TNI Influence Operation and Information Warfare Force; Noopolitik Perspective

Mahbi Maulaya[1]*, Fadhlil Wafi[2]
[1]Security Studies Program, Kansas State University
[2] Universiti Kebangsaan Malaysia (UKM)

mahbimaulaya@ksu.edu[1]*, wafiifadhlil@gmail.com[2]
*Corresponding Author

Article Info

Abstract

The news about the Indonesian National Army's, or Tentara Nasional Indonesia (TNI), budget for internet buzzers has led to public disapproval. This disagreement shows how the public is still unfamiliar with the idea that Influence Operations and Information Warfare (IOIW) is now a thing in national security and defense strategy. This article aims to make sense of why TNI should consider the IOIW capability. With the library research method, this article introduces the conceptual and theoretical argument of Noopolitik and IOIW to the Indonesian policymakers and the general public. Noopolitik is a concept explaining the existence of the noosphere, a world "thinking circuit" and "realm of the mind" that politicians today, in the era of advanced information and communication technology, also consider. Thus, Noopolitik allows us to rationalize that a country nowadays should consider not only the geosphere for its national interest but also the noosphere which one country may hijack and influence through information dissemination. Thus, the noosphere is now a new emergent battlefield, and IOIW refers to the combat that takes place on it, with the goal of gaining influence using information as a weapon. With that idea, this article argues that it is reasonable for TNI to procure the capability for IOIW. The IOIW ability will allow TNI to protect the Indonesian Noosphere from the attacks of its potential adversaries, as they might want to influence Indonesian public opinion and action in a hostile outcome for the nation's harmony and stability. The general public have to grasp the theoretical framework of Noopolitik, which elucidates the contemporary relevance of IOIW. It will lead them to have necessary understanding why should they provide support to TNI for the procurement of additional power for IOIW capabilities when required. This article may function as an initial evaluation for politicians and the public to recognize TNI's augmentation of the IOIW force.

INTRODUCTION

In January 2025, a screenshot revealed an indication that TNI is using internet buzzers. According to the leaked document, TNI allocated Rp100 billion for the project, saying that it is necessary for the army to apply the Information Response System and to reduce negative opinions circling the army. Furthermore, the document asserts that the project is essential for maintaining positive and conducive public opinion. The document explains that the project will create word-of-mouth phenomena as a way to deliver repeated information to a wider audience. The document explicitly mentions "buzzer" as another name for this method (Abdo, 2024; Musthafa, 2025; Saubani, 2025).

The issue became a hot topic among the public. They disagree that such a big amount of money from the state budget (APBN) is spent on, as they argue, manipulating information given to them. As one comment on the Republikaonline's Instagram post on the issue said, "(We are) tired of paying taxes, (but then) it is used to attack those who pay taxes (us)." Not long after the issue went viral, TNI clarified that the money is not to rent internet buzzers. However, TNI used the funds to establish an app that secures the circulation of information within its environment (Saubani, 2025).

Whether or not TNI's buzzer project is valid, the public's reaction to this matter signals the indication that they remain unfamiliar with what the intelligence, national security, and defense world calls Noopolitik and Influence Operation and Information Warfare (IOIW). Is it true that the TNI's internet buzzers, in which this article says it is an effort to procure IOWI force, only target tax-paying citizens if they exist? What is the importance of TNI procuring IOWI capabilities? The answer to this question is perhaps limited for the Indonesian public since IOIW is indeed a covert military strategy and both government policy consideration and the scholarly campaign on explaining IOIW and Noopolitik are also significantly limited.

Public's questioning of TNI's IOIW signals a disconnect between the IOIW and societal perceptions. This is not a shock. IOIW is very different from traditional warfare that uses swords and bullets. IOIW is soft because it does not use swords and bullets as weapons but rather invisible information. The purpose of IOIW is also not to destroy something that is physically real but to manipulate perceptions and influence human behavior. In addition to IOIW using deceptive narratives and tactics that blend with the normal flow of information, IOIW does have a mask that aims to manipulate public views without them realizing it. IOIW can even go beyond the expected results of the perpetrators because the targeted public are unaware of IOIW other's existence (Bingle, 2023). Information technology has also become an inseparable part of people's lives. Their habituation and comfort make them feel that information technology is not something that can threaten. This makes IOIW difficult to identify and track so that the public is surprised if it turns out that IOIW is something serious in today's military world.

Literature sufficiency becomes another issue why there is a gap between Indonesian society with IOIW. In Indonesia, the term "cybersecurity, social media, or information

warfare" may be familiar to researchers (Aferudin & Ramli, 2022; A. R. Arianto & Anggraini, 2019; Bagus & Fadli, 2021; Fransiska & Tobing, 2023; Indirwan & Aulianisa, 2020; Isjchwansyah, 2024; Iswardhana, 2021; Nastiti et al., 2018; Saleh & Winata, 2023; Sensuse et al., 2022; Septasari, 2023; Wijayanto et al., 2024).

Unfortunately, they have a heavy tendency toward technology-related or practical assessments and do not mention Noopolitik. This can leave the general audience, who seeks to understand why procuring sufficient technology and a practical strategy for IOIW matters, without a clear ideological answer. Technology is just one pole in the discussion of IOIW. Another pole is political and ideological, which is addressed by the term Noopolitik.

Noopolitik serves as the ideological foundation for the rationalization of IOWI. Improving technological capability for cybersecurity or any related information warfare capability requires a concrete understanding of why one should do it. Noopolitik understanding can play a role in it. Yet, in Indonesia, scholarly endeavors on Noopolitik are limited. It seems like the term remains alien in the Indonesian academic environment, especially in national security or defense studies. This article aims to rationalize the TNI's decision to establish an IOIW force, also generally known as internet buzzers, through an understanding of Noopolitik. Another objective of this article is to clarify the rationale behind TNI's need for the IOIW force. This article argues that the IOIW force will be necessary for TNI to protect Indonesia's Noosphere, the realm of hearts and minds, from the IOIW attack originated by its adversaries. This is essential for TNI to safeguard public legitimacy and stability. To come to this argument, this article makes itself stand by the explanation of Noopolitik, a theoretical framework devised by Arquilla & Ronfeldt (1999) as a reflection of the existence of the IOIW. The logic of Noopolitik helps us comprehend that modern military strategies now include the noosphere as well as the geosphere. A country should now understand the importance of maintaining its noosphere.

