未來軍用物聯網發展與應用介紹
(Introduction to the future development and application of military IoT)

譯者／趙本善先生

提要

一、物聯網(Internet of Things, IoT)主要透過感測技術、網際網路與智能分析服務的整合與應用，使不同的物件間達到互聯的智慧應用，可以廣泛的應用在機械、建築、車輛、國防、資通、物流與醫療等不同領域。

二、物聯網目前已逐漸應用在民間企業，許多國外國防單位也逐漸重視軍用物聯網的發展與建構，以提高軍事效益，降低人員的傷亡。然而，物聯網未來要應用在國防科技領域，仍然面臨許多的困難與挑戰。

三、本文主要依據最新國外物聯網相關的文獻與報導，說明物聯網發展趨勢與使用情境。尤其，本文將特別介紹物聯網未來在國防科技領域應用的潛力，同時說明軍用物聯網所遭遇的困難與挑戰，以提國軍未來在建構與發展軍用物聯網的參考與借鏡。

關鍵詞：物聯網、感測技術、雲端系統、大數據分析。

前言

物聯網最簡單的觀念就是要實現日常生活的物體(Physical Objects)或裝置(Devices)與網路進行連結，有人又將物體與裝置統稱為物件(Things)。然而，物聯網的真正目的，並非只著重在物件與網路的連接，其最終的目的是希望達成物件能夠具有智慧辨識(Intelligent Self-identification)，或者相互連接(Communication)的功能。為了達成智慧辨識與物件相互連結的功能，這些物件必須嵌入(Embedding)或配備許多電子元件(Electronics)、軟體(Software)、感測器(Sensor)與網路連接裝置(Network Connectivity)等，透過上述配備與裝置的運作，讓物件可以進行資料收集與交換。尤其，透過網路系統，更可以達成遠端控制，讓真實世界物件與電腦內部的系統可以連結，達成快速、有效與正確的指令與動作下達[1]。事實上，物聯網系統的興起並非是偶然，主要歸功於近年來感測器與處理器朝向短、小、輕、薄與多功能的發展趨勢與需求、智慧型手機裝置的蓬勃發展、雲端運算系統(Cloud Computing)的進步，以及大數據(Big Data)分析的使用，都是推動物聯網興起的背

[1] https://en.wikipedia.org/wiki/Internet_of_Things, 2015/11/20.

後重要推手[2]。其中，雲端運算系統意旨利用電腦運算能力，提供作為商業服務的一種工具，個人與企業都可以透過網路連結進入，大幅增加事件處理的速度；大數據分析則是指資料量規模巨大到無法透過人工處理，在短暫的時間內，透過擷取、管理與處理，並整理成為人類所能解讀形式的資訊。

物聯網可以應用的領域非常廣泛，包括:居家安全、個人娛樂、健康管理、交通運輸、貨物補給、停車服務、道路救援、工廠管理、貨物銷售、智慧量錶、情報收集與國防科技等。[3]除了上述的應用領域之外，目前物聯網也可用在通訊、智慧家庭、智慧電網、醫學、自動化建築與汽車等領域，透過網路物件的連結，可提高管理效率與安全性，如圖一。

