

臺灣對抗跨國組織犯罪的情報分享

張中勇

佛光大學公共事務學系教授

摘要

本文旨在探討近年來臺灣警察與安全情報單位對抗各種跨國犯罪的經驗與挑戰，文中將討論執法與情報單位間情報分享機制的功能與實踐情形，以及評估機制運作成敗及所可能面對的挑戰。本文認為，影響情報分享的因素至少包括組織利益、官僚政治、人權保障以及缺乏足夠資源等要項；此外，本文亦將探討臺灣對外情報分享與合作夥伴之影響因素，包括各國國家利益、腐敗政客與中共政治干擾、缺乏分享情報之誘因等因素，冀能藉以提出有效強化情報角色與分享機制之對策，增進打擊跨國犯罪之成效。

關鍵字：情報、情報分享、情報合作、跨國組織犯罪

Intelligence Sharing in Fighting Transnational Organized Crime in Taiwan

Chang, Chung-young

Professor, Department of Public Affairs, Fo Guang University

Abstract

This paper explores the achievements and challenges that Taiwan's police force and security intelligence services have been facing in their fight against various forms of transnational organized crime in recent years. It discusses the functions and practices of intelligence sharing mechanism among relevant law enforcement agencies and intelligence services within Taiwan, assessing on the successes and failures of its operations and challenges ahead. Organizational interests, bureaucratic politics, concerns of respect for human right and lack of sufficient resources are some examples of the reasons or causes to be examined. More importantly, this paper probes into the reality of Taiwan's external cooperation in sharing intelligence with its counterparts. A number of factors, including national interest concerns, political interferences from corrupted politicians and China, and lack of incentives for sharing intelligences, among others, are discussed to further understand and improve the performances of crime-fighting strategies and operations.

Keywords: intelligence, intelligence sharing, intelligence cooperation, transnational organized crime.

I. Background

In retrospect, there has been a growing change in the global security landscape since the end of the Cold War and, especially, the beginning of the 21st century. Despite strategic security and military conflict of high politics issues remain dominant in world politics, a number of low politics issues, including, but not limited to, natural disasters, international terrorism and various forms of transnational organized crime (TOC)¹ are on the rise and taking severe toll on the mankind, posing serious security challenges that have been threatening national security, economic welfare, social development and public order in many parts of the world.² It is suffice to say that while malicious dragons of the past may still be intimidating the international community and the whole human civilization, a jungle full of venomous snakes has been taking the place as a newer, and

¹ There are 18 major categories of transnational crime, including money laundering, illicit drug trafficking, corruption and bribery, infiltration of legal business, fraudulent bankruptcy, insurance fraud, computer crime, theft or infringement of intellectual property, illicit traffic in arms, terrorist activities, aircraft hijacking, sea piracy, hijacking on land, trafficking in persons, trade in human body parts, theft of art and cultural objects, environmental crime, and other offences committed by organized criminal groups. See Gerhard O.W. Mueller, "Transnational Crime: Definitions and Concepts," *Transnational Organized Crime*, Vol. 4, No. 3&4 (Autumn/Winter 1998), pp. 13-14.

² The long term threats to civil society from organized crime, especially transnational one, can be categorized as follows: political and economic destabilization, injustice, unfair competition, corruption, institutional delegitimization, monopoly pricing and organized crime extortion, unfair treatment, violence, intimidation, fear, oppression, and tyranny. Peter A. Lupsha, "Transnational Organized Crime versus the Nation-State," *Transnational Organized Crime*, Vol.2, No.1 (Spring 1996), pp. 43-45.

even greater, security threat in the present.

To successfully tackle or manage these newly emerging challenges of transnational security threat, it will require, among others, better cooperation among security intelligence services, law enforcement agencies and police forces domestically and internationally in different levels and many ways.³ A better horizontal coordination and vertical integration among all levels of government and relevant departments and agencies on the basis of the principle of whole-of-government and spirit of teamwork is critical and indispensable in the fight against TOC. It is even more important to construct an international web of cooperative relations and mechanisms among countries with common goals in dealing with TOC that often move across borders and operate beyond jurisdictions.⁴

³ Celina B. Realuyo, *Collaborating to Combat Illicit Networks Through Interagency and International Efforts* (Washington D.C.: William J. Perry Center for Hemispheric Defense Studies, August 2013), available on: <https://www.williamjperrycenter.org/sites/default/files/publication_associated_files/Collaborating%20to%20Combat%20Illicit%20Networks%20through%20Interagency%20and%20International%20Efforts.pdf>, accessed on January 4, 2019; Diane E. Chido, *Intelligence Sharing, Transnational Organized Crime and Multinational Peacekeeping* (Carlisle, PA: Palgrave Pivot, 2018).

⁴ FBI, *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*, Audit Report 04-10 (December 2003), available on: <<https://oig.justice.gov/reports/FBI/a0410/final.pdf>>, accessed on January 5, 2019.; U.S. White House, *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing* (October 2007). United States Government Accountability Office, *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*, October 12 2011, GAO-12-144T, available on: <<https://www.gao.gov/new.items/d12144t.pdf>>, accessed on January 3, 2019.

