美國情資融合中心的發展與評估
The U.S. Fusion Centers: Development and Assessment

王政(Cheng Wang)
中央警察大學公共安全學系助理教授

提　　要

美國在911恐怖攻擊以後，爲強化國內情報功能與促進情報與執法機關的資訊分享機制，設置了各州與地方情資融合中心，目的在整合政府機關的資源、專業與資訊，以便對各種犯罪及恐怖活動進行偵測、預防、調查及回應。本文探討911事件以後美國國內情報策略轉變，情資融合中心的設立背景、發展過程及運作機制，並摘述官方及民間機構對情資融合中心的調查與評估，最後歸納出情資融合中心值得借鏡與注意避免之處。

關鍵詞：情資融合中心、國土安全情報、國土安全資訊網絡、資訊分享與分析中心

Abstract

In the aftermath of the September 11 terrorist attacks, the United States established state and local fusion centers to strengthen domestic intelligence capabilities and promote information sharing among intelligence and law enforcement agencies, aiming at detecting, preventing, investigating, and responding to criminal and terrorist activities. This paper discusses the adjustment of the U.S. domestic intelligence strategy, explains the creation and development of fusion centers and their operations, summarizes reviews and performance evaluations conducted by various institutions, and finally lists lessons learned from the practice of fusion centers.

Keywords: Fusion Centers, Homeland Security Intelligence, Homeland Security Information Network (HSIN), Information Sharing and Analysis Centers (ISACs)

壹、前　　言

美國在911恐怖攻擊以後，隨即進行了情報體系的改革與資訊分享的促進，聯邦及州政府發起了一股前所未有的行動，對潛藏的恐怖威脅進行偵測與防範，其中的核心政策之一當屬「各州與地方情資融合中心」(state and local fusion centers)的建置。截至2013年6月止，全美國及其海外屬地（如關島、波多黎各、美屬維京群島）共有78個情資融合中心，這些中心獲得行政部門及國會的支持，但其組織型態、目標與任務卻不盡相同，且所受的監督十分有限，導致其績效難以評估，因而違反隱私權與公民自由的情

事亦時有所聞。

情資融合中心並非全新的概念，它是美國過去幾十年來各州和地方執法機關情報蒐集活動的具體化，不僅屬於「國內情報」(domestic intelligence)的一環，更是「國土安全情報」(Homeland Security Intelligence)的具體實踐。在反恐、犯罪偵查、緊急應變及災害防救等事項，具有舉足輕重的功能。因此，本論文將從911事件以後美國國土安全情報的概念與體系之建構為起點，進而說明情資融合中心的發展過程，再探討其運作模式與面臨問題，並摘述美國行政、立法機關、學術機構、智庫對情資融合中心的調查與評估報告，期盼我國安與執法機關能從美國的實踐經驗中獲得若干啟示與借鏡。

貳、911事件後國土安全情報的重視

冷戰時期，由於美、蘇兩國軍事競爭及外交對抗的需要，促使美國發展出現代化的國外情報(foreign intelligence)與軍事情報(military intelligence)體系。至於國內情報(domestic intelligence)則相對弱化，這是受到歷史因素及憲政精神的影響，以及1960年代聯邦調查局(FBI)對於國內政治活動的監控受到國會調查與民眾抨擊的影響。由於國內情報蒐集活動的萎縮，最後甚至造成國土安全的漏洞。在1993年紐約世貿大樓爆炸案及1995年奧克拉荷馬市政大樓爆炸案以後，各種調查委員會的報告和非政府組織紛紛建議聯邦政府重視國土安全的問題，特別是強化情報蒐集與分析的能力。[1]

2001年發生的911恐怖攻擊事件，撼動了美國以冷戰思維所建構的情報與國家安全體系。為因應具有跨國性及網絡性特徵的恐怖主義威脅，美國政府於911事件以後提升了預防與偵查恐怖主義的作為，並且建構國土安全情報(homeland security intelligence)體系，強化美國境內或關於美國人的資訊的蒐集與分析，包括個人活動的監視，書信、電話、網路通訊內容的蒐集與分析。此外，政府也大量使用由第三者所提供及分析的個人資訊，以及運用資料探勘(data mining)和電腦輔助風險評估(computer-aided risk assessment)等技術，用來過濾具有恐怖威脅的個人。[2]由於「情資融合中心」屬於國土安全情報體系的一環，茲將國土安全情報的概念與體系做一簡要說明。

一、國土安全情報概念

「國土安全情報」雖然尚未由法律條文加以定義，惟就情報內容而言，朗多(Mark A. Randol)認為，「國土安全情報」應可被視為「國土安全資訊」(homeland security information)，因為「國土安全法」(Homeland Security Act 2002)對國土安全資訊的定義如下：「任何聯邦、州、地方機關擁有之下列資訊：⑴關於恐怖份子活動的威脅資訊；⑵關於防止、攔截、瓦解恐怖份子活動能力的資訊；⑶有關促進辨識或調查恐怖份子或恐怖組織的資訊；⑷能夠改善對恐怖攻擊回應

1 Bruce Berkowitz, "Homeland Security Intelligence: Rationale, Requirements, and Current Status," in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovations* (Washington, DC: Georgetown University Press, 2008), pp. 281-283.

2 Daniel B. Prieto, *War about Terror: Civil Liberties and National Security after 9/11* (New York: Council on Foreign Relations, 2009), p. 44.

能力的資訊」。[3]

其次，就情報來源而言，不論是由聯邦或地方政府、官方或民間機構所蒐集之資訊，包含情報機關蒐集的國家安全情報、各級政府執法機關掌握的犯罪情資、民間部門所提供之關鍵基礎設施風險資訊，都屬於國土安全情報，目的均為防止恐怖主義攻擊。[4]

由此可見，國土安全情報是一種統合聯邦與地方、國內與國外、不同情報機構間的情報作為，目的在透過資訊的蒐集、分析、傳遞、分享，期能偵測與打擊恐怖主義，降低美國對恐怖主義的脆弱性，並且在攻擊發生後能將損害降至最低，儘速復原。

二、國土安全情報體系

911事件以後，美國於2002年成立了國土安全部(Department of Homeland Security, DHS)，將22個聯邦機關整合成為一個單一的部會，成為反恐的第一線單位。國土安全部成立時，即設置了「情報分析與基礎設施防護處」(Directorate for Intelligence Analysis and Infrastructure Protection, IAIP)，2004年12月17日國會通過「情報改革與恐怖主義預防法」(Intelligence Reform and Terrorism Prevention Act of 2004)，國土安全部復將「情報分析與基礎設施防護處」改為「情報分析局」(Office of Intelligence and Analysis, I&A)，同時成立了「資訊分享環境」(Information Sharing Environment, ISE)、「各州與地方的情資融合中心」(State and Local Fusion Center)、「跨機關威脅評估協調小組」(Interagency Threat Assessment Coordination Group, ITACG)等組織。[5]

在國土安全部所屬機構中，海關暨邊境保安局(U.S. Customs and Border Protection, CBP)設有「情報與調查聯絡處」(Office of Intelligence and Investigative Liaison, OIIL)、「全國查緝鎖定中心」(National Targeting Center, NTC)、「邊境地區情報中心」(Border Field Intelligence Center, BORFIC)；移民及海關執法局(Immigration and Customs Enforcement, ICE)設有「國土安全調查情報處」(ICE Homeland Security Investigations Intelligence Office, HSI-Intel)；運輸安全管理局(Transportation Security Administration, TSA)設有「情報分析處」(Office of Intelligence and Analysis, TSA-OIA)；美國海岸防衛隊(US Coast Guard) 設有「情報與犯罪調查處」(Intelligence & Criminal Investigations)；密勤局(US Secret Service, USSS)設有「國家威脅評估中心」(National Threat Assessment Center, NTAC)，在在顯示國土安全部強化情報蒐集與分析的決心。[6]

至於聯邦調查局(FBI)也進行了一連串的情報改革措施，例如，在2005年9月成立「國家安全處」(National Security Branch, NSB)，負責國內反恐、反情報、大規模殺傷性武器等業務。NSB並設有「恐怖份子過濾中心」(Terrorist Screening Center)，提供各州及地方

3 Mark A. Randol, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches* (Report No. RL33616) (Washington, DC: Congressional Research Service, 2009), p. 9.

