Konfrontasi Journal: Culture, Economy, and Social Changes
pISSN: 1410-881X (Print)
eISSN: 2716-3095 (Online)

Papua Separatis Terrorist Groups Detection Through Osint and Counter Intelligence Effort (Osint Detection Study On The Baintelkam Polri Separatist Management Unit)

Maekel Eugaliel Pindonta Sembiring[1], Arthur Josias Simon[2]
[1,2]*Sekolah Kajian Stratejik Dan Global, Program Studi Kajian Ketahanan Nasional, Universitas Indonesia*
maekeleugalielp@gmail.com, simonrbi@yahoo.com

Abstract

The Separatist Terrorist Group Movement (KST) is a group that demands independence or secession from Indonesia. Public demand for the police as a public institution that maintains the national security of the Republic of Indonesia is a big responsibility that must be implemented. The Separatist Terrorism Group (KST) movement and researchers will also analyze the role of the National Police's Baintelkam Separatist Countermeasures Unit in collecting OSINT-based information which is then processed into intelligence information, especially in terms of identifying threats that could threaten state sovereignty. The type of research used is qualitative research, the data collection strategy chosen is a qualitative data collection strategy. The results show that the large-scale use of OSINT has created new contexts and perspectives that help intelligence and security services to better understand the complexities of certain security developments in local or national contexts. On the movement of KST, among others. The intelligence community analyzes and collects data from all available open sources to try to find interesting data in the large amount of free information available.

Keywords
detection; terrorists; intelligence; countermeasures

I. Introduction

The Separatist Terrorist Group Movement (KST) is a group that demands independence or secession from Indonesia. The purpose of establishing this organization is to end Indonesian rule in Papua and make Papua an independent country (Tebay, 2005). Currently, the Papuan Separatist Terrorist Group (KST) is taking advantage of technological and communication developments to disseminate its actions online and gain support from the national and international community. Public demand for the police as a public institution that maintains the national security of the Republic of Indonesia is a big responsibility that must be implemented. The Security Intelligence Agency (Baintelkam Polri) is one of the elements implementing the main mission of the National Police in the field of security intelligence which is responsible for carrying out early detection of various threats, in this case KST.

Based on the Kabaintelkam Regulation Number 2 of 2020 concerning the task of personnel, it is stated that the National Police's Baintelkam Separatist Countermeasures Unit is tasked with carrying out police investigation, raising and counterintelligence activities in order to prevent and anticipate threats of espionage, sabotage, terror threats and separatist groups, threats of information system crimes. and communication as well as the threat of propaganda or psychological warfare that disturbs domestic security. One of

the functions of strategic intelligence is to detect, find problems and provide analysis and advice on various threats, risks and vulnerabilities (Prunckun, 2010).

When the ability to manage this threat is weak, new problems will arise for the stability of all lines and threaten Indonesia's interests. This perspective illustrates how important the role of open-source intelligence (OSINT) in the intelligence data collection process is so that it is liken-ed to the foundation of a building. Based on this, the researcher is interested in taking research related to "Threat Detection of Papuan Separatist Terrorist Groups (KST) through Open Source Intelligence (OSINT) in the Context of Counter Intelligence (Capabilities Study of the National Police Baintelkam Separatist Countermeasures Unit)".

Some of the problem formulations in this study are as follows: 1) What is the role of open-source intelligence (OSINT) in detecting the movement of the Separatist Terrorist Group (KST)?. 2). What are the efforts of the National Police's Baintelkam Separatist Countermeasures Unit in using OSINT to conduct counterintelligence against the KST movement.

The objectives of this research are: 1) Analyzing the role of open-source intelligence (OSINT) in detecting the movement of the KST Terrorist Separatist Group with the aim of optimizing the prevention role of the group. 2) Analyzing the efforts of the Baintelkam Separatist Countermeasures Unit in utilizing OSINT to conduct counterintelligence against the KST movement with the aim of increasing the effectiveness of organizational performance.

