Strategic Review of the Effectiveness of Open-Source Intelligence at the National Maritime Information Center

Okol Sri Suharyo[1], Avando Bastari[2], Ayip Rivai Prabowo[3]

[1,2,3]Indonesia Naval Technology College, STTAL Surabaya Indonesia

ABSTRACT: This research provides a qualitative analysis of having Open-Source Intelligence (OSINT) at the National Maritime Information Center (NMIC). Indonesia's geographic condition demands strong marine defense and has enormous challenges in the maritime sector, so it is necessary to integrate maritime information data systems through the National Maritime Information Center. Technological advances provide opportunities and threats related to the potential to obtain information quickly. New technologies help localize, process, and disseminate large amounts of data and prepare it for analysis coming from Open-Source Intelligence. NMIC is required to be able to meet the needs of its users in the form of short and fast intelligence reports by utilizing information from OSINT. This is what underlies researchers to conduct research with problem formulations that have the effectiveness of OSINT in the NMIC. This research uses a qualitative method with an exploratory approach to find and analyze more in-depth things that are not yet known about OSINT. Productivity theory is used by researchers to discuss problem formulations assisted by NVIVO 12 tools in processing data and Soft System Methodology (SSM) to analyze data. The results showed that to use OSINT effectively, NMIC must have large data analysis capabilities using artificial intelligence assistance.

KEYWORDS: OSINT, Maritime Security, Intelligence, Information Center

1. INTRODUCTION

Indonesia as a maritime country is formed into the largest archipelagic country in the world with abundant natural resources. The geographical location of the Indonesian archipelago is very strategic, located at the crossroads of two oceans and two continents. Four of the world's nine chokepoints are also in Indonesian waters. In this strategic geographical position, Indonesia faces various threats and also has economic opportunities. Therefore, its management requires an integral effort that combines all potential resources, including Ministries and Institutions.

Indonesia's geographical conditions require strong maritime defense in upholding sovereignty and maintaining maritime security by carrying out maritime operations. Indonesia has enormous challenges in the maritime sector, especially as Indonesian seas become world economic traffic with large economic value every year. Indonesia needs integrated maritime management efforts that combine all the potential resources of maritime stakeholders. One simple form of this synergy is the integration of information and efforts to increase awareness in the maritime sector with the National Maritime Information Center (NMIC).

NMIC is tasked with providing information to support maritime activities including maritime operations to increase the stability of Indonesia's maritime security by utilizing technology through communication, coordination, and collaboration in the fields of collecting, providing, and exchanging information. This collaboration is carried out between NMIC in Indonesia and internationally to maintain maritime security in the archipelago and the region (Caswell, 2010).

To improve defense at sea, maintain maritime security stability, and answer the challenges of NMIC's tasks in the future, the most important thing that must be done is to integrate data within maritime agencies and prepare maritime information systems, synergize with all stakeholders to build complex maritime big data, up to date and real-time, so that it can be used as material for leaders in determining policies (Davitch, 2017).

Technological advances in the modern era provide opportunities to obtain information quickly from open sources. Technology is a product produced by humans with benefits and uses to make human life easier, more advanced, and more modern. With updates from time to time, technology continues to show its sophistication and greatness which can be utilized by humans to support daily activities and help humans to increase work productivity. New technologies change the way people think, work, live, learn, communicate, behave, obtain, process, and use information. Increasing technological advances in today's life will

have an impact on the intelligence process in collecting information for analysis, although the basic method has not changed, namely by going through the stages of the intelligence cycle (Gibson, 2013).

Intelligence in obtaining information from open sources using Open-Source Intelligence (OSINT). The use of OSINT in national security, law enforcement, and corporate/business functions makes it valuable to analysts in responding to classified, unclassified, or proprietary intelligence requirements across all previous intelligence disciplines. OSINT is collected, exploited, and disseminated promptly to the appropriate audience to address a specific intelligence requirement (Wells & Gibson, 2017).

OSINT is any information that can be obtained from open sources including all types of media, government reports/other documents, research/scientific reports, commercial information vendors, the internet, and so on. The primary qualification for open source information is that OSINT does not require any type of clandestine collection techniques to obtain it and must be obtained through means that fully comply with the copyright and commercial requirements of the applicable vendor (Akhgar et al, 2017).