4 同註3，頁11-14。

5 Mark A. Randol, *Homeland Security Intelligence Enterprises: Operational Overview and Oversight Challenges for Congress* (Report No. RL40602) (Washington, DC: Congressional Research Service, 2010)

6 同註5。

政府執法單位所需的行動情報。

此外，為改善911以前情報體系各自為政的問題，而於2004年設立的「國家情報總監辦公室」(Office of Director of National Intelligence, ODNI)，亦設有「國家反恐中心」(National Counterterrorism Center, NCTC)，集合中央情報局、聯邦調查局、國防部及其他情報機關的專家，共同促進反恐情報的協調與分享。

最後，2002年美國國防部成立「北方司令部」(US Northern Command)，北方司令部設有「情報處」(Intelligence Directorate)，負責國土安全情報業務，尤其是與聯邦、各州及地方執法機關進行情資分享。目前聯邦調查局(FBI)、中央情報局(CIA)、國家安全局(National Security Agency, NSA)，國防情報局(Defense Intelligence Agency, DIA)、國家地理情報局(National Geospatial-Intelligence Agency, NGA)等機關在北方司令部內均設有辦公處，共同分享「每日情報簡報」(daily intelligence briefings)。[7]

由以上911事件以後所建構之國土安全情報體系觀之，其目的在消除反恐情報資訊分享的障礙、促進反恐行動的協調。其中由國土安全部大力支持與提倡的「各州與地方的情資融合中心」，尤為反恐資訊整合與分享的樞紐，其功能甚至擴及犯罪偵查與緊急應變，在整個國土安全情報體系中，具有關鍵性之地位。

參、情資融合中心簡介

一、情資融合中心的定義

依據美國司法部(Department of Justice)與國土安全部於2006年8月公布的「情資融合中心指導方針」(Fusion Center Guidelines)，情資融合中心是「兩個或兩個以上的機關共同合作，提供資源、專門技術和資訊給一個中心，其目的在強化有關犯罪及恐怖活動的偵查、預防、調查與反應能力。」[8]

美國智庫「憲法計畫」(The Constitution Project)則指出，「情資融合中心雖有不同形式，但基本功能仍是做為資訊分享中心，目的在集合聯邦、各州與地方執法和情報機關甚至其他政府部門、軍隊、民間部門的知識與專門技術」。[9]

圖1顯示的是情資融合過程(fusion process)的概念，所謂「融合」，是將各級政府（包括聯邦、各州、地方）的執法機關，以及消防、緊急管理、醫療、交通、矯治等單位，甚至民間部門的資訊，經由平臺集中合併，透過關聯性分析、摘錄、衝突排解、粹取等過程，將資料轉換成知識，再加上人為分析，即成為有價值之情報產品，並可主動分送情資，以達預警效果，或在事件發生

7 "United States Northern Command," *Wikipedia*, <http://en.wikipedia.org/wiki/United_States_Northern_Command>（檢索日期：2013年6月12日）

8 US Department of Justice and US Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, Aug, 2006, p. 2. 原文為："a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."

9 The Constitution Project, *Recommendations for Fusion Centers: Preserving Privacy and Civil Liberties while Protecting against Crime and Terrorism* (Washington, DC: The Constitution Project, 2012), p. 6.

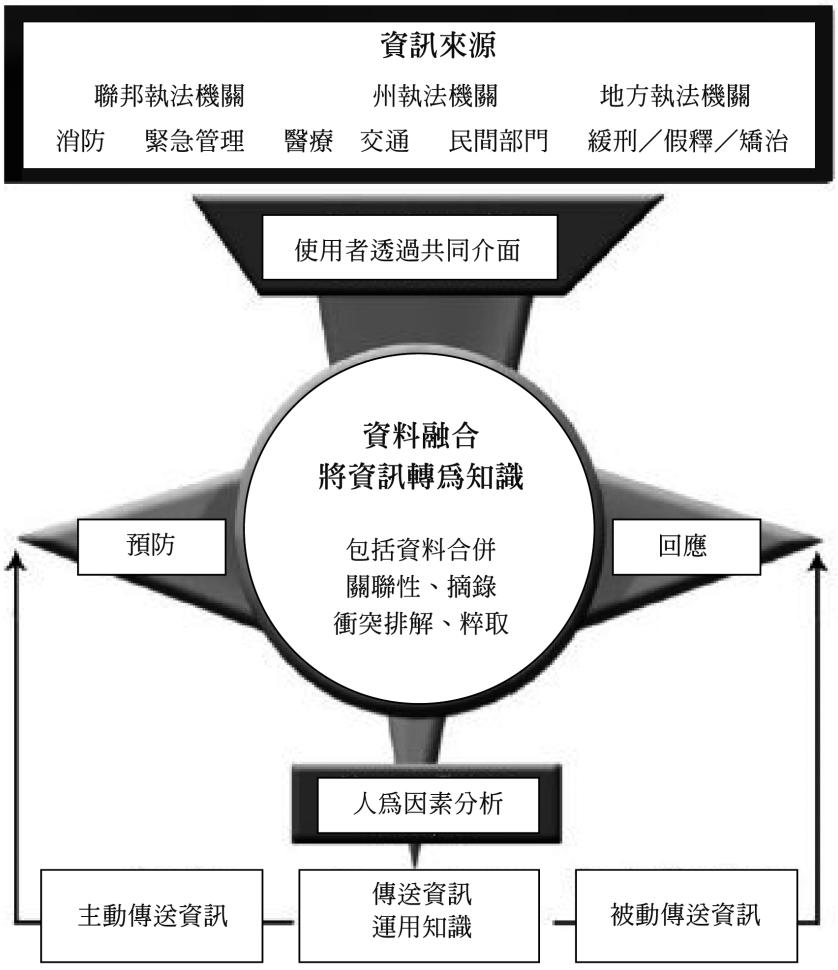

圖1　情資融合過程圖

資料來源：US Department of Justice and US Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, Aug, 2006, p. 11.

後提供情資，協助犯罪偵查或災後處理。

二、情資融合中心的由來與發展過程

羅林斯(John Rollins)指出，情資融合中心並非全新的概念，它是911事件以前各州和地方執法機關情報活動的延伸，因為大部分的州警察或調查機關的情報或分析單位已經運作了幾十年，大部分情資融合中心即由此演變而來。儘管如此，情資融合中心在國土防衛(homeland defense)與執法(law enforcement)的哲學上，還是象徵著一個新的轉變。第一，情資融合中心的興起，象徵著各州及地方執法機關在國土防衛與安全事務上扮演著重要的角色；第二，情資融合中心成為美國打擊全球恐怖主義上一個積極主動、先發制人的工具(proactive tool)。[10]

伊克(Kevin D. Eack)亦認為，情資的運用不是新的創舉，全美各州或地方政府執法機關運用情報打擊犯罪已有數十年歷史，這些情報內容涵蓋暴力幫派、毒品販運、賣淫、武器走私、竊盜等，一些大都市或郡(county)警察局均設有情報單位，至於資訊分享、將威脅重點轉移到反恐，才是911以後情資融合中心成立的新使命。[11]

根據莫那漢(Torin Monahan)的說法，加州在1996年成立的「洛杉磯郡恐怖主義預警中心」(Los Angeles County Terrorism Early Warning Center)，堪稱是美國第一個情資融合中心，隨著2004年7月22日「911委員會報告」(The 9/11 Commission Report)公布以後，各州陸續開始設立情資融合中心，但大部分

10 John Rollins, *Fusion Centers: Issues and Options for Congress* (Report No. RL34070) (Washington, DC: Congressional Research Service, 2008), pp. 1-2.

11 Kevin D. Eack, "State and Local Fusion Centers: Emerging Trends and Issues," *Homeland Security Affairs*, Supplement No. 2, 2008, pp. 1-2.

是和聯邦調查局的「聯合反恐小組」(Joint Terrorism Task Force, JTTF)聯合，後來，許多情資融合中心的定位陸續擴展成為「全災害」(all hazards)、「全威脅」(all threats)，例如對環境災害的反應，及對非恐怖主義的犯罪進行調查。[12]

雖然情資融合中心是因應911而生，並由國土安全部所支持，但直到2005年才開始大幅成長。歐巴馬總統(Barack Obama)於2008年上任以後，情資融合中心更被視為強化國內治安的重要工具，歐巴馬政府對情資融合中心情有獨鍾的原因，主要是其監視行為看起來比較消極、不那麼實質、而且比較客觀(passive, disembodied, and objective)，屬於一種軟性監視(soft surveillance)，因為針對抽象的資料進行監視，或稱為資料監視(data veillance)，相對於人身或財產搜索、監視器、監聽等方法，民眾感覺起來比較不具侵入性和威脅性。此種思維正好呼應了歐巴馬在國內外大量使用無人飛機(unmanned aerial vehicles, UAVs)的政策偏好。[13]

在歐巴馬政府的內閣中，現任國土安全部部長那波利塔諾(Janet Napolitano)在擔任亞歷桑納州州長任內曾建立的聲譽卓著的「亞歷桑納反恐資訊中心」(Arizona Counter Terrorism Information Center)，因此，那波利塔諾一直是情資融合中心的倡導者。另外，美國司法部長霍德(Eric Holder)也一再強調情資融合中心對於反恐戰爭的重要性，司法部亦承諾提供更多經費支持情資融合中心。[14]

羅林斯認為促成情資融合中心迅速發展的原因有三：第一，情報導向警政(Intelligence-Led Policing)的運用。[15] 情報導向警政最早在英國肯特郡(Kent, England)實施，1990年代肯特郡實施情報導向警政，三年後犯罪率下降了24%，故此種模式鼓勵了美國，同時期盛行的社區導向警政(Community-Oriented Policing)及問題導向警政(Problem-Oriented Policing)，也高度依賴情報與狀況警覺(situational awareness)，做為預先防範的執法策略。[16]

第二，「高度密集販毒區域中心」(The High Intensity Drug Trafficking Area Center, HIDTA Center)也影響情資融合中心的設立，自1990年起，美國共有28個區域被列為「高度密集販毒區域」，並由「國家毒品管制政策中心」(Center for National Drug Control Policy)設立「高度密集販毒區域中心」，透過跨部門運作，結合聯邦、各州及地方執法機關，共同打擊毒品犯罪。911之前，有幾個州政府看到「高度密集販毒區域中心」的成效，因而在打擊犯罪上仿效該制度，911事件以後，這些制度促成了情資融合中心的設立，甚至有些情資融合中心就設在「高度密集販毒區域中心」內。[17]

第三，來自基層的支持(grassroots

12 Torin Monahan, "The Future of Security Surveillance Operations at Homeland Security Fusion Centers," *Social Justice*, Vol. 37, No. 2-3, 2010, p. 85.