The outline for this article is as follows. First, it describes the methods that are used. Because this essay tries to introduce an idea and concept, library research is appropriate. It will go into the major papers that cover them. The discussion section comes next. Here we may discover what Noopolitik is, allowing us to rationalize IOIW. These two principles will serve as the foundation for establishing the aforementioned arguments. After that, the articles explained why the TNI IOIW Force is necessary. The examples from the UK, North Korea, China, and the United States are followed by a conclusion.

METHODS

This article uses library research to analyze works and research of others relevant to the presented argument. Library research is a methodology that utilizes library sources to obtain research data. Following the guidelines given by Library (2025) the research looks for sources relevant to the discussion by conducting keyword searches and subject searches for recent scholarly books and articles. In addition, this research employs citation searches within scholarly sources and published bibliographies, as well as

systematic browsing. The keyword uses are "information warfare," "influence operation," and "Noopolitik.".

The sources are then analyzed qualitatively to extract ideas or information that are relevant to support the main argument of this research. Articles regarding Noopolitik were read to understand how the concept emerged and how it is best understood. Then articles about IOIW were read to understand what IOIW is and how it was conducted by other countries. Ideas from both literatures are constructed to build the argument presented in this article.

CONCEPTUAL FRAMEWORK
Noopolitik

Rapid innovation and development of technology have allowed information and communication tools to expand in quality and quantity. Almost all individuals now have computers and smartphones. These privileges allow society to have access to information on a global scale, and thus they have global connectivity. Society's wide and open access to information makes their thoughts and behaviors can be easily shaped. Their mind and actions, which become the basis for human activity, are crucial for political, economic, and social-related life. With this, information the society consumed is now associated with power. Information, in other words, has the power to influence people. As digital communication develops, it becomes a reason for power holders like governments to benefit from their propaganda, disinformation, and political manipulation (Ivan et al., 2021).

Scholars have widely discussed and analyzed the power of information to influence people's hearts and minds, thus emphasizing the importance of information technology and systems. They see that sophisticated information technology and systems are determinant factors for a country's success in the information game. Then, John Arquilla and David Ronfeldt clarified that information strategy encompasses two poles, one of which is technological in nature. The other is political and ideological. Through their first Noopolitik article entitled "The Emergence of Noopolitik; Toward an American Information Strategy," Arquilla & Ronfeldt (1999) developed a concept that plays a crucial role in the understanding of the political and ideological pole of information as a tool for war and military operations. A 20-year-later article, "Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft," further develops this concept Arquilla & Ronfeldt (1999) refer to the concept as "Noopolitik."

The term Noopolitik comes from the idea that world politics is now not only about its land (geosphere) that makes politicians consider geopolitics, but now there is a noosphere to take into account. Noosphere, as they argued, is a world "thinking circuit" and "realm of the mind." The digital information revolution has shaped this collective form of intelligence Arquilla & Ronfeldt (1999) "Noo" in Greek means "the mind." Then the term "Noosphere" originated in 1922 when three European scholars, French theologian-paleontologist Pierre Teilhard de Chardin, French mathematician Édouard Le Roy, and visiting Russian geochemist Vladimir Vernadsky, were discussing in Paris about the answer to the question of whether humans, because of their advancement, will

develop a new layer of earth, which is the Noosphere. Teilhard interpreted the noosphere as a "realm of the mind," a "thinking circuit", while Julian Huxley described it as a "web of living thought" and "a common pool of thought" that would direct humans to an "inter-thinking humanity" (Ronfeldt & Arquilla, 2020).

Noosphere that the three European scientists discussed came into realization when countries, especially the powerful one, finds that they need to take seriously the ability to change people minds and actions through information. Arquilla and Ronfeldt's concept of Noopolitik allow us to understand this trend. They explained Noopolitik as "foreign-policy behavior for the information age that emphasizes the primacy of ideas, values, norms, laws, and ethics"—it would work through "soft power" rather than "hard power". Noopolitik, as a soft power, is a statecraft that can correspond to interfere on the ideas, values, norms, laws, and ethics in the realm of noosphere. It is different with Realpolitik in which dominantly associated with states and hard power. Noopolitik makes state needs to deal with non-state actors like media and press and to increase its soft power (Arquilla & Ronfeldt, 1999).

With Noopolitik seen as important for state soft power, Arquilla and Ronfeldt suggested the US develop its national military assets to address the Noosphere. In their 1999's article, both scholars have suggested several measures for it. One of them is to establish a "special media forces." This special force consists of soldiers who carry media and able to master information and communication technology instead of conventional weapons like firearms or shotguns. They further elaborated that these soldiers can be sent to conflict zones to discover or disseminate accurate information that can help settle the conflict and a national interest (Arquilla & Ronfeldt, 1999). Arquilla and Ronfeldt further developed their suggestion for the special media forces in a 2020 article. They have seen the US has been caught unawares and unprepared that adversaries have devised and deployed aggressive sharp power, the new term that they refer to as soft power. They also criticized Washington's leaders for neglecting the country's soft power, suggesting that they should reconsider their approach. They also suggest the same "special media forces" be considered by the US. But they added a new function for it as a tool for the "discovery and dissemination of accurate narratives and for purposes of rumor" control (Arquilla & Ronfeldt, 1999).

With Noopolitik now exist and need to be addressed, IOIW force is critical. Countries around the globe have been familiar with it. Research about how IOIW can change the public's mind has consequently been easy to find. The next section will explain how Noopolitik is now a factor in making IOIW widely executed by countries.

Influence Operation/Information Warfare; Research and Relevant Cases

IOIW are fundamentally about influence. It encompasses actions that are designed to collect tactical information about the adversary and to disseminate propaganda with the objective of altering the mindset, beliefs, attitudes, and behavior of the target (Arquilla & Ronfeldt, 1999; Bateman et al., 2021). IOIW has the potential to alter the human mind by delivering messages or constructing narratives that can cause confusion, distraction, division, or a loss of morale and rationality (Brangetto & Veenendaal, 2016).

