入區域全面經濟夥伴協定（RCEP），則必須台灣與中國大陸要有可溝通的政治關係，目前看來並不樂觀。在菲律賓、越南積極改善與中國大陸的關係，台灣在執行新南向政策時，至少有需要與大陸維持一個可溝通的政治氛圍。因此，如何突破大陸這一關加入區域經濟夥伴協定或簽定雙邊自由貿易協定，也是政府需要努力的方向。

六、要促進經濟成長，讓台灣變成老虎，基本條件還是加大在台灣的投資；台灣的投資增加，才能擴展新南向政策的效果，進而厚植台灣的經濟實力；否則仍然是過去台灣接單、海外生產的翻版，並無法落實產業升級的目標。川普上台後，預計美國政府將擴大投入基礎建設，並大幅減稅吸引資金投資美國。我們建議政府也應採行大幅度的寬鬆財政政策，落實執行政府、公營事業的有效投資，加大在台灣投資和研發的租稅優惠，而且是面向所有產業，全面推動創新升級。

七、為帶動我國產業轉型，創造就業機會，國發基金於今年 7 月匡列 1,000 億元設立「產業創新轉型基金」，將結合民間資金共同參與企業進行合併、收購、分割或其他有助於企業創新轉型投資計畫所辦理之募資，期有效引導民間資金共同參與產業結構調整，促進企業轉型升級。我們希望國發會能夠提高產業創新轉型基金的管理成效，抓住產業轉型的關鍵時刻。

（二十四）本院許委員淑華，鑒於媒體報導，日本防衛省及陸上自衛隊的資訊系統，今年 9 月疑似遭駭客侵入。面對現今資訊時代，「國家級」大規模駭客集體攻擊的格局，已經不是最大規模的資安威脅；基於人工智慧技術發展的攻擊技術，才是真正難以應付的危機。因此，要求行政院應援引最新的人工智慧科技，並發展防範資安威脅的人工智慧機制。爰此，特向行政院提出質詢。

說明：

一、媒體報導，日本防衛省及陸上自衛隊的資訊系統，今年 9 月疑似遭駭客侵入。日本當局雖否認情資遭竊，但專家認為駭客手法高明；且由於防衛學術單位的「開放系統」遭駭，只要透過可在「開放系統」與「封閉系統」間切換的電腦，即能進一步入侵連接「封閉系統」的其他防衛省和自衛隊資訊設施，以及駐地與基地的網路，情資恐有外洩之虞。

二、解讀這段訊息，可從目前常見駭客攻擊著手。一般而言，攻擊前階段，駭客會先鎖定目標作業系統尋找漏洞；其後即正式發動攻擊。透過「足跡蒐集」（Footprinting）、「列舉」或「掃描」工具，針對鎖定的區域或系統作全面偵查、分析，找到弱點或漏洞，設計攻擊方案，發動攻擊。

三、其間關鍵是，除非做到網路實體隔離，若單憑切換機制區分內外網絡管制，百密總有一疏

；倘若管制機制存有未被發現的漏洞或弱點，駭客只要以自動化工具「踩點」或掃描，要找到一個網路系統的入侵路徑，並非難事。

四、以惡意程式入侵被鎖定的弱點來說，方式大略有兩類。一是透過人為的系統操作，將惡意程式帶入系統。例如，當我們被誘騙打開不明郵件的夾檔，或開啟惡意郵件時，便會啟動內嵌的檔案，無意間促成惡意程式入侵；又如，瀏覽惡意網站時，被誘騙啟動夾帶惡意程式的超連結圖樣或按鈕，也可能透過瀏覽器，將惡意程式帶入作業系統。另外一類，則是以網頁或網路服務系統為攻擊對象，藉由網頁或服務系統中的程式互動，將惡意程式寫入系統；或竊取暫存於瀏覽器上的個人隱私資訊或系統資訊。後者透過健全的系統資安策略，即可進行防堵；唯人為無意間的惡意程式散布，則是資安控管中最具風險者。

五、各式各樣的「蠕蟲」攻擊，並不需要人為主動的特定動作來協助傳播，而是由蠕蟲程式，透過作業系統的安全漏洞，以類似癌細胞增生擴散方式，經由電子郵件與內部網路（LAN），鎖定未被蠕蟲感染的網路節點擴散，並感染整個互聯網路中的作業系統。2003 年 8 月間大爆發的「衝擊波蠕蟲」感染，便是利用微軟系統的安全漏洞，透過電子郵件與區域網路，於微軟 Windows 2000 與 Windows XP 系統之間增生擴散，難以收拾。

六、一般而言，惡意程式侵入，經由跳板擴散到被鎖定的網路區域後，其程式將直接竊取資訊、監控系統、操控系統，抑或是將大量的系統串聯形成「殭屍網路」，進行「阻斷服務攻擊」（DDoS，distributed denial-of-service），令被操控的所有作業系統同時針對一個網頁或網路服務，進行大量的瀏覽，導致該網頁或網路服務有限頻寬被占盡而癱瘓。

七、在資安要求特別高的軍事場域，完全的硬體分離最為有效。但，為了更徹底防堵駭客大規模攻擊，將網路資訊安全納入國防自主項目，確有其必要。具體的做法，包括發展加密的網路基礎建設，並制定獨立的通訊協定，避免使用開放通訊協定。最理想者，是發展自有的作業系統與資訊規格，這些目前在歐盟、日本與中國大陸，都是備受重視的國防發展目標。

八、隨著駭客技術日新月異，加上大數據應用與機械學習等人工智慧（AI）技術的發展，駭客攻擊手法也愈來愈難防範。然應用人工智慧技術，抵抗駭客攻擊的科技也已開始發展。一組由美國麻省理工學院電腦科學與人工智慧研究室（MIT CSAIL）偕民間機構專家組成的研究團隊，今年 4 月即公開發表一項運用機械學習抵抗駭客攻擊的人工智慧系統，有效預判駭客可能攻擊方式，並進行防禦的成功率已達 85%。

（二十五）本院許委員淑華，鑒於政府上月起擴大長照網的照顧對象，但台灣長照仍未能擺脫「缺錢、缺人」的苦情，隨著長照 2.0 上路，照顧服務員的人力缺口更上升至一・三萬人。長照 2.0 上路，要求行政院應視為照服員走出廉價粗工困境的契機，全盤體檢照服員的培訓、勞動條件、職涯前景，讓長照工作