圖一 物聯網於各領域應用示意圖

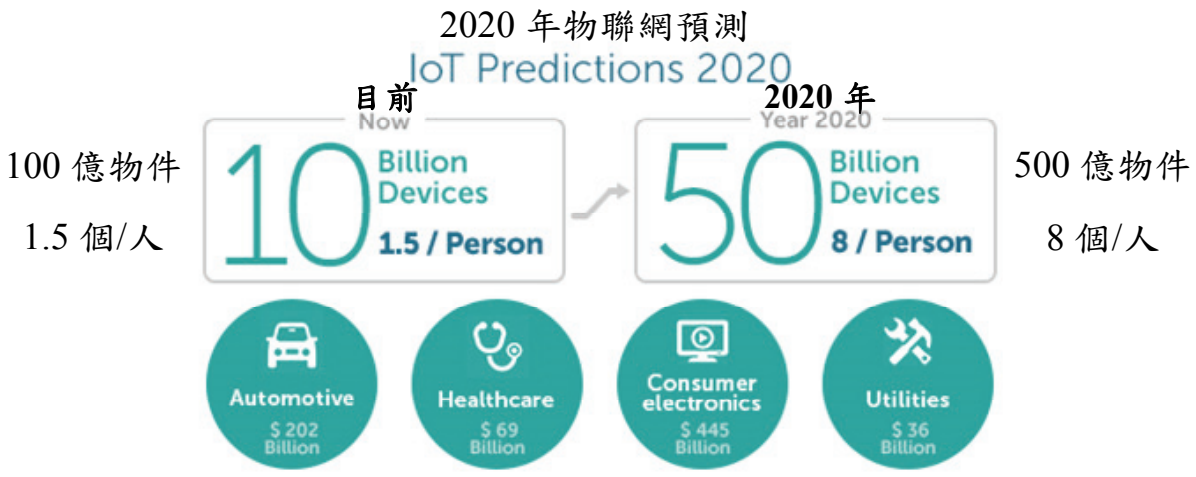
資料來源：http://www.w3.org/WoT/, 2015/11/20.

根據國際知名研究暨顧問機構 Gartner 預測，2016 年由物聯網所帶動的服務支出金額將達 2,350 億美元，較 2015 年增加 22%，成長力道相當驚人。針對物聯網於民間企業應用部分，該機構將物聯網的使用區分成兩大類：第一類屬於一般屬性(Generic)或用於多種跨產業(Cross-industry)的裝置。例如，為節省成本而裝設

[2] http://www.trentonsystems.com/applications/machine-to-machine/, 2015/11/20.
[3] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswamia, "Internet of Things (IoT): A vision, architectural elements, and future directions," http://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf, 2015/11/20.

的聯網燈泡、暖氣、通風與空調系統；第二類則屬於特定產業會使用垂直裝置(Vertical-specific Devices)。例如：醫院手術房專用設備與貨櫃與飛機的追蹤裝置等。未來物聯網的真正價值會在物聯網提供的服務，所有的焦點將聚集在終端用戶，以及廠商所提供的新型服務。[4]例如，最近有國內的壽險公司，在販售的保單內結合健康管理與物聯網概念，當客戶購買保單之後，可以獲得個人健康監控的手環，透過和健康管理機構的合作，以及利用資料收集與雲端管理系統，可以將客戶與健康管理連結，達成物聯網的運用，不但可以提高顧客的服務，也衍生出許多銀髮商機，更有機會因為這樣的管理，降低成本與提高客戶滿意度與投保意願。目前全球使用物聯網的物件據估計約有 100 億件，至 2020 年可成長至 500 億個物件。尤其，在消費性電子產品與汽車產業的成長力道最為強勁，分別可達 4,450 億美元與 2,020 億美元，如圖二。

圖二 未來物聯網的發展預測



資料來源：http://blog.claricetechnologies.com/wp-content/uploads/2014/03/clarice_Iol_predictions_20201.jpg, 2015/11/20.

