

第一篇

情報學總論、 概念與界定



情報之意義

例題

▲請說明情報之意義——情報之三大面向？

▲【相關問題】試說明情報的意義與重要性。(107 公安所)

擬答

可由 3 個面向說明：
一.知識：
(一)所必需具有之資訊。學者認為：
1.肯特 (Sherman Kent) 指出，「戰略情報」係國家平時或戰時，在處理對外關係所須具備之知識。
2.阿瑪瑞傑 (Charles D. Ameringer) 將情報分成 2 種類型：
(1)原始的情報：已蒐集但未經任何確認、證實之資料。
(2)完成的情報：係原始的情報經情報單位分析後產生之資料。而情報分析之
三步驟：
①首先須對環境進行了解，或確認事件之性質及事件之特性。
②對事件發展之重要性。
③預測未來之發展。
(二)蒐集類別：
1.已知事實：已公開周知之資料來源，具相當確定成分。
2.秘密：不欲外人所知之資訊，有兩大挑戰：
(1)確立情報分析之假設，且達成最佳研判。
(2)面對不確定性。
3.欺敵資訊：為誤導而刻意製造出之事實。
4.無解資訊：報無法解答之問題。



二組織：
是有關情報活動管理課題與組織型態等問題。我國國安局組織三法、調查局組織法，將職責、聯繫作為都定出來，是舉世無雙之罕見作法。而依司法院大法官釋字第 342 號解釋文，國安局組織三法應為「國家安全會議、國家安全局及行政院人事行政局之組織法律」。
三活動：
(一)情報活動應是有目的、有計畫、有組織的。
(二)情報之最佳賣點：
1.隱密性。
2.秘密蒐集能力。
(三)活動取向：
1.蒐集 (Collection)。
2.產製 (Production)。
3.保護 (Protection)：即為反情報工作。
4.秘密行動 (Covert action)。

情報的重要性：
學者藍森說過：情報為「決策之鑰」，情報對決策之制定，具有極大的影響力。情報（的產出與過程）係為政策規劃的耳目與決策的樞紐，亦即情報與政府政策的制定與執行有關，情報的主要目的在於維護國家的安全利益或處理來自外國敵人現實和潛在的威脅；而政策則為情報的方向舵與運用者。此外，「政策制定者（情報運用者）和情報體系（情報產製者）之間相互認知與態度，將是決定情報活動成敗的關鍵」。

 情報循環；情報周期

例題

- ▲請說明情報循環（intelligence cycle）之意涵為何？其流程涵蓋哪些階段與步驟？各個階段間如何溝通與協調？〈108 公安所〉

- ▲對於情報處理的流程，在傳統上多數學者均認為，基本上是遵循著所謂的「情報循環」（Intelligence Cycle）在進行。但當代美國情報學者克拉克（Robert M. Clark）則認為並非如此，並提出以「目標為中心」（Target-centric）的主張，才是較符合情報處理的實際過程，請比較說明前述二種主張的內涵及差異？〈108 警特三〉

- ▲【相關問題】請說明情報過程（intelligence process）之意涵為何？其涵蓋哪些步驟？情報管理者在情報過程中，如何指導、協調情報機關提供使用者精確情報（即情蒐指導要項／參後文）？〈110 公安所〉

擬答

情報循環 (intelligence cycle) 之意涵：
一般而言，情報資訊在取得後，常無法加以運用，必須經過一連串特殊的處理程序，才能將「原始情報」轉換為「完成情報」，以供決策者使用，此一情報產製 (Production) 之完整過程即稱為 <u>情報過程 (Intelligence Process)</u> 亦可稱為 <u>情報循環 (Intelligence Cycle)</u> 、 <u>情報作業程序或情報周期</u> 。
學者陳明傳提出「 <u>情報過程的 4 個步驟</u> 」：
依學者陳明傳指出，雖依不同學者之見解，情報循環之內容有所差異，惟均不脫離 <u>指導 (Directions)</u> 、 <u>蒐集 (Collection)</u> 、 <u>處理 (Processing)</u> 、 <u>運用 (Use)</u> 四大過程。(如下頁圖)。
美國國家情報總監 (DNI) 於西元 2013 年發布《USNI 2013 Overview (美國情報體系 2013 年概述報告)》，其特別指出「 <u>情報循環 (Intelligence Cycle)</u> 包括『六』個步驟」：
一、 <u>情報計畫與指導 (Planning and Direction)</u> 。
二、 <u>蒐集 (Collection)</u> 。
三、 <u>情報處理與開發 (Processing and Exploitation)</u> ：將原始材料轉變為可理解的形式，成為有用的完成情報產品。
四、 <u>分析與產製 (Analysis and Production)</u> 。
五、 <u>轉送 (Dissemination)</u> 。
六、 <u>情報評價 (Evaluation)</u> 。
在過去，各國情報學學者均認為情報循環有 4 ~ 5 個步驟，並將「 <u>情報評價 (Evaluation)</u> 」排除於情報循環或情報過程之外；惟依最新 DNI 《USNI 2013 Overview》文件，目前美國已將「 <u>情報評價</u> 」置於情報循環的「六」個步驟之一環。

情報循環
情報周期

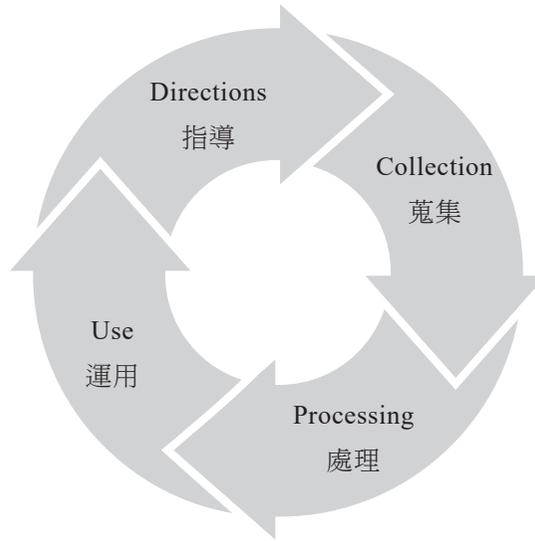


圖 情報循環（情報周期）

情報政治化

例題

- ▲何謂「情報政治化」(Politization of Intelligence)? 並說明「情報政治化」在何種情況下會發生。
- ▲【相關問題】何謂情報政治化? 在情報與政策的互動上應如何律定其關係? 〈110 公安所〉

擬答

一、情報政治化：
政策制定者對情報的認知與態度，並非全然肯定，甚至質疑情報對其政策的正面功能，顯示出「愛－恨」(Love-Hate)的複雜關係，也因此影響情報對於政策形成與執行過程的角色與功能。
情報也往往成為政治權力鬥爭的工具；易言之，政策面經常引用及運用情報(活動)以支持其政策；除了不希望情報消極地限制或扯其政策後腿外，政策制定者更積極主導情報角色，為求政策合理與妥當性尋求支持，產生「情報政治化」。尤其是政黨、輿論、壓力團體的影響力，均會造成國家政策變動來源，同時也就影響情報活動。政策面常會基於政治性因素、個人利益(選舉造勢)、領導人格與經驗背景等考量，因而將情報「政治化」(Politization)。政策制定者為強化其政策合理性，不惜另闢組織途徑，與不利於政策面之原情報機制相對抗或逕行取代，目的即在確實掌握情報對於政策的支持忠誠度。
二、「情報政治化」的發生有下列 3 種情況：
(一)當情報成為黨派、利益團體等政治勢力間的爭議問題，雙方或多方對於情報角色有不同意見，或對特定議題看法不同。
(二)某些情報議題曝光，成為社會輿論所關注與公共政策所面對的問題。
(三)專指情報體系、組織成員受到政策面壓力、影響與暗示，使得情報研判傾向政策面偏好方向、扭曲事實、將情報視為「討好」的工具。

「情報政治化」之政策面剖析與執行面剖析

例題

「情報政治化」(Politization of Intelligence) 是造成「情報失誤」(Intelligence Failure) 的主要原因之一，請試以西元 2003 年的第二次伊拉克戰爭為例，分別從「政策面」與「執行面」剖析美國情報機構如何受到「情報政治化」的影響？

擬答

一、政策面：
在西元 2003 年第二次伊拉克戰爭中，政策對於情報的影響，造成國家情報結論嚴重背離事實情況。
(一)美國政府為滿足政策需求，在情報來源不足，甚至分析結果錯誤之情況下，忽視中情局官員之意見。
(二)來自副總統辦公室及國防部長辦公室之壓力：以個人影響力壓迫情報機構選用有利於發動伊拉克戰爭之相關資料。
(三)美國政府已將可能與伊拉克相關之軍事行動，視為開戰之證據與事實，而不是持有具可能性的保守態度。
(四)決策者將情報機構之假設與質疑，作為背書與政策宣導。
二、執行面：
(一)美國政府擔憂情報相關之評估內容可能會阻礙攻打伊拉克之計畫，而派遣不具備情報官員身分之人員，尋找相關訊息，嚴重影響情報評估之流程。
(二)美國政府集結一群支持發動伊拉克戰爭之幕僚，除篩選有利於發動戰爭之資料外，並迫使情報機構對伊拉克與蓋達組織之關係及其所具備之大規模破壞性武器，作出最壞之解讀。

第二篇

情報蒐集與分析



情報來源之管道

例題

情報來源有很多管道，請試明之。

擬答

一、情報蒐集方式：
(一)秘密諜員蒐情：要能發揮接近對方核心機密、即時獲取原始情報、決策情報及內幕情報之作用。蒐情重點涵蓋戰略、戰術及戰鬥3個層面。目標是對象的決策和重要部門，以獲取與軍事防衛有關之政治、軍事、經濟、外交、科技等核心機密情報，而為國家和軍隊在制定方針、政策、作戰計畫方面提供依據。
(二)公開武官蒐情：武官在外交場合被認知為公開的軍事情報人員。可通過外交與社交活動、現場觀察、情報交換等來進行對駐在國、有關地區和全球性之軍事戰略動向；駐在國和有關地區之軍事及與軍事有關之各項情況；軍事科技情報，和其他有價值及臨時交付之軍事情報來進行蒐情任務。
(三)科技手段偵察：常用的是無線電技術偵察及衛星偵察。無線電數位偵察，包括無線電通信信號偵察和非通信信號偵察，是使用無線電技術設備，截收對手國所發射之各種無線電信號，從中獲取情報。衛星偵察則是藉由偵察衛星，進行對手國之機場、港口、飛彈基地、部隊及海面船艦活動等之情報蒐集。
二、情報處理後之分類，可概略分為以下2種：
(一)戰略情報：指導國家防衛所需之情報，亦即作為制定和實行國家戰略和軍事戰略，及指導戰爭之依據。包括對手國軍思想、戰略方針、軍備、戰爭潛力等。其任務是發現對手國發動戰爭，進行突擊徵候；查明其戰略意圖和作戰企圖；掌握重大戰略；注意國際情勢對戰爭立場之影響等。提供之情報，如軍事戰略概念之改變，預警、監偵、評估軍事與安全發展、預測未來情節而釐清國家之威脅與機會、預測對手之軍事能力等。另亦需慮及如何運用可能影響本國利益之衝突國家間的軍力平衡，及某種政治作為下，提供軍事援助之需求及衝擊。
(二)戰術情報：是組織實施作戰行動所需之情報，由於現代武器之提升，通信設備的保密，軍隊偽裝嚴密，部隊機動快速等特性，故以技術偵察為主要手段。任務是即時查明對手國軍事情況，及情況發展變化，為軍事將領研究敵軍活動規律、下定決心及作戰指揮，提供判斷之依據。分析的項目包含兵力結構之庫存及能力；軍事演習、維和等非傳統任務，國防安全政策之形塑與履行；國防建立之角色，包括軍文關係、擴散、低度衝突；武力部署之建構；軍事系統購買；軍事作戰行動之計畫與執行。此外尚有先進飛彈傳統武器之發展趨向、核武科技之輸出、合法及非法科技轉移、科技研發能力、能源使用情形等。

情報蒐集之途徑

例題

請概述情報蒐集之途徑。並請說明「人員情報」與「科技情報」之優勢及劣勢為何。

擬答

一、情報蒐集之途徑：
回顧情報蒐集活動歷史，吾人可發現：情報蒐集的途徑並無太大變化，仍以「人員情報」（Human Intelligence, HUMINT）及「科技情報」（Technical Intelligence, TECHINT）為主；改變的只是情報蒐集的能力高低而已。事實上，目前情報規劃下所進行之情報蒐集途徑仍以 HUMINT 及 TECHINT 為主，而僅將後者再予區分為信號情報及影像情報。情報蒐集即以前述情報種類為其工作對象。其次由情報蒐集途徑之過程加以區分，則情報蒐集又可分为二部分來探討：接近目標與蒐取情報。前者運用途徑包括：衛星、飛機、船艦、地面基地及海外工作據點等不同選擇；後者則利用高空照相設備、電子光學儀器、電訊監聽等特定或不特定之情報。
二、二者優劣勢：
科技情報（TECHINT）的水準雖然進步快速，且日趨重要，但傳統的人員情報角色及其功能仍然不可忽視，且無法被全然取代。一般而言，科技情報所蒐集的影像、訊號、通訊以及電磁波等資訊極為真實與寶貴，但通常只能提供靜態、片面、有限的訊息，雖能解答部分疑問，但卻難以提供完整的全貌，同時對於目標的意圖、戰略或政策更無法深入瞭解，因此，必須利用人員情報蒐集或竊取途徑，藉以彌補科技情報的侷限性；事實上，科技情報與人員情報之間應係相輔相成的互動關係。然而，由於運用與推動人員情報更需要組織力量，使得情報組織的重要性與必要性乃受到重視。

人員情報與間諜活動

例題

何謂人員情報（Human Intelligence, HUMINT）或間諜活動？

擬答

人員情報（Human Intelligence, HUMINT）亦被稱為間諜活動，為情報蒐集的第三種領域，可使用秘密幹員從敵人、對手、競爭者，有時甚至是友邦、盟國處竊取情報。長期以來，對從未接觸過情報工作的人而言，間諜活動是情報領域中最引人入勝之處，但實際狀況卻不如虛構小說所言那般刺激；可是有時可能像最精彩的間諜小說中所述一般危險與詭譎多變。
今日，美國の間諜活動仍然分屬中情局行動處，通常被稱為「秘密勤務」，以及國防部國防情報局之國防人員情報勤務處的職責。之所以要設立國防人員情報勤務處，係因中情局不會針對軍事戰術目標蒐集人員情報，故軍方需要增加人員情報蒐集的行動。之後在冷戰高潮期間，軍方特別成立蒐集人員情報的專責單位，但在國防部組織裁減時，這些單位也遭到解編，最後只剩下國防武官進行人員情報蒐集的工作，其工作通常涉及與駐在國聯絡單位的協調，而非典型的秘密間諜活動。
間諜活動應該是對付敵人的最終武器，而且應該在其他情蒐手段無法得手與根本無從下手時才能使用。因為全世界的間諜活動都是非法的，並且會讓遂行間諜活動的人以身涉險。儘管間諜活動是非法的，大多數國家卻也都接受自己可能淪為間諜活動的目標這個事實，所以容許外國情報官員進入國內任職，因為他們也可以在海外從事相同的間諜活動。

以目標為中心的情報分析流程

例題

- ▲美國情報分析家羅伯特·克拉克（Robert M. Clark）提出「以目標為中心」的情報分析流程，為情報體系提供了一種減少情報失敗的新嘗試及途徑。請試說明其內容為何？

- ▲【相關問題】對於情報處理的流程，在傳統上多數學者均認為，基本上是遵循著所謂的「情報循環」（Intelligence Cycle）在進行。但當代美國情報學者克拉克（Robert M. Clark）則認為並非如此，並提出以「目標為中心」（Target-centric）的主張，才是較符合情報處理的實際過程，請比較說明前述二種主張的內涵及差異？〈108 警特三〉

擬答

由於情報分析工作不斷的資訊化、一體化、複雜化，使得傳統的情報週期和情報過程理論的解釋力已不足。且美國情報體系檢討從珍珠港事件爆發後至 911 事件，再到誤判伊拉克擁有大規模毀滅性武器事件，發現導致情報失敗有 3 個共同原因：
一、情報蒐集與情報分析者未能充分的共享資訊。
二、情報分析者未能客觀的分析其所蒐集到的資料。
三、情報顧客未能根據情報及時採取行動。
而舊有的情報週期或情報過程概念上，存在很多缺陷，導致情報活動各個環節之間產生諸多隔閡和壁壘，使情報與決策、行動之間，產生孤立與脫節，並缺乏良好的互動，極易誘使情報失敗的情況發生。因此，美國情報體系極需要對「以目標為中心」的情報分析流程此一全新概念，進行深入的研究與探討，以改進傳統的情報理念，避免情報失敗的情形再度發生。
一、「以目標為中心」的情報分析流程強調，全部利益相關者（包括：情報顧客、情報蒐集人員、情報加工人員、情報分析者、情報規劃與建設系統，以及支持他們的其他人員），應更為直接的參與情報的生產流程，建立一個共享的目標圖，對最終情報產品共同負責。同時，參與人員也能夠根據自己的資源，圍繞著同一目標做出個別的貢獻，從而促使目標圖更為全面精準，讓所有的利益相關者，均能以目標圖為中心，獲取他們所需要的資源，來展開各項情報相關工作。基本上，該流程不是一個線性流程，也不是一個循環週期，而是一個網絡流程、社會流程，並且所有的利益相關者都以目標為中心。
與舊有的情報週期或情報過程不同，在於「以目標為中心」的情報分析流程中，情報顧客與情報蒐集人員也加入這個流程之中，他們對目標也同樣有一些具價值的見解。這也使得情報分析者必須履行建立和維護目標圖，找出並將情報顧客的情報需求轉化為新的資訊需求，提取可行性情報並確保將其傳遞給情報顧客等職能，並且還要管理情報分析流程並向其他參與人員傳遞資訊，以確保整個流程正常運轉。
二、目標的定義：
(一)把目標當做一個複雜的系統。
(二)把複雜的系統看作是一個網絡。
三、正確處理情報分析者與情報顧客之間的關係：
(一)使情報顧客理解資訊。
(二)使情報顧客採納資訊，並據以採取相應行動。

第三篇

反情報、 秘密行動、 公開情報



 反情報工作之爭議

例題

反情報常因其工作性質與手段方法特性等因素，往往遭到外界誤解、猜疑甚或排斥；試問，反情報工作通常會引起哪些爭議？

擬答

反情報工作主要引起下列爭議：
一、法律妥適性之質疑：
因反情報工作通常以具有侵犯性之手段進行，使該工作的適法性飽受質疑。而為避免造成警察國家或落入白色恐怖之中，國家應建立適當之法規範，建立有責性制度與受侵害時國家賠償之機制。
二、人權侵害的疑慮：
因反情報工作需要，將對於與情報活動對象相關之本國人民予以觀察、監視以獲取必要情報，此種作法勢必影響人民權益。

秘密行動之概念及類型

例題

「秘密行動」(Covert Action)之概念及類型為何？並說明其引起的爭議。

擬答

一、「秘密行動」之概念：
秘密運用金錢、物質、婚姻、關係等作為影響他方（人物或國家）而增進己方利益，且儘量不暴露己方介入角色之活動，以及運用其他介入角色之活動，以及運用其他介於武力（軍事力量）與外交（正面談判接觸）途徑之間的選擇，如「準軍事行動」（Paramilitary Operation）、宣傳、暗殺（已廣受爭議而遭明確禁止）等促使情勢發展有利己方利益之作為，皆與秘密行動的概念相符；故可將秘密行動的概念界定為以下 4 點：
(一)秘密行動的目的應配合國家政策目標並促進國家利益。
(二)秘密行動的屬性是為國家政策運用與執行之工具選擇。
(三)秘密行動的取向應多為外向、對外的，極少在國內進行。
(四)秘密行動的途徑係介於軍事與外交之間的選擇。
二、秘密行動之類型：
一般而言，約可分為 4 類：
(一)宣傳（Propaganda）：係最廣泛使用之秘密行動；有時亦稱為「心理戰」。其目的在於將己方信念、價值、觀點、「別有用心」之訊息等，散布、流傳與接收於特定對象（社會、國家）之內，進而影響其人民、政府對外（己方）政策，以符合己方期待獲取之利益。
(二)政治（秘密）行動（Political Covert Action）：基本上，宣傳應也是政治行動的一種。目的皆在影響對方社會輿論與信念。但後者更強調積極介入、影響當地政治（理念與勢力）平衡，支持或打擊特定派系、人物或政黨而更進一步擴大利益。
(三)經濟（秘密）行動（Economic Covert Action）：與政治行動相同的是，其目的均在影響對方政治及對外政策；不同的是，經濟行動偏重經濟手段的運用，擾亂對方經濟，達到政策面運用情報（秘密行動）活動之政策目的。
(四)準軍事（秘密）行動（Paramilitary Covert Action）：此項秘密行動的爭議性最高，同時也花費最高、不易維持秘密行動之隱匿機密特性。