13 同註12，頁85-86。

14 同註12。

15 John Rollins, *Fusion Centers: Issues and Options for Congress*, p.16.

16 US Department of Justice, *Intelligence-Led Policing: The New Intelligence Architecture*, Sep, 2005, p. 9.

17 John Rollins, *Fusion Centers: Issues and Options for Congress*, pp. 16-17.

support)也是情資融合中心迅速成長的因素之一。「高度密集販毒區域中心」是由聯邦政府出資與管理，但由各州及地方政府的政治領袖在911後也發出一股支持以情報協助執法的呼聲，代表地方政府願意擔負國家安全的責任，這是觀念上的一大改變，因為傳統上國家責任一直被認為應該由聯邦政府承擔。[18] 例如，2006年全美州長協會(National Governors Association, NGA)針對各州負責國土安全業務的主管做了一份問卷調查，有70%的受訪者認為「發展情資融合中心」是該州的優先任務。[19] 此外，全美州長協會在2007年公布的「州長國土安全指南」(A Governor's Guide to Homeland Security)亦指出，情報與資訊分享，特別是州政府層級的情資融合中心，將是新任州長的10大工作重點之一。[20]

尤其重要的是，情資融合中心受重視，代表各州、地方、原住民部落、救難先遣人員(first responder)、其他公、私部門等機構，在資訊蒐集、威脅辨識、威脅評估上的角色和地位受到肯定，因為這些人員與社區的關係密切，最適合做為國家安全的耳目。[21]

三、情資融合中心的現況

截至2013年6月止，全美國及其海外屬地（如關島、波多黎各、美屬維京群島）共有78個情資融合中心，其中包括53個「主要情資融合中心」(Primary Fusion Centers)及25個「被認可之情資融合中心」(Recognized Fusion Centers)。「主要情資融合中心」是由各州或地方政府所有，經由該州州長指定，在該州或地區作為接收、分析、蒐集、分享威脅資訊的重心，並且優先享有聯邦政府的資源，包括人員派遣及資料系統。[22] 由附錄一顯示，各州情資融合中心的名稱並不一致，除了「情資融合中心」外，尚有資訊與分析中心(Information and Analysis Center)、反恐資訊中心(Counter Terrorism Information Center)、威脅評估中心(Threat Assessment Center)、資訊分享與分析中心(Information Sharing and Analysis Center)、犯罪情報中心(Criminal Intelligence Center)、協調與分析中心(Coordination and Analysis Center)、情報運作中心(Intelligence Operations Center)、全威脅情報中心(All-Threat Intelligence Center)等。

至於「被認可之情資融合中心」，則是由各州政府所指定，在主要城市設立之情資

18 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 17.

19 National Governors Association, "2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships," *NGA Center for BEST PRACETICES*, Apr 3 2006, p.3, <http://www.nga.org/files/live/sites/NGA/files/pdf/0604HLSDIRSURVEY.pdf>（檢索日期：2013年6月15日）

20 National Governors Association, "A Governor's Guide to Homeland Security," *NGA Center for BEST PRACETICES*, 2007, p. 8, <http://www.nga.org/files/live/sites/NGA/files/pdf/0703GOVGUIDEHS.PDF>（檢索日期：2013年6月15日）

21 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 7.

22 Department of Homeland Security, "Fusion Center Locations and Contact Information, Primary Fusion Centers," *Homeland Security*, <http://www.dhs.gov/fusion-center-locations-and-contact-information>（檢索日期：2013年6月25日）

融合中心，彼等雖非「主要情資融合中心」，但同樣獲得聯邦政府之認可。[23]「被認可之情資融合中心」也有不同的名稱，例如區域情報中心(Regional Intelligence Center)、情報交換中心(Intelligence Exchange)、犯罪預防與資訊中心(Crime Prevention and Information Center)、區域恐怖主義預警組(Regional Terrorism Early Warning Group)、區域情報聯合中心(Joint Regional Intelligence Center)、執法協調中心(Law Enforcement Coordination Center)、威脅分析中心(Threat Analysis Center)等（參見附錄1）。

附錄1　全美情資融合中心一覽表（截至2013年6月）

一、主要情資融合中心(Primary Fusion Centers)
1. Alabama Fusion Center
2. Alaska Information and Analysis Center
3. Arizona Counter Terrorism Information Center
4. Arkansas State Fusion Center
5. California State Threat Assessment Center
6. Colorado Information Analysis Center
7. Connecticut Intelligence Center
8. Delaware Information and Analysis Center
9. Florida Fusion Center
10. Georgia Information Sharing and Analysis Center
11. Hawaii State Fusion Center
12. Idaho Criminal Intelligence Center
13. Illinois Statewide Terrorism and Intelligence Center
14. Indiana Intelligence Fusion Center
15. Iowa Intelligence Fusion Center
16. Kansas Intelligence Fusion Center
17. Kentucky Intelligence Fusion Center
18. Louisiana State Analytical & Fusion Exchange
19. Maine Information and Analysis Center
20. Mariana Regional Fusion Center (Guam)
21. Maryland Coordination and Analysis Center
22. Massachusetts Commonwealth Fusion Center
23. Michigan Intelligence Operations Center
24. Minnesota Fusion Center
25. Mississippi Analysis and Information Center
26. Missouri Information Analysis Center
27. Montana All-Threat Intelligence Center
28. Nebraska Information Analysis Center
29. New Hampshire Information and Analysis Center
30. New Jersey Regional Operations Intelligence Center
31. New Mexico All Source Intelligence Center
32. New York State Intelligence Center
33. North Carolina Information Sharing and Analysis Center
34. North Dakota State and Local Intelligence Center
35. Ohio Strategic Analysis and Information Center
36. Oklahoma Information Fusion Center

23 Department of Homeland Security, "Fusion Center Locations and Contact Information, Recognized Fusion Centers," *Homeland Security*, <http://www.dhs.gov/fusion-center-locations-and-contact-information>（檢索日期：2013年6月25日）

37. Oregon Terrorism Information Threat Assessment Network
38. Pennsylvania Criminal Intelligence Center
39. Puerto Rico National Security State Information Center
40. Rhode Island State Fusion Center
41. South Carolina Information and Intelligence Center
42. South Dakota Fusion Center
43. Southern Nevada Counter-Terrorism Center (Las Vegas, Nevada)
44. Tennessee Fusion Center
45. Texas Fusion Center
46. U.S. Virgin Islands Fusion Center
47. Utah Statewide Information and Analysis Center
48. Vermont Information and Analysis Center
49. Virginia Fusion Center
50. Washington Regional Threat and Analysis Center (Washington, D.C.)
51. Washington State Fusion Center
52. West Virginia Intelligence Fusion Center
53. Wisconsin Statewide Information Center

二、被認可之情資融合中心(Recognized Fusion Centers)

1. Austin Regional Intelligence Center; Austin, TX
2. Boston Regional Intelligence Center; Boston, MA
3. Central California Intelligence Center; Sacramento, CA
4. Central Florida Intelligence Exchange; Orlando, FL
5. Chicago Crime Prevention and Information Center; Chicago, IL
6. Cincinnati/Hamilton County Regional Terrorism Early Warning Group; Cincinnati, OH
7. Delaware Valley Intelligence Center; Philadelphia, PA
8. Detroit and Southeast Michigan Information and Intelligence Center; Detroit, MI
9. Houston Regional Intelligence Service Center; Houston, TX
10. Kansas City Terrorism Early Warning Fusion Center; Kansas City, MO
11. Los Angeles Joint Regional Intelligence Center; Los Angeles, CA
12. El Paso Fusion Center (MATRIX); El Paso, TX
13. Metro Operations Support and Analytical Intelligence Center; Dallas, TX
14. Nevada Threat Analysis Center; Carson City, NV
15. North Central Texas Fusion Center; McKinney, TX
16. Northeast Ohio Regional Fusion Center; Cleveland, OH
17. Northern California Regional Intelligence Center; San Francisco, CA
18. Northern Virginia Regional Intelligence Center; Fairfax, VA
19. Orange County Intelligence Assessment Center; Orange County, CA
20. San Diego Law Enforcement Coordination Center; San Diego, CA
21. Southeast Florida Fusion Center; Miami, FL
22. Southeastern Wisconsin Threat Analysis Center; Milwaukee, WI
23. Southwest Texas Fusion Center; San Antonio, TX
24. Southwestern PA Region 13 Fusion Center; Pittsburgh, PA
25. St. Louis Fusion Center; St. Louis, MO