Based on the background, the phenomenon was found that the effectiveness of OSINT use in NMIC has not been well measured. This is the basis for the author to carry out research with the problem formulation How effective is the use of OSINT in NMIC? This research aims to analyze the effectiveness of using OSINT in the intelligence cycle at NMIC. The research uses qualitative methods with an exploratory approach to explore and analyze in more depth things that are not yet known about OSINT.

2. MATERIALS AND METHODS

To obtain an overview of the subject to be researched and better understand the existing problems systematically and rationally, it is necessary to understand the concepts and theories put forward by experts. This is intended to ensure that the aims and objectives of the research are not obscured. A literature review is needed to provide an overview related to relevant theories to reveal a particular phenomenon or reality which is summarized into a concept of ideas, views, attitudes, and/or methods that describe certain values aims, and objectives.

2.1. Productivity and Effectiveness

According to Hassan (2018), productivity can be interpreted as a comparison between the amounts of expenditure divided by the amount of input in a certain period. There are two important aspects in the concept of productivity, namely efficiency and effectiveness. Efficiency is the ability to use minimum resources to achieve optimal results, while effectiveness is related to measuring success in achieving predetermined goals. Meanwhile, according to Johnson (2007), increasing productivity can be achieved by reducing all kinds of costs as little as possible, including utilizing human resources (do the right thing) and increasing output as much as possible (do the right thing). In other words, productivity is a reflection of the total level of work efficiency and effectiveness. The elements contained in productivity are efficiency and effectiveness. Efficiency as an output/input ratio is a measure of the efficiency of resource use (input).

Efficiency is a measure of comparing the planned use of input with the actual use of input. The definition of efficiency is input-oriented, while effectiveness is a measure that provides an idea of how far targets can be achieved both in quantity and time. The greater the percentage of targets achieved, the higher the level of effectiveness (Treverton, 2003).

2.2. Open Source Intelligence (OSINT)

The term Open Source Intelligence (OSINT) is known to originate from military, security, and law enforcement agencies. There are various descriptions and definitions given as characteristics of OSINT, although they tend to be broad and non-specific. Unver (2018) provides an example of the definition of OSINT by the United States (US) Department of Defense as follows: *"Open Source Intelligence (OSINT) is an intelligence that is produced from publicly available information and is collected, exploited, and disseminated promptly to an appropriate audience to address a specific intelligence requirement."*

According to Wells & Gibson (2017) Open Source Intelligence Handbook, there are four categories of open information and intelligence:

a. Open Source Data (OSD) is raw data that comes from primary sources and can be in the form of photos, satellite images, or personal letters.

b. Open Source Information (OSINF) consists of data that has undergone some filtering first. This can also be called a secondary source.

c. Open Source Intelligence (OSINT), has answered specific questions which are the output of the intelligence cycle. Open source material has been discovered, filtered, and processed to the extent that the processed information can be used directly in an intelligence context.

d. Validated OSINT (OSINT-V) is one step further than what was mentioned above, where the results of the intelligence cycle

are confirmed and verified by another source, which can be non-OSINT.

2.3. Maritime Security

An understanding of maritime security begins with an appreciation of how the concept of security is defined and used in international relations generally. From an academic perspective, security is understood in a different way that emphasizes that security is an important key in a country's decision-making and can warrant extraordinary measures to overcome certain problems. The term maritime security has different meanings depending on who uses the term or in what context security is used (Klein, 2011).

The International Maritime Organization (IMO) has discussed maritime security issues under the auspices of the Maritime Safety Committee since the 1980s, which states that there is a difference between maritime safety and maritime security. Maritime safety refers to preventing or minimizing the occurrence of accidents at sea which may be caused by substandard vessels, crew errors, or unqualified operators, while maritime security is related to protection against unlawful and intentional actions (Setzekorn, 2014).

Viewed from an international context, there is no solid definition of maritime security. Maritime security conceptually focuses on non-traditional security and is strongly influenced by non-traditional (security) schools of thought. Even though there is not yet a complete theoretical understanding of maritime security, Schaurer & Störger (2013) in their book on the transformation of military education, states that of the eight types of transnational organized crime, there are five that have a very strong maritime dimension, namely: terrorism, piracy at sea, arms smuggling, human trafficking, and illegal drug trafficking.