三秘密行動所引起的爭議：

秘密行動之所以引起爭議，主要係因為各類型之秘密行動的本質（道德問題、秘密色彩、不易監督等問題）以及其行動目的所欲達成之政策（是否合適、合乎國際法及相關規範等），另外，秘密行動是否容易「自行其事」、「回銷國內」而有失去控制及侵犯民權之虞，皆使得該項行動蒙上爭議色彩。

第四篇

美國情報制度



美國之情報體系

例題

試說明美國之情報體系結構特性、情報機關成員及任務為何。

擬答

美國情報體系（Intelligence Community, IC）之建立，係依據西元 1947 年之「國家安全法」，設立「國家安全會議」與「中央情報局」（CIA），開啟美國建構中央化情報體制的歷史。而鑒於 911 恐怖攻擊事件，美國為強化情報與國土安全防護能力，於西元 2004 年通過「情報改革與恐怖主義防制法」，重整其情報體制，提升反恐與國土安全情報能力，將兼任中情局局長職務的「中央情報總監」（DCI）改制為「國家情報總監」（DNI），領導整合協調各情報機關，並不再兼任中情局局長，在此組織整合的變動下，目前美國情報組織主要有以下單位：
一、獨立機關：
（一）中央情報局（Central Intelligence Agency, CIA）。
（二）國家情報總監辦公室（The Office of the Director of National Intelligence）。
二、國防部：
（一）國家安全局（National Security Agency, NSA）。
（二）國家偵察辦公室（National Reconnaissance Office, NRO）。
（三）國防情報局（Defense Intelligence Agency, DIA）。
（四）國家地理空間情報局（National Geospatial-Intelligence Agency, NGA）。
（五）美國網戰司令部（United States Cyber Command, USCYBERCOM）。
（六）美國航空情報中心（Twenty-Fifth Air Force, 25AF; National Air and Space Intelligence Center, NASIC）。
（七）美國陸軍情報及安全司令部（Intelligence and Security Command, INSCOM）。
（八）國土情報中心（National Ground Intelligence Center, NGIC）。
（九）海軍陸戰隊情報中心（Marine Corps Intelligence Activity, MCIA）。
（十）海軍情報辦公室（Office of Naval Intelligence, ONI）。

三國土安全部：
(一)情報及分析辦公室（Office of Intelligence and Analysis, I&A）。
(二)海岸警衛隊情報單位（Coast Guard Intelligence, CGI）。
四能源部：情報及反情報辦公室（Office of Intelligence and Counterintelligence, OICI）。
五國務院：情報及研究局（Bureau of Intelligence and Research）。
六財政部：恐怖主義及金融反情報辦公室（Office of Terrorism and Financial Intelligence, TFI）。
七司法部：
(一)毒品管制局（Drug Enforcement Administration, DEA）。
(二)聯邦調查局（Federal Bureau of Investigation, FBI）。

 美國聯邦調查局

例題

試述美國「聯邦調查局」在情報體系內所擔任的角色及其工作內容。

擬答

司法部聯邦調查局一直是美國國家情報體制內重要成員，而其主要職責除刑事執法
、犯罪偵查、國內反恐怖活動之外，反情報安全工作是聯調局另一重點任務。根據
雷根總統所發布之行政命令（E.O. 12333）規定，聯調局負責並協調國內反情報安
全工作，且可在國內蒐集外國情報活動資料，支援對外情報蒐集與通訊安全。
此外，面臨國際恐怖主義及其活動所形成之惡劣情勢，再加上本土極端偏右政治團
體之爆炸或破壞等恐怖活動所造成的安全威脅，聯邦調查局已然調整任務取向、資
源與人力配置，成立反恐怖任務中心，並加強國際治安合作與情報交換，增強反恐
怖的因應能力。同樣的，該局亦於西元 1993 年間，結合中情局、國防部、司法部毒
品管制局與國稅局等相關單位人力資源，以任務編組方式成立緝毒情報中心，強化
反毒能力。

第五篇

英國情報制度



英國情報體系

例題

試說明英國之情報體系結構特性、情報機關成員及任務為何。

擬答

一、首相內閣辦公室（Cabinet Office）之情報機構：
（一）首相國家安全顧問（Prime Minister's National Security Adviser）：主要負責提供國家安全建議、協調政府安全議題以及監督國家安全會議。
（二）聯合情報委員會（Joint Intelligence Committee, JIC）：主要職責在於提供政策建議，並有效協調各部會，確保情報與安全機關之運作和諧。
二、英國安全局（Security Service, MI5）：
舊稱為軍情五處；西元 1989 年通過《安全局法（Security Service Act）》後，確立其法律地位及法律任務，並受內政大臣督導。其職責如下：
（一）保護國家安全，尤以防止間諜活動、恐怖主義或其他可能破壞民主政治之手段為主要任務。
（二）阻止英國以外人士進行的威脅行動或意圖，以保障經濟利益。
（三）預防嚴重犯罪並支援其他執法機構。
又為統整情報之處理與分送，藉以因應國際恐怖主義的威脅，西元 2003 年於安全局內成立「聯合反恐中心」（Joint Terrorism Analysis Centre, JTAC），由軍事情報局、其他相關部門（如內政部、外交部）之代表以及警察單位組成。
三、秘密情報局（Secret Intelligence Service, SIS）：
通常被稱為軍情六處（MI6），主要進行安全、國防、外交、嚴重犯罪、經濟政策等領域之外國秘密情報蒐集。其執行任務則依聯合情報委員會（JIC）之指示與要求，而依《情報工作法（Intelligence Services Act）》規定，受外交大臣督導。
四、政府通訊總部（Government Communications Headquarters, GCHQ）：
隸屬於外交部，其主要任務為截取通訊蒐集信號情報（SIGINT），以及為國家技術管理機構提供服務和諮詢。
五、國防情報局（Defence Intelligence, DI）：
隸屬於國防部，主要任務在於蒐集軍事方面的情報並進行全源情報分析，以輔助決策，進行危機管理。

第六篇

他國與我國之 情報制度



中國情報體系

例題

試詳述現今中國之情報體系之主要成員組織及其任務。

擬答

中國現今之情報體系詳述如下：
一、黨系情報組織：
以下 3 個組織均由中央辦公廳直接管理。
(一)中央調查部：對內主要負責各地區之政、經、文化及社會等方面之調查，對外則藉各種方式進行情報蒐集活動。
(二)中共中央對外聯絡工作部：簡稱為中央聯絡部，主要任務為與世界各共產國家及非共產國家之共產團體或左派團體聯絡。
(三)中共中央統一戰線工作部：簡稱為中央統戰部，負責進行統戰活動。
二、軍系情報組織：
(一)總政系統：
1.總政治部保衛部：防範、偵查軍隊內部危害國家利益之行為及境內、外敵對勢力之滲透、破壞活動。
2.總政治部聯絡部：主要工作為從事攻勢反情報。
(二)總參系統：
1.總參二部：主要任務在於蒐集軍事情報。
2.總參三部：主要負責監聽。
3.總參四部：主要負責電子情報之蒐集。
三、政系情報組織：
(一)公安部：中共透過分布各地的公安分支機關與龐大公安警力，利用治安整頓、戶籍登記、交通控制、邊防守衛、偵查犯罪、入出境管制、警衛安全等管理作為，除維持社會秩序與安全外，並進行對內反情報、反顛覆以及打擊反革命勢力的保衛任務，達到全面性社會控制的目的。
(二)國家安全部：主要任務在於領導與管理國家安全和反間工作、密切注視與掌握外國及臺灣間諜活動、防範特務竊密與破壞陰謀、指導各部門有關反間諜、防策反工作等項目。

第七篇

情報改革與 國家情報制度發展



我國情報機制與能力之改進與強化

例題

美國情報工作一向非常落實，美國經驗對我國情報改革有何啟示，尤其對我國情報機制與能力之改進與強化，又可提供哪些建議？

擬答

<p>美國經驗對我國情報機制與能力之改進與強化，似可提供下列建議，包括：情報統合、情報蒐集、情報研析、情報分享與合作、反情報及安全防護、情報科技、國會情報監督等主要面向。謹說明如下：</p>
<p>一、情報統合方面：</p>
<p>(一)進一步確立並強化國家情報統合機制：觀諸 DNI (Director of National Intelligence, 國家情報總監) 朝向強化情報統合協調之實踐經驗，我國亦可考慮研議方案，經由立法（如國家情報工作法及相關子法等）途徑，再結合行政協調及國會監督，明確地發揮國安局統合情報工作之法定地位及權限，同時增強情報機關間以及情治機關間之協調與合作。</p>
<p>(二)釐清與定位情報和政策間之互動關係：觀諸美國近年來情報失敗之肇因，多係「情報政治化」所致，是以，國安局等情報首長於規畫政策及執行工作時，應妥慎掌握情報與政策間之分際，依循「情報國家化」、「情報中立化」等原則，堅持情報之客觀性與中立性，避免情報政治化之困擾。</p>
<p>(三)建立情報機關監督人員職位輪調或聯合任務制度：參照美國改革經驗，若能有可行之人事制度等相關配套措施，建立情報人員輪調制度或聯合任務作法，應可促進機關間之協調與合作，並可研議透過法制、機制、執行等途徑，改進情報與治安執法機關間之情資分享與工作協調關係，發揮情報所應有之及時性、引導性與輔助性作用。</p>
<p>(四)調整「情治分立」朝向「情治協力」發展：美國情報要點之一，即在增進情報面與執法面間之協調與合作，並強調「情治協調」；對於我方而言，基於安全威脅性質轉變，跨國安全威脅趨於嚴峻，再加上民主法治根基應已穩固，防治情報濫權之「情治分立」傳統原則亦已深植，情治之堅實須建構新的「協力」合作關係，方能因應新興安全威脅之挑戰，事實上，西元 2005 年「國家情報工作法」之立法意旨，即係將「情治分立」轉向「情治協調、合作」，增進情治雙方因應新興挑戰之效能。</p>

二、情報蒐集方面：
(一)重視人員情報蒐集能力：觀諸美國將人員情報賦予中央情報局（CIA）進行統合協調，藉以提升情報成效之作法，對於我方而言，人員情報是我國比較優勢所在，似應增加資源投入與政治重視，建立人員情報發展原則與策略，並結合我國優勢條件與最新科技，加強招募與吸納適當人員，進一步強化人員情報蒐集能力。
(二)建立綜合性情報蒐集能力：參照美國情報改革經驗，其亦強調各種情蒐途徑之強化與整合，事實上，提升情報能力，不能忽略人員情蒐、科技情蒐、公開情蒐、合作交流等四主要途徑，俾能建構綜合性情蒐能力，對於我國而言，加強人員情報及公開情資蒐研分析，即係值得重視的新方向。
三、情報研析方面：
(一)重視情報分析人力資源建設：觀諸美國大幅增加情報人員教育訓練預算，並建立國家情報大學、反情報訓練所等機制，目的在提升其情報分析人員素質；對於我方而言，情報人力資源建設，除應兼顧當前情報蒐集與研析外，應增加戰略情報研析單位之預算、人力、重視等支持，提升或鼓勵人員參加訓練、進修、參與會議或國外訪問等機會，並能結合外部專家學者研究成果。
(二)建立前瞻性趨勢評估機制：觀諸美國設立國家情報委員會（National Intelligence Council, NIC）及製作長期性趨勢研判報告等作法，對於我國而言，應有必要考慮設立長程戰略情勢分析機制，對於未來 10 年至 15 年之環境情勢發展，提出前瞻性、長程性或長期性之戰略研析報告，供政府及相關部會制定政策之參考。
(三)運用公開資訊以提升分析品質：觀諸美國擴大公開資訊運用層面與範圍，並建立公開情資中心等作法，對於我國而言，有效運用公開情資，應逐步擬定公開情資發展策略，引進與運用最新資訊科技，訓練公開情資專業人才，結合民間智庫資源，並建構公開情資與祕密情資之互動機制與規則。

四情報分享與合作方面：
(一)增進情治情報分享效能：研議如何透過法制、機制、執行等途徑，改進情報與執法機關間之情資分享關係，發揮情報所應有之及時性、引導性作用。此外，可利用資訊科技和網路科技優勢，建立情報資訊與研析報告資料庫，隨時更新資料，並在安全考量範圍內，開放情治機關加以運用。
(二)強化國際情報合作成效：研議擴大情報合作面向與範圍，持續加強國際情報合作關係，並積極拓展與國際重要智庫、國際組織、非政府組織或前官員之互動關係，建立更為綜合性之情蒐或察證管道。
五反情報及安全防護方面：
(一)進一步確立與強化國家反情報機制：觀諸美國建構國家反情報執行長（National Counterintelligence Executive, NCIX）以統合反情報體系之作法，對於我國而言，應有值得參考之處，建議可先修正「國家情報工作法」，確立反情報工作之法律地位與授權，提升反情報統合層級至國安局，並建立完整之反情報策略，兼顧防衛性與攻擊性反情報工作。
(二)進一步重視與落實保防機制及工作：觀諸我國保防工作時有漏洞，是以，有必要檢討現行反情報或三大保防體系成效，包括機關保防、軍中保防及社會保防，確立保防工作法律地位與受重視性，並增加預算資源，加強人員訓練，提升員工工作士氣，以增進保防工作成效。
六科技情報方面：
(一)結合電腦科技與網路資訊技術：觀諸美國重視科技設施規畫、購置和運用作法，以提升情報分析成效，對於我國而言，不僅最高情報機關應率先推動情報分析改革，引進最新電腦科技與網路資訊技術，並提升人員運用科技成效，且應協助其他情報機關與準情報機關，建構必要設施與提供教育訓練。
(二)運用科技創投或民間合作途徑：可仿效美國 CIA 設立科技創投公司（如 In-Q-Tel）作法，成立合法公司，透過公開及合法之投資研發途徑，以最低成本、較快速度，獲致符合情報工作需求之相關科技。此外，可整合情治機關之科技裝備需求，透過補助研究途徑，鼓勵大學或公私立研究機構投入情報科技研發與應用，以最低成本、較快速度，獲致符合情報工作需求之相關科技，如資料庫建構及資料搜尋系統等。

七國會監督方面：
(一)立法院應建立情報監督專責機制：觀諸美國情報改革動機，加強國會監督一向主要推動來源，是以，對於我國而言，為建立權力制衡制度，立法院應考慮設立專責監督委員會，並通過必要之配套措施，進一步落實施政質詢、調閱資料、聽取報告等作為，並將問政焦點置於情報機關之任務、能力、成效、控制與監督等議題。
(二)監察院應進一步發揮與強化情報監察功能：因我國現行法制，相對於立法院常用之調閱權，監察院應利用調查權，依法深入了解與探究情報機關運作，藉以監察情報機關及人員活動是否合法性與正當性，未來應朝向充實情報專業調查人力，提振與發揮監察功能之方向發展。

第八篇

情報監督 (或稱情報控制)



民主國家之情報監督機制

例題

- ▲民主法治的國家，對情報有哪些監督機制？

- ▲【相關問題】情報監督機制有那些種類？以我國而言，那一個情報監督機制最為有效？試說明理由。〈106 國安局〉

- ▲【相關問題】情報工作的效能與民主體制常無法取得精準的平衡點，但國會對情報單位的監督則是落實民主制衡的重要機制。試問國會有效監督情報單位的條件為何？〈106 警特三〉

- ▲【相關問題】國會監督為當前世界各國最主要的情報監督方式之一，但國會對於情報事務監督卻未必能完全發揮功效，而必須有相關條件的配合，試說明影響國會監督成效的主要因素有那些？〈107 國安局〉

- ▲【相關問題】在監督情報機關方面，一般民主國家的國會往往因為受到那些因素影響而難以完全發揮監督功能？〈109 國安局〉

- ▲【相關問題】「情報監督」(intelligence oversight) 是權力分立與制衡的重要機制，用以維護人權與確保民主。請說明：「情報監督」的概念與內容為何？〈110 警特三〉

擬答

一、行政監督：
(一)上級的監督：情報機構係屬於行政體系之一部，因此，在體制上自然必須接受所隸屬之各級長官以致於最高行政首長之指揮監督。
(二)機關的相互監督：將情報事務分別交由不同的情報機關掌理，不僅可使其職權單一易於發揮功效，又可使其權力分散並能相互制衡，而產生監督的效果。
(三)內部的監督：情報機關不論其內部的一切以及包括所負責的各項工作，一般皆極具敏感性或涉及國家重要的機密，故而情報機構皆會建立嚴密的安全管制措施，以防止機密的外洩。
二、情報國會監督（又稱情報立法監督）：
在民主憲政體制之中，由人民選出的代表所組成的國會，原本即負有監督政府之職責，而國會監督權的行使，主要係透過經費預算的審核，以及相關法案的審議，以使行政機關必須將其年度工作計畫、目標等工作重點向國會提出，以爭取國會的同意與支持，而通過其預算與相關之法案，國會亦可藉審查預算與法案的機會表達國會的意願與期望，或是制定行政機關應遵守的制度規範，以使行政機關的所作所為不至踰越國會所制定的規範。
情報國會監督（又稱情報立法監督）：係立法與行政部門間的制衡作用。國會監督是民主政治與有責任性理念的具體反映，也是各項情報監督中最重要的一項。具體的途徑包括：「情報預算及經費的審核」、「情報法規和情報監督法規的制定或修法」、「情報人事命令的同意權」、「情報失敗或醜聞的調查」、「國會議員的質詢與辯論」等。
(一)消極面：可以防杜不法與不當的情報活動。
(二)積極面：可強化情報組織的情報能力，並提升情報組織的形象。
至於國會監督的運用方式，包括：
(一)預算審查權。
(二)法律審查權。
(三)立法院針對特殊議案取得文件調閱權，此調閱權即為國會調查權。
(四)質詢權。
(五)彈劾權。
其中，預算審查權及法律審查權為主要監督方式；而質詢權及調閱權則較具實質手段及意義。
此外，若立法院對於情報機關（構）過度監督，將會對情報機關（構）整體運作產生嚴重影響，同時，對於涉及國家安全情報機密預算應予適度的保護。故關於情報機關（構）的預算編列及執行，應以秘密方式為之。

<p>另，國會有效監督情報單位的條件如下（另參汪毓璋著，2018，《情報、反情報與變革（上）（下）》，頁 692 ~ 694）：</p>
<p>(一)預算權屬立法院對於情報機關（構）經費運用的事前審查程序；而決算權則係年度結束後之事後經費支出審查機制，由監察院審計部掌理。因此，二者審查機制，並非由同一機關進行對其進行監督，此一監督機制尚有爭議性、易有弊端滋生。</p>
<p>(二)監察院審計部對於情報機關（構）之決算事項，具有實質的移送權，但爭點在於：1.審計部對於情報機關（構）的執行情況，無法掌握其具體運作模式、2.且決算權係屬事後審查機制、3.再加上審計部缺乏立法院之質詢權、調閱權，因此，審計部所能掌握的經費執行狀況，均以情報機關（構）公開之部分為之，而未公開部分則無法進行調查，致易產生弊案（例如國安密帳）。</p>
<p>(三)由於審計權的分立，立法院與審計部在法律制度上不能合作，致使立法院的預算審查權和審計部的決算審議權二者無法合一。建議策進作為：</p>
<p>1.審計部若發現不法情事，可求助立法院之文件調閱權取得相關資料由審計部審議，並據以決定是否移送司法院進行彈劾。</p>
<p>2.立法院之預算審查部分，亦可間接地把預算審查權與決算審議權結合成為一。然而，法制上的跨院際合作，須透過修法，才能符合法制化程序。</p>
<p>(四)現行立法院組織法中，尚未有超然的委員會（例如情報委員會）對情報機關（構）進行監督。因此，對於情報監督，僅能透過國防、外交或其他委員會等，組成聯席委員會對情報機關（構）進行監督。</p>
<p>(五)國會無法對情報事務進行統一的監督，在於缺乏有效的監督機制，而情報失靈（敗）現象就無可避免，無法實際對情報機關（構）進行合法性監督。因此，可仿效美國國會設置情報委員會，進行監督，以統一情報機關（構）之運作；另，對於情報機關（構）之機密的情報政策、預算、法案，若能透過情報委員會之監督，即能實際瞭解情報機關（構）內部的運作，而得以更加法制化、專業化。</p>
<p>最後，影響情報國會監督成效之因素如下（參王政著，《國家安全情報監督之研究》，警大版社，104.3，頁 57 ~ 60）：</p>
<p>(一)國會議員的監督意願是決定國會監督成效的首要因素。</p>
<p>(二)情報事務有其高度的複雜性，同時，也反映著國會議員關於情報事務專業度之不足。</p>
<p>(三)監督者與被監督者缺乏互信。</p>
<p>(四)情報機關拒絕提供必要資訊是情報監督機關是執行情報監督最大的障礙。</p>
<p>(五)國會議員可供質詢的時間不足，而且他們也不願意花時間在情報這個不易引起公眾矚目的議題上。</p>
<p>(六)黨派之爭常常會影響到國會情報監督的進行或易流於形式。</p>
<p>(七)國會資源不足，使國會議員常常無法有效發揮問政功能。</p>