Hence, intelligence cooperation in the forms of liaison, personnel exchange, data and intelligence-sharing, and others is often identified as a key in preventing and detecting criminal acts of TOC.⁵

Taiwan is no exception in fighting against TOC with the use of the intelligence and information sharing. Taiwan's intelligence apparatus and its activities not only face the problems in, among others, vertical integration and horizontal coordination of intelligence transferring and sharing domestically, but also need to expend and deepen the degree and extent of cooperative relations with the countries that do not recognize Taiwan as a sovereign state. How Taiwan has been struggling to construct and promote international intelligence cooperative mechanisms with its partners will be a good example for contemplation.

This paper will introduce the concept and practices of intelligence sharing as a basis to discuss the development and functions of intelligence sharing mechanism among relevant law enforcement agencies and intelligence services within Taiwan, assessing on the successes and failures of its operations and challenges ahead. Organizational interests, bureaucratic politics, concerns of respect for human right and lack of sufficient resources are some examples of the reasons or causes to be examined. More importantly, this paper will probe into the reality of Taiwan's external cooperation in shar-

⁵ Richard A. Best, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, Washington, DC: Congressional Service Report, RL33873 (13 February 2007), available on: <<https://fas.org/sgp/crs/intel/RL33873.pdf>>, accessed on January 25, 2019; Steven Chermak, "Law Enforcement's Information Sharing Infrastructure: A National Assessment." *Police Quarterly*, Vol. 16, No. 2 (June 2013), pp. 211-244.

ing intelligence with its counterparts. A number of factors, including national interest concerns, political interferences from corrupted politicians and China, and lack of incentives for sharing intelligences, among others, will be discussed to further understand and improve the performances of crime-fighting strategies and operations.

II. The Role of Intelligence in the Fight Against TOC

The role of intelligence has often been pointed out as the first line of defense against security threats, including transnational criminal activities, through its functions of avoiding strategic surprise, providing long-term expertise, supporting the policy process, and maintaining the secrecy of information, needs, and methods.⁶ In practices, the intelligence activities can be generalized into following four categories: collection, analysis, counterintelligence and covert action.⁷

In the area of collection, intelligence branches of security services and law enforcement agencies will make use of the following activities to gather relevant information or raw intelligence: human intelligence operations (HUMINT), collecting intelligence through the use of undercover, informant or other similar methods; technical

⁶ Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle," *Intelligence and National Security*, Vol. 21, No. 6 (December 2006), pp. 959-979; Antony Field, "Tracking Terrorist Networks: Problems of Intelligence Sharing within the UK Intelligence Community," *Review of International Studies*, Vol. 35, Issue 4 (October 2009), pp. 997-1009. Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Thousand Oaks, CA: SAGE, 2015).

⁷ Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Thousand Oaks, CA: SAGE, 2015).

intelligence operations (TECHINT), intercepting and deciphering communication and signal intelligence with the use of technological devices and other sophisticated technical means; open source intelligence (OSINT), gathering public available information with legal means from various sources of information, including medias, institutions, experts and others; and exchange and cooperation, sharing relevant intelligence with partners of common interest. The raw intelligence gathered or received will then be processed and provided for the intelligence analyst to produce the finished or final result of intelligence for the policy community.⁸

The product of intelligence analysis will serve different purposes as designed and required. A strategic intelligence will provide an analytical forecast on the long-term development or future trend of the object under analysis. For example, the International Criminal Police Organization, or Interpol, often stresses the importance of strategic intelligence in the innovation of new policing strategy and capabilities, including reforming the structure of the police forces, reallocation of resources and manpower, and adoption of modern technology, to cope with the emerging challenges of TOC. More importantly, a tactical intelligence about the current position, movement or gun-power of members of a criminal group is critical to the success of any police interception operations. Besides, an early warning based on intelligence analysis is of particular importance to avoid surprise attack, launch preemptive strike or paralyze those criminal activities that have been contemplated and undertak-

⁸ Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Thousand Oaks, CA: SAGE, 2015).

en for some time. In another word, an intelligence-led strategy for law enforcement or policing operations has been adopted by many police forces around the world as one of the mainstream policing strategies in recent years.⁹

The intelligence is a kind of knowledge that is used to reduce the uncertainty by getting to understand more about the target and the surrounding security situation. Therefore, it needs to be collected as much as possible in order to provide more and better information or data or raw intelligence for the purpose of intelligence analysis. While intelligence collection by all means is not or will never be sufficient for analysis purpose, information exchange or intelligence sharing then becomes necessary or imperative in order to enhance the quality of intelligence analysis.

In the case of Taiwan, while there is no single agency whose mission is specifically designed to prevent and detect TOC, there are a number of, if not all, law enforcement agencies and the police forces engaged in fighting against TOC. According to the National Intelligence Work Act of 2005, all ten organizations designated by the Act, including four intelligence organizations and six quasi-intelligence organizations, were tasked to perform intelligence collection of national security-related information, ranging from external security threats stemming from China to transnational criminal

⁹ Nick J. Maxwell and David Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*, RUSI Occasional Paper (October 2017), available on: <https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_aringstall_web_4.2.pdf>, accessed on January 2, 2019.

activities posing threats to the interest and welfare of Taiwan. As a matter of fact, this line of thought in tasking national security intelligence organization with the mission in support of the law enforcement agencies and the police forces in fighting TOC is quite similar to that of the security intelligence service of the UK.

