relevance for the respondents' field of work.

3) Sample Adequacy:

a) Based on the calculation of the minimum sample limit formula (Slovin) for a population of N=602 Baintelkam Polri personnel with a margin of error e=5%, the minimum sample limit required is n=240.8≈241 respondents.

b) With n=240 effective data collected, this sample size is in the adequate sample size category to meet the prerequisites for classical assumption testing, multiple linear regression, and structural equation modeling based on Partial Least Squares Structural Equation Modeling (PLS-SEM).

4) Impact on Testing:

a) Non-Response Bias Free: Since 100% of the questionnaires were returned and eligible for processing, the statistical estimation model is free from sample attrition.

b) Generalizability Reliability: The results of quantitative analysis (such as Mean value, TCR, coefficient of determination) *R*2, and the bootstrapping path coefficient) has strong legitimacy to be generalized at the Baintelkam Polri population level.

3.2. Sample Structure Instrument Quality Test

1) Test Statistics Construct Validity (Pearson Product-Moment) Sample Structure

Research instrument testing plays a crucial and fundamental role within the quantitative methodology framework, ensuring that the questionnaire instrument has an adequate degree of accuracy, precision, and reliability in carrying out its measurement function in the field (Arikunto, 2013). Epistemologically, construct validity is designed to demonstrate the extent to which the instrument is able to accurately and precisely measure the theoretical conceptual framework of the variables being studied (Sugiyono, 2019). In the context of this research, testing was conducted on all questionnaire items, starting from the indicators P_1 until P_{15}, to ensure that the theoretical representation of the independent to dependent variables is measured validly (Creswell & Creswell, 2018). The correlation technique applied is Pearson Product-Moment Correlation, where the score of each indicator item (X_i) is mathematically correlated with the total score of the construct of the relevant variable (Y), in accordance with established multivariate analysis standards in social and institutional research (Hair et al., 2014). The calculation uses the mathematical formula Pearson Correlation Coefficient (rcount):

$$r_{xy} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{[n\sum X^2 - (\sum X)^2][n\sum Y^2 - ((\sum Y)^2]}}$$

Where:

n= Effective sample size of respondents (240 respondents).

X= Respondent's answer score on a particular indicator item.

Y= Total score of the construct of the relevant variable.

$\sum XY$= The sum of the multiplication of the score of item X and the total score of Y.

$\sum X^2$= Sum of squares of item scores X.

$\sum Y^2$= Sum of squares of total scores Y.

To test the significance of the t-test (t count), use the formula:

$$t_{count}=\frac{r\sqrt{n-2}}{\sqrt{1-r^2}}$$

Meanwhile, for Validity Criteria, it is determined based on:

1) Comparison of Critical Values rtable:

For degrees of freedom df=n−2=240−2=238 at a significance level of α=0.05 (two-tailed test), the reference value r is obtainedtable=0.1267.

If rcount>rtable (0.1267), then the indicator item is declared VALID.

2) Probability Value (Sig. 2-tailed):

If the p-value is <0.05, then the indicator item is declared significantly VALID.

2) Test Statistics Reliability (Cronbach's Alpha) Sample Structure

Reliability testing aims to assess the level of consistency, reliability, and stability of a questionnaire instrument when measurements are taken repeatedly. In quantitative parametric statistics, the Cronbach's Alpha (α) coefficient is the primary criterion for measuring internal consistency reliability. It is calculated using the main Cronbach's Alpha (α) formula:

$$\alpha=\left(\frac{k}{k-1}\right)x\ \left(1-\frac{\sum si^2}{st^2}\right)$$

Where:

k= Number of statement indicator items in a dimension/variable.

$\sum si^2$= Number of variants of each indicator item.

st^2 = Variance of the total score of the variable/dimension.