軍用物聯網的興起與概念

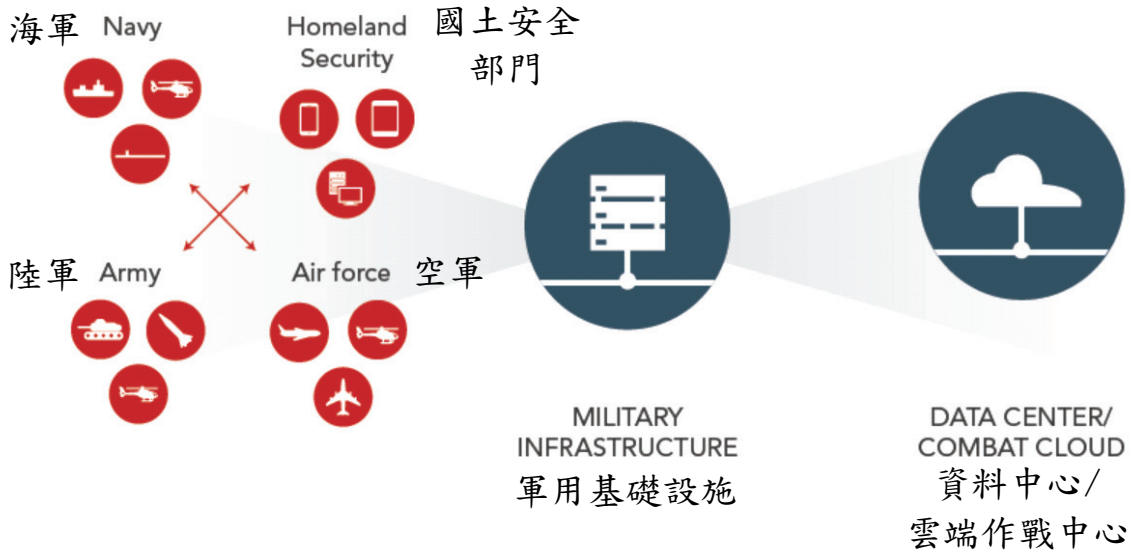
當 1996 年網路資訊時代的來臨時，美軍深刻的瞭解網路將會是未來戰場重要的決勝利器，故於當年提出網路技術發展優先(Internet Superiority)的政策，意即將全力的發展網路資訊技術，並將該技術與武器系統進行結合。[5]當時美軍希望透過網路基礎設施的建置，形成所謂的決策圈(Decision Cycle)，並將其應用在情報收

[4] http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081, 2015/11/20.

[5] Joe Mariani, Brian Williams and Brett Loubert, "Continuing the march: The past, present, and future of the IoT in the military," http://dupress.com/articles/internet-of-things-iot-in-military-defense-industry/, 2015/11/20.

集與後勤補給等行動，以利軍事指揮系統的決策者，可以快速與正確的指令下達，提高軍事行動的效率，後續又將網路技術的發展擴大至通訊方式、網路配線與資料處理等領域，以實現網路技術的全面運用。美軍目前規劃以現行的軍用網路基礎設施為中心，一方面可以透過陸海空軍與國土安全部門所收集的資料，透過網路連結的方式，將資料傳送至軍方資料中心或雲端作戰中心進行分析與儲存，後續可再利用資料分析的結果，進行相關的軍事行動，這就是物聯網的基本概念與做法。陸海空軍與國土安全部門可視為被連結的物件，進行資料與情報的收集，透過網路的連結，可將收集的資料與情報進行儲存與分析，達成終端使用者(美國國防部)可以參照這些資料與情報，進行後續的動作與指令，完全透過網路連結的方式，與過去單一與片段的資料與情報收集後，再進行彙整與分析的做法不同，如圖三。

圖三 美軍軍用物聯網使用情境示意圖



資料來源：http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf, 2015/11/20.

許多人會將軍用穿戴式裝置(Wearable Device)與軍用物聯網畫上等號，雖然兩者間有些類似之處，但嚴格來說，穿戴式裝置與物聯網屬於不同的技術。[6]以美軍而言，目前許多軍用穿戴式裝置可以利用感測器與軍用頭盔或軍服進行結合，藉此量測與監控士兵的生理狀況。另外，許多穿戴式電腦可配戴在士兵的身上，藉此可以遠端操控無人系統，以上的做法都僅是單純的監控與操作。相較之下，物聯網系統主要還是要透過整個網路系統，連結人或物件，透過感測裝置收集資

[6] http://www.afcea.org/content/?q=defense-department-awakens-internet-things, 2015/11/20.