As the Act authorizes, the following four organizations, such as National Security Bureau (NSB), Military Intelligence Bureau of the Ministry of Defense (MIB), Office for Telecommunication Development (OTD) and General Battalion of Military Security (GBMS) are designated as the intelligence organization whose primary or required task is to collect security intelligence regarding, among others, criminal activities of TOC. Moreover, there are six organizations, including the National Policy Agency (NPA), the Investigation Bureau of Ministry of Justice (MJIB), the Political Warfare Bureau, the Military Police Command, Taiwan Coast Guard, and the National Immigration Service (NIS), whose mission is in charge of law enforcement or policing work are also designated as intelligence organization when authorized to collect information relevant to national security. As the Act stipulates, the NSB is responsible for the coordination and integration of intelligence work and the intelligence that is collected and analyzed by the relevant intelligence and quasi-intelligence organizations through the framework of the National Security Intelligence Coordination Mechanism. The NSB will serve as the intelligence hub and the rest of nine members of the intelligence community will report to the NSB instead of sharing the intelligence among one and other.

All ten intelligence organizations or law enforcement agencies are equipped with intelligence function of collecting and analyzing the information of importance to their organizational mission. However, how to coordinate and share the intelligence within the security and law enforcement community is critical to the success of the fight against TOC. In addition, how to overcome diplomatic difficulties due to China factor that has been frustrating or obstructing international cooperation between Taiwan and other countries in intelligence exchange and sharing is also another challenge that Taiwan has been facing.

III. The Construction and Operations of Intelligence Sharing Mechanism

While the intelligence is vital to pursue and frustrate transnational organized criminal groups, a successful intelligence-sharing is the key for the intelligence to work. All relevant police and law enforcement forces and security intelligence services need to collaborate together under an agreed guidance and procedure to transmit and share intelligence through formal and informal channels or mechanisms. A formal channel or mechanism for sharing intelligence is authorized by laws and orders, or established on the basis of consents or agreements among participating parties. On the other hand, an informal one that can avoid or reduce red tape will be working based on inter-personal relations, mutual trust and reciprocity, through a channel and mechanism of trust.¹⁰

¹⁰ IACP, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing At the Local, State and Federal Levels*, August 2002, available

From the perspective of organizational structure of intelligence cooperation mechanism, it has been a common practice that multiple parties agree to share information or intelligence among them through bilateral or multilateral channels or a network of cooperative relations. Basically, there are four types of information and intelligence sharing systems:¹¹

First, hierarchical liner system: information moves from the top level of government agencies to the bottom level on the basis of a priority list so as to, among others, preserve authority of chain of command and ensure security. However, the information flow that goes through successive levels tend to be slow due to power politics that often hold information to flex the power. This model is often found in the totalitarian or authoritarian countries where power, or intelligence, is usually, if not always, centralized and under strict control.

Second, hub-and spoke systems: information will flow out of the center hub to its spoke partner agencies as through the spokes of a wheel. The system is effective in spreading information to the

on: <<http://www.justiceacademy.org/iShare/Library-COPS/cops-w0418-pub.pdf>>, accessed on January 2, 2019; U.S. DoJ, *The National Criminal Intelligence Sharing Plan-Solutions and Approaches for a Cohesive Plan to Improve Our Nation's Ability to Develop and Share Criminal Intelligence*, October 2003, available on: <<https://www.dni.gov/files/ISE/documents/DocumentLibrary/National-Criminal-Intelligence-Sharing-Plan.pdf>>, accessed on January 2, 2019.

¹¹ Joseph W. Pfeifer, "Network Fusion: Information and Intelligence Sharing for a Networked World," *Homeland Security Affairs*, Vol. 8, Article 17 (October 2012), available on: <<https://www.hsaj.org/articles/232>>, accessed on January 3, 2019.

overall network by pushing the information from a centralized location. However, one potential drawback of this system is its inability to handle the bidirectional exchange of information in a timely manner, especially during peak hour or critical moments when information exchange is always overwhelmed. The real danger is for this kind of system to become a modernized information stovepipe, where information originates from a place of limited perspective and is pushed only when the originating agency deems it necessary to do so. This model will also experience a problem of turf battles, that will consider information as a commodity that deserves a market value, among members of information sharing mechanism.

Third, co-located liaison system: a liaison is sent to a partner center that refuses to directly share information and only allows information to be relayed by voice through its liaison. This system may fail to get the right information to the right person at the right time. While there is face-to-face collaboration and communication, this kind of system may not be productive or constructive if members of the center do not possess shared responsibility and accountability. In addition, a lack of mutual understanding and trust among participants of the system will reduce the quantity and quality of the information flow throughout the system.

Fourth, network fusion: it is an information sharing system that fuses information and intelligence from multiple sources to allow decision makers to better adapt to a changing threat environment. The system will take advantage of modern technology to enhance awareness and collaboration across different disciplines by connecting various forms of information gathering devices at

classified and unclassified levels. It is a framework for linking multiple systems for pushing and pulling information and intelligence, providing a platform for connecting disparate organizations and their unique viewpoints. Successful network fusion possesses the following advantages: faster to communicate directly with decision makers and those closest to the information; smarter to understand the threat environment through multiple perspectives; cheaper to collaborate virtually rather than co-locate (Seagle, 2015). This model has been widely adopted and practiced in many law enforcement, security intelligence and police agencies of the world.