2.4. Research Methods

This research method uses qualitative methods to analyze the effectiveness of using OSINT in the intelligence cycle at NMIC using an exploratory approach. An explorative approach is taken to explore in more depth things that are not yet known. This type of exploratory research is intended to explore a new phenomenon that may not have existed in previous research.

This research uses a unit of analysis in the form of individuals. Overall, fifteen informants are research subjects who can be categorized into three groups, namely Regulators; Operator; and Expert. The analysis unit in the form of this research organization is NMIC which is tasked with providing information to support maritime operations to increase the stability of Indonesia's maritime security by utilizing technology.

The primary data source used in this research is interviews from informants according to the research subject. Secondary data sources for this research are literature, articles, journals, and sites on the internet relating to the research conducted. Primary data was obtained through interviews with a predetermined number of informants. Secondary data was obtained from related portals, the internet (other supporting data), and previous research.

Researchers carry out data processing using NVivo 12 software. NVivo 12 will assist in coding the findings in the field. The purpose of coding in qualitative research is to form main categories from the data sources obtained. Steps in processing data using NVivo 12 software. Then the data obtained was analyzed using Soft System Methodology (SSM) data analysis techniques. The use of SSM analysis techniques in this research is considered relevant because SSM has also been applied in the study of defense and security science since its initial development by Peter Chekland. In SSM there are seven stages of data analysis, namely identifying problems, expressing problems with rich pictures, formulating root definitions by doing system thinking, system modeling, comparing analysis results with conditions in the field, core analysis, and recommendations for solving problems (Burge, 2015).

3. RESULT AND DISCUSSION

OSINT is a source for creating intelligence reports based on information found from open sources. An information center whose output is information that can be used by users requires as many sources of information as possible to then collect, process, and analyze according to its purpose. The most relevant information source for providing information center needs is OSINT.

The use of OSINT in information centers is the largest supplier of information in responding to challenges regarding information needs. NMIC as an information center that provides maritime information requires data sources from various aspects related to the maritime sector which of course cannot be obtained by relying on just one source. There needs to be integration and different points of view to understand a particular situation/event in the maritime sector, so as much information as possible is needed in analyzing the situation/event to obtain objective information.

3.1. Findings from Regulatory Instruments

The findings obtained from the regulatory instrument state that the use of OSINT in the intelligence cycle at NMIC has not been effective because it has not followed the rules for obtaining information from open sources, for example by using the web scraping method which should make it easier to obtain information from open sources according to the OSINT Framework.

Strategic Review of the Effectiveness of Open-Source Intelligence at the National Maritime Information Center

The most concerning thing is the process of analyzing and filtering information originating from OSINT. NMIC must be able to make forecasts/make estimates of events that may be encountered/could occur in the future.

3.2. Findings from Operators Instruments

In obtaining OSINT, there are three important stages to carry out, including crowding, filtering, and collecting data. If all these activities can be carried out then collecting information using OSINT will be effective. To be able to obtain information effectively from OSINT according to the stages, reliable human resources who understand and master how to obtain OSINT, especially those from the deep web and dark web.

3.3 Findings from Experts Instruments

The findings are based on expert opinion that NMIC must obtain information that does not only come from OSINT, especially intelligence in nature so that the information is accurate and can be followed up, waste information (garbage) to a minimum. In data processing and analysis, the main key is data pre-processing and the classification algorithm used, and data evaluation using a confusion matrix.