資料來源：美國國土安全部網頁，2013年6月25日下載自<http://www.dhs.gov/fusion-center-locations-and-contact-information>

肆、情資融合中心的運作

一、人員

情資融合中心的人員數目因規模大小而不等，從3人到250人都有，一般而言，專職人員平均在30人左右，兼職人員數量則界乎於0到100之間。整體而言，執法人員是情資融合中心的主力，這些「編制內警察」

(sworn officer)[24] 是由州警局或調查局派遣到情資融合中心，但近年來情資融合中心也使用國土安全基金，雇用「非編制內警察」(non-sworn officer)，如犯罪或情報分析人員、專案支援人員、策略分析人員等。[25]

情資融合中心的人員也包括各州或地方執法機關及衛生、消防、緊急救護等單位，惟國土安全部、聯邦調查局、緝毒局(Drug Enforcement Agency)、移民及海關執法局(Immigration and Customs Enforcement)、海關暨邊境保安局(Customs and Border Protection)亦派遣分析師、語言專家、幹員進駐各情資融合中心，也有大約30%的情資融合中心與聯邦機構或國民警衛隊（或稱為國民兵，National Guard）合作。[26]

二、預算

大多數的情資融合中心都是由州政府管轄，並由州警察或州調查部門負責運作，而且座落在人口密集、關鍵基礎設施眾多的大城市，只有極少數情資融合中心是由地方政府所管轄。[27] 因此，情資融合中心的主要(80%)預算來自於各州及地方政府，至於由聯邦所補助的預算主要來自於國土安全部，由國土安全部「2013年全國整備補助計畫」(FY 2013 National Preparedness Grant Program)內容觀之，對情資融合中心的財政補助包括：國土安全補助計畫(Homeland Security Grant Program, HSGP)、州國土安全計畫(State Homeland Security Program, SHSP)、都市地區安全倡議(Urban Areas Security Initiative, UASI)、磐石計畫(Operation Stonegarden, OPSG)、部落國土安全補助計畫(Tribal Homeland Security Grant Program, THSGP)等。[28]

然而，由於國土安全部的「情報分析局」(Office of Intelligence and Analysis)為美國情報體系(U.S. Intelligence Community)16個情報機關之一，該局的預算被列為機密預算，因而國土安全部對各州情資融合中心的預算也被列為機密。一般相信，由於美國政府財政赤字過大，未來如果聯邦的補助停止，情資融合中心雖不至於裁撤，但若僅依靠地方政府的財力支援，其運作必然會大受影響。

三、法律依據

目前大多數的情資融合中心的設立並無特定的法律依據，即無州議會通過的法律或州長簽署的行政命令，其運作主要是由各參與機關共同簽署的了解備忘錄(Memoranda of Understanding)，或依據各州國土安全業務主管簽署的政策備忘錄(policy memorandum)，來規定情資融合中心的角色和責任。[29] 由於組織缺乏法律依據，未來一旦聯邦政府財政支出縮減，情資融合中心在爭取預算補助的

24 美國的警察係透過公開招聘，錄取為編制內警察需宣示就職，故稱為sworn officer。

25 John Rollins, *Fusion Centers: Issues and Options for Congress*, pp. 34-35.

26 Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires, *Counterterrorism Intelligence: Fusion Centers Perspectives* (Washington, DC: George Washington University Homeland Security Policy Institute, HSPI, 2012), p. 4. The Constitution Project, *Recommendations for Fusion Centers*, p. 7.

27 John Rollins, *Fusion Centers: Issues and Options for Congress*, pp. 19-20.

28 Department of Homeland Security, "DHS Announces Grant Guidance for Fiscal Year (FY) 2013 Preparedness Grants," *Homeland Security*, May 21 2013, <http://www.dhs.gov/news/2013/05/21/dhs-announces-grant-guidance-fiscal-year-fy-2013-preparedness-grants>（檢索日期：2013年6月25日）

29 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 20.

過程中，恐將處於不利地位。

四、指導綱領與策略

美國聯邦政府對於情資融合中心最主要的指導綱領是2005及2006年由司法部與國土安全部共同發佈的「情資融合中心指導綱領：新時期下資訊與情報的發展與分享」(Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era)，該指導綱領包括：如何遵守「全國犯罪情報分享計畫」(National Criminal Intelligence Sharing Plan)之規定；情資融合中心任務與目標之擬定；各代表機關的協力治理；情資分享環境的建立；各種備忘錄之落實；發揮各種資料庫、系統、網絡的效用；隱私權及公民自由之保護；各種設備、資料、人員的安全管理；科技、系統、人員之整合；人員之教育訓練；政策或執行流程的擬定；績效量測與評估；經費的使用；不同單位與人員的溝通協調等。[30]

2008年12月國土安全部公布「與情資融合中心之互動：操作概念」(Interaction with State and Local Fusion Centers: Concept of Operations)，內容包括情資融合中心的目標、相關利害人、角色與責任，並詳列國土安全部對情資融合中心的支援項目，包括情資分享、人員派遣、設備整合、技術協助與訓練等。[31] 至於其他聯邦政府所公布之資訊分享的策略或計畫，其中有提及情資融合中心者，經整理如表1。

五、任務與功能

表1　聯邦政府歷年來有關情資融合中心的指導綱領與策略

發佈機關	綱領或策略名稱	發佈日期
司法部 國土安全部	Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era-Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels-the Law Enforcement Intelligence Component	2005.7
司法部 國土安全部	Fusion Center Guidelines: Developing and Sharing Information in a New Era-Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels-Law Enforcement Intelligence, Public Safety, and the Private Sector	2006.8
白宮總統辦公室	National Strategy for Information Sharing	2007.10
國土安全部	Department of Homeland Security Information Sharing Strategy	2008.4
司法部 國土安全部	Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines	2008.9
國土安全部	Interaction with State and Local Fusion Centers: Concept of Operations	2008.12
國土安全部	Quadrennial Homeland Security Review	2010.2
聯邦調查局	National Information Sharing Strategy	2011
白宮總統辦公室	National Strategy for Information Sharing and Safeguarding	2012.12
國土安全部	DHS Information Sharing and Safeguarding Strategy	2013.1

資料來源：作者自行整理。

30 US Department of Justice and US Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, Aug, 2006.

31 Department of Homeland Security, *Interaction with State and Local Fusion Centers: Concept of Operations*, Dec 2008.

情資融合中心的運作已經有10年的經驗，整體而言，各情資融合中心的任務(mission)並不一致，在911事件以後第一波成立的情資融合中心，其任務清一色是反恐，但如今只有不到15%的情資融合中心將自己的任務定義在純粹的反恐，大多數已將其任務擴大為全災害及（或）全犯罪(all crimes)。[32] 由國土安全部網頁所呈現的「成功案例」(Success Stories)簡介（附錄2），顯示情資融合中心的任務除反恐之外，更擴及到犯罪偵查、緝毒、緊急應變等事項。

分析此種任務轉變的原因有下列可能

附錄2　情資融合中心成功案例

時　　間	案　　由	性　　質
2012.8.5	威斯康辛東南威脅分析中心(Southeastern Wisconsin Threat Analysis Center)協助警方偵辦當地橡樹溪錫克教寺廟(Oak Creek Sikh Temple)槍擊案。	反　　恐
2012.7	科羅拉多資訊分析中心(Colorado Information Analysis Center)協助科羅拉多緊急管理處(Colorado Division of Emergency Management)搶救森林大火。	緊急應變
2012.5	維吉尼亞情資融合中心(Virginia Fusion Center)協助警方找到逃家的青少年。	社區治安
2012.3	南內華達反恐中心(Southern Nevada Counterterrorism Center)協助警方偵查謀殺案。	犯罪偵查
2012.2	賓州犯罪情報中心(Pennsylvania Criminal Intelligence Center)協助謀殺案資料分析。	犯罪偵查
2012.1	肯塔基情資融合中心(Kentucky Intelligence Fusion Center)及中加州情報中心(Central California Intelligence Center)協助海關及邊境保護局(Customs and Border Protection)查緝毒品。	緝　　毒
2011.12	喬治亞資訊分享與分析中心(Georgia Information Sharing & Analysis Center)及維吉尼亞情資融合中心(Virginia Fusion Center)協助警方破獲一宗孩童謀殺案。	犯罪偵查
2011.10.26	阿拉斯加資訊分析中心(Alaska Information and Analysis Center)提供情資給海關及邊境保護局(Customs and Border Protection)及加拿大邊境安全局(Canadian Border Security Agency)，逮捕武裝要犯。	犯罪偵查
2011.10	科羅拉多資訊分析中心(Colorado Information Analysis Center)與警方合作降低汽車偷竊數量。	犯罪偵查
2011.8	科羅拉多資訊分析中心(Colorado Information Analysis Center)提供警方1名武裝危險逃犯資訊。	犯罪偵查
2011.6	賓州犯罪情報中心(Pennsylvania Criminal Intelligence Center)協助警方辨識逃犯資料。	犯罪偵查
2011.6	科羅拉多資訊分析中心(Colorado Information Analysis Center)協助FBI逮捕炸彈客。	反　　恐
2010.10	羅德島情資融合中心(Rhode Island Fusion Center)及康乃迪克情資融合中心(Connecticut Intelligence Center)協助紐約警察局查緝時代廣場(Times Square)1名可疑的卡車司機。	反　　恐
2010.8	賓州犯罪情報中心(Pennsylvania Criminal Intelligence Center)協助警方逮捕1名綁架及強暴犯。	犯罪偵查
2010.5	佛羅里達情資融合中心(Florida Fusion Center)協助調查2010年5月1日在紐約時代廣場發生的爆炸陰謀嫌犯Faisal Shahzad。	反　　恐