料，但是收集的資料需要經過分析與傳送，再傳遞給人或物件，進行後續有效的動作。簡言之，穿戴式裝置的功能比物聯網系統狹隘，透過穿戴式裝置收集的資料，並沒有進行智能分析，也無法與更多的人員或物件進行網路連結，較無法達成更有效率的管理與追蹤等目的。

軍用物聯網的應用與使用情境

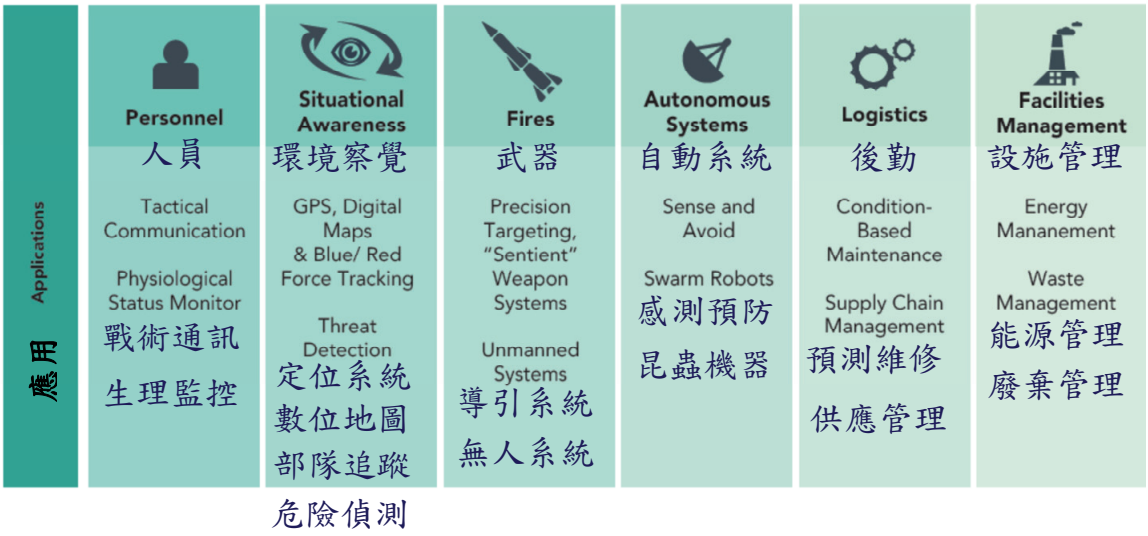
根據美國國防部的研討與規劃，未來物聯網系統將有機會應用在飛機、地面車輛、船艦、太空飛行器與其它各式武器系統。無論這些武器系統是大或小，或是由人或無人操控，都可以進行物聯網系統的連結。[7]然而，後續要將物聯網應用在國防科技領域，仍有許多困難與挑戰需要解決，包括：系統安全性(Security)與隱私權(Privacy)的問題，大數據儲存與分析技術，以及建構智慧與可程式(Programmable)的網路資訊系統，都是目前美國國防部關心的重要物聯網研發議題。[8]

未來物聯網系統在軍事應用方面，美軍就實際考量未來物聯網在戰場上的實際使用情境，以及對於戰爭型態的影響。試想若一位軍事指揮官將要帶領地面部隊進入危險的地面戰場，執行長時間的軍事行動，過去總是認為行動成敗的關鍵，可能取決於指揮官對於戰場實際狀況的瞭解與臨場應變。然而，部隊裝備的完備性、安全性與機動性，才是未來戰場的決勝關鍵。利用物聯網系統，各式軍用卡車與悍馬車可以裝載各式車用感測器，透過感測器的偵測，可以清楚的瞭解每台軍事車輛的油料容量、輪胎壓力，甚至是引擎的壽命，透過智慧型手機的軟體連結，可以顯示各車輛的狀況，提早警示何時需要補充油料，或是哪一台車輛的輪胎壓力異常，需要進行維修與更換。更先進的是，透過電腦的連結，還可以知道上述車輛的油料更換與輪胎檢修，是由哪位技工負責，當發現任何狀況時，透過物件收集的資訊與需求，傳遞給負責人員，即可迅速的完成所需的工作，減少在戰場上，因為機件與車輛疏於保養與維修造成士兵傷亡風險。[9]此外，許多生物型感測器，也可以穿戴在戰士的軍服上，可以即時的偵測(Real-time Measurement)與反應每一位戰士的生理狀況，舉凡如體溫、心跳、血壓與腎上腺素的反應等，並且可以警示有狀況的戰士與位置，當醫護人員收到上述的警訊時，可以立即前往照護。藉由提早的照護，可將傷亡降至最低，如此可以大幅提高戰場的戰鬥效率與成功機率。如前所述，這些穿戴式的裝置，必須要能與網路連結，而非只有