To test each variant using the Item Variance Formula (si^2) and Total Variance (st^2):

$$s^2 = \frac{\sum X^2 - \frac{(\sum X)^2}{N}}{N-1}$$

To see the Reliability Level Criteria (Reference Sekaran & Bougie / Hair et al.):

a. $\alpha \geq 0.90$: Very High Reliable / Very High

b. $0.80 \leq \alpha < 0.90$: Reliable / High

c. $0.70 \leq \alpha < 0.80$: Reliable / Sufficient

d. $0.60 \leq \alpha < 0.70$: Quite Reliable (Minimum Acceptable Limit)

e. $\alpha < 0.60$: Not Reliable (Inconsistent)

Referring to the calculation formula for the r testreliability (Cronbach's Alpha) and the criteria, then the following results will be obtained:

1) Internal Consistency Reliability Test Results:

The results of the calculations above can be sorted and analyzed according to the Respondents' Achievement Level from highest to lowest:

a. Indicator P13 (Improving Public Cognitive Resilience): Indicator P13 recorded a mean of 3.55 (TCR 71.08%, High Category - Lower Limit). A total of 156 respondents (65.00%) agreed that implementing cognitive warfare-based leadership would improve the public's critical thinking resilience in the digital era.

b. Indicator P15 (Prevention of Social Conflict and Disintegration): Indicator P15 obtained a mean score of 3.43 (TCR 68.67%, High Category - Lower Limit). Respondents assessed that effective cognitive domain protection could mitigate the risk of social division, although its current implementation was not felt to be fully optimal.

c. Indicator P14 (Direct Impact of Cognitive Mastery on Public Order and Security): Indicator P14 achieved a mean of 3.43 (TCR 68.58%, High Category - Lower Limit). This indicator recorded the lowest score across all questionnaire instruments, with 78 respondents (32.50%) stating that they Disagree and Strongly Disagree that current mastery of the cognitive domain has had a significant direct impact on the conduciveness of public order and security.

3.3. Analysis Descriptive Statistics and Respondent Achievement Level (TCR): Operational Gap Phenomenon

1) The Need for Human Resource Capacity Building as a Top Priority (Indicator P10)

a) Statistical Value: Mean = 4.39 | TCR = 87.83% (Very High Category)

b) Analysis Highlights: Indicator P10 (Indonesian National Police Intelligence and Security personnel require specialized training in mass psychology, neuro-linguistics, and cyber-social analysis) achieved the highest Mean and TCR scores among all 15 questionnaire indicators. A total of 220 of 240 respondents (91.67%) agreed and strongly agreed. These findings confirm the consensus in the field that technological transformation will not be effective without strengthening the intellectual capacity and psycho-cyber skills of operational personnel.

2) High Awareness of the Polarizing Impact of Cognitive Warfare (Indicator P4)

a) Statistical Value: Mean = 4.35 | TCR = 87.08% (Very High Category)

b) Analysis Highlights: Indicator P4 (Cognitive exploitation by threat actors can trigger social polarization and reduce public trust in the government/Polri) is the strongest point in the X1 variable dimension.

This proves that the National Police's Intelligence and Security Agency (Baintelkam Polri) personnel and related ranks are very aware that the modern cyber battlefield is no longer just about destroying network infrastructure (conventional cyber warfare), but also about destroying social structures and institutional legitimacy through manipulating public perception.

3) Counter-Narrative Capacity Demands and AI-HUMINT Integration (Indicators P7 & P8)

a) P7 Statistical Value: Mean = 4.28 | TCR = 85.58% (Very High Category)

b) P8 Statistical Value: Mean = 4.21 | TCR = 84.17% (Very High Category)

c) Analysis Highlights: In the Strategic Leadership dimension (X2), officers and operational implementers demand that leaders not only passively defend, but are also able to design and direct active counter-narrative strategies (P7).

In addition, P8 emphasized the urgency of adopting a hybrid intelligence approach, namely combining the data processing speed of Artificial Intelligence (AI) with the in-depth acumen of human intelligence (HUMINT).

4) Structural Caution Against Shifting Conventional Operational Focus (Indicator P3)

a) Statistical Value: Mean = 3.46 | TCR = 69.17% (High Category - Lower Limit)

b) Analysis Highlights: Indicator P3 (The National Police Intelligence and Security Agency needs to shift its focus from solely detecting physical threats to protecting the public's cognitive domain) recorded the lowest score on dimension X1. Seventy-seven respondents (32.08%) chose the Disagree or Strongly Disagree options.