Next, coding was carried out by combing through all interview transcripts. The results can be seen in the sources and reference columns, how often nodes are mentioned by informants. After the data was processed using NVivo 12, it was seen that not all informants had a focus on each category proposed during the interview process.
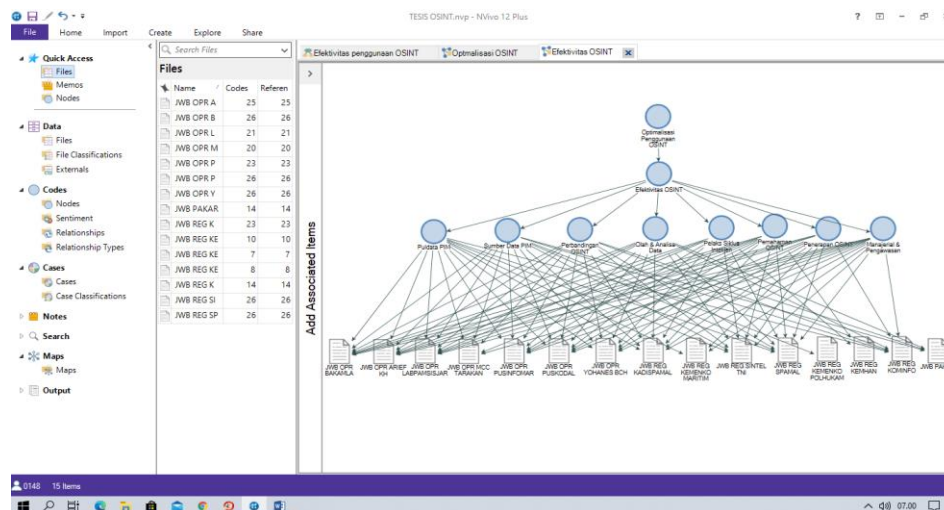

Figure 1. Data processing results with NVIVO 12
Source: Results processed by researchers, 2024

The final step is the reliability test, the main aim of the qualitative coding reliability testing technique (Inter-Coder Reliability/ICR) is to reduce the researcher's subjective bias. ICR in qualitative research is used to determine the consistency of coding results so that it requires more than one coding.
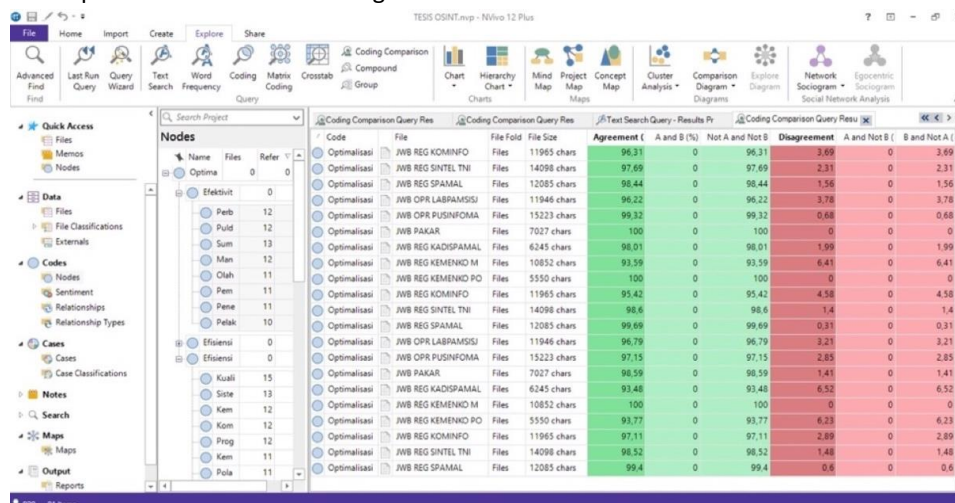

Figure 2. Data Reliability Test Results with NVIVO 12
Source: Results processed by researchers, 2024

Strategic Review of the Effectiveness of Open-Source Intelligence at the National Maritime Information Center

3.4. *Systems Thinking Human resource efficiency at the Maritime Information Center in utilizing Open Source Intelligence (OSINT).*

The root definition uses the PQR formula which is needed to answer the questions What, Why, and How, the PQR formula in question is as follows:

> **"Do P, by Q, to achieve R"**

Increasing the effective use of OSINT (P) for processing according to the stages of the intelligence cycle by using/utilizing artificial intelligence (Q) to meet NMIC information needs (R).

Table 2. CATWOE AND 3E Analysis

Efficacy	The use of all the necessary tools/software (artificial intelligence) will help in the process of collecting very large amounts of data found in open sources and make it easier to carry out big data analysis resulting in increased performance and speed.
Efficiency	Collaborating with domestic IT experts and academics to create their artificial intelligence according to their needs.
Effectiveness	Carrying out planning, research, development, and collaboration with domestic IT experts in creating and developing artificial intelligence by developments in information technology.

Source: Results processed by researchers, 2024

3.5. **Comparison of Conceptual Models with Reality**

The next stage is a comparison of the conceptual model with the reality found in the real world, namely findings in the field during data collection, which is carried out to find a comparison of models and the real world.