32 The Constitution Project, *Recommendations for Fusion Centers*, p. 6.

2010.5	亞歷桑那反恐資訊中心(Arizona Counter Terrorism Information Center)協助警方逮捕10名毒犯。	緝　毒
2010.5	科羅拉多資訊分析中心(Colorado Information Analysis Center)協助恐怖份子嫌犯Jamie Paulin-Ramirez之調查。	反　恐
2009.9	科羅拉多資訊分析中心(Colorado Information Analysis Center)協助FBI調查恐怖份子嫌犯Najibullah Zazi。	反　恐
2009.9	數個情資融合中心支援在賓州匹茲堡召開的G-20高峰會議維安工作。	反　恐
2008.7	明尼蘇達聯合分析中心(Minnesota Joint Analysis Center)協助2008年共和黨與民主黨全國代表大會維安工作。	反　恐
2008.5	中加州情報中心(Central California Intelligence Center)與FBI合作逮捕2名威脅炸彈攻擊達美航空(Delta Airlines)和美國駐義大利大使館之嫌犯。	反　恐
2008.5	中加州情報中心(Central California Intelligence Center)與警方合作防止一宗孩童綁架案。	犯罪偵查
2008.1	伊利諾州恐怖主義與情報中心(Illinois Statewide Terrorism and Intelligence Center)與維吉尼亞情資融合中心(Virginia Fusion Center)合作防止一宗校園槍擊案。	犯罪偵查

資料來源：作者整理自美國國土安全部網頁，Fusion Center Success Stories, <http://www.dhs.gov/fusion-center-success-stories>

性，首先，情資融合中心的主管意識到國內正興起一股全災害或全犯罪的安全管理思維。其次，地方政府執法機關一般而言並未強烈感受到恐怖主義的威脅，他們更在乎的是幫派、毒品、街頭犯罪等問題。因此，要取得地方政府的資源與支持，情資融合中心必須更貼近社區的需求。此外，採取全災害或全犯罪策略，亦有助於情資融合中心向各政府機關申請補助或各類資源。[33]

就功能而言，情資融合中心與傳統警政(traditional policing)的思維不同，傳統警政強調反應性、事後性、起訴功能，但情資融合中心更著重在預防、先制的功能。例如，2007年，歹徒在紐澤西州迪克斯堡陸軍基地(Fort Dix)附近將發動聖戰的錄影帶送到錄影帶店拷貝，由於國土安全執法官員在第一時間將資訊提供給FBI，才迅速逮捕6名恐怖份子，瓦解了一個殺害美國軍人的陰謀，如果是依照警察辦案的程序，由於這些歹徒並無犯罪紀錄，極可能躲過警方盤查，因而犯下大案。[34]因此，前國土安全部部長邱特福(Michael Chertoff)將情資融合中心視為一種「可讓執法人員搶先敵人行動的預警系統」。[35]

此外，情資融合中心亦具有連結(linkage)或翻譯(translator)的功能，例如，當國外發生恐怖攻擊爆炸事件，聯邦政府可以透過情資融合中心，經由系統或聯邦情報機關派駐在情資融合中心的人員，迅速地將有關爆炸的作法和戰術資訊傳給各州或地方政府，以便地方政府即時調整預防的資源與策略。[36]

33 John Rollins, *Fusion Centers: Issues and Options for Congress*, pp. 21-22. 依據「第8號國土安全總統指令」(Homeland Security Presidential Directive 8, HSPD-8)，「全災害」係指針對國內的恐怖份子攻擊、重大災難事件、其他緊急事件進行整備(preparedness)，因此，情資融合中心將可接收並檢視執法、消防、緊急管理、公共衛生等機關所傳送的資訊或情報，並且協助預防人為或天然災害，同時也具有協助減災和復原的角色。

34 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 25.

35 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 5.

36 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 6.

六、與其他機關的伙伴關係

情資融合中心最主要的功能，是透過與其他單位建立合作關係，達成反恐、打擊犯罪、緊急應變之目標。首先，由司法部所主導的「全國可疑活動報告倡議計畫管理辦公室」(Nationwide Suspicious Activity Reporting Initiative Program Management Office)，目的在建立可疑活動的鑑定與報告標準化作業流程，這套流程已與情資融合中心的網路整合。[37] 其次，情資融合中心與聯邦調查局的「聯合反恐小組」(Joint Terrorism Task Force, JTTF)及「外勤情報小組」(Field Intelligence Group, FIG)合作，間接或直接取得FBI提供的威脅情報或資訊。外勤情報小組由情報分析專家、調查幹員、語言分析專家、監視專家等組成，擔任聯邦調查局情報計畫的樞紐(hub)，作為該局與美國情報機關、各級政府執法部門、私營企業體系、情資融合中心之資訊分享與協調的渠道(conduit)。[38]

此外，情資融合中心與「國家毒品管制政策中心」在「高度密集販毒區域中心」設置之「調查支援中心」(Investigative Support Centers, ISCs)也有密切的合作關係。情資融合中心也提供資訊與情報支援「緊急事件行動中心」(Emergency Operations Centers, EOCs)之意外事件管理或回應行動，並且協助全美546個聯邦承認的部落、171個部落警察局、2,300個部落執法官員，強化偏僻地方參與國土安全、保護國際邊境、強化位處印地安部落地區的關鍵基礎設施（如水壩、運輸路徑）之防護。2009年9月14日，國土安全部進一步與國防部達成協議，允許情資融合中心完成安全查核之官員，可以透過國防部的「機密網際網路協議路徑網」(Secret Internet Protocol Router Network, SIPRNet)，取得機密性的恐怖主義相關情報。[39]

在保護國家關鍵基礎設施方面，國土安全部自2004年起推動「安全保護顧問計畫」(Protective Security Advisor program, PSA)，該計畫主要的任務包括：強化基礎設施安全防護、協助緊急事件管理、促進資訊分享。「安全保護顧問」必須接受關鍵基礎設施安全防護、減災、地理資訊系統等訓練，再派遣至各地區情資融合中心，提供各項諮詢給州、地方、部落和民間部門的關鍵基礎設施擁有者或操作者，協助他們履行「國家關鍵基礎設施防護計畫」(National Infrastructure Protection Plan, NIPP)，在緊急事件發生以後，協調連繫「緊急事件行動中心」(EOC)及「聯邦緊急事務管理總署」(FEMA)的區域辦公室，共同提升基礎設施的整備、減災、應變及復原能力。[40]

最後，在公私合作方面，由於情資融合中心重視人為或天然災害的預判與應變能力，故與民間企業合作，導入風險管理概念，例如，情資融合中心已普遍採用由總部位於維吉尼亞的「數位沙盒公司」(Digital Sandbox, Inc.)所開發之軟體，協助地區情報的蒐集、區域風險的評估、威脅的排序與分析。該軟體針對地區情報的整合，包括下

37 汪毓瑋，《國土安全（上）》（臺北：元照出版公司，2013年），頁271。

38 同註37，頁274。

39 同註37，頁276-280。

40 Department of Homeland Security, "Protective Security Advisors," *Homeland Security*, <https://www.dhs.gov/protective-security-advisors>（檢索日期：2013年9月20日）

列各種資訊來源：警察局與消防隊的報案電話、交通狀況、可疑活動、關鍵基礎設施資料、救護車所在資訊、錄影監視器資訊、個人及公共安全人員資訊等。[41]

伍、情資融合中心的調查與評估

情資融合中心運作十年以來，已經花費相當大的行政資源，因此，近年來陸續有行政部門、國會、學術機構及智庫針對情資融合中心的績效進行評估，並提出改善建議。以下摘述國土安全部（行政部門）、喬治華盛頓大學國土安全政策研究所（學術機構）、憲法計畫（智庫）、國會研究服務處、參議院常設調查小組委員會（國會）的調查研究報告。