In order to enhance the effectiveness of information sharing, it is important to provide sufficient incentives that will promote the quality of intelligence sharing. A study done by the RAND on behalf of the European Network and Information Security Agency (ENISA) in 2010 concluded that there are three tiers of incentives for better information sharing:¹²

High:

1. Economic incentives stemming from cost savings;
2. Incentives stemming from the quality, value, and use of information shared.

Medium:

3. The presence of trust among Information Exchange (IE) partners;

¹² European Network and Information Security Agency (ENISA), *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, September 08, 2010, available on: <<https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>>, accessed on January 11, 2019.

4. Incentives from receiving privileged information from government of security services;
5. Incentives deriving from the processes and structures for sharing;
6. Allowing IE participants' autonomy but ensuring company buy-in.

Low:

7. Economic incentives from the provision of subsidies;
8. Economic incentives stemming from gaining voice and influence;
9. Economic incentives stemming from the use of cyber insurance;
10. Incentives stemming from the reputational benefits of participation;
11. Incentives from receiving the benefits of expert analysis, advice, and knowledge;
12. Incentives stemming from participants' preferences, values, and attitudes.

In the case of the fight against TOC in Australia, it is argued that intelligence sharing needs to go beyond the sharing of information only. Sharing intelligence would mean the ability to identify and draw upon a broad base of experts, to work together across jurisdictional boundaries, to bring together a combination of different skills, knowledge and expertise. Moreover, a team or network of intelligence needs to be flexible and adaptive. The Joint Organized Crime Group (JOCG) and the Australian Crime Commission-led National Criminal Intelligence Fusion Capability are two examples

that are often pointed out to illustrate how such mechanism of intelligence sharing has been organized and put into practice with good result.¹³ However, such mechanism may be a successful example of effective collaboration and intelligence sharing, it is still a collective mechanism consisted of a number of individual agencies, with unique cultures, specific mandates, terms of reference and, more importantly, personal traits.¹⁴ It is organized as a task force or an ad hoc group that may not be consistent with the organizational interests of each participating agencies. Bureaucratic politics may also find its way to delay or derail intelligence sharing in security or criminal investigation.

From the perspective of structure of intelligence cooperation mechanism among nations, as organized criminal groups often operates across national boundaries in various ways, so should and will the security and law enforcement intelligence services with common concerns develop a cooperative relations in sharing intelligence that is crucial and useful in preventing and detecting serious organized crime. This cooperative relationship will be built upon a formal bilateral or multilateral treaty or agreement among participating countries. While intelligence exchange and sharing can be proceed in accordance with the arrangement, it is the trust

¹³ Claire Richards, "What are the Barriers to Gathering and Sharing Organised Crime Intelligence: An Australian Perspective," *The European Review of Organised Crime*, Vol. 3, No. 1 (March 2016), pp. 78-104.

¹⁴ Douglas Edward Abrahamson and Jane Goodman-Delahunty, "Impediments to Information and Knowledge Sharing Within Policing: A Study of Three Canadian Policing Organizations," *SAGE Open* (January-March 2014), pp. 1-17.

in partnership that will keep the momentum of intelligence sharing and other cooperative programs within the intelligence alliance. For example, it is the mutual trust within the ‘Five Eyes’ group that has been sustaining the close intelligence cooperation among partner countries for more than seventy years.¹⁵ However, it seems that lack of trust within the NATO and Europol members may have hindered the extent and degree of cooperation in intelligence exchange and sharing.¹⁶

In the case of Taiwan, while the NSB is authorized to direct, coordinate and assist the intelligence operations of all intelligence and quasi-intelligence organizations, it has no power of command to force these organizations to follow its orders. The NSB has been using political persuasiveness, the appropriation of funds and recommendation for advancement as an incentive to encourage intelligence dissemination or sharing with itself. It is interesting to note that the NSB discourages autonomous intelligence sharing among members of the community without its consent. However, the NSB’s strategy may be effective, but not always works and not for

¹⁵ Patrick F. Walsh and Seumas Miller, “Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden,” *Intelligence and National Security*, Vol. 31, No. 3 (January 2016), pp. 345-368.

¹⁶ Jan Ballast, “Trust (in) NATO - The Future of Intelligence Sharing within the Alliance,” *Research Paper*, No. 140 (September 2017), Rome: Research Division, NATO Defense College, available on: <<https://css.ethz.ch/en/services/digital-library/publications/publication.html/6cc75c52-8da8-4abf-a4ce-0824e3e448aa>>, accessed on January 13, 2019; Björn Fägersten, “Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol,” *Intelligence and National Security*, Vol. 25, No. 4 (December 2010), pp. 500-520.

long. As competition for more support and rewards from the policy level between the NSB and other law enforcement agencies and the police force has become increasingly intensive, the latter may seek to bypass the former by, among others, withholding key intelligence critical to successful operations against TOC. This kind of episode tends to be more common when the policy makers choose to strengthen their power of direct control at the expense of the established system in place.