IOIW have been numerous in quantity and increasing in quality. Numerous research studies have documented IOIW over time. The Partnership for Countering Influence Operations sponsored a study that examined eighty-two studies about IOIW published between 1995 and 2020. They looked at studies that talked about how influence operations affect certain groups of people, compared the results (behaviors or beliefs) of people who were targeted to those who were not, and other studies that assuredly met the basic requirements for statistical validity. The studies they choose addressed variable forms of influence operations; political disinformation, state propaganda, and health misinformation (Bateman et al., 2021). In sum, the study found that influence operations via pre-internet media such as newspapers, radio, and television have long-term effects and can be effective at influencing voters of political parties. The research also finds that campaigns using social media to try to sway people's opinions and actions only last a short time, but they are still able to change people's political views and actions, make them more racist or xenophobic, and make them doubtful and uncertain about medical information and vaccines (Bateman et al., 2021).

The ability of IOIW to shape and influence people's minds makes it no surprise. The advanced development of technology allows every individual to have information communication tools. They see and read repeated information almost every hour in a day. They even can make smartphones the first thing they see after waking up from sleep in the morning and the last thing they see in the evening before going to bed. This habit makes IOIW eventually able to control human minds. Once IOIW masters people's minds, it has the power to legitimize policies and cause public disorder (Reuter et al., 2024). This is the reason why Bouhnik & Admoni (2023) can say that modern IOIW is rooted in the technological development and social changes.

In regards to public legitimacy, IOIW can play a significant role in building or destroying public legitimation for a policy. During the Covid-19 pandemic, information about the illness and the vaccines has contributed to shaping people's awareness. Information can shape their willingness to stay at home or receive a vaccine shot. Their willingness, or more accurately, public legitimation, then influences the government's ability to effectively formulate policies regarding Covid-19 awareness measures and its vaccines (Di Domenico et al., 2022; Manfredi-Sánchez, 2023; Marco-Franco et al., 2021; Recuero & Bonow Soares, 2022; Sirola et al., 2021).

During an election, information also becomes a tool to make voters cancel their willingness to elect a candidate. In a day or two before the election time, one candidate's adversaries may disseminate information about one bad or negative track record. With the election time only a matter of hours away, the voters may consider not going on to choose the candidate as they get the information that changes their stance (Maulaya & Wafi, 2024).

There are numerous examples of how information can spark public riots or disorder. In the event of the Arab Spring, social media have triggered public protests and efforts to topple dictatorships in some Middle Eastern countries (Arafa & Amstrong, 2016; Baron, 2012; Browning, 2013; Jenaibi, 2014; Karolak, 2017; Salvatore, 2015; Tudoroiu, 2014).

In 2020, the death of George Floyd, which was shared and went viral on the internet, sparked a big wave of the "Black Lives Matter" campaign across the United States to urge the government to wipe out institutionalized racism in the country (Carney, 2016; Chang et al., 2022; Olson, 2021; Richardson, 2024; Upadhyay & Trifiro, 2021; Waterhouse, 2022).

Indeed, in today's world, every social and political unrest is accompanied with electronic accessories (Browning, 2013). Everyone has their smartphone as a weapon. They can record one problem happening in one particular area, upload it to the internet, and make it a problem for everyone in other areas.

The domestic instability caused by the influence of information makes a country subject to foreign entities IOIW. Modern history has shown how foreign countries try to influence the dissemination of information in other countries to make the public align with their interests. For example, researchers found that the Russian Internet Research Agency (IRA) executed an online campaign to affect the electoral behavior of select groups and influence the social conflicts happening in the United States during the 2016 presidential election (Badawy et al., 2019; Fisher, 2019; Inkster, 2016; Linvill et al., 2019; McCombie et al., 2019; Ziegler, 2017).

In addition, China also conducted information operations in Hong Kong in 2019. According to reports, the operation aims to influence political unrest in Hong Kong, undermining the legitimacy and power of the protest movement on the ground (Dotson et al., 2019; Yang et al., 2022).

China information operations also happened to Taiwan. Since 2010, in order to develop the notion that authoritarianism is superior to democracy in Taiwan, China has engaged in covert reliance on deceptive coercion and payment, as well as asymmetric exchanges of capital and information (Jaw-NIan, 2023).

Heart and mind are the most critical parts of being human. Nowadays, ideological, political, religious, and cultural wars that are brought on by influence operations are observable and even are coming with a new scale of threat to influence them (Ronfeldt & Arquilla, 2020). IOIW may cause the possibility of a global information dystopia, a condition where modern democratic self-government foundation, logic, truth, and reality are break into pieces (Lin, 2019). The heart and minds controller gains public legitimation or acceptance once they influence or control them. Consequently, the controller then has a determinant factor for continuing or ending a state of stability. How should Indonesia perceive and react to this issue?

RESULT AND DISCUSSION

The Indonesian public should understand that, in theory, IOIW is critical to a country's defense. But it seems like a challenge because the public has long perceived internet buzzers negatively. This section will go over why the Indonesians see internet buzzers negatively. Then it will explain why IOIW is still necessary for TNI. It claims that TNI should maintain public support and legitimacy in order for its operations to be effective. Following that, other countries' examples justified TNI's need for IOIW capabilities.

Buzzer and Its Negativity

A screenshot spread across social media in January 2025 indicated that TNI is utilizing internet buzzers. The leaked document indicates that TNI has allocated Rp100 billion for the project. It was said that the project is essential for sustaining favorable public opinion. The document outlines that the project aims to generate word-of-mouth phenomena to disseminate information repeatedly to a broader audience. The document clearly identifies "buzzer" as an alternative term for this method (Abdo, 2024; Musthafa, 2025; Saubani, 2025).

The issue emerged as a prominent subject of public discourse. The public contend that a substantial portion of the state budget (APBN) is allocated to what they perceive as the manipulation of information provided to them.