一、國土安全部「2011年全國情資融合中心網絡總結報告」

2011年，國土安全部公布了一份「2011年全國情資融合中心網絡總結報告」(2011 National Network of Fusion Centers Final Report)，針對72個情資融合中心的行動能力(operational capability)和必要能力(enabling capability)進行評估，行動能力包括資訊的接收、分析、傳送、蒐集；必要能力則包括隱私權及公民權利的保護、長期策略、溝通與擴大服務、安全性。有關情資融合中心待改進事項，經整理如表2。

二、喬治華盛頓大學國土安全政策研究所「反恐情報：情資融合中心觀點」

喬治華盛頓大學國土安全政策研究所(The George Washington University Homeland Security Policy Institute, HSPI)於2012年6月公布「反恐情報：情資融合中心觀點」(Counterterrorism Intelligence: Fusion Center

表2　情資融合中心待改進事項

能力	項目	待改進事項
行動能力	接收	只有59.7%（43個）的情資融合中心具有接收全國威脅資訊的書面計畫或標準作業流程。
	分析	● 只有68.1%（49個）的情資融合中心具有書面的資訊分析計畫。 ● 只有52.8%（38個）的情資融合中心對國家層級的風險評估具有貢獻。
	傳送	● 只有52.8%（38個）的情資融合中心具有傳送全國威脅資訊的書面計畫或標準作業流程。 ● 只有30.6%（22個）的情資融合中心具有資訊傳送出去後的確認流程。
	蒐集	● 只有62.5%（45個）的情資融合中心對於資訊的要求具備核准的文件。 ● 只有54.2%（39個）的情資融合中心具有核准的Standing Information Needs (SINs)。
必要能力	隱私權及公民權利的保護	只有23.6%（17個）的情資融合中心具有核定的隱私權及公民權利保護計畫。
	長期策略	只有48.6%（35個）的情資融合中心具有核定的長期策略。
	溝通與擴大服務	只有41.7%（30個）的情資融合中心具有核定的溝通計畫。
	安全性	只有61.1%（44個）的情資融合中心安全官員完成了Central Verification System的訓練。

資料來源：Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, p. iii.

41 Digital Sandbox, Inc. website, <http://www.dsbox.com/intelligence-fusion.html>（檢索日期：2013年9月20日）

Perspectives)，研究結果摘要如下：

㈠針對72個情資融合中心的人員進行問卷調查結果

1. 威脅程度若從1到10，10代表威脅最高，則有49%的受訪者認為恐怖主義威脅高於6。

2. 超過78%受訪者認為恐怖威脅會持續存在。

3. 當問及最大的恐怖威脅為何，超過65%受訪者認為是社區的聖戰份子或組織(hometown jihadi individuals or organizations)

4. 僅有29%受訪者指出，所屬的情資融合中心每年會進行區域威脅評估。

5. 僅有52%受訪者指出，所屬的情資融合中心訂有資訊蒐集的策略。

6. 當問及反恐資訊最重要的來源為何，48%受訪者選擇執法機關，26%認為是FBI的「聯合反恐小組」(Joint Terrorism Task Force, JTTF)。

7. 超過51%受訪者指出，該地區的關鍵基礎設施擁有者並未參與情資融合中心。

8. 51%受訪者認為，所屬的情資融合中心最需改善的是「分析能力」。

9. 65%受訪者認為，所屬的情資融合中心對於「網路威脅」的蒐集、接收、分析仍待加強。

10. 63%受訪者把「執法」列為情資融合中心最重要的功能，只有28%受訪者把「反恐」列為最重要的功能。[42]

㈡對情資融合中心的觀察與建議

整體而言，HSPI認為情資融合中心最需要強化的是關於網路威脅的偵測和分析，目前在政府與民間尚未建立有關網路威脅情報的交換管道，對於網路威脅的認知與反應能力亦明顯不足。HSPI指出，雖然各政府之間定期接收、傳送資訊，但情資融合中心只能稱為「資訊交換中心」，還不足以稱為「情報交換中心」，其中最主要的原因在於情資融合中心的人員專業背景同質性太高，其次是對於分析技術訓練的投資不足。

目前情資融合中心的人員以傳統的執法人員為主，導致時效性及功利價值較高的資訊受到青睞，明確性不足和沒有行動價值的資訊則易遭到忽視。執法人員比例過高，即可能產生偏見，並且習慣性依賴特定資訊，以致於忽略了威脅與組織之間的關係。因此，HSPI建議強化分析技能(analytical skill)與批判性思考(critical thinking)之訓練，同時配合誘因機制，獎勵高品質的分析報告，以鼓勵人員致力於情報研析的工作。[43]

三、憲法計畫的「情資融合中心的建議」

位於美國首都華盛頓的智庫「憲法計畫」(The Constitution Project)，於2012年發表「情資融合中心的建議：在打擊犯罪與恐怖主義之際保障隱私權及公民自由」(Recommendations for Fusion Centers: Preserving Privacy and Civil Liberties while Protecting against Crime and Terrorism)，這份報告主要是調查及分析情資融合中心在資訊蒐集、儲存與使用的過程中，可能對美國人民隱私權及公民自由所產生的傷害，報告重點如下：

㈠資料蒐集的問題

情資融合中心的資訊來源包括：聯

42 同註26，頁5-6。

43 同註26，頁34-35。

邦、各州、地方政府的資料庫、執法和情治機關的檔案、金融交易紀錄、公用事業帳單、保險詐欺資料庫等等。許多情資融合中心也定期向民間公司購買商業資料庫，例如信用報告、租車資料庫，通常這些資料庫可以立即取得房屋、車輛、電話等資訊。此外，聯邦政府亦鼓勵情資融合中心與各種民間部門合作，如銀行、教育機構、能源公司、旅館業等。

雖然資訊分享與合作可提升警察執法的效率，但有案例顯示，情資融合中心在資訊蒐集方法上亦有違憲的情形，美國憲法第一修正案確立了人民有表達信仰和政治理念的自由，但若干情資融合中心往往以種族測繪(racial profiling)、宗教測繪(religion profiling)、政治測繪(political profiling)等方式不當取得資訊，諸如派員臥底參加伊斯蘭社區、各類社會運動或政治團體的會議，對其負責人進行監視、監聽，例如：由明尼蘇達州「美國購物中心」(Mall of America)向該州情資融合中心提供的「可疑活動報告」(suspicious activity report)，即有三分之二涉及了少數族裔，而根據「美國購物中心」的安全主管指出，該中心是明尼蘇達情資融合中心最大的情報來源。

國土安全部利用情資融合中心建立了全國性資訊蒐集與分享的網絡，特別是可疑的與恐怖主義活動有關資訊，這項計畫稱為「全國性可疑活動報告倡議」(Nationwide Suspicious Activity Reporting Initiative)，但所謂「可疑活動」的定義卻很寬鬆。美國聯邦法規第28章第23條(Title 28, Part 23 of Code of Federal Regulation)要求執法機關「只有在合理懷疑個人確實涉及犯罪行為或活動，且該資訊與犯罪行為或活動相關，才能蒐集並持有該犯罪情報資訊」，但目前這套可疑活動報告系統所收到舉報資訊未經嚴謹的分析，卻可被傳送到「資訊分享環境」(Information Sharing Environment)和FBI的「電子衛士系統」(eGuardian System)[44]，由有甚者，如果沒有人員來檢視這些可疑資訊，某個人的檔案很可能就不斷的累積，甚至造成負面的後果，例如：被列為「不得登機名單」、失去工作、個人名譽嚴重傷害等。[45]

㈡資料儲存與使用的問題

情資融合中心所蒐集的個資必須以反恐情報或執法有關，分享的對象也應限制在此目的與範圍，對於資料的儲存與保管尤應慎重，但目前確有情資融合中心發生職員或民間外包商不當查詢個資情事，甚至包括總統候選人及其支持者的個資。

此外，民間部門已經成為情資融合中心重要的安全伙伴，甚至有大企業派遣人員進駐情資融合中心，但民間部門的參與也帶來下列風險，例如：未經安全查核人員可能不當接觸敏感資料，民間部門與情資融合中心的密切關係，導致民間部門無須法律規範，即可連結上執法或情報機關的資料庫，因此，情資融合中心必須確認，唯有在進行執法功能時，才能將個資與民間部門分享。[46]

四、國會研究服務處的報告

44 聯邦調查局(FBI)推出的「電子衛士」(e-Guardian)，是一個資訊分享系統，可與全國各地警察局互通反恐情報，讓全美各級執法機關透過資訊分享，及時掌握可疑的活動和人員的情況。

45 The Constitution Project, *Recommendations for Fusion Centers*, pp. 7-13.

46 The Constitution Project, *Recommendations for Fusion Centers*, pp. 16-17.

美國國會研究服務處(Congressional Research Service)研究員John Rollins於2008年1月18日完成一份報告「情資融合中心：議題與國會的選項」(Fusion Centers: Issues and Options for Congress)，該報告指出，國土安全部對情資融合中心提供經費資助、安全查核、人員派遣、指導訓練，最終目的在透過資訊與情報的分享，防止恐怖攻擊與快速回應天然災害，但情資融合中心在運作上，仍有下列問題需要檢討改進。