Table 3. Comparison of Conceptual Model with Reality

No	Activity	Implementation	Executor	Solution /Alternative
1.	Realizing that developments in technology and information are changing the paradigm of life.	It has been implemented as the initial basis for paradigm change.	Regulator and Operator	As a rationale for utilizing technological and information developments in life
2.	Understand the ease of obtaining information by utilizing technological and information developments.	It has been implemented by utilizing technological and information developments to obtain the required information.	Regulator and Operator	Use it as a basis for finding the right method for obtaining information.
3.	Identify methods of obtaining information according to developments in technology and information with OSINT.	It has been implemented but the implementation is not yet effective.	Regulator and Operator	There is a need for tools to help and make OSINT easier
4.	Formulating artificial intelligence to help and	This activity has been carried out	Regulator and	Special/additional attention is needed

	simplify OSINT.	but is hampered by the expensive price of artificial intelligence.	Operator	to implement artificial intelligence
5.	Create your artificial intelligence that is suitable for obtaining information from OSINT to collect, process, and analyze the resulting information	This activity has not yet been implemented.	Regulator and Operator	Empowering domestic IT experts to create their artificial intelligence
6.	Implementing artificial intelligence at NMIC	This activity has been partially implemented.	Regulator and Operator	Increased budget for procurement and creation of artificial intelligence.
7.	Evaluate the artificial intelligence used to adapt to developments in technology and information	This activity has not yet been implemented	Regulator and Operator	It needs to be implemented to provide artificial intelligence recommendations through developments in technology and information
8.	Provide recommendations for the artificial intelligence capabilities to be used according to the evaluation results	This activity has not yet been implemented	Regulator and Operator	Receive recommendations regarding the artificial intelligence capabilities used

Source: Results processed by researchers, 2024

Based on the results of the comparative analysis of conceptual models with reality, a range was found between reality and system thinking where activities had not been carried out either in whole or in part (research gap) by the relevant instruments.

Table 4. Gap Analysis

No	Gap of Research	Analysis
1	The method of obtaining information according to developments in technology and information using OSINT is not yet effective	- OSINT theory - Interview result - Previous research Libor Benes (2013)
2	Formulating artificial intelligence to help and simplify OSINT has encountered obstacles due to budget limitations.	- Interview result - Republic of Indonesia Law Number 32 of 2014 concerning Maritime Affairs
3	Creating your artificial intelligence that is suitable for obtaining information from OSINT to collect, process, and analyze the resulting information has not been implemented.	- OSINT theory - Intelligence Cycle Theory - Interview result - Previous research Dmytro V. Lande, Ellina V. Shnurko-Tabakova (2016)

4	Implementing artificial intelligence at NMIC has been partially implemented.	- OSINT theory - Intelligence Cycle Theory - Interview result - CATWOE analysis - Republic of Indonesia Law no. 17 Yr. 2011
5	There has been no evaluation of the artificial intelligence used to adapt to developments in technology and information.	- OSINT theory - Maritime Security Theory - Interview result - Codal Theory - Republic of Indonesia Law no. 11 Yr. 2008 - Republic of Indonesia Law no. 17 Yr. 2011 - 3E Analysis - Previous research Well, Douglas and Gibson, Helen (2017)
6	There is no recommendation for the artificial intelligence capabilities to be used according to the evaluation results	- Gap analysis results 5

Source: Results processed by researchers, 2024

First, the process of obtaining information according to technological and information developments by utilizing OSINT at NMIC is not yet effective because it does not yet have big data analysis capabilities. The solution to having big data analysis capabilities is to use the help of artificial applications/tools called artificial intelligence.

Second, the procurement of artificial intelligence at NMIC to assist and facilitate the use of OSINT encountered obstacles due to budget limitations. Artificial intelligence as supporting equipment/tools for NMIC to obtain information from OSINT so that it is effective in a short/fast time requires a large budget. The solution to overcome this obstacle is to create your artificial intelligence according to your needs.

Third, create your artificial intelligence through the cooperation/empowerment of domestic IT experts so that apart from the price being cheaper, security is more guaranteed and advances the domestic industry.