In addition, bureaucratic politics and organizational interests may also impair or facilitate intelligence sharing within and among the organizations. As the influence of the NSB has been on the decline since the lift of martial rule in Taiwan in 1987, the NSB was no longer able to control or commend the whole security and intelligence community. The NSB needs to employ more resources, such as financial subsidies or technical support, to enhance the effectiveness and quality of intelligence sharing within the community. Besides, civilian law enforcement agencies and the police may find it uneasy or uncomfortable to work with the NSB where the military takes the lead. The organizational culture of the civilian bureaucracy is different from that of the military one in several ways, with the former will hold greater respect for human rights and rule of law. As a result, the civilian bureaucracy may follow a stricter rule in engaging with information sharing and intelligence exchange.

As to intelligence cooperation with other countries, Taiwan may have to resort to the use of informal channels of intelligence sharing due to diplomatic restriction and political interference. For

example, high-ranking law enforcement officials and police officers will often pay annual visit to the police forces of south-east Asian countries in an attempt to develop a close personal relationship that will, among others, facilitate intelligence sharing and other cooperative activities as well. In spite of the lack of formal relations, Taiwan's NPA and NIS have managed to send a number of liaison officers to be stationed in major cities around the world.¹⁷ In the period of 2004-2018, the NPA has been able to dispatch 12 police liaison officer stationing overseas, including Philippine, Thailand, Vietnam, Indonesia, Malaysia, Japan, US, South Africa, Macau, Korea, Holland, and Singapore. In the case of the NIS, 28 overseas immigration posts have been established in Korea, Japan (2), Philippine, Vietnam (2), Malaysia, Singapore, Thailand, Myanmar, Indonesia, Hong Kong, Macau, India, US (5 cities), Canada (2), Paraguay, Belgium, UK, France, South Africa, Australia and New Newland. In addition, the NSB, MJIB and some related intelligence agencies and security services also send an unknown number of intelligence officers stationing in major countries. These officers from various organizations are in charge of intelligence liaison missions with their counterparts.

IV. Barriers and Challenges of Intelligence Sharing

While information and intelligence sharing is the lifeblood of the intelligence services and police forces, barriers in sharing infor-

¹⁷ Adam D.M. Svendsen, "Connecting Intelligence and Theory: Intelligence Liaison and International Relations." *Intelligence and National Security*, Vol. 24, No. 5 (September 2009), pp. 700-729.

mation within or across jurisdictions of different organizations still exist.¹⁸ According to a study on information and knowledge sharing within policing in three Canadian policing organizations, seven mutually exclusive impediments were found: processes/technology, individual unwillingness, organizational unwillingness, workload/overload, location/structure, leadership, and risk management. Among them, processes and technology that highlights the dark side of organizational structure was identified as the most common impediment, followed closely by individual unwillingness that has often been criticized as a common ailment of organizational culture.¹⁹

It is interesting to note that another study on Australian case points out that an alternative approach in diagnosing the barriers of intelligence sharing should consider changing the analyst rather the system. The study also identified serious legislative, technological, resource and cultural impediments to the flow of intelligence exchange and sharing in Australia.²⁰ There is an evident inconsistency in the legislative and regulatory framework between Australian federal level and local level of government or jurisdiction, making the

¹⁸ Gordon Corera, "Why Intelligence Sharing Still Has a Long Way to Go," *BBC News*, January 2016, <<http://www.bbc.com/news/world-europe-35154640>>, accessed on May 29, 2018.

¹⁹ Douglas Edward Abrahamson and Jane Goodman-Delahunty, "Impediments to Information and Knowledge Sharing Within Policing: A Study of Three Canadian Policing Organizations," *SAGE Open* (January-March 2014), pp. 1-17.

²⁰ Claire Richards, "What are the Barriers to Gathering and Sharing Organised Crime Intelligence: An Australian Perspective," pp. 78-104.

flow of security and criminal intelligence slower, harder and more difficult to proceed as desired. Moreover, outdated information and communications technology only makes the problems in sharing information and intelligence even worse. Therefore, how to overcome these barriers related to both organizations and persons becomes a great challenge to reform information and intelligence sharing.

In the wake of the September 11 terrorist attack, intelligence reform was considered a priority task to improve the coordination of national security intelligence services, law enforcement agencies and police forces and mechanism of intelligence sharing. As a result, fusion centers, whereby intelligence will be collected, stored, analyzed, and disseminated to other agencies, have been created in several countries, including the US and Australia. However, an Australian study argued that the structure and mission of law enforcement agencies undermines the very essence of fusion centers and what they are intended to do. Some of the traits, such as autonomy and interagency ego, will hinder the effective and efficient sharing of information and intelligence.²¹

Fusion centers in the US were also facing struggle to find their place in the post-99 world because of some of the intelligence surveillance operations of the police forces may have infringed upon the constitutionally protected or legitimate civil rights. For example, the information collected on a legitimate anti-war activity by the police surveillance operations may be deemed as a crimi-

²¹ Robert W. Taylor and Amanda L. Russell, "The Failure of Police 'Fusion' Centers and the Concept of a National Intelligence Sharing Plan," *Police Practice and Research*, Vol. 13, No. 2 (October 2011), pp. 184-200.