Key Findings: This indicates structural caution within the Indonesian National Police. Personnel believe that the shift to the cognitive domain should not override conventional

physical detection but should be implemented in tandem (a dual-track approach).

5) Concerns about Bureaucratic Complexity of Cognitive Control Center (Indicator P11)

a) Statistical Value: Mean = 3.82 | TCR = 76.33% (High Category)

b) Analysis Highlights: Despite its high value, indicator P11 (Establishment of a real-time cognitive intelligence unit or control center) was the lowest-scoring indicator in dimension Y1. Fifty-one respondents (21.25%) chose a neutral to disagree stance. This condition reflects personnel concerns about the emergence of overlapping new organizational structures (overlapping units) or the addition of bureaucratic reporting chains if the cognitive control center is not designed efficiently.

6) The Operational Gap Phenomenon: The Real Impact of the Gap on the Stability of Public Order and Security (Dimension*Y*2)

a) Y2 Dimension Statistical Value: Mean = 3.47 | Mean TCR = 69.44% (High Category - Lower Limit)

(1) P13 (Increasing Community Cognitive Resilience): Mean = 3.55 | TCR = 71.08%

(2) P15 (Social Conflict Prevention & Disintegration): Mean = 3.43 | TCR = 68.67%

(3) P14 (Direct Impact of Cognitive Mastery on Public Order and Security): Mean = 3.43 | TCR = 68.58%

b) Critical Insight: The Y2 dimension overall has the lowest TCR compared to other variables. This phenomenon shows a clear operational gap: Although the level of awareness of cognitive warfare threats (X1=79.21%) and strategic leadership demands (X2=82.25%) are classified as very high, the effectiveness of achieving national security stability (Y2=69.44%) is felt to be less than optimal in the field. This gap confirms that without real improvements in the aspects of Human Resources, Doctrine, Technology, and Regulation (Y1), strategic leadership has not been able to transform potential into optimally conducive security outcomes.

The description above reveals very crucial philosophical and empirical findings, there is a significant gap between the high level of threat awareness (X1=79.21%) and the high demands for strategic leadership (X2=82.25%) and the need for transformation (Y1=81.73%), with the achievement of national security stability results in the cognitive space which is still classified as sub-optimal (Y2=69.44%).

This scientifically proves that strategic leadership and understanding of threats do not automatically result in national security stability, if they are not effectively bridged by concrete Operational Capability Transformation (Y1) in the aspects of Human Resources, Doctrine, Technology, and Regulation.

This inferential statistical analysis aims to test the research hypothesis and measure the extent to which the Enabler Factor variables consisting of Cognitive Warfare Understanding (X1) and Strategic Intelkam Leadership (X2) have a real impact on Operational Capability Transformation (Y1) and National Security Stability (Y2) in a sample of N=240 respondents at Baintelkam Polri.

1) Research Variables:

a) Independent Variables (Enabler Factors):

*X*1 = Cognitive Warfare Understanding (Indicators P1−P4)

*X*2 = Strategic Leadership of Intelkam (Indicators P5−P8)

b) Mediating / Intervening Variables:

*Y*1 = Capability & Operational Transformation (Indicators P9−P12)

c) Dependent / Main Variable:

*Y*2 = National Security Stability (Indicators P13−P15)

2) Regression Modeling Path Structure:

a) Model 1 (Intermediate Path): $Y1=\alpha1+\beta1X1+\beta2X2+e1$

Regression Model 1 tests the extent to which variables X1 (Cognitive Warfare) and X2 (Strategic Leadership) are able to drive Y1 (Intelkam Operational Capability Transformation).

*Y*1 = Operational Capability Transformation (Dependent Variable)

*X*1 = Cognitive Warfare Understanding (Independent Variable 1)

*X*2 = Strategic Leadership of Intelkam (Independent Variable 2)

a= Constant Value (Intercept)

*b*1, b2 = Partial Regression Coefficient (Slopes)

b) Model 2 (Total Main Path): $Y2=\alpha2+\beta3X1+\beta4X2+\beta5Y1+e2$

Regression Model 2 tests the simultaneous and partial influence of X1, X2, and Y1 on the main variable of National Security Stability (Y2).