II. Review of Literature

2.1 National Resilience Theory

The State Intelligence Agency is clearly stated in Law Number 17 of 2011 concerning the State Intelligence Agency which is the front guard in the national security system, prevention, deterrence, as well as national interests and national security, overcoming security threats will take over. Copeland (2010) found that the essence of intelligence failure stems from several main factors. Copeland completes his explanation regarding intelligence failures on a number of key events in the decades prior to 9/11.

2.2 Indonesian National Security

National security can be defined as the ability of a nation to protect its internal values from external threats. The key to addressing Indonesia's many challenges with the hope of success is a safe and stable environment in which to put social, economic and political reforms into practice. Security issues have always been the focus of the central government. In the Suharto era, domestic stability was a top priority. The government during the New Order used a simple formula: the government sought to provide economic development and gradually increase prosperity for all. In return he imposed tight political controls and tolerated little criticism or political opposition.

2.3 Intelligence Analysis

According to Richard Helms, conducting analysis is at the heart of intelligence work. This is where all intelligence capabilities are combined to produce accurate information. The essence of intelligence is to reduce ambiguity for decision makers by providing understanding. The trick is to use a comprehensive intelligence analysis methodology,

which combines the collaborative use of structured analytical techniques, creativity, critical thinking, and sense-making, to leverage intuition and reduce bias. (Borg, 2017).

2.4 Open-Source Intelligence (OSINT)

Mark Lowenthal (2005) defines OSINT as all information that can be obtained from free or open sources. The open sources also vary, can be from various media, both conventional and online, government reports, research, satellite and the internet. Although it can be accessed publicly, of course the sources used do not violate copyrights and so on. Meanwhile, the investigation process using OSINT is not just a simple method, but a series of methods that involve creative ways and also require critical thinking. OSINT has a role that cannot be underestimated when compared to other types of information sources.

2.5 Threat Analysis Theory, Vulnerability Analysis, Risk Analysis

Threat analysis is the process used to determine which system components need to be protected and the types of security risks (threats) that should be protected. Vulnerability analysis is a review that focuses on security-relevant issues that have a moderate or severe impact on product or system security. Risk analysis is the process of identifying and analyzing potential issues that could negatively impact a key business initiative or project.

2.6 Organization Theory

In the book Erni Rernawan (2011: 15), the definition of organization put forward by Mathis and Jackson is quoted as: "The organization is a social unit of a group of people who interact with each other according to a certain pattern so that each member of the organization has their respective functions and duties, as an organization. a unit that has a specific purpose and has clear boundaries, so that it can be separated. Organizational theory is concerned with the relationship between an organization and its environment, the effects of these relationships on organizational functioning, and how organizations affect the distribution of privileges in society.

III. Research Methods

This study uses a qualitative approach. According to Moleong (2006, p.6), qualitative research aims to understand comprehensively and clearly the phenomena experienced by research subjects, such as behavior, perception, motivation, and behavior, in speech and speech. Using natural contexts and various scientific methods in certain ways.

The data collection system is based on the type of research conducted. Depending on the research plan and design of the researcher, there are several ways to collect data. The most commonly used methods are: published literature sources, surveys (email and letters), interviews (telephone, face-to-face or focus groups), observations, documents and notes, and experiments.

Counter Intelligence Theory

Counter Intelligence is part of action detection, which is "a capability inherent in institutions or personnel in terms of recognizing/knowing, finding, evaluating and presenting Intelligence products that contain an analysis and target of action which is the basis for policy making from security intelligence leaders. Holding intelligence activities/operations against targets that have implications for high-quality security disturbances until contingency situations arise" (Triatmo Hamardiyono, 2016: 16).