nal act involving extremists and sent to fusion centers for further sharing. The US fusion centers were set up in 2004 to be state-run information networks that would have guidance and support from the federal government and operate in conjunction with local law enforcement agencies in the war on terrorism. However, these fusion centers have become centers that communicate and analyze “all crimes” and “all hazards.” The fact that the result of the centers’ operation become more confusion than fusion invites complaints from civil right groups such as the American Civil Liberties Union (ACLU).²²

As to challenges in international cooperation in intelligence sharing, bureaucratic resistance has been identified as a barrier that impedes the proceeding and progress of intelligence cooperation among members of the Europol.²³ Firstly, states will weigh the costs and benefits over any decision regarding cooperation with other countries, friends or foes, since international cooperation may be expensive or even risky. In particular, states are more cautious about establishing cooperative relations in intelligence sharing because of grave concern on national security.²⁴

²² Brian Peteritas, “Fusion Centers Struggle to Find Their Place in the Post-9/11 World,” *Governing the States and Localities*, June 2013, <<http://www.governing.com/topics/public-justice-safety/gov-fusion-centers-post-911-world.html>>, accessed on May 29, 2018.

²³ James Igoe Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2009); Anna-Katherine Staser McGill, “Challenges to International Counterterrorism Intelligence Sharing,” *Global Security Studies*, Vol. 3, Issue 3 (Summer 2012), pp. 76-86.

²⁴ Björn Fägersten, “Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol,” pp. 500-520.

Secondly, bureaucratic personnel inherent with self-interest will try to pursue their own rational goals, including increased budget and workforce, personal advancement, self-realization, more power and authority in the decision-making process. They may react to any obstruction or change that will compromise their interest by delaying or even derailing the international agreement favored by the head of the state. As those bureaucratic people invest vast efforts and resources in developing a network of intelligence sharing, they may not easily agree to be transferred into or rebuild a new institutional arrangement. Hence, the role of bureaucracy in the process of policy formulating and implementing cannot be down played or ignored.²⁵

Thirdly, bureaucratic culture of intelligence services may also become a barrier to international cooperation. As organizational culture can be viewed as a common expectation shared by the group, norms that shapes the patterns of behaviors within the group, a form of social institution and facilitates internal coordination, it is assumed that the stronger a certain organizational culture grows, the harder it will be for that organization to collaborate with others, especially if its culture is built upon the trait of secrecy, isolation and organizational exceptionality. It is also argued that these traits of organizational culture may constitute a barrier to any change requiring increased contacts and cooperation with other agencies.²⁶

²⁵ Björn Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol," pp. 500-520.

²⁶ Björn Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol," pp. 500-520.

The ENISA study of 2010 also identified a list of barriers and challenges to information sharing.²⁷

High:

1. Poor quality information;
2. Misaligned economic incentives stemming from reputational risks;
3. Poor management.

Medium:

4. Type of participants;
5. Legal barriers related to fear of legal or regulatory;
6. Fear or leaks;
7. Group size;
8. Misaligned economic incentives stemming from group behavior – externalities;
9. Social barriers from government;
10. Misaligned economic incentives stemming from poor decision-making about investment in security;
11. Norms of rivalry.

Low:

12. Legal barriers related to freedom of information;
13. Misaligned economic incentives stemming from the costs from participating IE;

²⁷ European Network and Information Security Agency (ENISA), *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, September 08, 2010, available on: <<https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>>, accessed on January 11, 2019.

14. Misaligned economic incentives stemming from competitive markets;
15. Legal barriers related to competition law violations.

As to the barriers in information and intelligence sharing between Taiwan and other countries, lack of formal relations and China's political interference are two major issues that affect the effectiveness and quality of intelligence sharing. While several of Taiwan's intelligence services, law enforcement agencies and the police have been able to establish liaison relations with their foreign counterparts, the level and extent of information and intelligence sharing remains subject to the bureaucratic politics in host countries and the political pressure from China. While the policy maker may decide to cooperate in intelligence sharing, it is the bureaucracy that will be responsible for the actual implementation of that policy. Therefore, how to convince the policy level to agree to cooperate is one major task, it is another even greater task to persuade the bureaucracy to carry out the agreement and put intelligence sharing in practice. This is a kind of dual challenge that Taiwan has been facing.

V. Solutions for a Better Intelligence Sharing

It takes efforts and time to produce, and receive, the intelligence that is often deemed as indispensable in planning and executing major security investigations or policing operations. Hence, there is little doubt that information is the key to the success of the policy process, including policy making and policy implementation. However, information or intelligence does not come with no cost;

in another word, information is power and intelligence is commodity.²⁸ Therefore, a better intelligence collection and analysis product will require greater investment in terms of, among others, quality human resources, sufficient operational funds, state-of-art technological support, and reformed organizational management. When it comes to a better intelligence sharing domestically or internationally, more investment needs to be done.²⁹

Firstly, a strong political will and policy support. Cooperation in information and intelligence sharing with other agencies or foreign counterparts is almost impossible without a clear and strong political will, which is essential to ensure the policy process to be proceeded to the end. In addition, it also can make coordination in intelligence sharing among participating members easier and faster if the policy is endorsed by the political will.