三司法監督：
受限於情報活動之隱密性及司法的懲罰乃於行為後之被動性與事後性，亦難發揮事前防範監督之效，故透過訴訟由司法機關介入調查審理，形成判例與解釋，間接達到對情報機關監督之目的。憲法中亦賦予人民在刑事訴訟程序上的保障，包括偵查、搜索、監聽、逮捕、追訴、審判及刑之執行等人民身體自由及生存權的保障。若國家機關在犯罪調查及案件偵辦過程中，有違法或不當行為因而侵犯人民的權益，人民可以採取訴訟為之抗衡。
四情報媒體與社會監督：
民主之價值即在人民的參與，社會監督的要義就是透過大眾的輿論及媒體的報導來引起立法機關的注意，並敦促行政機關的守法與改善，這些都表現在「言論自由」與「新聞自由」上。經由輿論、媒體及學界對不法或不當的情報活動督促與評論，促使行政部門與國會採取必要的糾正措施，並可藉由宣傳喚起大眾對情報與國家安全的關切、認知及評議。
五調查委員會：
在民主國家，關於國家安全與情報的議題上，如係認為當前或過去的事件有調查必要時，可由行政部門或國會組成特別調查委員會（Commission of Inquiry）。

觀念補充

我國情報工作監督之相關法制問題研析（參立法院：<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6586&pid=84416>）：

「維護國家安全及利益」是國家情報工作法制定的目的之一，故情報手段在執行過程之適法性，實為我情報機關均應遵循之首要之務。由於情報工作之秘密性質以及涉及國家重大利益使然，一般對於情報機關在法律政策上皆有較特殊的設計，例如任務範圍廣泛、手段概括授權、監督方式秘密等，向來被視為理所當然。為維護國家生存與安全，情報機關得便行事，有時不免干涉人民基本權，由於情報活動的機密屬性，人民基本權若遭受情報機關侵害亦不自知，兼之以情報機關掌握許多資源，若不施予適當之監督，難保不會有濫權或侵害人民權益情事。

審視本法規範，情報資訊之蒐集，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星（光纖）偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。從前述偵蒐內容以觀，在在均有觸及人民隱私及資訊自決之可能，由於秘密蒐集方式，具有不易為對象察覺和容易滲透接觸到對象生活中各項行動的特點，也容易侵犯人民的合法權益。此外，資料蒐集後的運用、儲存及情報交流的過程，亦仍有再次侵犯人民權益的可能性，故情報機關於執行相關事項時不可不慎。另現行法定之情報機關及視同情報機關之功能與職掌，未將具爭議性之治安機關排除於情報機關之列，讓情報的歸情報、治安的歸治安，實難以消解人民對情治兼具可能違法濫權之疑懼，

情報工作具有特殊性和隱密性，在國家邁向民主化的過程中，若不將情報活動法制化，並予以適當規範，極易造成專制、濫權，並導致權謀違法、營私舞弊，甚而以監控迫害之手段打擊異己、戕害人權。因此情報活動常被稱為「法治國的黑森林」，對情報工作侵犯人民權益之可能性，亦為世人對情報工作的普遍觀感。然近代以還，世界各國對於情報活動應予法制化，並受人民監督之看法，幾無二致。基於民主法治國家之核心價值，國家安全亦不可無限上綱，國家權力的基礎是國民的付託，在民主國家中，任何具有國家權力職權，都是職權有限並負有義務的職務。國家機關取得權力只是手段，其目標是維護社會秩序及增進公共利益，故國家機關對違反公共秩序或對社會共同體造成侵犯的行為，應予以制裁，此不僅為國家的權力作用，亦為國家對人民的最低保護義務的履行。

國家情報工作所欲實施通訊監察的對象，並非以一般無害的人民為監察對象，允宜參酌先進民主法治國家，建立符合民主程序之情報監督機制，加強對情報的約制與監督，使情報嚴守政治中立，為民主服務，為國家服務至為重要。

第九篇

情報與國家安全



國家安全政策制定過程

例題

請以「理性行動」、「組織過程」、「官僚政治」、「個人決策」、「團體決策」等 5 個模式，說明如何應用於國家安全政策制定過程。

擬答

5 個常見的分析概念架構或研究途徑的內容如何結合應用於國家安全政策制定過程：
一、理性行動者模式：
(一) (國家) 政府行動乃方案選擇 (Choice) 之結果，目的在極大化其戰略目的與目標。
(二) (國家) 政府視為一理性、單一 (Unitary) 的行動或決策者。在選擇與實踐方案過程，政府行動者只有一組特定目標、認知方案及唯一的後果預估。
(三) (國家) 政府因應內、外威脅或機會而採取行動以增進國家安全與利益。但其選擇方案係靜態抉擇 (static selection)，目的就「所有」方案中選擇增進最大利益與價值的方案。
二、組織過程模式：
組織理論的假設基礎有最大理性與有限性 2 種；尤其後者強調人類因其生理與心理上能力之限制，勢必將侷限個人與組織的決策過程。而在組織過程中模式思維下，分析者將 (國家) 政府行為加以分解，強調組織利益常模程序、非單一理性的特點；其目的在於探討組織行為之運作及其聯合。
在國家安全政策制定過程中，其所思考的內容為：
(一) 政府由哪些組織單位所組合而成？
(二) 每個組織傳統上所負責面對的問題為何？該組織的相對影響力如何？
(三) 這些組織在政府決策過程中，提供資訊以解決各決策階級中所產生的問題，具有哪些標準作業程序 (SOPs)、行動計畫與既存方案？
(四) 各組織產生與執行方案選擇時，有哪些 SOPs、行動計畫與既存方案？

三官僚政治模式：
官僚政治的基本概念在於，參與政治過程之成員皆分享不同程度的權力；由於人
人意見不同而使得政府決策或行動成為政治過程的結果，詳言之：
(一)政府部門係由具有不同目標與目的之個人與組之所組成。
(二)所有政治過程參與者皆具有權力，雖權力大小不同但並無絕對優勢者。
(三)藉由政治過程所做之決定為「政治結果」，即所有參與者之議價與協調之結果。
(四)政治結果至其實踐仍有相當差距，亦即決策至實踐皆為政治過程。
四個人決策模式：
從「個人特性」（人格特點、信念、態度、價值、知識背景、生活經濟等）的特
徵，可提供推斷其政策行為取向。M. Hermann 提出下列命題，可作為解析個人決
策對於國家安全政策制定過程之重要參考。
(一)決策者的民族主義傾向（Nationalistic）愈強，其對外政策衝突取向愈強。
(二)決策者成就需求愈強烈，其政策行為取向愈趨向合作性。
(三)決策者愈教條化，愈不可能改變其費心制定之政策立場。
(四)決策者愈馬基維利（Machiavellian）權術追求取向，愈傾向密切互動對外政策。
五團體決策模式：
首先，在解析國家安全政策制定過程中，若以「團體」為決策分析單位，則由觀
察團體決策結果是否能夠迅速獲致共識與否，而決定該團體之內部動力（Internal
Dynamics）是否成為分析焦點。若要解析該團體所負責之國家安全政策制定過程
，只需集中焦點於該團體之內部動力特性即可。反之，若團體無法獲致迅速共識
，則必須考慮團體外之其他因素對於決策過程的可能影響。其次，若以團體為分
析單位，則團體決策的過程、型態及結果均將受到團體的特性所制約。

第十篇

精選歷屆試題



101年度考題

例題

面對當前經常無法預測的風險及隱藏與快速變化的威脅，情報工作已較以往面臨更大之挑戰。因此，在此等不同以往新的安全環境變化下，情報單位（Intelligence Community）要為總統等情報顧客（Customers）創造決策上的優勢，則其欲達成此項目標之努力必須基於哪些原則？又必須完成哪些任務，才能建構成為符合西元 21 世紀需求之情報企業？

擬答

在此等不同以往新的安全環境變化下，情報單位（Intelligence Community）要為總統等情報顧客（Customers）創造決策上的優勢。所謂決策優勢（Decision Advantage），係指調動情報所有相關方面以獲取或提供信息，而形成一種競爭性或邊緣性的優勢。此種優勢除了能夠消除決策者搖擺不定的心態，使其付諸行動之外，並能夠促進決策者的決策能力，以達到真正的情報客觀性。故為實現決策優勢，決策與情報之間必須保持相關性與客觀性。
一、為創造決策上的優勢，須基於下列原則執行之：
（一）由於未來的情報更需要具備評估、感知「微弱信息（Weak Signals）」、問題所在及安全風險的能力，故使決策者做好應對戰略突襲的準備，並準備關鍵性之早期徵兆以向決策者發出警報，為情報的關鍵性角色。
（二）競爭國家若掌握我方情報，應視其為騙局或假情報而加以否定；相同地，應獲得對於我方更具有優勢與重要性的信息。
（三）全球意識（Global Awareness）：係指開發、理解以及控制當今大量分離的全球信息。
（四）戰略預測（Strategic Foresight）：除了深入研究已存在的條件，亦應使用對於該條件的回應來改變假設與方案，並確定其聯繫與可能性。
二、為建構成為符合西元 21 世紀需求之情報企業，須完成下列任務：
（一）必須通過一個新的國家情報戰略，即能夠表示我方關鍵力量標誌的戰略路線圖，以及發展與管理規定任務和進度的年度實施計畫，以聯合情報企業。
（二）進行制度化的變革：可採用能夠確保短期勝利、評價以及獎勵業績、保證持續進步等方式；甚至高層人員必須致力於建立一種勇於承擔風險，並將構想付諸於實際的文化。
（三）情報界需要與外界展開合作交流，來為情報企業所有組織成員提供能量，故而需要強而有力的領導力量，以頑強不屈的奉獻精神，以及被授權變革的機構，組成改革的一大動力。
（四）許多關鍵領域必須共同承擔責任，如機構、計畫（項目）管理人、部門長官（職能領導）、任務（反恐、反擴散、反情報）等。

105年度考題

例題

- ▲ 情報分析者 (Intelligence Analyst) 居於情報蒐集者 (Collectors) 與情報運用者 (Customers) 之間，是情報活動的核心與成敗要素之一。請針對蒐集者與分析者之間、分析者本身、分析者與運用者之間等三個部分，分別說明影響情報分析失誤或失敗的原因為何？

- ▲ 【相關問題】情報分析 (intelligence analysis) 是情報過程 (intelligence process) 及情報工作非常重要的環節，亦是影響情報品質與決策的關鍵因素。請說明情報分析受那些因素的制約 (即指限制與約束)，影響研析人員和決策者的判斷？〈110 國安局〉

- ▲ 【相關問題】情報分析能力是影響決策過程的關鍵因素。試述情報分析在哪些因素的交互作用之下，影響研析人員和決策者的判斷？請列舉四項因素，並分別舉例說明之。〈107 公安所〉

- ▲ 【相關問題】危機處理過程中，情報是危機決策的重要依據。1996 年臺海危機事件，情報即發揮關鍵作用。請從情報蒐集、情報研析、決策者認知及決策者對情報過程的影響等四面向，說明情報在 1996 年臺海危機處理過程中的功能為何？〈110 國安局〉

- ▲ 【相關問題】有鑑於危機的反應時間有限，危機處理過程傾向於輕重緩急的考量；危機處理原則之目的是為了防止事態擴大，降低緊張情勢，最後得到解決的方案。請問：危機處理原則為何？

擬答

一、蒐集者與分析者之間：
(一)影響情報蒐集者情報蒐集之進行與成效之原因包括：
1. 情報蒐集者本身的思想、觀念或心理因素。例如：
(1) 先入為主的觀念。
(2) 情報機關的最新命令或指示。
(3) 情報組織作業的規定與情報思維。
(4) 為了消除不確定感大量蒐集情報。
2. 對於情報蒐集來源的態度。
3. 受到團體及團體所判斷的影響順從共識。
4. 蒐集本身對於情報及其相關資訊的理解力與認知的範圍和深度。
(二) 情報分析者面對蒐集者提供之原始情報，應充分理解並考量上述影響因素，以中立態度進行篩選；並敏感覺察可能闕漏建議蒐集者補正後方展開分析評估。
二、分析者本身：
情報分析的心理影響因素，決定了情報分析之成功與失誤：
(一) 各國情報機關對於情報分析的組織分工概念不一而足，加上政策面對於情報評估的認知，增加了影響情報分析、評估工作的非心理因素。
(二) 情報分析人員的心智組合、意象、信念、認知等會影響到他對於情報資訊的解讀而產生不同的分析及評估。
(三) 情報分析人員之分析、評估會受國際或國內環境當前情報正確與真實的影響，而忽視到警訊的存在與意義，產生過度信心及忽略事實的認知偏見。
(四) 情報分析人員會存在是否對於所有警訊均持續性的保持高度敏銳反應度的兩難抉擇。不一樣的警戒態度，將會產生不一樣的結果。
(五) 由於情報不確定性的本質，情報分析評估人員若低估或高估情報對事件發展的影響力，便會因為信心偏見而減少投注的時間、精力。
(六) 情報分析人員根據最容易獲得與運用或與本身想法類似的簡易原則認知偏見，易導致分析與評估上的錯誤。
(七) 情報分析人員因先入為主等成見、先前立場、承受組織壓力、團體共識影響力等之認知信念，因而產生認知惰性。

三分析者與運用者之間：
(一)通常，運用者（政策制定者）使用情報的目的不外有三：
1.作為政策選擇的參考。
2.對內部作為政策的辯護。
3.對外部作為行動的辯護。
基於上述，運用者往往期待情報支持其政策，甚至為了獲得情報機關之支持，因而任命一個與自己政治立場相同的情報機關首長等。此等壓力與暗示易對情報機關（蒐集者、分析者）形成沉重壓力。
(二)分析者進行情報分析及評估時，若力求減少情報的不確定性及模糊性，可能出現過於簡化的錯誤；若忠實的呈現出情報的不確定性及模糊性，則易為政策面批評而背負沉重壓力。若無法堅持中立原則，往往左右為難，最後導致情報失敗。
四危機過程情報與決策者之互動關係（參朱蓓蕾，〈全球化時代情報在危機處理過程之運用〉／《遠景基金會季刊》第十六卷第三期，2015.7，頁 203 ~ 211）：
(一)情報與決策者認知危機之關聯性：
情報與危機決策之關係，彰顯出情報在危機決策上之功能，主要在於提供國家決策者、政府領導層尋求威脅和機會二個層面的資訊。
布里哲強調：危機是由國家最高決策者的認知判定，決策者是危機決策過程的行為主體，亦是情報的最終使用者——無論情報機關（構）完成的情報有多優良、分析有多精確、甚或可發揮多大的及時功效，掌握情報適用與否之最終決定權，仍在決策者本身，而決策者是否運用或是否採用，並非情報機關（構）所能控制者。尤其是隨著全球化、資（通）訊科技的長足發展，各種正式與非正式機制提供更多元化的意見交換、溝通管道、與政策選項，促使決策者有關危機資訊的認知，不再侷限於情報機關（構）所提供的資訊與情報。
事實上，在危機處理的過程中，雖然可能有預警情報，卻不必然保證就可以防止危機的發生，因為，預警情報は必要的條件，但並非充份的條件。
預警情報は對危險的感知能力，而反應則是決策者與團隊的行動力；決策者若未對預警的威脅迅速作出反應，則預警情報將變得徒勞無功，無法發揮其功能。
因此，預警情報與反應能力間的重要關鍵，在於決策者對危機的評估和判斷。
換言之，情報機關（構）雖然及時提出預警情報，但若決策者未予採用，或是可能因為決策者解讀錯誤、或決策者評估時間過長，抑或是決策者認為處理這些資訊與情報，需要付出太大的代價，抑或因其他緊急問題而忽略這些重要的情報；當然，也可能受制於鏡（射）像（Mirror Imaging）作用／思維或發生「狼來了／警訊例行化」的效應的影響，導致決策者嚴重輕忽情報的預警功能，因而誤判危機情勢，導致危機預防有利時機的錯失，美國 911 事件即是顯例。

<p>同時，有鑑於危機情勢常係具突發性及時間緊迫性，因此，對危機事件決策效率的要求，常更甚於一般常態性的決策程序。通常，在緊迫的危機壓力狀況下，「集體思考症狀（Groupthinking Syndrome）」可能導致決策者對危機情勢的誤判。事實上，在危機事件的發展過程中，許多關鍵性的問題，往往是無法被預見（測）到的，即使早有周全的應變計畫，亦無法確保危機出現時，沒有意外情況發生，尤其是當對手將「突襲／突擊」視為其主要戰略時。因此，預警情報並非總是必然成功的，而失敗的預測實乃係無法避免的。據以，傑尼斯（Irving Janis）強調：少數意見在「集體思考」的無形壓力下常常受到排擠，他主張在決策過程中，應鼓勵那些表達不同意見的少數人，如果可採取「魔鬼主張（Devil's Advocacy）」的討論模式及機會趨向（Opportunity Approach）的分析思考模式等，再經由正、反更兩方不同意見的辯論，將可提升情報分析品質與效益，並可提出各種可能的措施、計畫、或方案，而形成有利的決策，且可避免因「集體思考」所導致的誤判作為。西元 2003 年美國攻打伊拉克的決策失誤即是顯例。</p>
<p>此外，決策者和情報機關（構）對於危機情勢的認知判斷，常會受到鏡（射）像（Mirror Imaging）作用／思維的負面影響——亦即把己方的意識型態、軍事戰略與作為、及期望值等，不加思索地移植到對手，導致在判斷對手真實的國情、能力、及意（企）圖時，產生明顯偏差。例如西元 1973 年，以埃贖罪日（Yom Kippur）的戰爭期間，以色列的情報研（分）析人員僅按照軍事實力對比概念，而遂予推測阿拉伯國家不可能率先發動戰爭，而未能將情報置於宏觀的戰略層次以作出評估與預判，他們忽略了關於對手意（企）圖的分析，使決策者因情報研（分）析人員的誤判，而導致決策者的錯誤決策，險些使以色列就此陷入絕境。</p>
<p>在風險評估層面，冒險存在內在的邏輯性，決策者及情報機關（構）對於對手是否會發動「突襲／突擊」之誤判，通常源自於情報研（分）析人員錯誤地解讀對手的進攻意（企）圖，此乃思維模式的侷限，及心理和政治預期等因素所造成。事實上，並非所有「突襲／突擊」的發起者，均出於侵略性的目的，有些只是由於自我防衛動機即採取先發制人的策略，因此，情報研（分）析人員應確實了解對方的動機、意（企）圖、目的、和行動，再作出適當的反應，若是過度的軍事層面反應，反而可能會加速危機的惡化。例如西元 1995～1996 年的臺海危機期間，我國情報機關（構）藉由人員情報、科技情報、與公開來源情報等全來源情報（All Source Intelligence）蒐集途徑，先期掌握共軍的能力、動機、和意（企）圖等預警情報，據以，而正確地研判共軍飛彈試射的意（企）圖與行動。另外，亦經由國際情報合作交換（Intelligence Cooperation and Exchange）途徑，妥善運用危機處理合法性原則，尋求並獲得美國友邦的有（強）力支持，成功化解臺海可能形成的衝突危機，達到轉危為安之目的，其乃情報在危機處理運用上的成功案例。</p>

<p>(二)決策者與情報過程間之結構性問題：從情報過程觀察，決策者與情報體系在情報實際運作過程中，存在諸多深層結構性問題如下：</p>
<p>1.決策者與情報管理者與研析人員之間，針對重大議題的溝通（包含正式與非正式溝通管道），是情報過程中產製者與使用者關係的核心意涵。換言之，情報體系與決策者之間應保持何種分際，以及法制層面如何管控二者間的關係，實乃關鍵之所在，更攸關情報在危機決策與危機處理之成效。舉例如下：</p>
<p>(1)在計畫與指導階段，律定情報優先順序（intelligence priorities）的能力，即決策者對情報機關優先順序清單之關注與否？</p>
<p>(2)情報管理者對於情報機關的情報蒐集與情報分析是否滿足決策者之需求？</p>
<p>2.情報分析能力是影響決策過程的關鍵因素。在實際運作面向，大量的情報增加情報分析與預測的難度；而情報綜合分析能力的不足則會造成關鍵細節情報之疏漏。因此，如何從大量的情資中沙裡淘金，篩選及時有效的情報，是情報分析既繁重又關鍵的任務；此有賴於研析人員綜合分析能力之優化與提升。情報分析在下列因素的交互作用之下，影響研析人員和決策者的判斷：</p>
<p>(1)情報的本質是從不確定因素中擷取真實的部分，以及在無條理、不連貫的環境中促成有條理且連貫的決策。因此，研析人員在降低證據的模糊性、不確定性時，往往因過度簡化和通論化（oversimplification and overgeneralization）實際的真實情況，而忽略隱匿其中的重要事實的錯誤。</p>
<p>(2)集體思考、類比推理等情報分析模式易衍生鏡像思維、機械類比等邏輯謬誤。研析人員面對資料不足、矛盾或模糊的情況下，由於證據的模糊性而導致研判的衝突困境，亦即小心謹慎的結果為模稜兩可、有失機先；大膽進取則易造成失誤、信度受損。</p>
<p>(3)研判對手的能力及意圖時，如何辨別訊號與雜訊、如何在達成情報準確性的同時兼顧時效性等問題，是情報分析中最重要也是最困難的任務。</p>
<p>(4)情報預警面臨成功的預警與錯誤的預測難以區分之困境，不發警訊將導致措手不及，警訊過多則會削弱預警情報的信度。例如美國 911 事件的檢討報告即指出許多原始情報皆提出警訊，但這些情報不是被忽略，就是當時以不重要的情報被摒除。</p>