IV. Results and Discussion

4.1 The Role of Open Source Intelligence (OSINT) in Detecting the Movement of Separatist Terrorist Groups (KST)

Das (2008), made five main instruments with the help of the mind in obtaining information, namely (1) the human mind (HUMINT), collecting information through human contact, often in the form of information about the name, location, time, target movement and target intent; (2) Signal Intelligence (SIGINT) is a collection of information from a single point of contact. Electromagnetic radiation (separation), in general, from electronic devices; (3) Intelligence Illustration (IMINT) is a collection of information from sources. Space target image. Open Source Intelligence (OSINT) means the open collection of data-based information through various channels such as radio, television, newspapers, Internet, business data, videos, photos, and various social networks. OSINT is based on mobile phone or patient travel data. This method at least from the security intelligence agency (Kahana, 2020). In this study, the focus is on the role of OSINT in dealing with Separatist groups. Here are some understandings of OSINT, namely:

Open-source intelligence comes from data and information available to the general public. This is not limited to what can be found using Google, although the so-called "surface web" is an important component. 1) As valuable as open-source intelligence is, information overload is a real problem. Most of the tools and techniques used to conduct open-source intelligence initiatives are designed to help security professionals (or threat actors) focus their efforts on specific areas of interest. 2) There is a dark side to open-source intelligence: anything a security professional can find (and use) a threat actor can also find. 3) Having a clear strategy and framework for open-source intelligence gathering is essential — simply looking for anything that can be interesting or useful is bound to lead to burnout.

The advantages of OSINT are emphasized by security consultants, scientists, media and the intelligence community that it is cheaper and more widely available than traditional public information obtained through clandestine services. In addition, it also provides additional information that other intelligence sources sometimes cannot (eg human intelligence). In addition, as a result of the widespread availability of (local) news coverage across the internet, the use of online open sources allows security and intelligence agencies to be more up-to-date (Pouchard, 2012). Simultaneously, open source online may in times of crisis e.g. war be a more reliable and secure way to obtain intelligence than with polarized human intelligence. The large-scale use of OSINT has created new contexts and perspectives that help intelligence and security services to better understand the complexities of particular security developments in local or national contexts. This allows intelligence and security agencies to verify (secret) information with multiple sources and open media data. Finally, it has been argued that because compared to other sources, online information is more widely available and less confidential, the use of OSINT for intelligence purposes has lowered the threshold for information sharing between intelligence and security services.

OSINT is open source information is information that is publicly available. In other words; what is not secret and out there in the public domain (digital). This is information that can be obtained legally by anyone through a request, purchase, or observation in its use which is used as a tool for dealing with separatist groups. The KST movement plays a role in information security. The purpose of safety has received little attention in the literature, besides that OSINT has a role in detecting security threats. locally and internationally, Open Source Intelligence (OSINT) provides an open platform to search for

information about people or entities of interest. These open sources include social networking sites, forums, blogs, videos, and news sites. With the evolution of the internet, a wide variety of information can be obtained at the click of a mouse. In addition to this accumulation of valuable data, the internet also contains a large amount of personal information, often posted online by people themselves via social networking sites, blogs, or apps. The Role of Open Source Intelligence (OSINT) in Detecting the Movement of Separatist Terrorist Groups (KST), namely:

1. Ethical Hacking and Penetration Testing. Security professionals use open source intelligence to identify potential vulnerabilities in friendly networks so they can be fixed before being exploited by threat actors. Weaknesses that are often found include: Accidental leakage of sensitive information, such as through social media, Open unsecured internet-connected ports or devices, Unpatched software, such as websites running older versions of common CMS products and Leaked or exposed assets, such as ownership codes on pastebins.
2. Identify External Threats. As we have discussed many times in the past, the internet is an excellent source of insight into the most pressing threats to organizations. From identifying which new vulnerabilities are actively exploited to intercepting threat actor "chats" about upcoming attacks, open source intelligence enables security professionals to prioritize their time and resources to address today's most significant threats. In most cases, this type of work requires the analyst to identify and connect multiple data points to validate threats before action is taken. For example, while one threatening tweet may not be cause for concern, the same tweet will be viewed differently if it is associated with a threat group known to be active in a particular industry. One of the most important things to understand about open source intelligence is that it is often used in combination with other subtypes of intelligence. Intelligence from closed sources such as internal telemetry, closed dark web communities, and external intelligence sharing communities is regularly used to filter and verify open-source intelligence. There are a variety of tools available to help analysts perform this function, which we'll look at later.
3. Uncover the dark side strategy in terrorism crimes through OSINT. This process is the main reason why so many small and medium-sized businesses are hacked every year. This is not because threat groups are particularly interested in them, but rather because vulnerabilities in their network architecture or websites are discovered using simple open-source intelligence techniques. In short, they are targets of the new strategy to use OSINT is also designed to play a role in anticipating national security threats such as international terrorism. While it is unlikely that a terrorist will post the location of his chosen target online, these measures help in monitoring violent extremist views. In 2012 this was confirmed by the Dutch Public Intelligence and Security Service (AIVD) Report 'Jihadism on the Web', in which the internet was labeled as 'the most important medium for the spread of this (jihadist) ideology.4 Returning to the core duty of the state to provide safety and security for citizens, we argue that gathering Open-Source Information is a legitimate tool for security governance (Hayes, 2010). However, the increasing legitimacy of the use of OSINT cannot be derived solely from pursuing security or safety concerns. The (side) effects on human rights must also be considered.