Secondly, a workable mechanism for intelligence sharing. While there are several types of information and intelligence sharing, a fusion network with technical support of internet technology has been regarded as a more effective model of information and intelligence sharing. The fusion network model that stresses the

²⁸ Calvert Jones, "Intelligence Reform: The Logic of Information Sharing," *Intelligence and National Security*, Vol. 22, No. 3 (June 2008), pp. 384-401.

²⁹ Patrick Miller, *How Can We Improve Information Sharing among Local Law Enforcement Agencies?* (Monterey CA: the Naval Postgraduate School, September 2005); United States Government Accountability Office, *Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective*, March 26, 2013, GAO-13-233. Available on: <<https://www.gao.gov/assets/660/652995.pdf>>, accessed on January 3, 2019.

concept of network transmitting information was introduced in the wake of September 11 terrorist attacks as a response to the barriers in intelligence sharing among partners. The effectiveness of the model will be enhanced with the use of communication and internet technology that will allow information to be better collected, identified, stored, sorted, compared, analyzed, transmitted and shared.

Thirdly, a combination of institutional structure and multiple incentives. All organizations or mechanisms are managed by individuals who will be affected by the nature, shift, loading, and satisfaction of the work. A human resource management system that will provide multiple options of incentive, including, but not limited to, overtime payment, paid or unpaid leaves, advancement track or job rotation, overseas trip, and academic training should be able to reduce the job inertia or resistance to any innovation and be able to promote the morale and output of the work force.

Fourthly, a better strategy of managing bureaucratic politics and organizational interests. The problem of bureaucratic politics can be found in many, if not all, organizations and it is almost an inevitable barrier that will affect the quality of information and intelligence sharing. While raising the awareness of the causes and effects of bureaucratic politics through lectures and group dynamics is not new or strange to managers of organization, it is more important to learn to live with and try to alleviate its negative effect.

Lastly, while Taiwan will continue to broaden and deepen substantial relations with its partners, due to Beijing's "One China" stance that will restrict Taiwan's international space, informal channels of information and intelligence sharing seems to be a

more promising option for Taiwan to invest its efforts and resources. Looking into the future, this cooperative relationship has to be based on the principles of reciprocity and mutual trust.

IV. Conclusion

It takes resources and strategies to fight against TOC. In addition to policy commitment, professional manpower, sufficient funds, and technical support, the importance of a good strategy in constructing an effective framework of cooperative mechanism with an aim to facilitating information exchange and intelligence sharing cannot be overemphasized.

This paper has discussed the role of intelligence and its use in fighting against TOC, the establishment of intelligence sharing and its barriers and challenges, and the solutions for a better intelligence sharing. It also takes Taiwan as one example to illustrate and explain how it fights against TOC with the use of intelligence and what kind of barriers and challenges it faces. There remain many questions to be explored and answered. This paper is only an initial step toward a better understanding the reality and problems that information and intelligence sharing has been facing.

(收稿：2019年10月3日；第一次修正：11月30日；接受：12月23日)

Reference

Books or the Chapter in the Book

- Chido, Diane E. 2018. *Intelligence Sharing, Transnational Organized Crime and Multinational Peacekeeping*. Carlisle, PA: Palgrave Pivot.
- Lowenthal, Mark M. 2015. *Intelligence: From Secrets to Policy*. Thousand Oaks, CA: SAGE.
- Miller, Patrick. September 2005. *How Can We Improve Information Sharing among Local Law Enforcement Agencies?* Thesis, Naval Postgraduate School.
- Walsh, James Igoe. 2009. *The International Politics of Intelligence Sharing*. New York: Columbia University Press.

Journal Essays

- Abrahamson, Douglas Edward and Jane Goodman-Delahunty. January-March 2014. "Impediments to Information and Knowledge Sharing Within Policing: A Study of Three Canadian Policing Organizations," *SAGE Open*, pp. 1-17.
- Chermak, Steven. June 2013. "Law Enforcement's Information Sharing Infrastructure: A National Assessment." *Police Quarterly*, Vol. 16, No. 2, pp. 211-244.
- Fägersten, Björn. December 2010. "Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol," *Intelligence and National Security*, Vol. 25, No. 4, pp. 500-520.
- Field, Antony. October 2009. "Tracking Terrorist Networks: Problems of Intelligence Sharing within the UK Intelligence Com-

- munity,” *Review of International Studies*, Vol. 35, Issue 4, pp. 997-1009
- Jones, Calvert. June 2008. “Intelligence Reform: The Logic of Information Sharing,” *Intelligence and National Security*, Vol. 22, No. 3, pp. 384-401.
- Lupsha, Peter A. Spring 1996. “Transnational Organized Crime versus the Nation-State,” *Transnational Organized Crime*, Vol. 2, No. 1, pp. 43-45.
- Matei, Florina Cristian (Cris). August 2009. “The Challenges of Intelligence Sharing in Romania,” *Intelligence and National Security*, Vol. 24, No. 4, pp. 574-585.
- McGill, Anna-Katherine Staser. Summer 2012. “Challenges to International Counterterrorism Intelligence Sharing,” *Global Security Studies*, Vol. 3, Issue 3, pp. 76-86.
- Mueller, Gerhard O.W. Autumn/Winter 1998. “Transnational Crime: Definitions and Concepts,” *Transnational Organized Crime*, Vol. 4, No. 3&4, pp. 13-14.
- Pfeifer, Joseph W. October 2012. “Network Fusion: Information and Intelligence Sharing for a Networked World,” *Homeland Security Affairs*, Vol. 8, Article 17. Available on: < <https://www.hsaj.org/articles/232> >, accessed on January 3, 2019.
- Rickards, Claire. March 2016. “What are the Barriers to Gathering and Sharing Organised Crime Intelligence: An Australian Perspective,” *The European Review of Organised Crime*, Vol. 3, No. 1, pp. 78-104.
- Seagle, Adriana N. May 2015. “Intelligence Sharing Practices Within NATO: An English School Perspective.” *International*