Indonesian public distrust of internet buzzers is not without basis. Indeed, most of the time, an internet buzzer's job is to lie and spread it. Since the last decade, buzzers were initially a product marketing strategy or a way of branding public figures. However, the task of buzzers has evolved. The task of buzzers today is no longer just to increase product sales figures or improve the image of certain figures but, ironically, is also to be able to lower the value of a product or bring down the image of the figure (Faulina et al., 2021). The lies circling Anies Baswedan's, ex-Governor of Jakarta, political journey become an example. Some research has revealed that buzzers have done significant work to influence the public to think that Baswedan is a radical Islamist.

Furthermore, buzzers help political players manage and ward off issues that frequently do prioritize personal interest rather than civil society interests (Faulina et al., 2021; Mustika, 2019). This tendency was visible by the emergence of "palace buzzer," which refers to specific accounts or individuals who are often regarded as parties who support every policy released by the Indonesian government (Faulina et al., 2021). For example, during Covid-19, the government was said by a researcher to utilize buzzers to disregard the call for implementing lockdown at the time the public said they needed it most (Syahputra et al., 2021). The buzzers' obsessiveness with the government suggests that they do not care about the public interest, as their existence implies that there is no opportunity for criticism at all. It is a reason to serve to explain B. Arianto (2020) findings that there is a widespread misperception about the term buzzer and its role, with many people referring to buzzers as paid social media accounts that only spread falsehoods and disinformation.

Public concerns about the TNI's desire to hire buzzers are understandable. There is a negative perception of buzzers that is naturally held by the public, considering that the role of buzzers in Indonesia tends to be negative. Therefore, there needs to be a movement to inform the public that there are interests that must be considered by the TNI in order to have their own buzzers, aka IOIW.

TNI IOIW Force

Scientists have explained that Noopolitik is now one of the indicators of state national interest across the globe (Ronfeldt & Arquilla, 2020). The Noosphere, which contains ideas and concepts as well as the heart and mind of human, is the target of IOIW. It is

worth considering that the Indonesian Noosphere can be attacked by other countries through IOIW. Find a way to respond to this accurately and effectively; thus, it is important for TNI.

Indeed, enhancing its information system is a viable approach for Indonesia to mitigate the risks posed by influence operation attacks. Indonesia should have an advanced communication and information security system that other countries cannot penetrate. However, this is not the sole solution, nor is it sufficient. Indonesia must also think about how it can keep its people's minds and hearts clean and safe from the indoctrination of foreign actors. Indonesia must be able to protect its Noosphere.

As explained earlier, two leading American researchers working at the RAND Corporation, a non-profit organization that always has the opportunity to provide defense advice and policies to the United States Government, have suggested what is called a special media force, which this article refers to it as IOIW force. This force is tasked with finding information and spreading it for national interests, such as rumor control or combatting fake news.

This force will be very important for the TNI to implement IOIW. There are three main conditions for a successful IOIW according to Maschmeyer et al. (2025) First, the ability to produce narratives that effectively convey persuasive messages. Second, the ability to disseminate this information sufficiently to the public so that it can influence national-level public decision-making. Third, the ability to embrace a large public. These three abilities might be achieved by the TNI through the IOIW Force.

IOIW is essential for TNI to attain two key objectives: public legitimacy and social stability. The public's recognition of TNI's legitimacy holds significant importance. First, TNI fundamentally exists to serve the people. The history of TNI is deeply connected to the people. TNI was born from the people and developed within the essence of the people (Pawana et al., 2021). TNI has adopted the slogan "With the People, TNI is Strong." Second, TNI serves Indonesia, a democracy. In a democracy, the public's approval matters significantly. If the people do not grant legitimacy for the TNI to take action or execute an operation, then the TNI will be unable to carry it out. For instance, if the community disallows TNI from conducting an operation to eliminate a separatist armed group in a particular area of Indonesia, the TNI will encounter an unwarranted obstacle by entering the field, even though they intend to safeguard the nation's sovereignty.

Consider a scenario that highlights the significance of this influence operation for Indonesia's interests. If a region in Indonesia seeks to declare independence, intervention from other nations may occur. Other nations that oppose Indonesia will perceive this as a chance to create divisions within the country. Consequently, the adversary will initiate an influence campaign aimed at persuading the Indonesian populace that the region seeking independence has been subjected to prolonged oppression by the central government. The adversary will attempt to sway the sentiments and perceptions of the Indonesian populace by asserting that the central government is the oppressive entity due to its neglect of the region. The Indonesian people may empathize with the separatists due to their feelings of compassion. The

opposing nation can now effectively persuade, overtly through IOIW strategies, the Indonesian public to support the separatist movement through its calculated influence initiatives. This will complicate the TNI's efforts to gain public support for entering the area and secure the rebels. In a situation where another nation or adversary seeks to undermine the TNI's authority in safeguarding Indonesia's unity, the IOIW will be crucial in supporting the TNI's efforts to uphold public legitimacy and align with the institution.

TNI, utilizing its IOIW force, can uphold public legitimacy against the threat of influence operations from other nations by engaging in IOIW of its own. Let's revisit the scenario mentioned earlier. The area seeking independence receives backing from foreign nations to initiate an uprising. The nation backing the separation engages in IOIW to alter the perceptions of the Indonesian populace. In addressing this, TNI's IOIW force should be capable of executing precise information discovery and dissemination, along with effective rumor control as proposed by Ronfeldt and Arquilla (Ronfeldt & Arquilla, 2020).

The proposed TNI IOIW strategy, information discovery and dissemination, aims to find facts in the field that show how the TNI's presence in the area has a big positive effect and is for a good reason. For example, the TNI can show how separatist troops destroy people's houses and bring a lot of suffering to the local population. Photos and texts illustrate that separatists only want progress for their group, not the region they want to exclude from Indonesia. In addition, if the enemy carries out an influence operation to slander the TNI and raise negative rumors, then presenting field facts and disseminating them will help the TNI to counter the rumors.