(三)決策者對情報過程之影響：
從供需原理觀察危機處理中決策者對情報過程之影響：儘管情報機關（構）在事前掌握，並及時提出預警情報，但卻仍無法防範危機情勢的發展，而導致情報失敗的關鍵決定性因素，通常並非由於情報的失誤，而是由於「決策者對情報的不信任、或錯誤使用，抑或是無法對情報作出迅速反應」。亦即，在情報過程中，決策者對情報失敗往往必須比情報機關（構）擔起更多、更大的責任。
從著名情報失敗案例可以發現，大部分決定性的錯誤，很少肇因於情報蒐集人員的原始情資，偶而發生在專業的完成情報研析者，絕大部分則「係由於決策者所造成者」。因為，政策前提壓縮了預見，且行政工作量制約（即指限制、約束）了決策者的反應。因此，導致情報失敗通是「政治和心理層面的因素」遠大於組織層面。例如：西元 1941 年日本偷襲珍珠港事件、西元 1973 年以埃贖罪日（Yom Kippur）戰戰爭、西元 2001 年的美國 911 事件、及西元 2003 年的美國攻打伊拉克戰爭等，即係實例。
面對危機過程的處理中，決策者的決策過程通常並非係憑空操作者，當決策者作決定時，往往面對各種情報或資訊，基於其他因素的考量、或出於己方的期望、及合理私利（Rrational Self-interest）——諸如國家利益、國內的政治支持、個人的政治價值判斷、或目標、以及意識型態和政治偏見等，而致使決策者對情報加以取捨，而刻意忽略情報機關（構）的分析、或決策者試圖影響情報機關（構）的研析。
其次，「決策者可能不會對重要的情報評估採取行動」。究其原因：一是決策者可能認為若採取因應作為，會具有高風險性或代價；二是決策者可能因其他急迫性的問題，而使其忽略了這個重要的情報。有鑑於在情報的實務運作過程中，決策者往往就是情報運用與否或採用與否的最終決定者，因此，若要情報機關（構）對具權力的決策者說明真相，就會變得非常困難，同時，決策者通常會選擇拒絕建言、反對、或拒絕非其所偏好的情報，因此，導致即使決策者及時獲得準確的情報，他亦未必會做出正確的決策，例如西元 2003 年美國攻打伊拉克的戰爭，亦即為顯例。

事實上，情報與決策者間，是不對稱的現實關係，決策者處於絕對優勢的（權力）地位；而情報能發揮多大程度的功效，往往取決於其與決策者期望值相符多高的程度所決定。再者，決策者與其挑選的情報管理者間之信任關係與所建立合作的程度，亦係情報過程中的關鍵要素；亦即，如何在二者緊密互動關係與超然獨立之間，保持微妙的平衡，是情報被實行與否的重要因素。誠如克勞塞維茲（Carl von Clausewitz）所言之「決策者的敏感性和識別性判斷，以及挖掘真相的能力。」亦即，這些問題的解決方案，在於「決策者的領導品質」。
基此，決策者對情報之採用和運用，應出自於決策者理性的思考，而非決策者的直覺判斷或先入為主的想法。直覺的判斷，是快的思考（Fast Thinking），易導致月暈效應（Halo Effect）〔「月暈效應」也稱光環效應或成見效應，指在人際交互作用過程中形成的一種誇大的社會印象。月暈效應往往是在個人掌握有關知覺對象的訊息很少而又要作出整體判斷的情況下，產生以偏概全的效應，它實際上是個人主觀推論的泛化與擴張，造成過高或過低評估的失真現象。〕，即係決策者過度自信後見之明的虛幻確定感。據以，情報在危機處理之功能與運用，應是情報機關（構）於情報過程中，發揮仔細求證的實證經驗及理性思考模式功能之結果，亦即透過邏輯的思考、慢的思考（Slow Thinking），方能輔助或彌補決策者因直覺思考所可能衍生或產生的錯覺，進而導致決策者的錯誤決策。
五有鑑於危機的反應時間有限，危機處理過程傾向於輕重緩急的考量；危機處理原則之目的是為了防止事態擴大，降低緊張情勢，最後得到解決的方案。綜合喬治（Alexander L. George）等學者相關危機處理原則如下（參朱蓓蕾，〈全球化時代情報在危機處理過程之運用〉／《遠景基金會季刊》第十六卷第三期，2015.7，頁 201～203）：
(一)合理的限定目標，預防對峙情勢升高，預留政策之迴旋空間。
(二)限制為實現目標而使用過當手段，避免大意的發出最後通牒，尋求務實解決之道。
(三)情報的必要性：情報機關（構）是決策者的支援機制，其有助於決策者掌握複雜的情勢發展，俾利決策者之危機處理判斷與相關政策之制定。

而情報在危機處理之功能如下：
1.是先期預見危機、尋求威脅和機會的相關情報：在危機發生之前，提供預警情報，而透過警訊與預警，俾利避開或排除即將到來的突襲危機。
2.是在危機期間，掌握危機情勢之發展，以為因應，並得以提升危機事件處理之應變能力：在危機爆發期間，若能密切關注並掌握危機情勢發展〔包括對手能力、意（企）圖、及可能的行動等動態情報，以及相關事件與內、外環境的反饋（FEEDBACK）資訊，和特殊領域範圍內可資隨時有效運（利）用的情報和資訊〕，將可使決策者、負責危機處理人員、與政策執行的相關危機處理單位或部門，提前獲得有利的確實情報，並據以研擬相關應變對策與計畫。
3.是對危機情勢的可能發展，進行情報分析，以提出指標性與預警性情報，增進我方危機偶發事件的反應及應變能力。
4.是在危機事件發展過程中，經由各項情報活動過程，從中尋找並提醒決策者危機中可能之機會。
亦即，危機處理對國家安全往往有結構性的影響，可能是一個重要的分水嶺，甚至會威脅到國家的生存與發展上的利益。誠如科迪維拉所言：情報在危機處理過程中，可以發揮制敵機先、知己知彼、百戰不殆的關鍵作用。
(四)建立和維繫敵對雙方間之溝通管道：應保持內部及與對手間資訊交換及溝通管道之暢通，增進了解彼此的立場、要求與企圖，避免誤解和誤判的產生。
(五)建立危機處理機制、應變措施、替選方案之計畫及能力。
(六)尋求與獲得合法性，以獲取國內與國際社會間的廣泛支持。
(七)避免創建不好的處理先例，以免成為日後處理類似危機事件的障礙。

例題

- ▲近期我國屢次發生共諜事件，中國有那些單位可能滲透臺灣蒐集情報？我國應如何反制與因應？〈106 國安局〉
- ▲【相關問題】為反制習近平提出要藉由「惠臺利民」的融臺政策，實現「一國兩制臺灣方案」鋪路；並因應中共不斷派人以留學、經商名義滲透臺灣，發展組織或刺探國家、企業機密，請問我國安單位應如何加強共諜線索的佈蒐與發掘？如何加強國安偵防工作提升偵防能量？請分述之。〈108 公安所〉
- ▲【相關問題】西元 2008 年 5 月 20 日馬總統執政後，積極擴大兩岸交流活動，持續開放陸客來臺自由行、陸生來臺就學、陸企、陸媒、陸辦、陸銀等來臺駐點，勢予中共對臺情報滲透攻堅可趁之機；加上來自境外的安全威脅因素日增，影響我國國家安全。對此，我國國安單位情報幹部面對內外安全威脅之挑戰，在工作上應持之基本原則為何？請論述之。〈105 公安所〉
- ▲【相關問題】中共國務院台灣事務辦公室於今（107）年 2 月 28 日藉由例行記者會片面宣布「關於促進兩岸經濟文化交流合作的若干措施」，通稱「對（惠）台 31 項措施」，冀從臺灣引進技術、資本及人才，協助解決其經濟發展所遭遇的困難。對此，行政院於 3 月 16 日宣布推動「八大強臺策略」，嚴肅面對，務實因應。請列舉大陸「對（惠）台 31 項措施」及行政院「八大強臺策略」內容重點，並申論情報機關應有的情報作為。〈107 公安所〉
- ▲【相關問題】兩岸分治迄今，中共從未終止對我進行情報滲透攻堅行動，此由歷年國安單位偵破之共諜案涉案對象遍及總統府、國安、軍情、調查、科研、及教育等單位，可見一斑。請列舉國人涉入共諜案之主客觀因素，並研提反制對策，以維護國家安全與利益。〈106 公安所〉
- ▲【相關問題】為有效因應及反制中共「一國兩制臺灣方案」對我國國家安全的巨大挑戰，確保中華民國國家主權與自由民主，蔡英文總統在今（108 年 3 月 11 日召開國家安全會議，提出「因應及反制《一國兩制臺灣方案》指導綱領」，作為國安團隊與行政部門因應這項挑戰的行動準則。請列舉「因應及反制《一國兩制臺灣方案》指導綱領」內容重點，並申論情報機關應有的作為。〈108 公安所〉

- ▲【相關問題】中共成立中央國家安全委員會的目的為何？中國目前最為迫切的國家安全威脅有那些？中國如何透過國家安全委員會來因應與反制？〈106 國安局〉

擬答

一、中國可能滲透臺灣蒐集情報之中國國家安全體系單位：

- (一)中央對外聯絡（工作）部：屬黨系情報機關。前身為國際聯絡部，於西元 1956 年成立。其任務主要係負責與世界各共產國家及非共產國家之共產組織或左派團體等國際共黨組織之聯繫、爭取、運用等各項工作。是中國對外政策工具之一。
- (二)中央統一戰線工作部：屬黨系情報機關。為中國進行國內統戰、海外統戰及對台統戰工作的領導機關。除在中央設中央統一戰線工作部外，在各省、市、州、縣的黨委之下均設統戰部，進行統戰活動，可稱為公開的特務工作。
- (三)中央辦公廳：屬黨系情報機關。直接管制中央調查部、中央對外聯絡（工作）部及中央統一戰線工作部。
- (四)國家安全部：屬政系情報機關。西元 1983 年 7 月 6 日成立，是中國國家安全工作從公安系統內區隔出來，正式建立國家安全制度的開始。西元 1987 年國家安全部成立起草小組，草擬《中華人民共和國國家安全法》¹，於西元 1992 年 12 月 8 日提交國務院常務委員會通過，並於西元 1993 年 2 月 22 日由第 7 屆全國人大常務委員會會議通過，公布實施。

1.組織體系：依據西元 1993 年《中華人民共和國國家安全法》，中央設立國家安全部，是一個針對他國之國家資源作全面性諜報工作的情報組織，本部設有 17 個局，職掌包括國內、外一切情報與反情報任務，其第四局專責台港澳地區之情報工作，在組織基本上採「機關公開、人員保密」之處理原則。它在行政體系上隸屬國務院管理，但實際工作係受中共中央書記處領導。省級設國家安全廳，直轄市級設國家安全局，地區設國家安全處，縣級設國家安全局，基層設分局或組。

2.任務：國家安全部之性質，有情報與反情報的雙重任務。

(1)對內：

- ①監視、跟蹤外國使館人員、外國通訊機構記者、赴大陸講學、訪問、旅遊、商貿之外國人。
- ②調查自海外進入大陸歸僑活動。
- ③防範民主運動組織與大陸反革命分子掛勾。

(2)對外：

- ①加強信檢工作。
- ②對間諜嫌疑分子進行跟蹤、監視、偵蒐工作。
- ③偵辦及鎮壓反共民主運動組織活動，查緝大陸反共地下組織。
- ④對台的滲透與破壞工作。
- ⑤在軍中布置安全秘密小組，偵鑑六軍官兵思想工作。

1 西元 1993 年版《中華人民共和國國家安全法》已於 2014 年被廢止，同時由《中華人民共和國反間諜法》取代，其國家安全制度之組織與任務法條並未變動。西元 2015 年 7 月 1 日通過之新版《中華人民共和國國家安全法》則多為原則性規定，對未來相關配套法律預留空間。

(五) 珍珠鏈戰略 (string of pearls, 又可稱為「鄭和珍珠鏈」) (參: <https://zh.wikipedia.org/wiki/珍珠鏈戰略>): 是指中國透過經濟援助等方式, 取得海外的港口、機場經營權或者租用權, 或是發展特別外交關係, 甚至建立軍事基地等的戰略。由於涉及此項戰略投資的國家, 主要分布於南亞、印度半島、以及非洲, 其相關港口、機場等地點在地圖上連起來像珍珠, 因此得名。

這是一項由印度政治界提出的概念, 描述了對中國在印度洋施加影響力的意圖的猜想。它指的是從中國大陸到非洲之角上蘇丹港之間, 中國的民用和軍用設施, 以及這些設施與中國重要航道的關係。中國的重要航道經過了幾個「瓶頸」, 包括曼德海峽、馬六甲海峽、荷姆茲海峽和龍目海峽, 以及沿岸的巴基斯坦、斯里蘭卡、孟加拉國、馬爾地夫和索馬利亞等國家。

大量印度的評論家認為, 珍珠鏈戰略和中巴經濟走廊一道, 會威脅到印度的國家安全。這個戰略會形成一個體系, 威脅到印度的力量投射、貿易, 甚至是領土完整。另外, 中國與巴基斯坦——印度的「世仇」——的緊密關係, 以及中國在瓜達爾港的發展, 加上中國海軍在瓜達爾港設立海軍基地的可能, 都被印度視作眼中釘。在東面, 皎漂深水港也同樣引起了印度的擔心。

這個詞第一次出現是博思艾倫漢密爾頓控股公司在 2005 年的內部報告《亞洲的能源未來 (Energy Futures in Asia)》。這個詞也經常在印度的地緣政治和外交政策文件中使用, 以強調印度對一帶一路在南亞施行的擔憂。根據歐洲安全保障研究所的說法, 美日印澳形成的「四邊安全對話」正是對中國在印太地區積極外交政策的直接反制。

「珍珠鏈戰略」的出現, 說明了中國正有計劃地增加對機場、港口的控制, 擴充、升級軍隊, 以及與貿易夥伴增強關係, 來施加日益增長的地緣政治影響力。中國政府一直表示, 中國海軍堅持和平發展的路線, 只負責保護區域內的貿易利益。中國領導人, 例如胡錦濤和習近平都聲稱, 中國不會在國際關係中尋求霸權。西元 2013 年, 《經濟學人》發表分析, 認為中國的舉動本質上只與貿易有關。有分析認為, 中國的舉動將造成與印度之間的安全困境, 但是也有分析認為, 中國的戰略存在脆弱之處。

近年來, 中國的珍珠鏈戰略, 對外勢力發展手段, 有著下述的發展與影響:

1. 扼守「非洲之角」交通要衝之曼德海峽: 有「非洲之角」之稱位處紅海進入印度洋的要衝—曼德海峽, 扼守亞丁灣, 更掌控地中海到印度洋、非洲內陸到阿拉伯半島的航線, 其戰略地位十分重要。中國自西元 2008 年以「打擊索馬利亞海盜」之名, 獲得吉布地共和國同意讓中國解放軍使用吉布地港, 並建立永久軍事基地、發展海軍特種部隊。
2. 擴張南海、印度洋之「一帶一路」: 中國發展軍事設施, 在南海諸島礁(人工島礁) 逐步填島造陸、建築港口機場, 亟欲發展「一路一帶」戰略昭然若揭, 其增強「珍珠鏈戰略」的軍事補給建設, 彰顯中國近年來的「大國崛起」戰略, 策略性的逐步推進其於南海與印度洋等地的經濟、軍事地位。

二、中共之中央國家安全委員會（簡稱中央國安委、國安委）（參《展望與探索》中華民國 106 年 4 月第 15 卷第 4 期，胡瑞舟，〈中共中央國家安全委員會及其運作：從總體國家安全觀及國家安全工作座談會觀察〉／https://www.mjib.gov.tw/FileUploads/eBooks/5e521832d74643ed821d2af9a5643496/Section_file/fac6f571a363486a8f6bceacd36f7a55.pdf）：

(一)中央國家安全委員會（簡稱中央國安委、國安委）是中共中央決策和議事協調機構，直屬於中共中央總書記，負責國家安全工作，以「完善國家安全體制和國家安全戰略，確保國家安全」。中央國家安全委員會向中央政治局、中央政治局常務委員會負責，統籌協調涉及國家安全的重大事項和重要工作。

(二)職責：與世界其它國家的「國家安全委員會」和「國家安全會議」不同，中央國家安全委員會雖然「不是國家機構」，也「不是政府部門」，但作為中共黨內領導機關將把對外的國家安全和對內的國家安全結合在一起進行統一政治領導：公安部、國家安全部、司法部、武警總部、中央軍委聯合參謀部情報局、中央軍委政治工作部聯絡局、解放軍戰略支援部隊網絡系統部、外交部、中央外宣辦等部門，將被全部揉並在一起。國家安全委員會將成為總管領導軍隊、公安、外交、情報領域的強有力的機構。

(三)沿革（參：<https://zh.wikipedia.org/wiki/中央國家安全委員會>）：中共中央和國務院原先設有中央國家安全工作領導小組（是中央外事工作領導小組的牌子）和國家安全部等數量眾多的安全部門，無論是對外還是對內，一定程度上存在「各自為戰」的問題，情報交流有可能也不一致，缺乏有效溝通，影響安全部門的效率，因此中共中央認為需要一個黨內機構來對國家安全力量進行統一的決策和協調。

中國於西元 1997 年首次提出成立國家安全委員會的方案。當時，江澤民訪問美國時看到美國國家安全委員會後，便計劃組建國家安全委員會但未果。西元 2000 年 9 月，中共中央決定組建「中央國家安全工作領導小組」，與「中央外事工作領導小組」合署辦公，一個機構兩塊牌子。中央國家安全工作領導小組辦公室即中央外事工作領導小組辦公室。

中國共產黨於西元 2013 年 11 月召開第 18 屆 3 中全會，決議成立中央國家安全委員會，藉以完善國家安全體制和國家安全戰略，確保國家安全。

西元 2014 年 1 月 24 日，中共中央政治局召開會議，研究決定中央國家安全委員會設置。會議決定，中央國家安全委員會由中共中央總書記習近平任主席，中央政治局常委李克強、張德江任副主席，中央政治局委員栗戰書兼任國安委辦公室主任，下設常務委員和委員若干名。

西元 2014 年 4 月 15 日，中央國家安全委員會第一次會議舉行，由中共中央總書記、中央國家安全委員會主席習近平主持，他在會上表示，國安委要既重視國土安全，又重視國民安全，中國要「堅持總體國家安全觀，走出一條中國特色的國家安全道路」。這次會議被視為國安委正式運轉的標誌。

西元 2017 年 2 月 17 日，中共中央總書記、國家主席、中央軍委主席、中央國家安全委員會主席習近平主持召開國家安全工作座談會並講話，強調「堅持黨對國家安全工作的領導，是做好國家安全工作的根本原則。各地區要建立健全黨委統一領導的國家安全工作責任制，強化維護國家安全責任，守土有責、守土盡責。」並對當前和今後一個時期國家安全工作提出要求。

(四)總體國家安全觀：西元 2014 年 1 月 24 日，中共中央政治局會議確定設置中央國家安全委員會，並明確將其定位為中共中央關於國家安全工作的決策和議事協調機構，向中央政治局、中央政治局常務委員會負責，統籌協調涉及國家安全的重大事項和工作。西元 2014 年 4 月 15 日，習近平在中央國家安全委員會第一次全體會議上首次正式提出《總體國家安全觀》，並將其確立為新時期國家安全工作的指導思想。

中共基於國內外深刻複雜變化，國家安全面臨諸多壓力和風險因素，認為治黨治國必須增強憂患意識，做到居安思危；尤其，黨要鞏固執政地位，保障國家安全是頭等大事，因此決定成立中央國家安全委員會。習近平強調《總體國家安全觀》，明確指出設立國家安全委員會的目的是推進國家治理體系和治理能力現代化、實現國家長治久安的迫切要求，是全面建成小康社會、實現中華民族偉大復興「中國夢」的重要保障，目的就是更能適應國家安全面臨的新形勢新任務，建立集中統一、高效權威的國家安全體制，加強對國家安全工作的領導。國家安全委員的主要職責則是制定、實施國家安全戰略，推進國家法制建設，制定國家安全工作方針政策，以及研究解決國家安全工作中的重大問題。