[7] http://eecatalog.com/military/2014/05/09/the-military-internet-of-things/, 2015/11/20.
[8] http://www.defenseinternetofthings.com/wp-content/uploads/2014/09/MIOT_C_fl14.pdf, 2015/11/20.
[9] https://www.boozallen.com/content/dam/boozallen/documents/2014/12/Internet_of_Things.pdf, 2015/11/20.

單純的進行每位士兵的生理監控，再由士兵透過配戴的行動裝置，如智慧型手機的軟體進行個人的即時監控，這種僅是屬於穿戴式裝置的技術，而非物聯網技術，物聯網必須讓所有收集的數據，進行網路收集與儲存，最後還要進行分析與動作。因此，包含的範疇比穿戴式裝置與技術廣泛，功能也比穿戴式裝置強大。在國防科技使用情境中，未來軍用物聯網可能可以應用在人員、環境察覺、武器、自動系統、後勤與設施管理等。在人員應用方面，包含戰術通訊與生理監控；在環境察覺應用方面，包含定位系統、數位地圖、部隊追蹤與危險偵測；在武器系統應用方面，包含導引系統與無人系統；在自動化系統應用方面，包含感測預防與各式機器人的自動化應用；在後勤補給應用方面，包含預測維修與供應管理；在設施管理應用方面，包含能源管理與廢棄物管理系統，如圖四。

圖四 未來軍用物聯網的應用領域



資料來源：Denise E. Zheng and William A. Carter, "Leveraging the internet of things for a more efficient and effective military," http://csis.org/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf, 2015/11/20.

發展軍用物聯網遭遇困難與挑戰

美國戰略與國際研究中心(Center for Strategic & International Studies, CSIS)研究人員表示，未來在軍用物聯網系統發展過程中，美國國防部所遭遇的困難與挑戰還是非常大，茲簡述如下:[10]

一、許多資料仍需要藉由人工輸入

許多國防軍事資料仍然需要倚賴人工進行輸入，尤其是後勤補給的工作任務。雖然目前美軍使用無線射頻辨識技術(Radio Frequency Identification, RFID)，

[10] Denise E. Zheng and William A. Carter, "Leveraging the internet of things for a more efficient and effective military," http://csis.org/files/publication/150915_ Zheng_LeveragingInternet_WEB.pdf, 2015/11/20.

加快補給的效率與速度。然而，若遇到系統故障，或是在其它沒有配備該辨識系統的倉儲，許多的工作就必須仰賴人工，這也意味需要進行人工資料輸入，也勢必會產生人為的錯誤。事實上，物聯網系統也將面臨相同的狀況，若許多資料無法自行感測與輸入，透過人工輸入的方式，即便系統可以連結物件或人員，也可能因為人為輸入的錯誤，進而衍生錯誤的動作與指令的風險。

二、現行資料處理的限制

使用物聯網系統，最大的問題就是會利用嵌入式的感測器收集許多的資料、資訊或數據。然而，目前許多收集的資料都是未經處理，無法與物聯網系統連結。即便是有些資料可由藉由人工進行分析與處理，勢必也需要花費許多的時間，故無法透過物聯網，達成即時的反應與動作。簡言之，未經分析的資料或是需要時間分析，無法即時提供資料的數據，未來都無法使用物聯網系統。

三、武器系統缺乏自動化操作

自動化是物聯網非常重要的關鍵，目前許多美軍的武器系統，仍然無法達成全面的自動化操作。例如：許多部署的無人系統(Unmanned Systems)，雖然號稱「無人」，然而都需要藉由遠端遙控系統，進行人員操作，若未來能將武器系統完全自動化，不但可以減少人為操作的失誤，也能增加與物聯網系統的相容性，藉此提高使用效率。