The preceding scenario demonstrates how critical it is for the TNI to have non-political capabilities and influence operations via the presence of the IOIW force. In the modern era, where information technology can be used to manipulate public perceptions and then influence their legitimacy over a country's armed forces, the TNI is now tasked with protecting Indonesia and its people both physically and non-physically. The threat of IOIW forces the TNI to safeguard not just Indonesia's geographical territory and the physical safety of its residents, but also the Noography, in other words, hearts and minds of its people. Threats from other countries today include not just actual troop attacks, bombs, missiles, tanks, and aircraft, but also information strikes that might damage Indonesia's noosphere. TNI must be able to make Indonesia's noosphere secure so that its people can remain safe from foreign influence. If the hearts and minds of Indonesians are clear from attacks, they can give TNI proper and suitable legitimacy according to their interest and need, which aligns with TNI's mission to protect national interests. This warning is more than just hyperbole; other countries have already planned for and taken action against this new threat.

Examples of IOIW Force

Countries around the world have their own IOIW forces. The United Kingdom 77th Brigade of the British Army is worthy of mention in this regard. The Brigade was established in January 2005 (Army, 2025) and is based in Hermitage, near Newbury, in

Berkshire MacAskill (2015) According to the official website of the British Army, the Brigade is a hybrid unit that consists of regulars and reservists equipped with special skills to combat any battles and wars in the information domain in support of the UK defense and interest in foreign territories (MacAskill, 2015).

This Brigade is a UK innovative formation to combine information operations and capacity building (Giegerich & Mölling, 2018). Some refer to them as "Facebook warriors," since anyone who would like to join this brigade must be accompanied with journalism skills, familiarity with social media (C. King & Miller, 2020), and sufficient capability in psychological operations and counter-adversarial information activity Paul Ottewell (2022) to engage in unconventional warfare in the information age (MacAskill, 2015).

The Brigade is not engaged with hard power-related activities or holding any conventional weapons, but it wages 'nonviolent warfare' to the narrative' on online platforms, such as Facebook, Twitter, and YouTube (Anglim, 2015). They are soldiers who have the task of editing videos, recording podcasts, and writing viral posts (Miller, 2018). This Soft Power Brigade has been seen conducting an operation during Covid-19 to help the UK interest in combating the pandemic (Verrall, 2022). An analyst also revealed that the Brigade secretly gives advice to the Israeli military on psychological warfare techniques (Mcevoy, 2024).

In North Korea, we may find Bureau 121 of the country's military serving the role of IOIW forces. North Korea established the Bureau in September 1998. It is a unit established to do research and development on cyberattack methods, software engineering, cryptography, and networking, as well as prepare cyber operations from abroad. In this unit, North Korea empowers well resourced, talented, highly trained, and well-staffed cyber team (Nah, 2023). In essence, the main objective of the bureau revolves around offensive and defensive cyber operations, including targeting critical information infrastructure (Raska, 2020). For a psychological warfare, the country established "Unit 204" in 1999 (Park, 2023).

In the case of China, the Chinese government has been alleged to have hired millions of people to insert huge numbers of pseudonymous and other deceptive writings in social media posts to support the government in political and policy debates (Han, 2015; G. King et al., 2016). Observers label these hired people as the "50 Cents Army." Rumors that these armies receive a payment of 50 renmimbi cents per post give rise to the name (Lau, 2016) Furthermore, research has indicated that China has also conducted a Noopolitik move through its state-controlled media for its South China Sea claim (Maulaya & Wafi, 2023).

The US has the US Army Psychological Operations Command (PSYOP), which was established in 1952, under the name Psychological Warfare Center, at Fort Bragg, North Carolina Howard (2024) according to the official website of the US Army, soldiers of PSYOP master excellent communication skills and unconventional tactics to help the U.S. Army achieve its objectives by using intelligence, interpersonal skills, cultural sensitivity, and foreign language proficiency. The aim is to influence the behavior and minds of foreign individuals, groups, and governments. In PSYOP, the soldiers influence

the target with information. Military Information Support Operations (MISO) missions include activities such as exchanging specific information with the foreign public to shape the emotions, motives, reasoning, and behavior of governments and citizens (Army, 2025).

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

The public anger and unacceptance of TNI's budget allocation for internet buzzers indicate how a strategy for countering IOIW remains foreign. The public tends to believe that internet buzzers will have the sole objective of attacking them. This article aims to explain that TNI requires an IOIW force not to attack them but rather to protect them.

Noosphere, the realm of heart and mind, is now a domain for battle among countries. Countries around the globe have been familiar with IOIW to shape the Noosphere based on their interest. The noosphere becomes vital as it determines how people behave and act. Consequently, countries' militaries now consider not only geopolitics but also Noopolitik. To adapt to the changing global environment, TNI must consider how it will respond to the Noopolitik dynamics and IOIW conducted by other countries. Indonesian society can be influenced by other countries through IOIW in accordance with their interests. What will be the outcome if Indonesian adversaries implement IOIW in order to influence Indonesian society's perception of TNI in a hostile manner? How should the TNI protect the nation from the Noopolitik attack launched by its adversaries? It is rational then to allow TNI to think about how it can expand its power for IOIW. Other countries, for example the UK, North Korea, the US, and China, have taken IOIW seriously as they have prepared their military to counter and even execute IOIW.

This article is rather a modest explanation for why TNI needs to establish an IOIW force. The ideologies, theories, and literature given in this article may act as an early departure for either the public to allow TNI to think and do more about the establishment of its IOIW force and TNI to devise strategy to gain public understanding of its plan for IOIW.

Public comprehension is critical because it allows TNI to be more flexible in conceptualizing their IOIW capability requirements. It is difficult for the TNI to carry out steps deemed necessary for the IOIW force while facing public criticism and opposition. A delayed progress in acquiring IOIW power will prevent the TNI from catching up to a rapidly evolving security environment in which security forces from other countries have achieved considerable improvements. Finally, if TNI lacks sufficient IOIW capabilities, it will confront an issue of public legitimacy induced by foreign interference, which may impede future operations for national interest.

Table 1. The logic for the importance of public understanding of Noopolitik and IOIW for TNI.

Public Understanding	→	TNI's IOIW Plan Flexibility	→	TNI's IOIW Force	→	Secure Noosphere	→	TNI's Ops & Public legitimacy

However, this article limits itself to the technicalities and moral use of IOIW force. Therefore, research needs to delve deeper into the specific details of the

institutionalization and administration of the IOIW force to effectively implement the recommendation. Future research should focus on moral considerations that could serve as the ethical guidelines for TNI's IOW force. This topic can also reduce public skepticism about TNI's use of IOIW. Also, how the TNI's IOIW force can work with the existing groups and institutions that deal with information or cyber-related issues is another intriguing question that should be studied further in the future.