Fourth, the implementation of artificial intelligence that already exists and is used at NMIC cannot yet cover all the needs and work of collecting information from OSINT. The solution to overcome this is by adding other artificial intelligence to automate the stages of data processing according to the intelligence cycle so that the resulting output is intelligence that is accurate and valuable and can be followed up.

Fifth, the evaluation of artificial intelligence used by NMIC by technological and information developments must have the ability to: be able to automatically differentiate categories of information from an open source which is increasingly complex; framework-based by integrating various applications to obtain information by the OSINT framework and can support Kodal; big data analysis and forecasting; able to carry out crowding, filtering and collecting data, especially from the deep web and dark web as well as from social media; minimum possible waste information; able to carry out data pre-processing and classification algorithms well; and can evaluate data automatically with a confusion matrix.

Sixth, the recommendation for artificial intelligence capabilities used by NMIC to increase the effectiveness of its work is that it must have capabilities according to the fifth gap analysis.

4.   CONCLUSION

New technological advances provide opportunities and threats related to the potential to obtain information quickly. New technologies help localize, process, and disseminate large amounts of data and prepare it for analysis originating from open sources. Intelligence in obtaining information from open sources using Open Source Intelligence (OSINT). In facing change, NMIC must be able to meet the needs of its users in the form of short and fast intelligence reports. With the OSINT concept, NMIC must review the use of information from open sources in line with advances in information technology. To be able to use OSINT effectively, NMIC must have big data analysis capabilities using artificial applications/tools called artificial intelligence. Creating

artificial intelligence through the cooperation/empowerment of domestic IT experts will save costs, ensure security, and advance domestic industry. The artificial intelligence that is created can give rise to features of the intelligence cycle from processing to distribution.

Recommendations to regulatory instruments and operators in procuring artificial intelligence for NMIC by creating their artificial intelligence according to needs through collaboration/empowerment of domestic IT experts who can automatically differentiate increasingly complex categories of information from open source; framework-based by integrating various applications to obtain information by the OSINT framework and can support Kodal; big data analysis and forecasting; able to carry out crowding, filtering and collecting data, especially from the deep web and dark web as well as from social media; minimum possible waste information; able to carry out data pre-processing and classification algorithms well; and can evaluate data automatically with a confusion matrix.

REFERENCES

1) Akhgar, B., Bayerl, P. S., & Sampson, F. (Eds.). (2017). Open-source intelligence investigation: from strategy to implementation. Springer.Best, C, Open Source Intelligence. Mining Massive Data Sets for Security, Amsterdam: IOS Press, 2008.

2) Bajagic, M., & Mijalkovic, S. SECRET INTELLIGENCE TECHNICAL AND TECHNOLOGICAL PROJECTS–ENDANGERING NATIONAL AND WORLD SECURITY1. DANI ARČIBALDA RAJSA ""ARCHIBALD REISS DAYS, 21(1), 129-144.

3) Caswell, K. L. (2010). Establishment of the National Maritime Intelligence Center: understanding the foundations of trust to support a collaborative environment in homeland security (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

4) Davitch, J. (2017). Open Sources for the Information Age. Joint Forces Quarterly, 87(4), 18-25.

5) Gibson, S. D. (2013). Open-source intelligence. In Routledge Companion to intelligence studies (pp. 123-132). Routledge.

6) Hassan, N. A., Hijazi, R., Hassan, N. A., & Hijazi, R. (2018). The evolution of open source intelligence. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, 1-20.

7) Johnson, L. K. (Ed.). (2007). Handbook of intelligence studies (Vol. 2). London: Routledge.

8) Klein, N. (2011). Maritime Security and the Law of the Sea. Oxford University Press, USA.

9) Setzekorn, E. (2014). Open Source Information and the Office of Naval Intelligence in Japan, 1905–1920. International Journal of Intelligence and Counterintelligence, 27(2), 368-386.

10) Schaurer, F., & Störger, J. (2013). The evolution of open source intelligence (OSINT). Comput Hum Behav, 19, 53-56.

11) Treverton, G. F. (2003). Reshaping national intelligence for an age of information. Cambridge University Press.3.

12) Unver, A. (2018). Digital open source intelligence and international security: a primer. EDAM Research Reports, Cyber Governance and Digital Democracy, 8.

13) Wells, D., & Gibson, H. (2017). OSINT from a UK perspective: Considerations from the law enforcement and military domains. Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union, 16, 84-113.