Journal of Intelligence and CounterIntelligence, Vol. 28, No. 3, pp. 557-577.

Svendsen, Adam D.M. September 2009. "Connecting Intelligence and Theory: Intelligence Liaison and International Relations." *Intelligence and National Security*, Vol. 24, No. 5, pp. 700-729.

Taylor, Robert W. and Amanda L. Russell. October 2011. "The Failure of Police 'Fusion' Centers and the Concept of a National Intelligence Sharing Plan," *Police Practice and Research*, Vol. 13, No. 2, pp. 184-200.

Walsh, F. Patrick and Seumas Miller. January 2016. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden," *Intelligence and National Security*, Vol. 31, No. 3, pp. 345-368.

Hulnick, Arthur S. December 2006. "What's Wrong with the Intelligence Cycle," *Intelligence and National Security*, Vol. 21, No. 6, pp. 959-979.

Walsh, James Igoe 2006. "Intelligence-Sharing in the European Union: Institutions Are Not Enough." *JCMS: Journal of Common Market Studies*, Vol. 44, No. 3, pp. 625-43.

Resources from the Internets

Ballast, Jan. September 2017. "Trust (in) NATO - The Future of Intelligence Sharing within the Alliance," Research Paper No. 140. Rome: Research Division, NATO Defense College. Available on: < <https://css.ethz.ch/en/services/digital-library/publications/publication.html/6cc75c52-8da8-4abf-a4ce-0824e3e>

448aa>, accessed on January 13, 2019

Best, Richard. A. 13 February 2007. *Sharing Law Enforcement and Intelligence Information: The Congressional Role*. Washington, DC: Congressional Service Report, RL33873. Available on: <<https://fas.org/sgp/crs/intel/RL33873.pdf>>, accessed on January 25, 2019.

Corera, Gordon. January 2016. “Why Intelligence Sharing Still Has a Long Way to Go,” BBC News, <<http://www.bbc.com/news/world-europe-35154640>>, accessed on May 29, 2018.

European Network and Information Security Agency (ENISA). September 8, 2010. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. available on: <<https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>>, accessed on January 11, 2019.

FBI. December 2003. *The Federal Bureau of Investigation’s Efforts to Improve the Sharing of Intelligence and Other Information*. Audit Report 04-10. Available on: <<https://oig.justice.gov/reports/FBI/a0410/final.pdf>>, accessed on January 5, 2019.

IACP. August 2002. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing At the Local, State and Federal Levels*. Available on: <<http://www.justiceacademy.org/iShare/Library-COPS/cops-w0418-pub.pdf>>, accessed on January 2, 2019..

Maxwell, Nick J and David Artingstall. October 2017. *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*. RUSI Occasional Paper. available on: <<https://rusi>.

org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf>, accessed on January 2, 2019.

Peteritas, Brian. June 2013. “Fusion Centers Struggle to Find Their Place in the Post-9/11 World,” *Governing the States and Localities*, <<http://www.governing.com/topics/public-justice-safety/gov-fusion-centers-post-911-world.html>>, accessed on May 29, 2018.

Realuyo, Celina B. August 2013. *Collaborating to Combat Illicit Networks Through Interagency and International Efforts*. Occasional Paper, William J. Perry Center for Hemispheric Defense Studies. Available on: <https://www.williamjerrycenter.org/sites/default/files/publication_associated_files/Collaborating%20to%20Combat%20Illicit%20Networks%20through%20Interagency%20and%20International%20Efforts.pdf>, accessed on January 4, 2019.

Sander, Todd. 2010. *Law Enforcement Information Sharing and the Implications for Local Government (A Technical Reference)*, digital communities, 2010. <https://cdn.ymaws.com/www.ijis.org/resource/collection/232074EF-6453-4014-BC4E-018BF818D291/Law_Enforcement_Information_Sharing_and_the_Implications_for_Local_Government.pdf>, accessed on May 29, 2018.

U.S. DoJ. October 2003. *The National Criminal Intelligence Sharing Plan-Solutions and Approaches for a Cohesive Plan to Improve Our Nation’s Ability to Develop and Share Criminal Intelligence*.

U.S. White House. October 2007. *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing*.

United States Government Accountability Office. March 26, 2013. *Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective*. GAO-13-233. Available on: <<https://www.gao.gov/assets/660/652995.pdf>>, accessed on January 3, 2019.

United States Government Accountability Office. October 12 2011. *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*. GAO-12-144T, available on: <<https://www.gao.gov/new.items/d12144t.pdf>> , accessed on January 3, 2019.