四、現行網路通訊設備系統的不完整性

目前美軍使用的許多網路設備，都由不同承包單位建置而成，缺乏一套完善與連續的網路通訊設備系統。不同的網路通訊設備系統，可能需要使用不同的輸入介面，缺乏硬體系統設備的相容性。

五、網路資訊安全的疑慮

未來的軍用物聯網可以獲取與傳送部署、撤離與移動的軍隊之資訊，資訊的交換非常的頻繁與廣泛。因此，如何做好資訊安全的工作，更顯得非常重要。資訊安全的工作，包括網路安全與人員管制。許多網路安全的漏洞，會讓敵人的網路軍隊趁機而入，侵入電腦系統，竊取資訊與情報。此外，許多的機密資料，也有可能因為人為的洩密，造成嚴重的資安問題。

六、內部人為的威脅與資安漏洞

目前隸屬於美國國防部的人員，包括文職、軍職、後備軍人，以及其它相關國安人員，高達三百萬人以上，對如此龐大的組織而言，要確實管制資安，確實非常的困難。雖然透過不斷的資安訓練與教育，可以達到某種的成效。然而，只要有少數的不法分子，或一些無心的錯誤，都可能造成嚴重的資安問題，確實不得不謹慎面對。

七、系統容易遭受電子戰的破壞

大部分的物聯網系統，都會透過無線傳輸技術進行資料的傳送，這些資料 也可能會被敵人攔截，進而暴露軍隊的行蹤，或是直接進行阻礙，造成資料無法傳送。因此，如何強化資料傳輸的安全性，是未來軍用物聯網的關鍵。

八、現行技術的限制與不足

目前美軍強調仍然需要加強連結性(Connectivity)、數位訊號分析(Digital Analytics)與軟體通用性(Interoperability)等三方面技術，以利未來物聯網的應用。在連結性技術方面，還是希望可以健全網路通訊設備的基礎設施，提高網路傳輸的安全性；在數位訊號分析方面，由於物聯網都需要接收感測單元的訊號，並進行即時的分析，必須要強化數位訊號分析的技術，才能因應龐大的訊號分析的需求；在軟體通用性方面，必須要確保所有的軟體系統都能夠相容，尤其現在許多軟體還需要搭配硬體設備，希望可以建立硬體的標準化規範，提高軟硬體的相容性。

九、先期研發投資金額過高

目前美軍在發展軍用物聯網，遭遇的最大困難還是經費的問題。對於任何的研究計畫而言，都需要研究經費支持，才能順利的進行。然而，對於開發軍用物聯網系統而言，所需的經費非常的龐大，因此美國國防部，是否願意在現階段投資大量的經費，研發「未來」才可能用得到的技術，仍然是一個很大的變數。

十、民間產業發展與國防武器研發的衝突

軍用物聯網的發展，勢必要與民間廠商進行共同合作開發，才有成功的機會。然而，目前美國的民間企業與國防產業間，仍充滿了許多的歧見。例如，受限於許多法規與國防機密保護法，許多民間企業對於投資或與軍方合作，抱持裹足不前的態度，且許多文化與思想的差異，都造成民間企業與國防產業合作成果不彰。就物聯網系統而言，目前在民間企業比較容易實施，勢必將從民間轉移至國防，這中間如何去克服雙方之間的差異與限制，也是決定未來美軍是否能成功運用軍用聯網的關鍵契機之一。

十一、智慧財產權與技術輸出控制

智慧財產權也是投資者或民間企業，是否願意積極參與軍用物聯網的研發與建置的重要關鍵因素之一。就民間研發物聯網企業而言，最高的宗旨就是希望能夠進行商業獲利，若將開發的物聯網技術轉移或銷售給其它的民間企業，則可以獲得較高的技轉費用與銷售費用。相較之下，若將相同的技術轉移給國防軍事單位，則獲得的利益則非常有限。另外，技術的輸出許可，也是造成美國民間企業不願與美國國防部合作的原因之一。美軍使用的任何軍事技術，都將會被美國國