《總體國家安全觀》對國家安全的內涵和外延，可以概括歸結為五大要素和五對關係。五大要素就是以人民安全為宗旨，以政治安全為根本，以經濟安全為基礎，以軍事、文化、社會安全為保障，以促進國際安全為依托。貫徹落實總體國家安全觀則必須重視五對關係，亦即既重視外部安全，又重視內部安全；既必須既重視外部安全，又重視內部安全；既重視國土安全，又重視國民安全；既重視傳統安全，又重視非傳統安全；既重視發展問題，又重視安全問題；既重視自身安全，又重視共同安全。

面對國家安全的新形勢與新變化，中國大陸體認成立國家安全委員會的急迫需要；但是，做為一個社會主義國家，中國大陸顯然更堅持走「中國特色國家安全道路」。這個構想又係透過五項堅持完成：堅持黨對國家安全工作的絕對領導，堅持國家利益至上，堅持以人民安全為宗旨，堅

持共同安全，堅持促進中華民族偉大復興。其中，第一項堅持明顯最為寫實，它強調堅持黨的絕對領導是國家安全工作的根本政治原則、國家安全工作以保證政權安全和制度安全為首要任務、以及切實加強黨對國家安全工作的絕對領導。因此，不同於一般國家的建構運作方式，中央國家安全委員會是隸屬於中國共產黨的機制，習近平也要求建立黨委統一領導的國家安全工作責任制，分層負責總管強化維護國家安全。

在中央國家安全委員會的集中統一領導下，構建及維護 12 種重點領域國家安全是其運轉重心。2014 年首先提出政治安全、國土安全、軍事安全、經濟安全、文化安全、社會安全、科技安全、網絡安全、生態安全、資源安全、核安全等 11 種領域安全工作，但在 2016 年出版的《總體國家安全觀幹部讀本》中又增列了第 12 種安全：海外利益安全，緊密與中國大陸經貿發展、對外投資和「一帶一路」戰略建設鏈結。

《總體國家安全觀》提出後，中共中央針對此一戰略思想體系也藉由堅持統籌國內國際兩個大局、倡導共創安全合作新局面、加快國家安全法治建設和確立新時期的國家安全戰略予以充實、發展和完善。關於國家安全法治建設，全國人民代表大會及其常務委員會相繼起草頒布安全領域的綜合性和專門性法律，摘列如表 1。根據推進國家安全法治建設要求，中國大陸 2016 年 3 月 17 日頒布《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要（《十三五規劃綱要》）》也特別對加強國家安全法治建設做出規劃。其中，除了強調貫徹落實國家安全法，制訂相關實施細則，推進國家經濟安全、防擴散、國家情報、網絡安全、出口管制、外國代理人登記、外資安全審查等涉及國家安全的立法工作，加快健全國家安全法律制度體系，充分運用法律手段維護國家安全。關於兩岸關係，內容還包括推進兩岸關係和平發展和統一進程、促進兩岸經濟融合發展、加強兩岸人文社會交流；尤其強調堅持「九二共識」和「一個中國原則」，堅決反對「臺獨」。

堅持《總體國家安全觀》必須確立新時期的國家安全戰略，以為全面建成小康社會、實現「中國夢」的重要保障；因此，2015 年 1 月 23 日中央政治局召開會議，審議通過《國家安全戰略綱要》。該綱要雖未見完整對外公布，但從相關資料及部分報導顯示，中共國家安全戰略係以《總

體國家安全觀》為指導，堅決維護國家核心和重大利益，以人民安全為宗旨，在發展與改革開放中促進安全，走「中國特色國家安全道路」做好各領域國安工作，推進各種保障能力建設，把法治貫穿於維護國家安全的整個過程。中共中央特別重視政治安全和社會安全，《國家安全戰略綱要》還強調對內重發展、對外重合作。分別針對內外構成國家實現安全的兩條戰略主線：對內，《總體國家安全觀》強調發展是安全的基礎，富國才能強兵；對外，《總體國家安全觀》倡導實現共同、綜合、合作、可持續的安全。

2015 年 7 月 1 日中共頒布施行《國家安全法》，訂定每年 4 月 15 日為全民國家安全教育日。2016 年 4 月 15 日首個國家安全教育日時，習近平指示以設立教育日為契機，以《總體國家安全觀》為指導，全面實施國家安全法，深入開展國家安全宣傳教育，增強全民國家安全意識。此外，由栗戰書擔任主任的編委會組織編寫《總體國家安全觀幹部讀本》，從小學到大學不同層次的國家安全教育讀本也將齊備。不僅各級黨校和行政院校將對黨政領導幹部進行國家安全教育，各級各類學校更開設針對性的國家安全課程，高校也設有專門的國家安全學課程和國家安全專業。

註：中國大陸審議或通過法律日期暨法律名稱：

2014.11.1《中華人民共和國反間諜法》。

2015.7.1《中華人民共和國國家安全法》。

2015.12.27《中華人民共和國反恐怖主義法》。

2016.4.18《中華人民共和國境外非政府組織管理法》。

2016.11.7《中華人民共和國網絡安全法》。

三我國反情報及反間諜之各項反制與因應措施及對策：

(一)反情報之意義：其係關於嚇阻（deter）、及偵測（detect），聚焦於安全功能。

- 1.依美國西元 1947 年頒布之《國家安全法案（National Security Act of 1947）》規定，情報（Intelligence）包括「國外情報（Foreign Intelligence）」與「反情報（Counterintelligence）」。前者指關於外國政府、外國組織、或外國人、或國際恐怖分子活動之能力、意圖、或行動之資訊；而後者，則係指執行資訊之蒐集、與行動，以對付代表外國政府、外國組織、或外國人、或國際恐怖分子活動之間諜、其它情報作為、破壞、或暗殺等活動。
- 2.西元 1958 年 4 月 21 日，美國國安會公布《第 5 號國安會情報指令（National Security Council Intelligence Directive 5, NSCID 5）》，該指令除了規定由中央情報局（Central Intelligence Agency, CIA）負責執行海外之反間諜行動外，並將「反情報」定義如下：其係用以摧 有敵意外國情報活動之有效性，且保護國家及其人民、資訊、與設施之安全，以對付間諜、破壞、和顛的一種情報活動。同時，「反情報」包括取得、發展、記錄、和分發關於敵對秘密行動的資訊，且必須滲透、操控、或施壓欲採取此等行動之組織、團體、或個人。
- 3.西元 1981 年 12 月 4 日總統雷根所發布的《第 12333 號行政命令（E.O. 12333）》，只要中央情報局之工作不是針對美國公民和機構的國內活動，均可以在美國境內秘密蒐集重要的外國情報，也可在總統批准下於不影響美國政治進程、公眾輿論和宣傳工具的前提下，於美國境內進行秘密行動或準軍事行動。其將「反情報」定義如下：資訊的蒐集和行動之執行，以對抗間諜、其它來自於或代表外國勢力、組織、或個人、或國際恐怖分子之情報活動、破壞、或暗；但是不包括人員、實體、文件、或通訊安全。該行政命令並於西元 2008 年再度修正：「反情報」指的是識別、欺騙、利用、摧毀、或防止由代表外國勢力、組織、或個人、或其代理人、或是國際恐怖主義組織、或活動之實施之間諜、其它情報活動、破壞、或暗殺，而所進行之資料蒐集以及執行之活動。
- 4.美國中央情報局（Central Intelligence Agency, CIA）指出，「反情報」不僅只是抓間諜，事實上，它關切的是了解與可能抵消國外情報之所有面向；而除了蒐集與處理關於敵人之情報，及向消費者報告外，情報圈（即情報體系）也需面對來自國外情報勢力之情報威脅之鑑定、了解、定出優先事項、與反制作為之問題，而所有的這些行動，即係反情報。

綜之，「反情報」是關係到資訊之蒐集與行動之執行，以對抗間諜、及代表外國政府、組織、與個人之破壞行動與暗殺等之其它情報活動。其指導原則，包括：偵測（detect）、鑑定、避免、與反制，並有以下五個步驟：

- 1.進行重要資訊分析：以找出必須保護之重要資訊。
- 2.威脅分析：以找出對重要資訊之威脅。
- 3.弱點分析：進行全面性的調查，以找出目前所保護重要資訊之系統性弱點。
- 4.危險評估：檢討需要保護之重要資訊、特定來源之威脅及弱點，以定出危險等級。
- 5.安全有效性評估：以履行授權之反制措施。同時，需定期檢討現有反制措施之有效性，據以調整與變化。

- (三)反間諜之意義：其係與偵測（detect）、欺騙（deceive）、及抵消（neutralize）對手情報活動之有效性有關。
- (四)保防（現稱：安全防護）與反情報之意義：我國法務部於中華民國 108 年 12 月 11 日函頒《全國安全防護工作作業要點（原名稱為：保防工作作業要點）》第 7 點規定：全國安全防護工作之業務範圍如下：
- 1.機密維護。
 - 2.安全維護。
 - 3.機密及安全維護教育。
- 日前，法務部調查局並已經重新詮釋保防（現稱：安全防護）工作，指保防（現稱：安全防護）即係：「保衛國家安全，防制敵諜滲透。也就是國家對抗外力對我情蒐滲透、破壞之反情報工作。」《全國安全防護工作作業要點》第 1 點規定：「為貫徹『執行有關危害國家安全及違反國家利益之安全防護工作』，特訂定本要點。」此並將「保防」工作，修改為「安全防護」工作。同時，《全國安全防護工作作業要點》第 2 點復規定：「全國安全防護工作，由法務部主管，並指定調查局協調執行。」
- (四)依《國家情報工作法》第 3 條第 1 項第 6 款規定，間諜行為：指為外國勢力、境外敵對勢力或其工作人員對本國從事情報工作而刺探、收集、洩漏或交付資訊者。
- (五)依《國家情報工作法》第 22 條（反制間諜工作）第 1～3 項規定：
- 1.情報機關從事反制間諜工作時，應報請情報機關首長核可後實施，並應將該工作專案名稱報請主管機關備查。但屬反爭取運用者，應經主管機關核可後實施。
 - 2.情報機關從事前項反制間諜工作時，得經機關首長核准，向其他政府機關（構）、單位調閱涉嫌間諜行為之人及其幫助之人之有關資料，該管監督機關（構）、單位除有妨害國家安全或利益者外，不得拒絕。
 - 3.前述 1.但書之情形，應由主管機關報告國家安全會議秘書長，於經最高法院檢察署檢察總長或最高軍事法院檢察署檢察長同意後，由主管機關協調各該情報機關決定案件移送偵辦時機、移送之對象及移送之內容。

(六)依學者張中勇看法，反情報之主要工作內容如下：

反情報之主要工作，包括以下二部分：

1.安全防護（Security）：即為保密工作，係反情報工作中之消極面、靜態面，具有內導性，主要作法即為「安全控制管理」，包括：

- (1)強化機密檔案管理與防護。
- (2)人員安全查核與保密等級鑑別。
- (3)加強機關（機構）設施防護措施。

總之，反情報安全工作的防制對象，即為防止「神秘滲透」，而反情報安全工作係以全面防守、守株待兔、鞏固安全的理念，針對其人員、設施及作業機密的安全，加以有效維護與落實。惟本項工作較為被動，無法有效防範內間。

2.反諜報（Counter-Espionage，又稱反間諜）：即為防諜工作，係反情報工作中之積極面、動態面，係具有外導性的安全防護概之作為，主要作法包括：了解、掌握並反擊敵方、甚至於友好方的情報組織及其活動、防止滲透及布署內間等。亦即反諜報工作，主要係經由滲透對方組織與利用變節者自白以獲取相關情報，同時，了解其對己方滲透活動，並對具有敵意的外國組織、情報活動、組織結構及管理運作等加以研究及分析，以進行干擾性及抵銷性的對抗行動，期能有效發揮功能、有效滲透、干擾，並化解、消除對方的情報活動能力。

其具體作法包括：

- (1)藉由公開和機密的來源，蒐集並建立敵方、甚至於友好方的情報安全組織及其活動的資料。
- (2)對變（叛）節者自白提供之情報，進行評估，以蒐集與建立情報資料。惟應注意變節者是否另有目的、虛假或隱瞞，以免落入對方陷阱之中。
- (3)經由神秘滲透（Penetration）而暗中獲取重要情報，這個方法最直接有效且成果可觀。神秘滲透可分為：刻意安排人員進入該組織工作及收買與利用目前既有該組織人員二種方式，亦即可直接「拉出」對方組織重要部門人員、可安排人員長期打進對方組織潛伏發展、也可收買雙面間諜（Double Agent，或稱反間諜）提供情報。

(4)其他獲取情報之方式：

- ①利用情報交流及情報交換方式，透過第三國管道而獲取敵方的滲透行動及計畫。
- ②針對特定外國人士的行蹤與接觸關係進行跟監，並加以記錄、調查而獲取重要情報。
- ③對於機密外洩事件的相關人、事、機構等，加以調查、追查洩密因素，而找出安全維護漏洞，進而循線進行反情報工作。
- ④對民眾或其他途徑檢舉可疑諜報事件及人物，進行調查。
- ⑤利用郵件及電訊檢查或安全資料查核過程中，主動發現可疑分子並進行調查。惟本對象必須經過合理挑選，並有足夠證據支持，且經過法律申請許可，方得進行。

由上述二項主要工作內容可知，「安全」與「守密」是反情報工作最重要的情報組織管理理念。因此，組織管理上必須加以分隔，嚴格執行安全等級制度，並對反情報工作的方法及情報來源充分保密。

(七)反情報功能²：

- 1.調查：進行調查，以逮捕那些為外國情報機關（構）進行諜報、或協助國際恐怖主義分子、或犯下其它國家安全罪行的叛徒。
- 2.行動：透過行動，以阻礙、挫敗、與利用外國情報努力及其它外國破壞國家安全之隱蔽（或秘密）行動。
- 3.蒐集：運用各項蒐集作為，以獲取有關外國情報機關（構）、其它隱蔽（或秘密）行動、以及國際恐怖主義組織的網絡資訊。
- 4.分析與生產：融合、評估、解釋、及分發任何與反情報相關之資訊，同時，要作為一個得動見觀瞻並能提供具洞察力的反情報分析者。
- 5.提供功能服務：支援其它情報、或是運作活動的其它反情報行動。包括提供專業的防衛性反情報服務—例如提供數位鑑識、進行網絡脆弱性評估等。

(八)中國「一國兩制臺灣方案」因應方針與機制／〈因應及反制「一國兩制臺灣方案」指導綱領〉（參總統府：<https://www.president.gov.tw/News/24140>）

108年1月2日，中國國家主席習近平在所謂「告臺灣同胞書」四十週年紀念談話中，已經明白揭示「一國兩制臺灣方案」的統一進程。中共近日召開的兩會，也將習主席的談話列為今後對臺灣工作的核心事項。這些動作都在在顯示，北京當局已經將統一臺灣的工作納入政治議程，這讓兩岸關係進入極為嚴峻複雜的階段。

蔡英文總統於108年新年談話時，提出建構兩岸交流的三道防護網：也就是民生安全、資訊安全、和民主防護網。她強調，「我所領導的政府，致力維持兩岸和平穩定，支持兩岸的正常交流。不過，我們堅決反對一國兩制，也拒絕任何被統一的過渡性安排。這不是戰爭或者是和平的抉擇，而是維持中華民國主權獨立現狀、或被中國統一的抉擇。」

至108年03月11日國家安全會議報告：會後蔡總統提出〈因應及反制「一國兩制臺灣方案」指導綱領〉，作為國安團隊與行政部門因應這項挑戰的行動準則。蔡英文總統指出：為因應中國「一國兩制臺灣方案」對國家安全之重大挑戰，確保國家主權與世代國人對臺灣未來前途的選擇權利，總統特裁示本指導綱領，作為國安團隊及行政部門行動之準則，以強化國安作為，避免國家經濟社會正常運作受到衝擊。並提出以下行動準則：

- 1.兩岸：正面看待兩岸交流，堅持對等尊嚴原則，以民主為互動基礎，參考主要民主國家作為，全面檢視兩岸交流相關規定的落實。積極反制中共假借交流，對我國統戰滲透，干預我國內事務。
- 2.民主法制：立即推動兩岸條例修正案，加速完成民主防護網的法制工作，以強化民主監督程序與防衛機制。

2 參汪毓瑋著，2018，《情報、反情報與變革（上）（下）》，頁1443～1604。

- 3.經濟：因應美中經貿衝突及國際經貿局勢變遷，積極協助台商回臺投資，致力促進產業轉型升級，強化國際佈局，穩定總體經濟發展。提升臺灣在全球產業鏈的優勢與戰略地位，積極與主要貿易夥伴洽簽多邊、雙邊經貿協議。
- 4.外交：善用國際友我新情勢，結合國際社會，反制中共消滅中華民國主權行徑。
- 5.安全：嚴密掌握中國大陸的政經社會情勢變化，防制中共對我國進行輿論操弄、社會滲透、竊取國防及核心產業機密，以維護國家安全與社會安定。
- 6.國防：穩定增加國防預算，全面提升國軍戰力，以嚇阻中國軍事冒進，確保中華民國主權及民主自由。
- 7.社會：全面加強社會溝通，凝聚人民對兩岸政策共識，團結內部，以一致行動捍衛國家主權。

因應及反制 「一國兩制台灣方案」 指導綱領

第61次
國家安全會議



總統 蔡英文





副總統 賴清德 行政院院長 蘇貞昌 行政院副院長 陳其南

總統召開國家安全會議，確立因應兩岸關係新情勢的政策方針與機制，強化國安作為，避免國家經濟社會正常運作受到衝擊，特擬具『因應及反制「一國兩制台灣方案」指導綱領』作為國安團隊及行政部門行動之準則。

外交

善用國際友我新情勢，結合國際社會，反制中共消滅中華民國主權行徑。



外交部部長 吳釗燮

安全

嚴密掌握中國大陸的政經社會情勢變化，防制中共對我國進行輿論操弄、社會滲透、竊取國防及核心產業機密，以維護國家安全與社會安定。




國家安全會議主任委員 李大維 國家情報局長 蔡新智

因應及反制 「一國兩制台灣方案」 指導綱領

第61次
國家安全會議

因應及反制 「一國兩制台灣方案」 指導綱領

第61次
國家安全會議

兩岸

正面看待兩岸交流，堅持對等尊嚴原則，以民主為互動基礎，參考主要民主國家作為，全面檢視兩岸交流相關規定的落實。積極反制中共假借交流，對我國線戰滲透，干預我國內事務。



經濟部長 陳其南

民主法制

立即推動兩岸條例修正案，加速完成民主防護綱的法制工作，以強化民主監督程序與防衛機制。




經濟部部長 陳其南 內政部長 陳其南

經濟

因應美中經貿衝突及國際經貿局勢變遷，積極協助台商回台投資，致力促進產業轉型升級，強化國際佈局，穩定總體經濟發展。提升臺灣在全球產業鏈的優勢與戰略地位，積極與主要貿易夥伴洽簽多邊、雙邊經貿協議。

國防

穩定增加國防預算，全面提升國軍戰力，以嚇阻中國軍事冒進，確保中華民國主權及民主自由。




國防部部長 嚴德發 參謀總長 李喜明

社會

全面加強社會溝通，凝聚人民對兩岸政策共識，團結內部，以一致行動捍衛國家主權。



內政部長 國顯英

因應及反制 「一國兩制台灣方案」 指導綱領

第61次
國家安全會議

例題

- ▲ 隨著科技的進步，「科技情報」(Technical Intelligence) 的蒐集日益重要，英國也早於 1946 年起正式成立「政府通訊總部」(Government Communications Head Quarters, GCHQ)，請說明「政府通訊總部」的性質與權責？以及該機構從冷戰以來的發展及與「五眼聯盟」(Five Eyes International Intelligence Alliances) 之間的關係？
(108 國安局)

- ▲ 【相關問題】當代情報蒐集途徑多元化，科技情報 technical intelligence 的意涵為何？包括哪些類型？請從科技情報類型，論述美國情報體系從事科技情報蒐集的機關有哪些？其任務職責各為何？
(106 公安所)

- ▲ 【相關問題】影(圖)像情報與信號情報有何不同？各有何重要性？請分別說明之。(109 國安局)

- ▲ 【相關問題】由於科技的進步，各國情報蒐集的方法與技術日新月異，「科學技術情報」(Technical Intelligence: techint) 越來越受重視，請問何謂「科學技術情報」？「科學技術情報」有那些類型？(109 警特三)