REFERENCES

Abdo, N. (2024). Israel's Settler Colonialism and The Genocide in Gaza. *Studies in Political Economy / Recherches En Économie Politique*, *105*(1), 94–106. https://doi.org/10.1080/07078552.2024.2325298

Aferudin, F., & Ramli, K. (2022). The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. *Budapest International Research and Critics Institute (BIRCI-Journal)*, *July 2022*. https://doi.org/10.33258/birci.v5i3.6297

Anglim, S. (2015). *77 Brigade and Orde Wingate ' s Real Heirs*. RUSI. https://www.rusi.org/explore-our-research/publications/commentary/77-brigade-and-orde-wingates-real-heirs

Arafa, M., & Amstrong, C. (2016). " Facebook to Mobilize , Twitter to Coordinate Protests , and YouTube to Tell the World ": New Media , Cyberactivism , and the Arab Spring. *Journal of Global Initiatives*, *10*(1), 73–102.

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia's National Cyber Defense and Security To Face the Global Cyber Threats through Indonesia Security Incident Response Team on Internet Infrastructure (Id-Sirtii). *Jurnal Pertahanan & Bela Negara*, *9*(1), 17. https://doi.org/10.33172/jpbh.v9i1.515

Arianto, B. (2020). Dampak Pandemi COVID-19 terhadap Perekonomian Dunia. *Jurnal Ekonomi Perjuangan (JUMPER)*, *2*(2), 106–126.

Army, U. S. (2025). *Become a Master of Influence. Psychological Operations (PSYOP) Soldiers use expert communication skills and unconventional tactics to support U.S. Army objectives.* U.S Army. https://www.goarmy.com/careers-and-jobs/specialty-careers/special-ops/psychological-operations

Arquilla, J., & Ronfeldt, D. (1999). *The Emergence of Noopolitik Toward an American Information Strategy* (National Defense Research Institute (ed.)). RAND.

Badawy, A., Addawood, A., Lerman, K., & Ferrara, E. (2019). Characterizing the 2016 Russian IRA Influence Campaign. *Social Network Analysis and Mining*, *9*(1), 1–11. https://doi.org/10.1007/s13278-019-0578-6

Bagus, T. I. G., & Fadli, M. (2021). Indonesia Maritime Information Center Strategy in Dealing With Information Warefare in Indonesia's Sea Area. *Russian Journal of Agricultural and Socio-Economic Sciences*, *116*(8), 191–202. https://doi.org/10.18551/rjoas.2021-08.23

Baron, L. F. (2012). International Review of Information Ethics Ethics of Secrecy International Review of Information Ethics. *International Review of Information Ethics*, *17*(2010), 60–70.

Bateman, J., Hickok, E., Chourchesne, L., Thange, I., & Shapiro, J. N. (2021). *Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/06/measuring-the-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research?lang=en

Bingle, M. (2023). *Information Warfare & Ukraine : The Donetsk Cadavers*. The Henry M.Jakson School of International Studies. file:///C:/Users/ASUS/Downloads/Bingle

Bouhnik, D., & Admoni, A. (2023). "We Had No Homefront": Another Piece of The U.S Part in The Information Warfare Story. *Information Security Journal: A Global Perspective*, *32*(6), 469–480. https://doi.org/10.1080/19393555.2022.2111005

Brangetto, P., & Veenendaal, M. A. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. In NATO CCD COE Publications (Ed.), *International Conference on Cyber Conflict, CYCON* (Vols. 2016-Augus, pp. 113–126). NATO CCD COE. https://doi.org/10.1109/CYCON.2016.7529430

Browning, J. G. (2013). Democracy Unplugged: Social Media, Regime Change, and Governmental Response in the Arab Spring. *Michigan State International Law Review*, *21*(1), 63–86.

Carney, N. (2016). All Lives Matter, but so Does Race: Black Lives Matter and the Evolving Role of Social Media. *Humanity & Society*, *40*(2), 180–199. https://doi.org/10.1177/0160597616643868

Chang, H. C. H., Richardson, A., & Ferrara, E. (2022). #JusticeforGeorgeFloyd: How Instagram Facilitated the 2020 Black Lives Matter Protests. *PLoS ONE*, *17*(12 December), 1–19. https://doi.org/10.1371/journal.pone.0277864

Di Domenico, G., Nunan, D., & Pitardi, V. (2022). Marketplaces of Misinformation: A Study of How Vaccine Misinformation Is Legitimized on Social Media. *Journal of Public Policy and Marketing*, *41*(4), 319–335. https://doi.org/10.1177/07439156221103860

Dotson, J., Rich, T., Dahmer, A., Dirks, E., Salas, S., & Beauchamp-Mustafaga, N. (2019). Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations. *John Hopkins - School of Advanced International Studies*, *19*(16), 24–37.

Faulina, A., Chatra, E., & Sarmiati. (2021). Peran Buzzer dalam Proses Pembentukan Opini Publik di New Media. *Jurnal Pendidikan Tambusai*, *5*(2), 2806–2820.

Fisher, K. (2019). *Russian Interference in The 2016 United States Presidential Election*. The University of Texas at Austin.

Fransiska, F. B., & Tobing, F. B. L. (2023). Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era. In *Nucl. Phys.* (Vol. 13, Issue 1). Universitas Indonesia.