*Y*2 = National Security Stability (Main Dependent Variable)

*X*1 = Cognitive Warfare Understanding (Independent Variable 1)

*X*2 = Strategic Leadership of Intelkam (Independent Variable 2)

*Y*1 = Operational Capability Transformation (Predictor / Mediator Variable 3)

a= Constant Value (Intercept)

*b*1, b2, b3 = Partial Regression Coefficients (Slopes)

By using the Ordinary Least Squares (OLS) simultaneous equation method and the Matrix Operations / Gaussian Elimination method on the two regression models above, we obtain:

1) Regression Equation Model 1:

$\hat{Y}1=1.9634+0.3558X1+0.5317X2$

Specifically, the regression equation of model 1 tests the ability of variables X1 and X2 to encourage modernization of doctrine, improvement of human resource quality, and adoption of technology in the Indonesian National Police's Intelligence and Security Agency.

2) Regression Equation Model 1:

$\hat{Y}2=-1.9895+1.3815X1-0.6041X2+0.0280Y1$

Specifically, the regression equation of model 2 tests the extent to which the variables*X*1,*X*2, and*Y*1 able to predict the conduciveness of public order and security as well as the cognitive resilience of the community.

After testing the two regression models above, each was calculated using Partial Hypothesis Testing (t Test) and Simultaneous Test (F Test / ANOVA) & Determination Coefficient (R2), then the following results are obtained:

Table Results of partial hypothesis inferential statistical testing (t-test)

Hypothesis Path Statement	Model Path	Path Coefficient (b)	t-count	t-table	p-value	Hypothesis Decision	Theoretical & Operational Conclusions
Understanding Cognitive Warfare (X1) has a positive effect on Capability Transformation (Y1)	Model 1	0.3558	7,3880	1,9700	0.0000	**ACCEPTED**	Improving internal operational capabilities
Intelkam Strategic Leadership (X2) has a positive influence on Capability Transformation (Y1)	Model 1	0.5317	10,4590	1,9700	0.0000	**ACCEPTED**	Becoming the main driver of modernization of doctrine & human resources
Understanding Cognitive Warfare (X1) has a positive effect on National Security Stability (Y2)	Model 2	1.3815	12,5970	1,9700	0.0000	**ACCEPTED**	The main driving factor for public order and security stability
Strategic Leadership of Intelkam (X2) influences National Security Stability (Y2)	Model 2	-0.6041	-4,7880	1,9700	0.0000	**ACCEPTED**	Acts as a corrective/suppressor adjustment factor

Capability Transformation (Y1) has an impact on National Security Stability (Y2)	Model 2	0.0280	0.2100	1,9700	0.8340	**REJECTED (DIRECT)**	Indirect Mediation

Source: Data Processed by Researchers 2026

Table The results of simultaneous inferential statistical testing (F Test / ANOVA) and coefficient of determination (R^2)

Regression Model	Predictor Variables	Regression Coefficient (b)	F valuecount	F valuecount	*R2* (%)	Significance (p-value)	Status & Conclusion
Model 1	**Cognitive Warfare (X1)**	0.3558	7,388	**4,518.22**	**97.40%**	0,000	**Positive & Significant**
(Y1 = Capability)	**Leadership (X2)**	0.5317	10,459			0,000	**Positive & Dominant**
Model 2	**Cognitive Warfare (X1)**	1.3815	12,597	**704.21**	**90.00%**	0,000	**Dominant Main Effect**
(Y2 = Stability)	**Leadership (X2)**	-0.6041	-4,788			0,000	**Corrective Adjustment Effect**
	Transformation (Y1)	0.0280	0.210			0.834	**Indirect Mediation**

Source: Data Processed by Researchers 2026

From tables above, the regression equation for each model can be analyzed, namely:

1) Regression Model Analysis 1: The Influence of Enabler Factors on Operational Capability Transformation (Y1)

a) Regression Equation Model 1: $\hat{Y}1=1.9634+0.3558X1+0.5317X2$

b) Partial Hypothesis Test Results (t-Test)

(1)Constant ($\alpha1=1.9634$): Shows that if the Cognitive Warfare and Strategic Leadership understanding scores are zero (constant), the basic score of Intelkam Operational Capability Transformation remains at a positive value of 1.9634.