擬答

一、科技情報 (Technical Intelligence, TECHINT) (=科學技術情報)：即運用技術器材和手段所取得的情報。

(-)本質：是戰略性科技體系的攻防策略，能夠進入科技情報活動範疇的對象，基本上一定是核心的、關鍵的具有戰略性意義的科學技術。

(-)功能：

- 1.保護自己的戰略性科技成果不外流、不受到外部威脅。
- 2.獲取別人已經擁有而組織自身不具備的戰略性科技成果。
- 3.阻止別人發展某種戰略性科技成果的路線與基礎。
- 4.基於競爭態勢上之未來科技發展規劃。

(-)種類：又可區分為信號⁹情報 (Signal Intelligence, SIGINT) 及圖像情報 (Imagery Intelligence, IMINT, 或稱影像情報)。

1.信號情報 (Signals intelligence, SIGINT, 又稱訊號情報)：西元 1972 年 1 月 17 日修訂的《NSCID 6, Signal Intelligence》，指明美國國家安全局 (NSA) 的職掌為「依據中央情報總監¹⁰ (Director of Central Intelligence, DCI) 所頒訂之目標、要求、優先順序，產製信號情報」，並將信號情報分為：通訊情報 (Communication Intelligence, COMINT) 及電子情報 (Electronic Intelligence, ELMINT)。

2.影 (圖) 像情報 (Imagery intelligence, IMINT)：指透過圖像詮釋或分析的科技、地理與情報資訊，獲得方式包括照相、雷達影像與紅外線感測器等。其蒐集透過衛星和資訊航拍。這種試圖以目視觀察敵人、捕捉敵人影像並分析成果的方法，可追溯至美國內戰時期。當時北方聯邦軍與南方邦聯軍均派遣斥候，乘著以控制繩索繫於地面的汽球，來觀察戰場並進行拍照。

二英國政府通訊總部：

(-)背景：政府通訊總部 (Government Communications Head Quarters, GCHQ) 之沿革：西元 1919 年在海軍下設立政府電碼與密碼學院 (GC&CS)，於西元 1922 年改隸屬外交部；後於西元 1946 年改名為政府通訊總部 (GCHQ)。

(-)任務：西元 1994 年英國通過之《情報組織法》，確立政府通訊總部之法律地位與職權，其任務為：

- 1.監視及介入電磁、聲音及其他發射訊號的設備，及產生該訊號之設備，並從中獲取資訊。
- 2.提供軍隊及政府有關語言及加密技術的諮詢及協助。

9 信號 (Signal) 是資訊的載體，通常是以某種物理量表現出來的。通信技術不同，採用的傳輸信號形式就不同。亦即信號的特性必須是可變化、可觀測和可實現的某種物理量。

10 自西元 2004 年《情報改革與恐怖主義預防法 (IRTPA)》通過後，改制為國家情報總監 (DNI)。

三、五眼聯盟（Five Eyes International Intelligence Alliances）（參：<https://zh.wikipedia.org/wiki/五眼聯盟>）：是由五個英語圈國家所組成的情報聯盟，在英美協定下組成的國際情報分（共）享團體，成員國包括澳大利亞、加拿大、紐西蘭、英國和美國。五眼聯盟的歷史最早可以追溯到第二次世界大戰，同盟國所發布的《大西洋憲章》。

冷戰期間，五眼聯盟開發梯隊系統，用於監視蘇聯及其東歐盟友。

五國擁有共同的歷史溯源，所有成員國均曾為大英帝國的一部分，英國、澳洲、紐西蘭和加拿大亦為大英國協成員；美國、加拿大與英國同時也是北約成員國。

各國情報機構，以及對應的情報方式		
國家	機構	角色
澳洲	澳大利亞秘密情報局（ASIS）	人工情報
	澳大利亞信號局（ASD）	信號情報
	澳洲安全情報組織（ASIO）	安全情報
	澳大利亞地理空間情報組織（AGO）	地理情報
	國防情報組織（DIO）	軍事情報
加拿大	加拿大武裝部隊情報司令部（CDI）	軍事情報
	通信安全機構（CSE）	信號情報
	加拿大安全情報局（CSIS）	人工情報
紐西蘭	國防情報安全局（DDIS）	軍事情報
	政府通訊安全局（GCSB）	信號情報
	紐西蘭安全情報局（NZSIS）	人工情報
英國	英國國防情報局（DI）	軍事情報
	政府通信總部（GCHQ）	信號情報
	軍情五處（MI5）	安全情報
	秘密情報局（軍情六處）（MI6）	人工情報
美國	中央情報局（CIA）	人工情報
	美國國防情報局（DIA）	軍事情報
	聯邦調查局（FBI）	安全情報
	美國國家地理空間情報局（NGA）	地理情報
	美國國家安全局（NSA）	信號情報

例題

- ▲我國針對 2017 年臺北世界大學運動會反恐情報係透過那些單位蒐集？倘若現階段我國無法加入國際刑警組織，可透過那些方式取得國際犯罪情報？〈106 警特三〉

- ▲【相關問題】國與國之間的「情報合作」，為國際社會中常見的情報交流手段，請說明國與國間常見的「情報合作」的類型。並以日本與美國為例，說明雙方進行「情報合作」的方式與內涵。〈107 國安局〉

- ▲【相關問題】本（106）年八月即將在臺灣舉行的「世界大學運動會」，屆時將有來自世界各地百餘國及萬人以上之選手抵臺參賽，為國內歷來所舉辦最大規模之國際性活動，也是對維護我國國家安全的機關一項空前的挑戰，請試從情報工作的觀點，剖析說明相關機關應如何加以因應？〈106 公安所〉

- ▲【相關問題】民國 98 年 7 月份於高雄所舉行的「世界運動會（World Games）」，為我國所舉辦的最大規模的國際性活動（包括美、英、中國大陸、以色列等國均已報名參加），請試從「非傳統性安全威脅（Non-traditional Security Threats）」的角度，說明此項活動是否有可能對我國的國家安全造成影響？而相關部門又應如何加以因應？〈98 警特三〉

擬答

一、針對台北世界大學運動會反恐情報蒐集與非傳統安全威脅對國家安全造成的影響，茲簡要說明如下：

自西元 1990 年代起，對美國及其他特定國家而言，其國家安全的利益內容與行動趨向也有所轉變：包括區域衝突、恐怖主義活動、顛覆戰爭、跨國販毒走私、經濟競爭及低密度衝突（Low Intensity Conflict, LIC）等當前國家安全的重要內容，已然取代冷戰時間之高政治性的軍事安全議題，亦即，後冷戰時期以來，由於國際情勢的變遷，導致各種恐怖主義、大規模毀滅性武器（Weapons of Mass Destruction, WMD，亦可稱為大規模殺傷性武器，本書則統一稱為「大規模毀滅性武器」）、區域性軍事衝突或內戰等各種「非傳統性安全威脅（Non-traditional Security Threat）」不斷的出現及升高，而使所謂的「國土安全（Homeland Security）」問題日益受到世界各國的重視。

也因此，自西元 1990 年代起，各國舉凡情報工作對象、情報活動方式及情報運用途徑等，均和過去傳統方式極為不同：

- (一)因為處理低密度衝突（LIC），必須結合軍事、外交及情報秘密行動等各式途徑，因此，LIC 相關的情報需求變得非常重要，而其所採取相關的情報途徑，迥異於以往，例如：對恐怖組織、跨國販毒、走私集團進行滲透，以及建立各國的情報合作聯繫模式等，均為新的趨勢與挑戰。
- (二)後冷戰時期，經濟、商業及科技性的競爭日漸激烈，而其他衍生出來的問題，也是當前情報工作的重要挑戰。例如有人主張，今後的情報工作應新增著重於經濟情報。
- (三)全球化議題下，所產生的一些例如全球環保、碳排放問題、雨林保護、難民問題、傳染性疾病蔓延等新的問題，也會為各國帶來新的情報需求。

總之，國家安全的威脅來源或許有所轉變，環境或許有所調整，然而，國家安全的重要性不會因此而改變。同時，這些新的調整與轉變，反而增強了情報的功能與角色，也加重了情報活動的負擔，使情報工作的困難度因此提高了，事實上，情報活動與國家安全也如影隨形地變的更加緊密了。

本題，由於 911 事件發生後，突顯出攻擊者的不確定、手段方式多樣性，且造成的傷亡更加嚴重，也使情報體系更加重視非傳統安全可能帶來的威脅，例如國際賽會（事）的場合，更是非傳統安全威脅份子亟思表達其理念的場合與管道。以台北舉辦世界大學運動會為例，這是一場國際賽會（事），各國選手與會、齊聚一堂，對於我國的國家安全將會是一大挑戰，無論是中共的藏獨、疆獨、或法輪功等異議團體，是否會對藉此場合，對我國進行抗議，甚或採取其他恐怖主義等暴力手段等作為？！身為主辦國，必須透過我國及其它國家之各種情報機構（關），分（共）享情報資訊，並彼此密切合作，注意並加強各種情報活動，同時，應採取預警機制，加強各項防範作為。

二我國身為主辦國，面臨各式跨國組織犯罪之威脅，針對各項國際犯罪情報之蒐集與取得，相關部門應有的反恐情報蒐集作為，茲略述說明如下：

(一) 情報的交換與國際情報合作 (International Intelligence Cooperation)：學者杜陵曾說：「與有關盟國採取合作方式，以交換戰爭情報，來抵抗共同敵人，是不可少的措施。」尤其在當代複雜無比且激烈的情報戰中，各國政策制定者對於情報的需求，往往無法再只由自己的情報機關來滿足，因此，國與國之間、情報機關與情報機關之間的各種情報活動的合作網絡因運而生，其目的在進行各種形式或各種內容的雙邊或多邊的「秘密情報」交換。國家安全情報活動的工作中，有部分是透過對外情報支援，來獲得相對攸關本國安全的情報，此種相互支援網絡之秘密情報交流，最重要的即是電訊情報之合作，而這整個情報活動展現的既是秘密情報的重要來源，也是各國情報合作的形式。(參蕭台福，《情報的藝術》，2015.2，時英出版社，頁 661 ~ 667)

(二) 我國之情報交換規定：依我國《國家情報工作法》第 17 條第 1、2 項規定：各情報機關與外國情報機關進行情報合作事宜時，應通知主管機關，並由主管機關協助統合及節制。

前項情報合作包括情報交換、情報會議、人員互訪、情報訓練、技術交流、電訊偵蒐及情戰行動等。

(三) 兩岸之刑事司法互助，始於西元 1990 年由兩岸紅十字會所簽署之金門協議，該協議的重點乃人員遣返，包括對雙方偷渡犯、犯罪嫌疑人或刑事罪犯，得請求遣返己方處理或受審。迄西元 1993 年辜汪會談後，正式將兩岸溝通合作之管道制度化，進而取代紅十字會權宜協調及相關作業程序。民國 98 年 4 月 26 日，為保障海峽兩岸人民權益，維護兩岸交流秩序，財團法人海峽交流基金會與海峽兩岸關係協會就兩岸共同打擊犯罪及司法互助與聯繫事宜，經平等協商，達成《海峽兩岸共同打擊犯罪及司法互助協議》。其中，共同打擊犯罪之合作範圍，乃係雙方同意採取措施共同打擊雙方均認為涉嫌犯罪的行為。

(四) 兩岸犯罪情資交換：為妥適執行《海峽兩岸共同打擊犯罪及司法互助協議》(第 5 條) 有關犯罪情資交換事宜，遂行共同打擊犯罪目的，我方相關機關(或機構)曾於民國 100 年 1 月 3 日函頒之辦理兩岸共同打擊犯罪及司法互助作業規定—《海峽兩岸犯罪情資交換作業要點》。此乃一情報資料合作與交換之具體實踐。



觀念補充



國際刑警組織：

一國際刑警組織係全球性警察合作組織，並無對各國警察指揮權亦無專屬部隊，功能乃以特有通報系統傳遞犯罪手段及重大情資，協助偵查國際犯罪與逮捕犯罪嫌疑人。架構除大會、執行委員會，透過秘書處與區域局向會員國聯絡據點（國家中央局），傳送犯罪訊息並提供支援；區域局屬秘書處，促進有效率處理或協助請求，或協調結合各國執法行動，為區域執法困境尋求之解決方案。

二國際刑警組織積極串聯區域及全球性執法合作組織，並與歐盟警察署及國際刑事法院，設置核心國際犯罪聯絡點，主要任務乃在協助國際刑事法院進行調查、追訴與逮捕移交，提供核心國際犯罪資訊，協調促進相關機關採行措施或支援合作行動。歐盟本身已與國際刑事法院締結合作互助協定，範圍限於成員國間常態性聯繫，歐盟警察署更就此積極參與，充分實踐與國際刑警組織之執法合作。



例題

- ▲反情報（counterintelligence, or CI）雖是情報活動的主要面向之一，然而，我國於2005年所通過之「國家情報工作法」內，雖對「情報工作」之界定與內容有所規範，但卻無有關「反情報」或「反情報工作」之用語與說明。試由相關法制以及實踐面，說明與比較：反情報工作與情報工作之異同。（107 警特三）

- ▲【相關問題】「情報（Intel l igence）」與「反情報（Counter- intel l igence）」之界定，不僅眾說紛紜，且常係學者與實務界所爭辯之議題；試說明反情報工作與司法警察工作有無異同之處？並由「知識」、「組織」與「活動」等三面向，對於情報與反情報之意義、內容和目的，加以說明與比較。（93 警特三）

- ▲【相關問題】請依據我國相關法令、情報學理與實踐經驗，說明：反情報之概念與界定、範圍與類型，以及當前之工作挑戰為何？（108 公安所）

- ▲【相關問題】觀察近年來國內外案例的啟示，保防體系運作之成敗，攸關國家安全與利益維護。請依據我國相關法規、情報學理與實踐經驗，說明「保防」之概念和界定，以及其與反情報之關聯性為何？現階段我國「保防」工作體系運作及各單位分工與職掌各為何？（109 公安所）

- ▲【相關問題】反情報的定義及其活動方式為何？（110 公安所）

- ▲【相關問題】觀察國際與我國近年間諜案例，反情報工作攸關國家安全與機密維護。請說明反情報（counterintelligence）、反諜報（counterespionage）與安全防護（security）的關聯性及異同處為何？現階段我國安全防護工作體系的制度運作及各單位分工與職責為何？（110 國安局）

擬答

一、情報工作之定義：

(一)我國：

- (1)學說：情報學學者杜陵認為情報工作即在於提供決策者與行動所需之消息。而一般將情報工作分為狹義與廣義二種解釋：
 - 1.狹義：指產生情報的過程，即情報的蒐集及情報的處理。
 - 2.廣義：除了前述狹義的解釋外，尚包括利用情報以進行的各種行動在內，亦即產出情報（知敵的工作）、反情報（防敵的工作）、情報戰（攻敵的工作）的總稱。
- (2)法規：據《國家情報工作法》第3條第1項第2款：情報工作係指情報機關基於職權，對足以影響國家安全或利益之資訊，所進行之蒐集、研析、處理及運用。應用保防、偵防、安全管制等措施，反制外國或敵對勢力對我國進行情報工作之行為，亦同。（註：研析即評估和分析。）

(二)外國：美國情報學學者藍森（Harry Howe Ransom）指出：情報工作即提供決策者與行動所需之消息；另外，情報為一動態觀念，係一項未有明顯起點或終點的過程；又情報是指包括從蒐集、處理到分發運用，周而復始進行其間各階段中之每一功能。

二、張中勇認為反情報的意義與目的：

(一)反情報之意義：反情報是一種情報活動，亦稱保防安全工作、保密防諜工作。其對應之情報即為「國內安全情報」。

(二)反情報之定義：

- 1.**狹義的定義**：反情報角色之界定限為防止外國情報勢力的諜報活動。
- 2.**廣義的定義**：由狹義的定義再將其擴展至尋找內間（Moles，英國情報用語）¹⁹，以及積極打擊敵對情報組織及其活動，並且應包括分析檢討本身安全防护弱點及其活動之可能威脅²⁰。

19 內間指利用敵方官員，成為為己方效力之間諜。

20 參張中勇著，1993，《情報與國家安全之研究》，三鋒，頁412。

(三)反情報的目的：不僅在防制外來間諜竊密、維護國家機密安全，並且是政府當局用來對抗顛覆組織行為、壓制反對勢力及打擊恐怖活動等安全威脅的重要手段，即協助政府掌握社會動態、排除各項安全威脅來源。簡言之，了解敵情、破壞敵人的情報工作並以確保我方安全為目的的一種情報活動即為反情報。此外，反情報工作和情報工作相同，都是在了解敵情並加以運用，而其間最大的不同點在於，前者為守勢作用、消極情報活動，後者則為攻勢作用。

雖然反情報工作與人權保障不易獲取平衡，易於衍生爭議或產生弊端，惟其目的在於防範或反制外力竊密、滲透、破壞和顛覆等作為，不僅是維護社會安定之基本力量，更是確保國家安全與利益的重要憑藉，故其存在仍為必要之惡。總之，反情報之情報安全活動，其理論目的在維護國家安全，對外在防止其他敵友國家情報活動、打擊恐怖主義活動，對內則在確保機密安全、防止顛覆及叛節行為，基本上，反情報理念及其作法應無可議之處，然而，其具體實踐上卻往往衍生出不少問題：

1. 情報活動應保護國家安全，但卻常以犧牲人民的基本權益作為代價。
2. 情報活動應促進國家利益，但卻常損及人民的權益與福祉。

因此，反情報之情報安全活動在國家安全維護過程中所扮演的角色，必須更加強其理念、內容及作法的時代意義及法治意義。

(四)我國國家情報法制對「反情報」之定義與機制：

1. 依《國家情報工作法》第 3 條第 1 項第 2 款後段規定可知，應用保防、偵防、安全管制等措施，反制外國或敵對勢力對我國進行情報工作之行為，即為反情報。
2. 依《國家情報工作法》第 3 條第 1 項第 6 款規定，間諜行為：指為外國勢力、境外敵對勢力或其工作人員對本國從事情報工作而刺探、收集、洩漏或交付資訊者。
3. 《國家情報工作法》第 22 條（反制間諜工作）第 1～3 項規定：
 - (1) 情報機關從事反制間諜工作時，應報請情報機關首長核可後實施，並應將該工作專案名稱報請主管機關備查。但屬反爭取運用者，應經主管機關核可後實施。
 - (2) 情報機關從事前項反制間諜工作時，得經機關首長核准，向其他政府機關（構）、單位調閱涉嫌間諜行為之人及其幫助之人之有關資料，該管監督機關（構）、單位除有妨害國家安全或利益者外，不得拒絕。
 - (3) 前述(1)但書之情形，應由主管機關報告國家安全會議秘書長，於經最高法院檢察署檢察總長或最高軍事法院檢察署檢察長同意後，由主管機關協調各該情報機關決定案件移送偵辦時機、移送之對象及移送之內容。

三、保防（現稱：安全防護）與反情報：

(一)保防（現稱：安全防護）的意義：我國法務部於中華民國 108 年 12 月 11 日函頒《全國安全防護工作作業要點（原名稱為：保防工作作業要點）》第 7 點規定：全國安全防護工作之業務範圍如下：1.機密維護。2.安全維護。3.機密及安全維護教育。

日前，法務部調查局並已經重新詮釋保防（現稱：安全防護）工作，指保防（現稱：安全防護）即係：「保衛國家安全，防制敵諜滲透。也就是國家對抗外力對我情蒐滲透、破壞之反情報工作。」《全國安全防護工作作業要點》第 1 點規定：「為貫徹『執行有關危害國家安全及違反國家利益之安全防護工作』，特訂定本要點。」此並將「保防」工作，修改為「安全防護」工作。同時，《全國安全防護工作作業要點》第 2 點復規定：「全國安全防護工作，由法務部主管，並指定調查局協調執行。」

(二)保防（現稱：安全防護）之界定與情報、反情報的異同比較，分述如下：

1.情報工作之發展，先有情報而後有反情報，為使保防工作更具法制化、專業化，而後來以「保防」取代反情報。之後，法務部調查局並將「保防」工作，修改為「安全防護」工作。

依法行政國家，反情報工作就是反制間諜，須以法律命令作為規範，以免違法違憲之虞，更有侵害人權情事。目前依現行法令，以由「保防（現稱：安全防護）」工作取代之。

2.保防（現稱：安全防護）工作與反情報工作相同，在於防止間諜竊取並洩漏國家機密，而保防重點也就是所謂的保密防諜，其工作區分如下：

(1)保密：防止敵人或非友好國家及任何非法定人員取得或知悉國家情報機密所採取的各項措施。

(2)防諜：防止與破壞任何足以危害國家安全的非法組織與人員，取得與知悉國家安全情報機密的一切安全防護措施。

3.反情報工作就是反制間諜工作，是情報機關的另一個工作重點。

4.情報機關（構）對於保防工作，更要加強改進反制間諜工作之方法手段。

(三)現階段保防體系建構、制度運作、及各單位與職掌事項，分述如下：

1.體系建構：依《保防工作要點》規定，保防工作區分為機關保防、軍中保防、社會保防。機關保防工作，由法務部調查局辦理；軍中保防工作，由國防部總政治作戰局辦理；社會保防工作，由內政部督導警政署辦理。其主管事情報事務範圍內，視為情報機關，應受主管機關（國家安全局）指導、協調、統合國家情報作為，指導各情報機關。