Giegerich, B., & Mölling, C. (2018). *The United Kingdom's Contribution to European Security and Defence*. The International Institute for Strategic Studies. https://dgap.org/system/files/article_pdfs/the_united_kingdoms_contribution_to_european_security_and_defence.pdf

Han, R. (2015). Manufacturing consent in cyberspace: China's "Fifty-Cent Army." *Journal of Current Chinese Affairs*, *44*(2), 105–134. https://doi.org/10.1177/186810261504400205

Howard, C. F. (2024). *The Upward Spiral Continues*. U.S Army Special Operations. https://www.army.mil/article/281509/the_upward_spiral_continues_u_s_army_special_operations_command_celebrates_35_years

Indirwan, & Aulianisa, S. S. (2020). Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia. *Lex Scientia Law Review*, *4*(1), 30–45. https://doi.org/10.15294/lesrev.v4i1.38197

Inkster, N. (2016). Information Warfare and The US Presidential Election. *Survival*, *58*(5), 23–32. https://doi.org/10.1080/00396338.2016.1231527

Isjchwansyah, Y. R. (2024). *Indonesia's New Cyber Force Needs to be Planned, Not Rushed*. The Strategist. https://www.aspistrategist.org.au/indonesias-new-cyber-force-

needs-to-be-planned-not-rushed/

Iswardhana, M. R. (2021). Cyber Diplomacy and Protection Measures Against Threats Of Information Communication Technology In Indonesia. *Journal of Islamic World and Politics*, *5*(2), 343–367. https://doi.org/10.18196/jiwp.v5i2.12242

Ivan, C., Chiru, I., & Arcos, R. (2021). A Whole of Society Intelligence Approach: Critical Reassessment of The Tools and Means Used to Counter Information Warfare in The Digital Age. *Intelligence and National Security*, *36*(4), 495–511. https://doi.org/10.1080/02684527.2021.1893072

Jaw-NIan, H. (2023). China's Propaganda and Disinformation Operations in Taiwan: A Sharp Power Perspective. *China: An International Journal*, *21*(2), 143–170. https://doi.org/10.1353/chn.2023.a898346

Jenaibi, B. N. A. Al. (2014). The Promise of Social Media in Arab Spring Nations. *Global Media Journal Arabian Edition Fall*, *2*(2), 63–86. https://doi.org/10.1386/ajms.3.2.241

Karolak, M. (2017). The Use of Social Media from Revolution to Democratic Consolidation: The Arab Spring and The Case of Tunisia. *Journal of Arab and Muslim Media Research*, *10*(2), 199–216. https://doi.org/10.1386/jammr.10.2.199_1

King, C., & Miller, P. D. (2020). *UK Information Operations in The Time of Coronavirus*. Deslassified UK. https://www.declassifieduk.org/uk-information-operations-in-the-time-of-coronavirus/

King, G., Pan, J., Roberts, M. E., Allen, D., Bol, P., Fair, B., Harrison, C., Johnston, I., Keller, F., Miller, B., Ravich, S., Stockmann, D., Walder, A., Wang, Y., Zheng, C., & Zhu, Y. (2016). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction,not Engaged. *American Political Science Review*, *111*(3), 484–501. https://doi.org/https://doi.org/10.1017/S0003055417000144

Lau, J. (2016). *Who Are the Chinese Trolls of the "50 Cent Army"?* VOA News. https://www.voanews.com/east-asia-pacific/who-are-chinese-trolls-50-cent-army

Library, P. U. (2025). Library Research Methods. *Princeton University Library*, *11*(1), 1–14.

Lin, H. (2019). The Existential Threat from Cyber-Enabled Information Warfare. *Bulletin of the Atomic Scientists*, *75*(4), 187–196. https://doi.org/10.1080/00963402.2019.1629574

Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). "The Russian are Hacking My Brain!" Investigating Russia's Internet Research Agency Twitter Tactics during The 2016 United States Presidential Campaign. *Computers in Human Behavior*, *99*(October), 292–300. https://doi.org/https://doi.org/10.1016/j.chb.2019.05.027

MacAskill, E. (2015, January). *British Army Creates Team of Facebook Warriors*. The Guardian. http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

Manfredi-Sánchez, J. L. (2023). Vaccine (public) Diplomacy: Legitimacy Narratives in The Pandemic Age. *Place Branding and Public Diplomacy*, *19*(3), 398–410. https://doi.org/10.1057/s41254-022-00258-2

Marco-Franco, J. E., Pita-Barros, P., Vivas-Orts, D., González-De-Julián, S., & Vivas-Consuelo, D. (2021). COVID-19, Fake News, and Vaccines: Should Regulation be Implemented? *International Journal of Environmental Research and Public Health*, *18*(2), 1–11. https://doi.org/10.3390/ijerph18020744

Maschmeyer, L., Abrahams, A., Pomerantsev, P., & Yermolenko, V. (2025). Donetsk Don't Tell–'Hybrid War' in Ukraine and The Limits of Social Media Influence Operations.

Journal of Information Technology and Politics, *22*(1), 49–64. https://doi.org/10.1080/19331681.2023.2211969

Maulaya, M., & Wafi, F. (2023). Global Times' Framing for China's Noopolitics in the South China Sea. *International Journal of Media and …*, *4*(2), 17–32.

Maulaya, M., & Wafi, F. (2024, February). *"Dirty Vote": A New, Cleaner Form of "Serangan Fajar."* The Jakarta Post. https://www.thejakartapost.com/opinion/2024/02/13/dirty-vote-a-new-cleaner-form-of-serangan-fajar.html

McCombie, S., Uhlmann, A. J., & Morrison, S. (2019). The US 2016 Presidential Election & Russia's Troll Farms. *Intelligence and National Security*, *35*(1), 95–114. https://doi.org/10.1080/02684527.2019.1673940

Mcevoy, J. (2024). *UK Psychological Warfare Unit Collaborated with Israeli Army*. Declassified UK. https://www.declassifieduk.org/uk-psychological-warfare-unit-collaborated-with-israeli-army/

Miller, C. (2018). *Inside the British Army's secret information warfare machine*. Wired. https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military

Musthafa, S. A. N. (2025, January). Viral TNI AL Anggarkan Rp100 Miliar untuk Rekrut Buzzer, Instansi Beri Klarifikasi. *Pikiran Rakyat*, 2024–2026.

Mustika, R. (2019). Pergeseran Peran Buzzer Ke Dunia Politik Di Media Sosial. *Diakom : Jurnal Media Dan Komunikasi*, *2*(2), 144–151. https://doi.org/10.17933/diakom.v2i2.60

Nah, L. T. (2023). North Korean Hackers. *North Korean Review*, *19*(1), 91–98.