(2)The Influence of Cognitive Warfare Understanding (X1→Y1): Obtaining the t valuecount=7,388>ttable=1.9700 with a significance level of p=0.000<0.05 (Coefficient b1=0.3558).

Meaning: Hypothesis 1 (H1) is accepted. Every 1 unit increase in personnel understanding of Cognitive Warfare is proven to significantly increase the acceleration of Operational Capability Transformation by 0.3558 units.

(3)The Influence of Intelkam Strategic Leadership (X2→Y1): Obtaining the t valuecount=10,459>ttable=1.9700 with a significance level of p=0.000<0.05 (Coefficient b2=0.5317).

This means that Hypothesis 2 (H2) is accepted. Strategic leadership is the main driver (the biggest driver) for internal institutional transformation. Every 1 unit increase in Strategic

Leadership quality will drive an increase in Capability Transformation by 0.5317 units.

4. Conclusion

This research confirms that the primary intelligence battleground has shifted from territorial boundaries to the realm of public awareness. Cognitive warfare no longer places weapons or physical threats as the primary instrument, but has instead expanded into the cognitive domain of narrative manipulation that targets people's emotions, perceptions, and mindsets, necessitating an adaptive and proactive intelligence approach. Therefore, the National Police's Intelligence and Security Agency (Baintelkam Polri) is required to fundamentally transform from merely a conventional security guard to a national cognitive defense fortress. Strategic leadership not only serves as a key driver of institutional modernization but also acts as an ethical steward. In the face of cognitive threats, leaders play a role in ensuring that every step taken to prevent and respond to digital information remains measured, transparent, and aligned with the law, democratic principles, and human rights, as well as proportional, so that it does not become a tool for restricting freedom of expression. This study concludes that there is a gap between the high level of strategic awareness at the leadership level and the effectiveness of control at the lower level. Although leadership commitment and internal institutional capabilities have been established at a very high level, implementation in the field still faces obstacles in the form of operational gaps. The high level of commitment at the top has not been fully realized in the field due to limited digital outreach tools and a persistent reliance on traditional intelligence work patterns, which often results in a delayed response at the grassroots level to anticipate the spread of disinformation. This indicates that the leadership's grand vision has not yet been optimally translated into stable cognitive resilience at the frontline community level.

5. References

Journals:

Asnawi, Anita (2022). *Kesiapan Indonesia Membangun Ekonomi Digital Di Era Revolusi Industri 4.0*. Syntax Literate; Jurnal Ilmiah Indonesia7, no. 1.

Bertalanffy, L. von. (1968). *General System Theory: Foundations, Development, Applications*. George Braziller.

Burda, R. (2024). *Cognitive Warfare: Problem for the Brain, Opportunity for the Machine*. Journal of Strategic Security, 17(1), 45–62

Clapper, T. C. (2021). *Getting better together: The two-team training approach in simulation-based education*. Journal of Continuing Education in Nursing, 52(9), 417–422.

Hung, T.-C., & Hung, T.-W. (2022). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. Journal of Global Security Studies, 7(4), ogac016. https://doi.org/10.1093/jogss/ogac016

Ienca, M. (2023). On artificial intelligence and manipulation. Topoi, 42, 833–842. https://doi.org/10.1007/s11245-023-09940-3

Ireland, R. D., & Hitt, M. A. (1999). *Achieving and Maintaining Strategic Competitiveness in the 21st Century: The Role of Strategic Leadership*. Academy of Management Executive, 13(1), 43–57.

Ireland, R. D., & Hitt, M. A. (2005). Achieving and maintaining strategic competitiveness in the 21st century: The role of strategic leadership. Academy of Management Executive, 19(4), 63–77. https://doi.org/10.5465/ame.2005.19417908

Jones, B. R., & Smith, K. L. (2022). *Algorithmic Intelligence and National Security: Rethinking Intelligence Gathering in the 2020s*. *Intelligence and National Security*, 37(4), 512–530.