4.2 The efforts of the National Police's Baintelkam Separatist Countermeasures Unit in using OSINT to conduct counterintelligence against the KST movement

OSINT takes up more space in the intelligence community. Its operational specificity is in line with the multimedia world which now has a crucial weight in people's lives. The

speed with which news spreads, the ease with which information can be obtained, and the public's anxiety about getting more and more timely information now make Osint a very attractive intelligence specialty. The following are the efforts made by the National Police's Baintelkam Separatist Countermeasures Unit in utilizing OSINT to conduct counterintelligence against the KST movement, including:

1. The intelligence community analyzes and collects data from all available open sources to try to find interesting data in the large amount of free information available. During collection and analysis, everything is based on operational protocols that allow standardization of the final product, which simplifies operations but at the same time makes it rigid due to incomprehensibility of problem variables at birth or earlier. Real manifestation of the problem itself. Basically, data can be collected, which also allows us to understand that something is going on, but does not give the exact direction of public opinion on a particular topic. Terrorism falls into this particular category.
2. Conducting evaluations and assessments in counter-terrorism activities based solely on collecting information from open sources with the currently used model does not guarantee an accurate analysis of the psychological, logistical, and opinion support needed for terrorism. More or less broad consensus among population classes, and it is this consensus that defines and determines the strength and weight of social cohesion.
3. Make an assessment of the terrorist phenomenon under consideration and understand the types of terrorism that fall into the category being observed, because this is a very complex world. Terrorism is divided into categories and subcategories: international, internal, state, revolutionary, separatist, war, aggressor.
4. Understanding turbulence at the embryonic level and taking the information-gathering approach in the field of OSINT that should be substantially modified by trying to find a fully national path that takes into account the studies previously carried out by indigenous scholars and not to take for granted "wasting gold" only foreign manuals that are operationally based on structures that may have much higher budget availability. Therefore, analysis must be understood jointly between gathering information from open sources and controlling the orientation of public opinion, because only the two things combined offer a vision that corresponds to reality.

Open-source security (OSINT) has increased the range of security tools available to security and intelligence officials or police officers. However, the side effects of this new method of intelligence gathering must be balanced with adequate forms of accountability both in theory and practice. To illustrate, in most Western societies there are strict laws for wiretapping phones — or the internet, but for social networking sites or apps these are less clear. In addition, many security officials may not see the need for greater accountability for OSINT. They may argue, for example, that social networking sites are part of the public domain and therefore anyone can access them. OSINT can indirectly or directly affect a person's personal life or future opportunities. As noted earlier, the use of OSINT for intelligence purposes has real-life consequences. From a human rights perspective, these side effects must be balanced (Rotenberg, 2001).