Nastiti, F. E., Prastyanti, R. A., Taruno, R. B., & Hariyadi, D. (2018). Social Media Warfare in Indonesia Political Campaign: A Survey. In IEEE (Ed.), *Proceedings - 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2018* (pp. 49–53). IEEE. https://doi.org/10.1109/ICITISEE.2018.8720959

Olson, R. E. (2021). *Roles of Social Media in the Black Lives Matter Movement During COVID-19*. Grand Valley State University.

Park, B. (2023). *A Way forward to Counter North Korea ' s Evolving Cyber Threats*.

Paul Ottewell. (2022). The Disinformation Age: Toward a Net Assessment of the United Kingdom's Cognitive Domain. *Expeditions with MCUP*, *29*(3), 152–153. https://doi.org/10.1017/S0030605300021062

Pawana, J., Pambudi, K. S., & Muhaemin. (2021). Mengembalikan Kemanunggalan TNI dan Rakyat: Analisis Kritis terhadap Tradisi Pembinaan Calon Perwira TNI. *Jurnal Lembaga Ketahanan Nasional Republik Indonesia*, *8*(2), 10. https://doi.org/https://doi.org/10.55960/jlri.v8i2.305

Raska, M. (2020). North Korea's Evolving Cyber Strategies: Continuity and Change. *SIRIUS – Zeitschrift Für Strategische Analysen*, *4*(2), 1–13. https://doi.org/doi:10.1515/sirius-2020-3030

Recuero, R., & Bonow Soares, F. (2022). #VACHINA: How Politicians Help to Spread Disinformation about COVID-19 Vaccines. *Journal of Digital Social Research*, *4*(1), 73–97. https://doi.org/10.33621/jdsr.v4i1.112

Reuter, C., Lee Hughes, A., & Buntain, C. (2024). Combating Information Warfare: State and Trends in User-Centred Countermeasures Against Fake News and Misinformation. *Behaviour and Information Technology*, *July*, 1–14. https://doi.org/10.1080/0144929X.2024.2442486

Richardson, A. V. (2024). Social Media, Citizen Reporting, and Journalism 1 Police Killing

of George Floyd, 2020. In J. Vernon (Ed.), *Milestones in Digital Journalism* (1st ed., pp. 1–223). Routledge Taylor & Francis Group. https://doi.org/10.4324/9781003316152

Ronfeldt, D., & Arquilla, J. (2020). Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft. In Library of Congress Cataloging-in-Publication Data (Ed.), *RAND Corporation*. RAND Corporation. https://doi.org/10.7249/pea237-1

Saleh, A. I., & Winata, M. D. (2023). Indonesia's Cyber Security Strategy: Problems and Challenges. *Proceedings of the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023)*, *2023*(Ijcah 2023), 1675–1696. https://doi.org/10.2991/978-2-38476-152-4_169

Salvatore. (2015). A Public Sphere Revolution? Social Media Versus Authoritarian Regimes. In L. Sadiki (Ed.), *Routledge Handbook of the Arab Spring* (1st ed., p. 11). Routledge Taylor & Francis Group.

Saubani, A. (2025, January). *Beredar Tangkapan Layar Laman LKPP TNI AL Sewa Buzzer Rp100 M, Ini Klarifikasi Kadispenal*. Republika.Co.Id. https://news.republika.co.id/berita/sq16mo409/beredar-tangkapan-layar-laman-lkpp-tni-al-sewa-buzzer-rp100-m-ini-klarifikasi-kadispenal

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. *Information (Switzerland)*, *13*(12), 1–10. https://doi.org/10.3390/info13120580

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, *5*(2), 227–233. https://doi.org/10.30604/jti.v5i2.231

Sirola, A., Kaakinen, M., Savolainen, I., Paek, H.-J., Zych, I., & Oksanen, A. (2021). Online Identities and Social Influence in Social Media Gambling Exposure: A Four-Country Study on Young People. *Telematics and Informatics*, *60*(2), 101582. https://doi.org/https://doi.org/10.1016/j.tele.2021.101582

Syahputra, I., Ritonga, R., Purwani, D. A., Masduki, Rahmaniah, S. E., & Wahid, U. (2021). Pandemic Politics and Communication Crisis: How Social Media Buzzers Impaired the Lockdown Aspiration in Indonesia. *SEARCH Journal of Media and Communication Research*, *13*(1), 31–46.

Tudoroiu, T. (2014). Social Media and Revolutionary Waves: The Case of the Arab Spring. *New Political Science*, *36*(3), 346–365. https://doi.org/10.1080/07393148.2014.913841

Upadhyay, A., & Trifiro, B. M. (2021). Legislative Agenda-Setting Power of Social Media #BlackLivesMatter and the George Floyd Justice in Policing Act of 2020. *The Agenda Setting Journal*, *5*(2), 292–313. https://doi.org/https://doi.org/10.1075/asj.21006.upa

Verrall, N. (2022). COVID-19 Disinformation, Misinformation and Malinformation during The Pandemic Infodemic: A View from the United Kingdom. In R. Gill & R. Goolsby (Eds.), *COVID Disinformation: A Multi-National, Whole of Society Perspective* (pp. 81–112). Springer International Publishing. https://doi.org/10.1007/978-3-030-94825-2_4

Waterhouse, J. C. (2022). *Critical Political Implications of Twitter Discourse in the Wake of George Floyd*. The University of Tennessee.

Wijayanto, Berenschot, W., Sastramidjaja, Y., & Ruijgrok, K. (2024). The Infrastructure of Domestic Influence Operations: Cyber Troops and Public Opinion Manipulation

Through Social Media in Indonesia. *International Journal of Press/Politics*, *11*, 1–19. https://doi.org/10.1177/19401612241297832

Yang, L., Driscol, J., Sarigai, S., Wu, Q., Chen, H., & Lippitt, C. D. (2022). Google Earth Engine and Artificial Intelligence (AI): A Comprehensive Review. In *Remote Sensing* (Vol. 14, Issue 14). https://doi.org/10.3390/rs14143253

Ziegler, C. E. (2017). International Dimensions of Electoral Processes: Russia, The USA, and The 2016 Elections. *International Politics*, *55*(5), 557–574. https://doi.org/10.1057/s41311-017-0113-1