㈠資訊分享障礙亟須克服

目前由聯邦政府到各州政府或情資融合中心的資訊分享仍不夠積極主動，同時，當情資融合中心向聯邦機構提供資訊以後，往往得不到聯邦的回應，由於聯邦各情報機關對於本身產製的情報存有一種「擁有」(ownership)的心態，造成機密浮濫(over-classification)的現象，致使執法機關、州政府官員、關鍵基礎設施操作者無法獲得關鍵的情報，成為情報分享的另一項障礙。[47]

此外，聯邦各機關均已開發不同的資訊分享系統，例如：國土安全部建置的「國土安全資訊網絡」(Homeland Security Information Network, HSIN)、「國土安全資料網路」(Homeland Secure Data Network, HSDN)、Federal Protective Service (FPS)入口網站、聯邦調查局建置的Law Enforcement Online (LEO)、司法部司法協助局資助的Regional Information Sharing Systems (RISS)。雖然絕大多數情資都會複製(duplicate)到不同的系統，但為了確保不致遺漏，各情資融合中心人員仍須逐一查核每一個系統，同樣的，當情資融合中心提供聯邦機構情資時，也必須每一個系統逐一上傳資料，造成大量時間的浪費。[48]

還有，各州所使用的情報管理系統往往與他州的系統介面無法連結，由於目前缺乏強制性的統一規範，各情資融合中心仍然依據本身的想法購買自己的系統，導致與其他系統連結時必須購買其他的設備和支出額外的成本，招致效率不彰之批評。[49]

㈡民間部門參與仍須加強

有關情資融合中心與民間部門，特別是主要關鍵基礎設施的擁有者及操作者的合作關係仍待進一步提升，原因包括：情資融合中心尚未體會到民間部門所能提供資訊的價值，以及聯邦政府缺乏一套策略讓民間部門的資訊融入情資融合與分析的過程。[50]

由國土安全部所支持的主要關鍵基礎設施資訊分享機制包括「資訊分享與分析中心」(Information Sharing and Analysis Centers, ISACs)[51]及「受保護關鍵基礎設施資訊計畫」

47 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 31.

48 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 30.

49 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 30.

50 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 54.

51 ISACs之設立依據為1997年柯林頓總統發佈的第63號總統決策指令(Presidential Decision Directive 63, PDD-63)，911事件以前，只有金融服務、資訊科技、通信、電力等少數幾個ISACs被建置，911事件以後，陸續又建置了化學、食品、能源、大眾運輸、陸地運輸、水、房地產等ISACs。由於PDD-63並未明確規定ISACs的運作模式，以及ISACs與聯邦政府的關係，因此，ISACs的品質、結構、經費來源、管理、運作等都不相同。其他問題如民間企業與政府分享資訊的意願和能力為何？政府對於私人擁有的基礎設施的監控應該介入到什麼程度？政府與民間在進行資訊分享時會面臨那些法律問題，例如隱私權和義務？這些問題至今仍然無

(The Protected Critical Infrastructure Information Program, PCII)。由於美國85%的關鍵基礎設施都是私有性質，包括大型購物中心、辦公高樓、銀行、醫院、製藥廠、電力供應及傳輸設施、化學工廠、航空公司等。因此，民間業者比政府更了解企業運作的資訊，ISACs設置的目的即在促進企業與聯邦政府之間的資訊分享，但目前情資融合中心並未充分利用民間部門的資訊來源，也很少有民間部門的代表派駐情資融合中心。同樣的，情資融合中心也很少利用PCII所擁有的關鍵基礎設施脆弱度資訊。[52]

五、美國參議院常設調查小組委員會

2012年10月3日，美國參議院常設調查小組委員會(U.S. Senate Permanent Subcommittee on Investigations)公布了一份「聯邦對各州及地方情資融合中心的支持及參與」(Federal Support for and Involvement in State and Local Fusion Centers)，在這份歷時兩年，由兩黨共同完成的調查報告指出，自2003年起，國土安全部花在情資融合中心的經費估計在美金2億8,900萬元至14億元之間，然而，情資融合中心不僅沒有生產出有用的反恐情報，還有許多問題。

㈠由國土安全部派駐在情資融合中心人員所提供之情資，品質參差不齊，往往十分粗糙、過時、重複，甚至損害公民自由或違反隱私權法，某些情資直接取自已出版之文件或媒體新聞報導等公開資訊，大多數情資則與恐怖主義無關。

㈡由國土安全部所公布的情資融合中心資訊非但不完全正確，有些中心甚至根本不存在，如懷俄明州情資融合中心(Wyoming Fusion Center)及座落在賓州費城的德拉瓦流域資訊中心(Delaware Valley Information Center)，尤其後者自2006年起獲得國土安全部數百萬美元經費補助，但在2012年8月時，該中心仍未實際存在(physically exist)，足見整個計畫缺乏監督與評估。

㈢參議院認為，國土安全部無法提出證據，證明情資融合中心對於協助聯邦政府反恐具有特殊貢獻，或其情資瓦解或防止任何恐怖主義陰謀。國土安全部所宣稱情資融合中心的「成功案例」，通常只是誇大其詞。

㈣國土安全部從未有效監督聯邦補助情資融合中心的經費的使用情形，以及經費是否確實用於反恐。根據參議院的調查，許多經費被花在購買平面電視、運動型多用途汽車(Sport Utility Vehicle, SUV)、手機追蹤裝置或其他監視設備等與反恐情資分析無關的器材。

㈤國土安全部對於派駐至情資融合中心的人員，並未提供足夠的法律、情報蒐集與報告等訓練，通常僅在派遣前一週內施以短期教育。至於經常性提供品質低劣的「國土情報報告」(Homeland Intelligence Reports, HIRs)的人員，則從未受到糾正或處分。

㈥國土安全部官員顯然知道情資融合中心的問題，但從未告知國會或大眾問題的嚴重性，更未保證問題會在一定期限內獲得改善，當參議院常設調查小組委員會要求國土安全部澄清相關問題時，國土安全部卻以情

法獲得圓滿答案。參見Daniel B. Prieto, "Information sharing with the private sector," in Philip E. Auerswald,ed., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York: Cambridge University Press, 2006), pp. 406-407.

52 John Rollins, *Fusion Centers: Issues and Options for Congress*, p. 55.

資融合中心享有特權、資料太敏感、受限於保密條款、資料不存在等理由加以搪塞。

㈦情資融合中心提供的服務，對於犯罪調查、公共安全、災害回應與復原的貢獻顯然超過反恐，因此，國會建議國土安全部重新釐清情資融合中心的任務與目標，並且將經費補助與績效做一連結。[53]

陸、綜合檢討與結論

911委員會報告(The 9/11 Commission Report)指出，造成各情報點之間無法連結的最大障礙，當屬人為或系統性的抗拒資訊分享。[54] 為了解決情報機關各自為政的現象，美國政府在911事件後進行了組織的調整，同時強化國土安全情報機制，並且透過情資融合中心的運作，試圖經由改變情報與執法機關的思維及文化，促進各級政府甚至與民間部門的情資分享。由美國情資融合中心的運作經驗，可以歸納出值得借鏡學習與警惕避免之處。

㈠可供借鏡學習之處

911事件以後，美國政府體認到反恐必須採取全方位途徑，突破以往情報蒐集區分國內與國外、中央與地方、政府與民間的作法，整合政府、情報、執法、緊急管理、醫療、交通、矯治等機關，全面蒐集國家安全、犯罪預防、關鍵基礎設施等情資，才能防範恐怖主義攻擊。因此，從國會、聯邦政府的國土安全部、司法部，到各州及地方政府的執法機關，莫不全力支持情資融合中心之運作，使之成為資訊蒐集、分析、傳遞、分享的樞紐，進而發揮偵測與打擊恐怖主義之功能。從歐巴馬總統、國土安全部部長那波利塔諾、司法部部長Eric Holder、全美州長協會對情資融合中心的重視，足見政治領袖的願景與決心，朝野的共識，配合強有力的執行力，才是政策成功的關鍵。

其次，情資融合中心的任務，從一開始的反恐，逐漸演變擴大至犯罪預防與偵查、毒品查緝、緊急應變、災害防救等事項，不僅回應「全災害」或「全犯罪」的安全管理思維，更具體實踐「情報導向警政」及「社區導向警政」的治安策略，對於喚醒社區民眾「風險共受」的意識具有重要意義。例如，國土安全部於2010年7月發起一項「如果你看到什麼，就報告什麼」(If You See Something, Say Something)的全國性運動，目的在喚起公眾意識，留心周邊恐怖主義的徵候及與恐怖主義有關的犯罪活動，提醒民眾看到可疑的活動應立即向執法機關或情資融合中心舉報，對於維護治安、降低犯罪貢獻良多。