As a concept, accountability has a normative aspect related to the notion of justice, responsibility, integrity, justice and democracy (Rotenberg, 2001). This form of accountability is characterized by its focus on the rule of law and good governance, as well as the involvement of civil society or ordinary people.49 This could mean that heads of security and intelligence services, or those who are politically responsible, do not just publicly announce the purpose of the collection, processing, mining, or sharing OSINT, but also limits its use to predefined threats such as national security (e.g. for cyber espionage, international terrorism). Furthermore, international and/or national lawmakers must

determine what the boundaries are (rules of law) and how data subjects can seek re-address (internal or external accountability mechanisms). Finally, software designs that enable OSINT and simultaneously emphasize accountability (data protection by design) should be modified accordingly. These include privacy-enhancing technologies or transparency-enhancing technologies (Hildebrandt, 2011). These steps can be considered as a form of good governance in terms of balancing the use of security forces from OSINT.

In addition to the need to protect national security interests, which can undermine transparency efforts, there is another accountability dilemma associated with OSINT. Ensuring accountability is more complex if the information is not collected by the security agencies themselves, but by other public or private entities. It is not uncommon for intelligence and security agencies to share information at an international level (and since 9/11 it has become more common for law enforcement agencies to do so as well. This is a recent development as 'traditionally there have been differences between gathering intelligence for national security purposes and gathering evidence for criminal investigations, as the two serve different purposes (Van Ginkel, 2011).

V. Conclusion

Based on the discussion that has been conveyed regarding the use of open source intelligence (OSINT) in detecting the movement of the Separatism Terrorism Group (KST) by the National Police's Baintelkam Separatist Countermeasures Unit, the following conclusions can be drawn, including:

1. The large-scale use of OSINT has created new contexts and perspectives that help intelligence and security services to better understand the complexities of particular security developments in local or national contexts. Broadly speaking, OSINT's role in information security for safety purposes has received little attention in the literature, besides that OSINT plays a role in detecting local and international security threats, Open Source Intelligence (OSINT) provides an open platform for finding information about people or entities of interest. These open sources include social networking sites, forums, blogs, videos, and news sites.
2. Efforts made by the National Police Baintelkam Separatist Countermeasures Unit in utilizing OSINT to conduct counterintelligence against the KST movement, including the intelligence community analyzing and collecting data from all available open sources to try to find interesting data in the large amount of free information available, Conduct evaluations and assessments in counter-terrorism activities are only based on collecting information from open sources with current models, Making an assessment of the terrorist phenomena being considered and understanding the types of terrorism that fall into the categories being observed, and Understanding turmoil at the embryonic level and taking an approach to gathering information in that OSINT field should be substantially modified by trying to find a way.

References

Borg, L. C. 2017. '*Improving Intelligence Analysis: Harnessing Intuition and Reducing Biases by Means of Structured Methodology'*, *International Journal of Intelligence, Security, and Public Affairs*, 19(1), pp. 2–22

Djopari, John RG. 1993. Pemberontakan Organisasi Papua Merdeka. Jakarta: PT. Grasindo.

Lowenthal, Mark.,2009, Intelligence: from Secrets to Policy, Virginia: CQ Press.

L. Pouchard, J. Dobson and J. Trien, ‘A Framework for the Systematic Collection of Open Source Intelligence’, 2009, p.1. Retrieved 29 July 2012.

McDowell, D. (2009) *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users, Scarecrow professional intelligence education series*.

M. Hildebrandt, B. Koops and K. De Vries, ‘Where Idem-Identity meets Ipse-Identity. Conceptual Explorations’, in Future of Identity in the Information Society, 2008. Retrieved 26 July 2012.

Moleong, J. Lexy (2004). *Metodologi Penelitian Kualitatif*, Bandung: PT. Remaja Rosdakarya.

Prunckun, H., 2010. Handbook of Scientific Methods of Inquiry for Intelligence Analysis. United Kingdom: The Scarecrow Press Inc.

Rernawan, Erni. 2011. Organization culture, budaya organisasi dalam perspektif ekonomi dan bisnis. Bandung: Penerbit Alfabeta.

Widjojo MS. 2014. *Melanesia in Review: Issues and Events, 2013*: l'apua The Contemporary Pacific, 26(2):506-516.

Weston dan Copeland. 2010. Manajemen Keuangan Jilid 2. Jakarta : Binarupa Aksara Publisher.

Peraturan Kabaintelkam Nomor 2 Tahun 2020 Tentang Pentelaan Tugas Personel,