2.制度運作方面：保防工作即反制間諜工作，國家情報工作法授權制訂《情報機關反制間工作辦法》，前項法律明確規範，反制間諜工作，係指情報機關對所屬常人員，所採取之監督、檢查、調查及反爭取運用等作為，反制外國或對勢力接觸、吸收、利用而破換我國情報活動及作為。情報機關對違常員採取之反制間諜工作，應經機關首長核定後，以秘密方式為之。

3.單位及職掌項目：

(1)社會保防：係由內政部警政署負責督導事宜，依《內政部警政署辦事細則》說明，警政署設保防室，負責所屬警察機關之機關保防工作之規劃、督導、考核事項；社會保防工作之規劃、督導、考核事項；偵防內亂、外患及危害國家安全案件之規劃、督導、考核事項；社會治安調查之研究、規劃、指導、蒐集及處理事項。

前項職掌事項，基於主管情報事務範圍內，視為國家情報工作法之情報機關，須受國家安全局的指導監督。

(2)機關保防：係由法務部調查局負責督導事宜，依《法務部調查局組織法》規定，本局設國家安全維護處、國內安全調查處、保防處，辦理機關保防業務及全國保防、國民保防教育之協調、執行事項；國內安全及犯罪調查、防制之諮詢規劃、管理事項；上級機關特交有關國家安全及國家利益之調查、保防事項等。該局為實施全國性調查、保防業務，得於各省（市）、縣（市）及重要地區，設調查處、調查站或工作站辦理保防工作事項。

前項職掌事項，基於主管情報事務範圍內，視為國家情報工作法之情報機關，須受國家安全局的指導監督。

(3)軍中保防：係由國防部總政治作戰局負責督導軍中保防事宜，依《國防部總政治作戰局組織條例》規定，國防部總政治作戰局 承國防部部長之命，主管國軍政治作戰事項，本局下設保防安全處，辦理軍機保密、安全調查、諮詢部署、安全防護、保防教育之規劃、督導及執行事項，前項事項分述如下：國軍人員安全調查、防諜情報蒐集與敵（間）諜案件、軍防範秘密破壞工作、國軍保防教育國軍反情報等保防工作。

前項職掌事項，基於主管情報事務範圍內，視為國家情報工作法之情報機關，須受國家安全局的指導監督。

四警察的國家安全保衛業務：梅可望先生於其著作《警察學》（2008）一書中指出，各國警察業務的範圍包括以下 10 項：國家安全的保衛、犯罪預防、犯罪制壓、交通管制與交通事故的處理、公共安寧秩序的保護、善良風俗的維持、災害的防止與搶救、家戶訪查、為民服務、諸般行政的協助與其他行政執行事項。其中，保衛國家安全的警察業務是側重在政治顛覆性的工作，亦即消滅國內政治性的顛覆活動。

108年度考題

例題

▲在各種情報機構所提供的「情報產品」(Intelligence Product)中，以「動態情報」(Current Intelligence)通常最為決策者所重視，但此種情況卻常引發一些爭議，請說明何謂「動態情報」？以及上述情況所引發的爭議為何？〈108 國安局〉(參 Abran N. Shulsky 所著《無聲的戰爭 - 認識情報世界》，金城出版社，2020.5.，頁 94 ~ 102)

▲【相關問題】依據 Abran N. Shulsky 所著《無聲的戰爭 - 認識情報世界》，情報產品可區分為那幾種？請分別說明之。〈109 警特三〉

擬答

依 Abran N. Shulsky 所著《無聲的戰爭 - 認識情報世界》一書，情報產品的種類分為以下三類：包括動態情報、基本情報、情報評估。茲分述說明如下：

一、動態情報 (Current Intelligence)：

(一)動態情報 (Current Intelligence)，又稱當前情報、現時情報、動向情報：著重於當前情勢之說明。

(二)動態情報 (Current Intelligence) 對於情報機構 (關) 而言，其所引起的作用與新聞媒體類似。即其所提供的資訊範圍，取決於該國情報機構 (關) 興趣的範圍，用肯特的話來說，必須基於「當前國家面臨的問題及將來可能面臨的其它問題」，來確立其優先順序。儘管體系內存在一個正式的確立其優先順序的機制或制度，然而，什麼東西對情報用戶而言最重要，情報生產者必須先有自己的判斷，這是對制度必要的補充。反過來說，此種判斷基礎不僅取決於情報分析人員自己的常識，還要取決於他們與決策者接觸的密切程度。例如美國的《總統每日簡報 (PDB)》，即屬於動態情報類別。然而，此項作為存在著一個問題 (或稱爭議)，就是美國情報機構 (關) 花費了太多的時間與精力 / 或稱浪費的大多的資源，來完成動態情報的工作 / 或稱履行動態情報的職能 (掌)，從而削弱了情報分析人員對形勢作深度分析的能力。這種現象，影響了危機預警質量，不利於情報分析人員認清事物發展的長期趨勢。亦即，過於短視地關注動態事件 (動態情報) 的最新發展，而反而未能對日積月累的具相互關聯性的證據進行系統性的考察——往往對這些資訊中的潛在因素與相互關係視而不見。因為決策者希望了解最新的時事熱點，所以情報分析人員也就不得不使用動態事件 (動態情報) 的分析方式——而此種分析常常壓制了情報分析人員進行深度研究的意願。

(⇒)情報產品——以美國為例：美國「國家情報」及其類別：

- 1.《總統每日簡報（PDB）》：屬於當前情報類別。
- 2.《國家情報日報（NID）》：屬於當前情報類別。
- 3.《國家情報情勢報告（NISR）》：屬於當前情報與警訊情報類別。
- 4.《國家情報評估（NIEs）》：屬於情報評估類別。
- 5.《情報備忘錄（IIM）》：屬於情報評估類別。
- 6.《國家情報分析備忘錄（NIAM）》：屬於情報評估類別。
- 7.《國家情報評估（National Intelligence Estimates, NIEs）》：屬於情報評估類別。

二基本情報：基本情報係利用公開資料和各種情報來源提供相關訊息（全源情報），為特定情形提供可能較完整的情報資訊。同樣，關於一個國家政治制度的基本情報報告可能涉及所有的主要政治力量和政治人物、觀點概念與相互關係。

三情報評估：情報產品中最具挑戰的一種，除了描述當前情況，且嘗試預測未來趨勢，美國情報用語稱之為「情報評估」，例如：《國家情報評估（National Intelligence Estimates, NIEs）》，代表著每美國情報機構就最有權威之報告，前項所稱之情報機構係依據西元 1981 年 12 月 4 日總統令第 12333 號發佈《美國國家情報活動規範》定義的中央情報局、聯邦國家安全局、國防情報局、國家偵察辦公室、國務院情報研究局、聯邦調查局、財政部、能源部等情報組織，共同研議情報評估分析報告、評估情報整合所有情報機構的觀點。

《國家情報評估（National Intelligence Estimates, NIEs）》之定義：美國「評估性情報」最主要的表現形式即為《國家情報評估（National Intelligence Estimates, NIEs）》。依美國《國家戰略情報法》之定義，任何情況下，提供國家安全情報的事實，對可能性或概率進行認真的權衡，並對這種事實、可能性或概率作出結論，而此過程的最終產品即為《國家情報評估》。

例題

▲對於「反情報」(Counterintelligence)工作，許多國家多採取「防禦性」的作法，但事實上，「反情報」工作仍可採用積極的或是主動攻擊的手段去進行，請說明「防禦性」與「攻擊性」反情報工作的內涵？以及若採取「攻擊性」的反情報作為，則與「秘密行動」(Covert Action)有何關聯？〈108 警特三〉(參汪毓璋著，2018，《情報、反情報與變革(上)(下)》，頁1504～1520)

▲【相關問題】反情報的定義及其活動方式為何？〈110 公安所〉

擬答

一、反情報的工作內涵，分為「攻擊性」與「防禦性」反情報工作，茲說明如下：

(一)「攻擊性」反情報工作內涵：「攻擊性」「反情報」係針對外來諜報活動，採取更積極的反制行動，利用滲透、收買、或說服等手段而取得對方情蒐機密，達成化解、消弭或瓦解外來諜報威脅的目的。其原則及活動內容如下：

1. 嚇阻原則：嚇阻是指預防敵對者取得進入資訊的能力。亦包括使敵對者放棄獲取資訊的行動，及能夠使其滲透行動無效的能力。
2. 偵測原則：指察覺及鑑定到值得注意的事件、涉及事件的人士、利益者的組織關聯性、利益者之當前地點、蒐集到可以指參與事件人士的相關事實。

(二)「防禦性」反情報工作內涵：「防禦性」「反情報」係指反情報工作之另一方面而言，「安全情報」的目的則不僅在防制外來間諜竊密，維護國家機密安全，且是政府當局對抗顛覆組織、壓制反對勢力、打擊恐怖活動等安全威脅的重要手段，其目的在於協助執政者掌握社會動態，排除安全威脅來源。事實上，對於排除安全威脅的需求而言，安全情報角色的重要性與必要性通常較為顯著，同時也是國家建構情報機關(構)常見的動機與目的。其原則及活動內容如下：

1. 欺騙原則：欺騙的目的是誤導敵方所做的決定使他們採取的行動失去效用。其手段包括：誘餌行動、偽裝行動、藉口(移花接木)、及詭計。欺騙可以誤導敵對決策者有關的一些機構行動、能力、或企圖的方向，也包括隱藏正在進行滲透行動之人。→雙面間諜(Double Agent)行動就是具體實例。
2. 抵銷原則：抵銷的方法就是阻斷敵方資料蒐集的執行。可以透過抵銷的反情報原則來破壞或癱瘓敵方的資料蒐集情形、減低敵方行動的熱情及利益，使他們感到行為及信心的受挫。→化解的手段中，最突出的即為反間諜行動(Counterespionage)中之「虛構間諜(Fictional Spy)」類型。

二反情報之型態分類，包括：國家安全反情報、軍事反情報、執法反情報、商業反情報〔商業情報（Business Intelligent）：係關注於競爭者情報（Competitor Intelligent）—或稱競爭者情報（Competitive Intelligent）、企業情報（Corporate Intelligent）；而商業反情報則著重於保護貿易資訊（Trade Information）〕、私人反情報。

三反情報的工作內涵，與「秘密行動」工作內涵，兩者具相當性關聯角色運用，說明如下：

(一)就情報功能分工而言，情報蒐集、分析的目的，在提供政策過程所需之決策資訊。同時，情報的四項廣泛功能（情報的要素）包括：「間諜（蒐集資訊）」、「觀察（以觀看方式來蒐集資訊）」、「研究」、「分析」。→「間諜與觀察」是用來支援「研究與分析」；而接續結合「間諜、觀察、研究、分析」之作為，就是要用來支援「秘密行動」。

而反情報（的要素）是由反情報（Counterintelligent）與反間諜（Counterespionage）二要素組成。前者是關於嚇阻與偵測，聚焦於安全功能（Security Function）（但是不等於「安全」）；後者則與偵測、欺騙、和抵銷敵方（對手）情報活動之有效性有關。

此外，反情報包括調查被懷疑者的或是已經發生的安全漏洞，因此，其與執法者角色有關；而反情報也涉及了研究與分析，因此，其與情報功能亦有關。→就本質言，情報與執法都是反情報的功能，亦即，反情報融合了「安全、執法、與情報」。

(二)「秘密行動」的工作內涵：「秘密行動（或稱隱蔽行動）」是處於灰色地帶的情報工作，則係扮演政策執行的工具角色：

1.戰爭時期：「秘密行動」除可蒐集情報外，更可藉由各種政治、經濟、社會、心理、宣傳、準軍事、情報協助等秘密手段，達到擾亂、破壞、削弱、或瓦解軍心、戰備能力、或國民意志的目標，抑或是影響活動對象國的政策走向與內容的目的，或是排除軍事行動的障礙，協助軍事攻擊的進展。

2.另外，和平時期：當軍事與外交政策手段皆不宜、無法使用或成效有限時，「秘密行動」則可發揮「靜默方案」的功能，或扮演「第四武力」的角色，包括利用宣傳策略、經費援助、選舉諮詢、培養影響力內線、協助組成民間團體、或學會組織等政治性秘密活動手段，目標在直接或間接達成政策目標。

例題

- ▲請說明情報（intelligence）與政策（policy）間應如何維持妥適之互動關係，以避免情報政治化的負面效應？〈109 公安所〉

- ▲【相關問題】何謂情報政治化？在情報與政策的互動上應如何律定其關係？〈110 公安所〉

- ▲【相關問題】情報是攸關國家安全的實用學科，向來受到各國政府的重視。請從情報學理與實踐經驗，說明情報（intelligence）與政策（policy）之關係為何？在制度面向與實際運作面向，二者應如何維持妥適的互動關係，以避免情報政治化（politicization of intelligence）的負面效應？〈110 國安局〉

擬答

一、情報與政策互動的認知：為發揮情報活動功能及達成情報任務，情報與政策二者間應有以下相互的認知與態度：

（一）在政策制定者方面：政策制定者應關切情報活動過程：

1. 政策制定者應清楚表明政策趨向與議題重點。
2. 政策制定者應直接要求情報產製者提供或禁止蒐集特定情報，以免政策面陷入尷尬或驚訝。
3. 政策制定者應盡量提出自身所不知道的情報需求：這是一項情報管理的策略，使情報體系（情報產製者）能於利用有限的時間與精力，獲致最大的情報工作效果。
4. 政策制定者應學習面對情報世界的不確定性：尤其不可導致情報體系因情報不確定性之本質，而扭曲其價值中立的角色來逢迎政策需求。
5. 政策制定者應去除自以為是的心態：以免決策者因為自認有能力分析評估情報，而不願參考情報體系所提供的另一項評估結果。
6. 決策者應體認情報體系能力有限，而有效地管理及運用情報資源，以發揮其有限能力下的最大作用。
7. 決策者應對於情報體系之情報活動成果，提供肯定或要求的回饋（Feedback），引導情報產製者進一步了解政策制定者的政策焦點及情報需求，以提升情報與政策間的良好互動。

(二)在情報產製者方面：情報產製者應關切情報制定者的認知與態度，並就其本身政策角色、工作性質及環境特性等層面，以支持政策過程為目標而扮演其應有的功能與角色，其中，又以加強情報資源之運用與管理為其須特別重視者。茲略述如下：

1. 情報產製者應提供當前情報評估以供現時的政策需求，並提供長期情報評估作為政策的長遠基礎。此外，亦應針對主要議題，提供特別情報評估報告。
2. 情報產製者應儘量避免養成濫用模糊或曖昧用語的習慣，以降低情報評估內容的不確定性，因其易失去決策者的信心與注意力。
3. 情報產製者無需刻意強求情報評估結果之一貫性與一致性：有必要修正情報評估結論時，絕不可因畏懼受批評或怕失去決策者信心而置之不理。事實上，情報分析評估活動與政策面間的認知關係，決定於情報提供者保持主動的態度。
4. 情報產製者之情報評估必須抓住重點，並注意精簡扼要：這是情報管理上所必須掌握之重要原則。
5. 情報產製者必須坦然面對情報世界的特質，無須勉強應付全局，更無須刻意顯出神通廣大。
6. 情報產製者對於無重大動態發展的重要情報活動對象，仍應維持相關情報工作之進行，並持續提醒決策者有關其作為或不作為之資訊，以免被誤解該對象已經不再成為重要情報活動的目標。
7. 情報產製者應建立自我分析制度，以隨時檢討本身情報工作之優、缺點，並予以及時改進。

(三)情報與政策間相互距離方面：過去，肯特（Sherman Kent）曾認為，情報與政策過程間必須保持距離，以求客觀中立，並隨時提供決策者情報，以檢討政策面之效果與缺失。惟後冷戰時期，隨著國際局勢演變，情報角色已不同於以往在美、蘇兩極對抗、目標明確時代下之任務內容。如今，情報活動對象變得日趨多元，並呈現多樣型態，使得政策的需求變得更趨機動、彈性，並增進時效性的要求，因此，出現另一種主張，認為情報必須與政策緊密聯繫、相互認知，並運用情報分析的四個主要思維趨向²²，並與政策需求密切配合，以提供務實、及時的協助。

22 參本書後述，即機會趨向分析、自覺趨向分析、互動趨向分析與差異趨向分析。

二、「情報為政治服務」的理論如果發揮至極限，則在極權國家可能變成情報機關是統治者鎮壓異己的工具；而在民主國家，也希望情報能夠成為「支持執政者的政策」。因此，信息的獨立性與情報政治化一直在現實運作中拉鋸。

(一)情報政治化發生的情況：

- 1.當情報成為黨派、利益團體等政治勢力間的爭議問題，雙方或多方對於情報角色有不同意見，或對特定議題看法不同。
- 2.某些情報議題曝光，成為社會輿論所關注與公共政策所面對的問題。
- 3.專指情報體系、組織成員受到政策面壓力、影響與暗示，使得情報評估傾向政策面偏好方向、扭曲事實，將情報視為「討好」的工具。

(二)情報政治化可分為：

- 1.情報機關政治化。
- 2.情報蒐集政治化。
- 3.情報分析政治化。

為避免情報政治化，我國係透過《國家情報工作法》建立情報法制化，規範國家情報工作職權，予以適當監督，可避免「情報政治化」，維持政治中立。同時，建立情報監督法制亦可以獲取人民對於情報機關的信賴。而情報監督（又稱情報控制）之意義在於：經由監督的審查和責任追究的管控情報作為，使情報機關的決策及活動，符合正當法律程序（包括：合法性、合目的性及正當性），並藉以建立情報機關之中立化、專業化。

110年度考題

例題

▲網路安全 cyber security 受到各國政府的重視並列為國家安全的優先目標。何謂網路威脅情報 (cyber threat intelligence) ? 請以美國及我國為例, 說明情報體系如何因應網路安全威脅? (110 公安所)

▲全球化時代伴隨著資通訊科技的發展趨勢, 伊斯蘭國等激進暴力恐怖主義組織利用網際網路迅速發展組織並遂行恐怖攻擊。網路安全成為當代各國政府國家安全的優先目標, 試述網路情報 (Cyber Intelligence) 之意涵為何? 以我國及美國為例, 從組織面向及情報作為論述情報體系如何因應網路安全威脅? (105 公安所)

擬答

一、網絡情報 (Cyber Intelligence, 或稱網路情報) 的內涵 (參汪毓璋著, 2018, 《情報、反情報與變革 (上) (下)》, 頁 194、198 ~ 200): 用以評估對手在網路領域的能力、意圖、和活動 (技術和其它) 之網絡情報, 應該支援和通知整個組織的網路運營, 包括進攻和防衛過程。網絡情報的定義: 經由情報循環的產品與流程, 而評估網路領域潛在對手和競爭之能力、意圖、和活動 (技術和其它)。其對手範圍, 包括使用網路領域進行犯罪和相關詐欺活動的所有個人與組織。

網絡情報分析人員應該具備的核心技能:

(一) 資訊與通訊技術、網路安全相關的技術能力。

(二) 從各種來源, 進行包括戰略基礎、系統思維等對資訊與資料進行複雜分析的社會科學基礎分析能力。

(三) 規劃和組織資訊蒐集、開發與應用工具等之知識管理能力。

(四) 從具體領域、國家地區、心理社會或社會文化等基礎分析複雜問題的脈絡能力。

(五) 要有能明確表達意見與推理, 同時有效溝通自己想法等之溝通與組織的能力。

二、由於網際網路的普及, 網絡情報 (Cyber Intelligence, 或稱網路情報) 的獲取也變得容易, 此時, 情報分析人員通常採用二種分析模式來進行分析工作, 首先是透過軟體模式進行計算機海量資訊過濾, 以濾除無用資訊, 然後第二步再採用人工模式進行情報分析, 以獲得正確的情報。因此, 情報可以說是人類智能的體現。

三第三期的美國《國家情報戰略》係由美國國家情報總監（DNI）於西元 2014 年 9 月 17 日所公布之美國《2014 年國家情報戰略（2014 National Intelligence Strategy, NIS）》，成為當前美國國家情報工作的具體政策目標。該份《國家情報戰略（NIS）》指出七大任務目標：第四項任務目標、網絡情報（Cyber Intelligence）／網路威脅情報（cyber threat intelligence）：察覺並了解網絡威脅，以通知並賦予國家安全決策的能力、網絡安全性、和網絡相關作用的操作（作戰）業務。

網絡情報は對全來源情報之資訊進行蒐集、處理、分析和傳播，而這些全源情報的資訊是來自外國參與者的網絡上的程式、意圖、能力、研究和開發（研發 R&D）、戰術、業務活動和指標；它們對國家安全、資訊系統、基礎設施和資料，發生衝擊或潛在的影響；同時還包括電腦網絡的表徵或構成要素、結構、用途的洞察，及外國的資訊系統的安全漏洞。