Moore, M. H. (1995). *Creating Public Value: Strategic Management in Government*. Harvard University Press.

Peyton, K., Sierra-Arévalo, M., & Rand, D. G. (2019). A field experiment on community policing and police legitimacy. Proceedings of the National Academy of Sciences, 116(40), 19894–19898. https://doi.org/10.1073/pnas.1910157116

Prasetyo, H., & Wibowo, A. (2023). *Transformasi Fungsi Intelijen Keamanan Polri Menghadapi Polarisasi Sosial di Ruang Digital*. Jurnal Ilmu Kepolisian, 17(2), 89–104.

Rahmani, Azis (2018). *Network Centric Warfare Dan Perang Asimetris Di Afghanistan*. Jurnal Keamanan Nasional 4, no. 2

Santoso, B. (2021). *Perang Kognitif dan Tantangan Ketahanan Nasional Indonesia di Era Disrupsi Informasi*. Jurnal Ketahanan Nasional, 27(1), 15–33.

Sekaran, Uma, & Bougie, Roger. (2016). *Research Methods for Business: A Skill-Building Approach* (7th ed.). John Wiley & Sons.

Singh, A., Lim, W. M., Jha, S., Kumar, S., & Ciasullo, M. V. (2023). The state of the art of strategic leadership. Journal of Business Research, 158, 113676. https://doi.org/10.1016/j.jbusres.2023.113676

Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Taylor, M., & Clarke, D. (2021). *Hacking Minds, Not Systems: Defining the Operational Boundaries of Cognitive Warfare*. Strategic Studies Quarterly, 15(2), 112–135.

Tigre, F. B., Henriques, P. L., & Curado, C. (2025). The digital leadership emerging construct: A multi-method approach. Management Review Quarterly, 75, 789–836. https://doi.org/10.1007/s11301-023-00395-9

Wang, X. H., Liu, Y. Y., Zhang, C., & Wang, G. F. (2022). *Digital leadership and organizational resilience: A dynamic capability perspective*. Frontiers in Psychology, 13, 953445.

Books:

Arikunto, S. (2013). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Rineka Cipta.

Bryson, J. M. (2018). *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement* (5th ed.). John Wiley & Sons.

Claverie, B., & du Cluzel, F. (2019). *Cognitive Warfare: The Future of Operations*. NATO Defense College (NDC) Perspectives.

Claverie, B., Prébot, B., Buchler, N., & du Cluzel, F. (Eds.). (2024). Cognitive warfare: The future of cognitive dominance. Springer

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.

Dupuy, F. (2020). *The Context of Modern Conflict: From Information Warfare to Cognitive Warfare*. Paris: Institut de Recherche Stratégique de l'École Militaire (IRSEM).

Gujarati, D. N. (2003). *Basic Econometrics* (4th ed.). McGraw-Hill.

Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis* (7th ed.). Pearson New International.

Hitt, M. A., Ireland, R. D., & Hoskisson, R. E. (2019). *Strategic Management: Competitiveness and Globalization: Concepts and Cases*. Cengage Learning.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative Data Analysis: A Methods Sourcebook* (4th ed.). SAGE Publications.

North, R. (2021). *Hacking the Human Mind: Understanding the Threat of Cognitive Warfare in the Digital Age*. London: Oxford University Press.

Etc:

Du Cluzel, F. (2021). Cognitive warfare. NATO Allied Command Transformation, Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf

Ministry of Defence of the Republic of Indonesia. (2023). White Paper on Cyber Defence and National Cognitive Domain Resilience. Jakarta: Ministry of Defence of the Republic of Indonesia.

Headquarters of the Indonesian National Police. (2020). Regulation of the Chief of the Indonesian National Police Number 4 of 2020 concerning the Security of Intelligence Documents and Information Materials. Jakarta: Indonesian National Police Headquarters.

NATO Allied Command Transformation (ACT). (2020). Cognitive Warfare Concept Paper. Norfolk, VA: NATO.

Republic of Indonesia. (2002). Law Number 2 of 2002 concerning the Indonesian National Police.

Republic of Indonesia. (2011). Law Number 17 of 2011 concerning State Intelligence.

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.