此外，情資融合中心在打破各情報與執法機關本位主義的藩籬上亦功不可沒。情資融合中心係由國土安全部支持所成立，但與國土安全部所屬機關的情報單位、聯邦調查局的「聯合反恐小組」及「外勤情報小組」、國家毒品管制政策中心設置的「調查支援中心」、國防部、各地方政府執法機關建立密切的情報交流與分享機制。另與民間

53 U.S. Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, Oct 3, 2012.

54 Thomas H. Kean & Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004), p. 416.

的關鍵基礎設施擁有者、企業、大型購物中心、醫療機構等維持安全管理的伙伴關係，共同推動風險管理的概念，落實「警力有限、民力無窮」的精神，讓情資融合中心在災時能夠作為聯邦與地方、政府與民間的聯繫窗口，發揮訊息傳遞及資源整合功能。

㈡必須警惕避免之處

國家安全與個人自由之間必然有一個權衡關係(trade-off)，在緊急時期，某些社會可能願意為了安全而犧牲若干個人自由。由於恐怖主義之目的是破壞社會秩序，因此對抗恐怖主義需要運用民防(civil defense)及深度防禦(defense in depth)的策略，亦即整個社會都必須參與國土安全，才能保障社區安全。然而，採用「深度防禦」必然會改變個人自由與國家權力之間的平衡點，由於法律、軍事行為、警察權力、資訊蒐集作為之改變，導致社會衝突與爭議無可避免。[55]

911以後美國政府對於監視的強化，例如公共場所的監視器、邊境與機場的安檢、群眾抗議的壓制、公共場所的警察巡邏等，均令民眾感到疑慮不安。情資融合中心對於隱私權及公民自由(civil liberties)可能造成的侵犯，尤為民主社會必須戒慎避免。情資融合中心向民間部門購買資料，進行資料分析，並與其他伙伴分享資訊，這套流程必須有所規範，否則極易造成執法人員利用情資進行種族測繪(racial profiling)、政治測繪(political profiling)、非法資料探勘(illegal data mining)等行為，導致情資融合中心發生行動偏離原定目標的「任務偏離效應」(mission creep)或「功能偏離效應」(function creep)。[56]例如，情資融合中心設置的檢舉熱線，雖然用意在鼓勵民眾檢舉可疑的活動，但也造成許多無辜的民眾遭到警方調查。[57] 因此，情資融合中心更應加強人員的倫理訓練，才能減少情報濫用和違反隱私權的現象。

在個人資訊的蒐集方面，應該符合下列原則：特定目的原則（明確指出由誰授權蒐集個資、蒐集的目的、使用的方式）、資料最少原則（個資的蒐集應以最少、與目的最相關為原則，持有該個資的時間應以達成特定目的所須的時間為原則）、使用限制原則（個資的使用僅以原來蒐集之目的為限）、資料品質與誠實原則（確保個資的正確性、相關性、即時性、完整性）、安全原則（採取最安全的方法，避免個資遭到遺失、未授權之濫用、毀損、修改、無心或不當的公開）、課責與審核原則（對使用個資的職員或外包人員實施教育訓練）。[58] 有關資訊儲存的安全性尤須謹慎，並有管道與機制提供民眾申請檢視並更正個人資料，方不至於侵犯人權，造成無辜民眾受害。

最後，美國政府投入大筆預算與人員所建置的情資融合中心，雖在反恐及打擊犯罪任務上發揮若干功能，仍有資源浪費、浮

55 Jonathan R. White, *Terrorism and Homeland Security* (Belmont, CA: Wadsworth, 2008), pp.459-464.

56 同註12，頁85。

57 Torin Monahan & Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue*, Vol. 40, No. 6, 2009, pp. 628-631.

58 Department of Homeland Security, The Privacy Office, "Privacy Policy Guidance Memorandum," *Homeland Security*, Dec 29, 2008, <http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf>（檢索日期：2013年6月15日）

誇不實、目標偏移、違反人權、獎懲不明等問題，足見監督機制之完善對於國土安全政策落實之重要性。所幸美國的行政部門、學術機構、智庫、國會均能夠以客觀、甚至批判的態度對情資融合中心的運作加以檢討，此舉不僅有助於情資融合中心重新定位本身的目標與任務，也能促使情資融合中心朝向更透明化的方向努力，進而減少民眾對情資融合中心的疑慮與敵意。

由於國內外威脅來源不斷變化，對國家安全與社會治安造成的挑戰也更嚴峻。臺灣遭受恐怖攻擊的威脅雖較低，但國內仍有中共潛伏的間諜、重大刑事案件、選舉暴力事件、各種民眾陳情抗爭活動等問題，必須重視情資蒐集、整合與分析，才能完成應變整備。美國情資融合中心的運作經驗，應可提供我國安與執法機關若干啟示與借鏡。

收件：102年08月21日
修正：102年10月01日
接受：102年10月03日

參考文獻

中文部分

專書

汪毓瑋，2013。《國土安全（上）》。臺北：元照出版公司。

外文部分

專書

Cilluffo, Frank J., Joseph R. Clark, Michael P. Downing, and Keith D. Squires, 2012. *Counterterrorism Intelligence: Fusion Centers Perspectives*. Washington, DC: George Washington University Homeland Security Policy Institute.

Kean, Thomas H, and Lee Hamilton, 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States.

Prieto, Daniel B., 2009. *War about Terror: Civil Liberties and National Security after 9/11*. New York: Council on Foreign Relations.

The Constitution Project, 2012. *Recommendations for Fusion Centers: Preserving Privacy and Civil Liberties while Protecting against Crime and Terrorism*. Washington, DC: The Constitution Project.

White, Jonathan R., 2008. *Terrorism and Homeland Security* (6th edition). Belmont, CA: Wadsworth.

專書論文

Berkowitz, Bruce, 2008. "Homeland Security Intelligence: Rationale, Requirements, and Current Status," in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, DC: Georgetown University Press, pp. 281-294.

Prieto, Daniel B., 2006. "Information sharing with the private sector," in Philip E. Auerswald et al., eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. New York: Cambridge University Press, pp. 404-428.

期刊論文

Eack, Kevin D., 2008. "State and Local Fusion Centers: Emerging Trends and Issues," *Homeland Security Affairs*, Supplement No. 2, pp. 1-6.

Monahan, Torin, 2010. "The Future of Security Surveillance Operations at Homeland Security Fusion Centers," *Social Justice*, Vol. 37, No. 2-3, pp. 84-98.

Monahan, Torin, and Neal A. Palmer, 2009. "The Emerging Politics of DHS Fusion Centers," *Security Dialogue*, Vol. 40, No. 6, pp. 617–636.

官方文件

Department of Homeland Security, 2008/12. *Interaction with State and Local Fusion Centers: Concept of Operations*.

Department of Homeland Security, 2012/5. *2011*

National Network of Fusion Centers Final Report.

US Department of Justice, 2005/9. *Intelligence-Led Policing: The New Intelligence Architecture*.

US Department of Justice and US Department of Homeland Security, 2006/8. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*.

US Senate Permanent Subcommittee on Investigations, 2012/10/3. *Federal Support for and Involvement in State and Local Fusion Centers*.

研究計畫

Randol, Mark A., 2009. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches* (Report No. RL33616).Washington, DC: Congressional Research Service.

Randol, Mark A., 2010. *The Department of Homeland Security Intelligence Enterprises: Operational Overview and Oversight Challenges for Congress* (Report No. RL40602). Washington, DC: Congressional Research Service.

Rollins, John, 2008. *Fusion Centers: Issues and Options for Congress*. (Report No. RL34070). Washington, DC: Congressional Research Service.

網際網路

Department of Homeland Security, 2013/5/21. "DHS Announces Grant Guidance for Fiscal Year (FY) 2013 Preparedness Grants," *Homeland Security*, <http://www.dhs.gov/news/2013/05/21/dhs-announces-grant-guidance-fiscal-year-fy-2013-preparedness-grants >.

Department of Homeland Security, "Fusion Center Locations and Contact Information, Primary Fusion Centers," *Homeland Security*, <http://www.dhs.gov/fusion-center-locations-and-contact-information>.

Department of Homeland Security, "Fusion Center Locations and Contact Information, Recognized Fusion Centers," *Homeland Security*, <http://www.dhs.gov/fusion-center-locations-and-contact-information>.

Department of Homeland Security, "Protective Security Advisors," *Homeland Security*, <https://www.dhs.gov/protective-security-advisors>.

Department of Homeland Security, The Privacy Office, 2008/12/29. "Privacy Policy Guidance Memorandum," *Homeland Security*, <http://www.dhs.gov/xlibrary/assets/privacy/policyguide_2008-01.pdf>.

National Governors Association, 2006/4/3. "2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships," *NGA Center for BEST PRACETICES*, <http://www.nga.org/files/live/sites/NGA/files/pdf/0604HLSDIRSURVEY.pdf>.

National Governors Association, 2007. "A Governor's Guide to Homeland Security, 2007," *NGA Center for BEST PRACETICES*, <http://www.nga.org/files/live/sites/NGA/files/pdf/0703GOVGUIDEHS.PDF>.