國家和非國家行為者，使用數位的技術來實現經濟和軍事優勢、挑起不穩定、透過網絡空間中的內容增加控制權，並實現其他的戰略目標——往往比我們了解的安全問題和降低潛在風險的能力更快。為推進國家目標，客戶越來越依賴於情報體系提供及時、可操作的情報和更深入地洞察當前和潛在的網絡威脅和意圖。情報體系還提供了所需的專業技能與其他重要的通信網絡和國家基礎設施，一起捍衛美國政府的網絡。為了更具效率，情報體系將發展其網絡能力，包括我們認為某人或某事具有的攻擊能力。情報體系將側重於查明趨勢，並提供客觀的認知來增進客戶對威脅、安全漏洞和衝擊的認識。

為了實現這一目標，情報體系將：

- (一)提高我們對關鍵的外國網絡威脅行為的體認和了解——包括他們的意圖、能力和行動，以滿足日益增多和複雜性的網絡相關的需要；
- (二)擴展量身訂做的情報產品和可操作的網絡情報的宣傳，來支援維持生命所必需的資訊網絡和重要基礎設施之防禦工作；
- (三)擴大我們使網絡運作產生影響的能力，以保護和支援美國的國家利益。

四網絡威脅和情報整合中心（CTIIC）：

(一) CTIIC 的職能：西元 2015 年 2 月，美國總統歐巴馬要求國家情報總監（DNI）成立網絡威脅和情報整合中心（Cyber Threat Intelligence Integration Center, CTIIC），該機關將協調整合國土安全部（DHS）、聯邦調查局（FBI）、中央情報局（CIA）、國家安全局（NSA）等多部門的情報力量，提高美國防範和回應網絡攻擊的能力，該機關將成為美國政府防範和應對網絡威脅的主要部門及全國性的網絡威脅情報中樞。CTIIC 是根據西元 2004 年透過的《情報改革與恐怖主義預防法》授予 DNI 的權力建立的情報中心，其將對影響美國國家利益的國外網絡威脅和網絡事件提供整合的全來源情報分析，並扶持政府，以應對國外網絡威脅。

(二) CTIIC 與其他網絡安全中心的關係：CTIIC 不是一個運營中心，不參與蒐集情報、管理網絡安全事件的應對工作，也不直接調查或代替目前現有部門、機關或政府網絡中心的其他職能。CTIIC 的主要任務為 NCCIC 完成網絡防禦和事件響應的任務提供支持；同時，也將為 NCIJTF 完成協調、整合和共享與國際網絡威脅調查相關資訊的使命提供協助；並配合美國網絡司令部抵禦網絡空間的重大攻擊。基於此，CTIIC 將為上述機關以及其他部門和機關提供開展其網絡安全任務所需的情報。

111年度前瞻時事性考題

例題

▲拜登上任後，其國家安全戰略調整為全政府形式，透過多邊主義途徑下，結合盟邦進行全球新合縱行動。請問：有關〈重審美國優勢：暫行國家安全戰略指導〉文件（Renewing Americans Advantages: Interim National Security Strategic Guidance），其主要的內容為何？（參：遠景基金會，〈美國新總統拜登上臺後對中戰略互動意涵〉／<https://www.pf.org.tw/article-pfch-2168-6982>；財團法人國防安全研究院，國家安全所李哲全副研究員，〈拜登首份國安戰略報告及其對中政策輪廓〉／台灣戰略研究學會，翁明賢／https://indsr.org.tw/tw/News_detail/3341/ 拜登首份國安戰略報告及其對中政策；<https://taiwan-strategy.com/news/2021-08-26/123->美國新政府的國際戰略與外交佈局 -- 「拜登時代的國際關係：新佈局與新挑戰」線上時事論壇；《展望與探索》中華民國 107 年 1 月第 16 卷第 1 期，王高成，〈美國《國家安全戰略報告》的內涵與影響〉／https://www.mjib.gov.tw/FileUploads/eBooks/a100022c2b0b4efa8927d1a98f7f7dc0/Section_file/8567fc32ff2941a3beb9190434cf4076.pdf）

擬答

西元 2021 年 3 月 3 日，距離美國總統拜登 1 月 20 日就職以來，僅僅 1 個月多時間，華盛頓就提出標題為〈重審美國優勢：暫行國家安全戰略指導（Renewing Americans Advantages: Interim National Security Strategic Guidance）〉出台文件。喬·拜登總統親自寫序，表達美國以民主為依歸，重新回歸全球領導地位，為了達到上述目標，拜登提出一個主要戰略核心命題：「美國必須重新強化其持久的優勢，以便從實力地位因應今日的挑戰。我們將會重建會到更好的經濟基礎。重建我們在國際組織的地位，提升我們的價值在國內，捍衛在海外利益，現代化軍事能量，以外交來領導世界，以及活化美國盟幫與夥伴的無可匹敵的網路鏈結關係。」

在前言部份，喬·拜登總統提出以「民主（Democracy）」為主軸的國家安全戰略方針，並在最後提出「美國已經回來（America is back）」、「外交已經回來（Diplomacy is back）」與「盟邦已經回來（Alliances are back）」之「三個回來」用語，相較於前任川普總統西元 2017 年 1 月 20 日就職，當年 12 月提出《國家安全戰略報告》時程，清楚顯示出喬·拜登總統「國家安全戰略一超前部署」之決心，全盤改變前總統的全球與區域安全戰略思考。一方面，呈現喬·拜登國安團隊早已做好準備，按「牌理出牌」，建構穩建的治國形象，另一方面，在 COVID-19 肺炎疫情衝擊內政情勢下，做好「國際宣傳」，一定程度可以轉移大眾視聽，靜待一個全新美國的出現。

在上述「三個回來」的戰略指導架構下，針對主要威脅來源，基本上延續西元 2017 年川普第一份「國家安全戰略報告 (National Security Strategy Report)」所言，在「美國優先 (America First)」主軸下，強調：「美國國家安全戰略願景在於保衛美國民眾及其生活方式，提升經濟繁榮，透過實力保持和平，增強美國在世界的影響力。」並直接點出：「中國與俄羅斯挑戰美國的權力與影響力，並且嘗試腐蝕美國的安全與繁榮。」而且「中國追求取代美國在印太區域地位，擴大其國家補助企業的經濟模式，以及重建有利於北京的去秩序。」

因此，拜登的「暫行國家安全戰略指導」點出中國為美國最關鍵安全威脅，強調：「尤其是中國對外行為更加獨斷性。中國也是唯一一潛在競爭者具有能力能夠整合其經濟、外交、軍事與科技能力來持續挑戰一個問定與開放的國際制度」。在因應「中國一大國崛起」戰略方面，於西元 2021 年 2 月 12 日，喬·拜登首次與中國國家主席習近平電話通話，喬·拜登重申他的首要任務是保護美國人民的安全、繁榮、健康與生活方式，以及維護自由開放的印太地區，對北京強制性與不公平的經濟作為，對香港的鎮壓、在新疆侵犯人權，以及對包括臺灣在內區域的專斷作為，表達出高度的關切。在此戰略指導下，美國國務院國務卿安東尼·約翰·布林肯 (Antony John Blinken) 在西元 2021 年 3 月 3 日，發表美國外交政策，提出三個問題：「What will our foreign policy mean for American workers and their families? What do we need to do around the world to make us stronger here at home? And what do we need to do at home to make us stronger in the world?」並且提出八項主要工作項目，其中為「地緣政治的挑戰」—「我們將應對二十一世紀最重要的地緣政治挑戰：我們與中國的關係。」(And eighth, we will manage the biggest geopolitical test of the 21st century: our relationship with China.) 同時，布林肯確認中國的威脅與挑戰在於「中國所造成的挑戰是不一樣。中國是唯一的國家在經濟、外交、軍事與科技力量方面挑戰一個穩定與開放的國際制度：所有規則、價值，以及我們型塑世界關係走向，反映出美國人民的價值。我們與中國的關係將會是競爭性的，或是可能可以合作性的，或必須是對抗性的，上述三項關係的共通性在於美國要從實力的角度來應對中國。」他點名中國在外交、經濟、軍事、與科技等方面，對於美國的威脅與挑戰。於同年 3 月 10 日下午，喬·拜登視察美國國防部時，宣布針對中國成立一支國防部特別工作小組，利用 4 個月時間，檢討美軍面對北京挑戰的戰略方針，制定就美國對中國的軍事戰略、科技，以及部隊架構和態勢、聯盟及美中雙邊防禦關係，也將與跨部門合作夥伴對話，確保美國拜登政府的中國政策保持一致。

在具體執行方面，喬·拜登的國家安全戰略調整為全政府形式 (或全政府途徑，whole of government approach)，透過多邊主義途徑下，結合盟邦進行全球新合縱行動，例如同年 3 月 12 日舉行「四方安全對話 (QUAD)」之視訊會議，主要討論聚焦於印度—太平洋地區的安全挑戰、一致反對中國片面改變現狀，也討論 COVID-19 肺炎疫情、新興科技、供應鏈、和氣候變遷等重大議題。其中，具體在對抗 COVID-19 肺炎方面，四國決定由美、日出資贊助印度藥廠，生產美國嬌生 (Johnson & Johnson) 和諾瓦瓦克斯 (Novavax) 等藥廠研發的疫苗，由澳洲負責運送，以西元 2022 年前產製 10 億劑為目標，盼藉此解決東南亞地區疫苗缺乏的問題，某種程度也是舒緩第三世界國家疫苗的需求。一定程度也是要抵銷中國透過「一帶一路」沿線國家的「疫苗外交」所帶來的地緣政、經影響力。

事實上，基於中國近幾年在臺海第一島鏈的戰略與戰術作為，例如西元 2021 年 2 月 22 日通過《中華人民共和國海警法》，並於同年 3 月 1 日起正式實施，引發日本強烈反彈，除了正式抗議中國之外，也開始洽商美國進行相關軍事演習加以因應。在臺海方面，近年來，中國解放軍機艦在臺海中線附近，以及臺灣西南海域的灰色地帶騷擾性演習，已經成為國際危機處理組織認為的高風險區域。再加上，中國在南海地區的人工島礁組建軍事化，企圖將南海地區軍事化，未來伺機宣布「南海防空識別區」，更有力於中國掌握南海航道、突破第一島鏈，建構兩洋海洋戰略目標。

相較於美國與盟邦開始建構因應中國改變現狀的戰略布局，於西元 2021 年 3 月 10 日，在中國兩會外交記者會上，中國外長王毅直接提出中美關係三原則，強調「一中原則」是中美關係「不可逾越的紅線」，在臺灣問題上「沒有妥協餘地，沒有退讓空間。」同時，王毅「敦促美國新一屆政府充分認識臺灣問題的高度敏感性，切實恪守一個中國原則和中美三個聯合公報，徹底改變上屆政府越線、玩火的危險做法，慎重和妥善處理涉臺問題。」顯示出，北京也開始觀察美國後續戰略布局，採取「謀定後動」，在確認美國對中戰略意圖與目標之後，必定會採取積極「超前部署、步步為營」。

在上述喬·拜登公布的〈重審美國優勢：暫行國家安全戰略指導（Renewing Americans Advantages: Interim National Security Strategic Guidance）〉文件中，美國總統拜喬·登提及臺灣一次，明確表態「美國支持臺灣是先進民主政體及美國關鍵經濟與安全夥伴，此符合美國長期承諾」。北京方面，在延續將「一個中國原則」與「美中關係」互動基礎聯動之餘，是否會將所謂「臺灣問題」與其他香港、新疆問題區隔，成為美中「共管分歧」議題？涉及到美國戰略上支持一個民主自由的臺灣立場，以及如何落實的問題。因此，臺北方面應該審慎觀察後續美國新全球合縱機制的建立，未來「四方安全對話」會進一步「實體化」，除了研議中的疫苗分配行動，其他傳統與非傳統安全議題，例如稀土供應問題，因應科技競爭問題等等。從四方對多方建制，臺灣是有很多地緣戰略的優勢與利基，端賴如何加以整合各部會能量，建構後疫情時代因應中國戰略挑戰的國家安全戰略方針與作為。

西元 2021 年 3 月 18 日至 19 日，美中兩國在阿拉斯加安克治外交與國安高層對話—「阿拉斯加對話」，美國國務院國務卿安東尼·約翰·布林肯（Antony John Blinken）在開幕式上直接點出：「我們美國政府承諾以外交來領導世局，藉以強化美國的利益，以及以規則為基礎的國際秩序。」（Our administration is committed to leading with diplomacy to advance the interests of the United States and to strengthen the rules-based international order.），同時，布林肯強調：「不是以規則為基礎的國際秩序或許是適當地、讓贏者全拿，但是卻帶來一個更加暴力與不穩定的世界。今天我們有機會來討論美國的優先性問題，包括國內與全國議題，讓中國理解我們的意圖與途徑。我們也會與中國討論我們所關切的課題，包括：新疆、香港與臺灣，對美國的網路攻擊，以及針對我們盟邦的經濟脅迫。這些中國的行動威脅，以規則為基礎的國際秩序的全球穩定。上述議題並非僅僅是內部事務，也是美國在此有義務提出討論。」

在雙邊關係方面，西元 2021 年 4 月 16 日，首度舉辦美日華盛頓高峰會議，拜登強調美國與日本重構新的聯盟關係，以究成為印太與世界和平與安全的基石。並且首度提出：「美日兩國強調台灣海峽和平與穩定的重要性，以及鼓勵和平解決海峽爭議」的用語。

西元 2021 年 5 月 21 日，美韓舉行元首高峰會議，雙方確認「一個共享的經由民主規範、人權與法治的國內與國際願景。我們尋求一個夥伴關係藉以持續提供和平與繁榮，並成為區域與全球穩定基石。」同時，「美國總統拜登與南韓文在寅大總統強調確保台灣海峽和平與穩定的重要性。」

西元 2021 年 6 月 13 日，在英國舉行「七國工業國家會議（G7）」高峰會議，強調因應 COVID-19 肺炎疫情的決心，並且重建更好過去的理念，並在多邊以規則為基礎的國際體系強化此一機制的能量。會後發表聯合公報，其中在第 60 項中提到：「我們再度強調維繫一個基於法制基礎的自由與開放的印太區域的重要性。我們強調台灣海峽和平與穩定的重要性，同時鼓勵和平解決海峽爭議。我們嚴肅的關切東海與南海的情勢，並且強力反對任何單方面改變現狀與增加緊張情勢。」

西元 2021 年 6 月 14 日，美國與北約組織舉行高峰會議之後發劬聯合公報，強調「北約（NATO）」依舊是盟國之間的集體防衛與安全諮商與決策的重要平台。北約是一個防衛性聯盟，將會持續致力於全歐洲大西洋區域的和平、安全與穩定。我們承諾以規則為基礎的國際秩序。中國持續增加的影響力與其國際戰略形成對於北約組織的挑戰，我們必須以整體聯盟角色加以因應。面對中國，我們將以整體防衛北約安全利益的觀點因應。在後會聯合公報中，第 55 項目中提到：「中國展現其企圖心與專斷式行為，挑戰以規則為基礎的國際秩序，以及與聯盟有關的區域安全。」主要在於中國持續擴張其核武庫配備更多彈頭與精密投射系統，以建構核武三角能量。解放軍持續現代化腳步，及其軍民融合戰略。並且與俄羅斯軍事合作，包括參與俄羅斯在歐洲大西洋區域的軍事演習。是以，北約組織依舊關切中國缺乏透明度與運用假訊息，希望中國遵守其國際承諾，並且在國際體系上以主要大國身份負責任的行事，包括：太空、網路與海洋領域等。

西元 2021 年 6 月 15 日，美國也與歐盟舉行元首高峰會議，會後發表共同公報表達：「我們美國與歐洲聯盟國家領袖重建跨大西洋夥伴關係，建構一個後疫情時代的共同跨大西洋議程。」並且我們承諾以聯合國為核心，堅守以規則為基礎的國際秩序，強化與改革我們所需的多邊機制，以及與其他共享此種目標的國家合作。

此外，繼西元 2021 年 3 月 18 日至 19 日，美中兩國外交與國安高層的「阿拉斯加對話」之後，直到同年 7 月 25 日至 26 日，美中兩國副部長層級在天津再度會晤。美國副國務卿雪蔓（Wendy Sherman）推文表示，她和中國外交部副部長謝鋒討論重要問題，包括氣候危機、COVID-19，以及美國對中國在香港、新疆和台灣海峽作為的嚴重關切，並強調「美國和盟友、夥伴永遠支持我們的價值觀」。反之，謝鋒隨即表示，「中美關係」陷入僵局原因，是因為美國某些人將中國當成「假想敵」，中國也在會中向美國提交 2 份清單，要求美國不要再干涉中國「內政」。

綜之，美國透過多種層次進行國際戰略與國交往，除了一再確認以規則為基礎的國際秩序之外，增取國際間理念相近國家雙邊與多邊途徑的支持。除了傳統美國的跨大西洋盟國關係的爭取之外，也透過爭取非傳統的親近國家，例如國務卿布林肯（Antony Blinken）於7月26日至29日對印度首都新德里和科威特城進行訪問，同時，7月23日，國防部長奧斯汀（Lloyd Austin）出發對新加坡、河內及馬尼拉進行訪問，也是首位到訪東南亞國家的拜登政府閣員。事實上，奧斯汀會向地區領導人表明美國對中國在南中國海行為的看法，並向地區盟友和夥伴們重申美國繼續是一個可靠的夥伴、一個關鍵時候會出現的朋友。

同時，美國透過建構自由與開放的印太區域理念，一方面，型塑「台海地區的和平與穩定的重要性」，同時也強調「鼓勵和平解決海峽爭議」。上述理念出現在美國對外的雙邊與多邊機制的正式議程上，已經被行成為一個國際和平與穩定的共識。是以，台灣在持續強化以理念相近為基礎的「美台關係」深化與廣化之餘，如何進一步扮演促進「和平解決海峽爭議」角色與功能，應該是台灣在面臨美中戰略競逐下的戰略思考之道。

書 名	作 者 / 出 版
《情報與國家安全之研究》	張中勇著 民國82年，三鋒
《新安全威脅下之國家情報工作研究》	汪毓璋著 財團法人兩岸交流遠景基金會
《美國情報組織揭密》	高慶德等著 民國99年，時事
〈析論我國情報通訊監察法制 —以美國法制為比較〉 《軍法專刊》	李榮耕著 民國99年，國防部
《情報學之間諜研究》	蕭銘慶著 民國103年，五南
《情報學破題奧義》	李如霞 民國111年，新士明
〈美國網路安全防護經驗對我國網路安全情勢之啟示〉 《國防雜誌》	陳育正著 民國104年，國防部
〈積極面對「非傳統安全威脅」〉 《海軍學術雙月刊》	毛正氣、崔怡楓、程國峰合著 民國102年，國防部
〈非傳統安全與台灣軍事戰略的變革〉 《台灣國際研究季刊》	王崑義著 民國99年，台灣國際研究學會
〈公開來源情報在軍事上的價值 、趨勢與運作策略〉 《陸軍學術雙月刊》	王官德、洪志安編著 民國101年，國防部
《恐怖主義威脅及反恐政策與作為（上）》	汪毓璋著 民國105年，元照
《情報：從秘密到政策》	馬克·洛文塔爾著 民國104年，金城
《國土安全導論》	陳明傳、駱平沂著 民國99年，五南
〈情報分析與決策過程問題之研究 —一個社會心理學之觀察〉 《警政學報》	張中勇著 中央警察大學
《情報學之間諜研究》	蕭銘慶著 民國103年，五南
《美國國家安全暨情報機制》	姚祖德著 民國101年，時英
〈美國設置國家情報總監對情報組織管理 與工作執行的啟示〉 《警學叢刊》	蕭銘慶著 民國101年，中央警察大學

情報學 專業題庫集

名譽編輯 ◆ 李如霞老師

執行編輯 ◆ 趙國華、歐思怡、邱筠婷

封面設計 ◆ 迪生設計公司

發行 ◆ 新士明文化有限公司

門市地址 ◆ 402-51 台中市南區永和街 287 號

網路商城 ◆ www.MOEX.com.tw

購書專線 ◆ 090-557-6667

LINE ID ◆ 0905576667

ATM轉帳 ◆ (013) 236-50-6089895 (國泰世華)

ATM轉帳 ◆ (013) 235-03-5016578 (國泰世華)

ATM轉帳 ◆ (013) 23503501657-8

讀者信箱 ◆ will0107moex@gmail.com

登記字號 ◆ 局版業字第0231號

出版日期 ◆ 中華民國111年02月25日出版 二版一刷 / PD060-D-1

定價900元

法律顧問 ◆ 嘉誠國際法律事務所

本書如有缺頁、倒裝或其他裝訂不良等情形，請電洽公司，將有專人為您服務

版權所有 · 翻 (盜) 印 必 究