防部歸類為軍用技術(Military Technology)或軍民通用技術(Dual-use Technology)，這些技術若要輸出至海外，必須要獲得輸出許可證明。就民間研發物聯網的企業而言，受限於國防科技與設備輸出管制(Export Control)，將會嚴重影響公司商業利益，也將會嚴重影響民間企業，投入軍用物聯網的技術研發與技術轉移給美軍單位使用的意願。

未來我國軍用物聯網發展策略與建議

綜上所述，國外物聯網的發展與應用，已經具有相當的雛形與落實。尤其，民間企業物聯網的技術，目前已逐漸落實在許多產業與各層面的應用，極具產業的應用優勢。相較之下，軍用物聯網雖然對於未來建軍備戰也具有相當關鍵的影響因素，但受限於許多條件，故仍然屬於發展初期。筆者特別提出以下的幾點建議，以供國軍未來發展軍用物聯網技術參考，茲敘述如下：

一、軟體優於硬體

本文前面曾經提及穿戴式裝置與物聯網具有相同與相異之處。相同之處就是都需要使用感測裝置；相異之處就是穿戴式裝置僅是單純監控與操作，而物聯網是要將監控獲取的資料進行分析，再透過網路系統，再傳遞給人或物件，進行後續的指令與動作。故未來在發展物聯網的技術過程中，可以參考穿戴式裝置的發展過程。一般而言，穿戴式裝置可以簡單的區分成軟體、硬體與服務等三個部分。以筆者過去多年輔導產業界的經驗而言，國內有許多廠商因具有手機製造的經驗，故而跨足進入技術層次較低的穿戴式裝置市場，然而因為一味的著重穿戴式硬體裝置，意即感測器與感測單元開發，也喪失市場的競爭優勢，甚至遭到市場的淘汰。由於硬體裝置開發門檻與技術層次較低，容易被許多感測器大廠或製造商取代，且國外對於硬體裝置布局已經非常完整，非常容易陷入智慧財產的泥淖之中。有鑒於此，未來國軍在開發物聯網系統過程中，仍應考慮優先發展資料傳送系統、資料分析技術與網路連結技術，或相關的軟體與系統介面等，而非僅著重於硬體感測系統的開發。

二、加強資訊安全

就國防單位而言，資訊安全永遠都被列為部隊最重要，不可觸犯的「天條」之一。就物聯網系統而言，必須使用大量的資料收集、傳輸與分析等動作。因此，如何在進行上述的網路連結動作，又可以確保電腦系統不會被入侵，造成資料外洩的情形發生，是一項非常困難的挑戰。因此，國軍在發展物聯網系統時，應該設法強化網路的安全性，同時對於防止人員洩密也應該進行相同的嚴格管制，透過定期的教育訓練、資安檢查或是強化資安意識都可以達到某種程度與效果。雖

然要完全杜絕洩密的情事發生非常的困難，然而利用上述的做法，還是可以將洩密的事件降至最低，減少因人員洩密或是網路安全漏洞所造成的損失。

三、後勤管理優先

每個國家因為國情不同，也會影響軍用物聯網系統的使用。目前軍用物聯網多使用在武器系統與後勤補給與管理等。就使用在武器系統而言，由於牽涉的技術較高，所需要投資的金額也高。以我國而言，由於我國國防科技研究單位，都以發展防禦性武器為主，初期的研發重心，可以擺放在後勤補給與設施管理等。就研發的觀念而言，通常都是採循序漸進方式，分階段進行，先以較容易達成的為優先目標，不但可以減少初期的投資成本，在獲得相關的成果後，也較容易去發展其它需要高成本的技術。

四、標準感測介面

「感測」是物聯網的起始重要過程，必須透過感測才能收集資料，進行後續的分析。但目前的感測裝置種類非常多，每個感測裝置也經常使用不同的介面系統，造成許多系統不相容的情況發生。在軍事應用上，由於必須使用許多的感測裝置，尤其軍用的感測裝置的規格與功能，都會依照軍規的規範，也會較一般民間企業所使用的感測裝置精密與堅固。即便如此，如何統一所有感測介面是一項非常重要的課題。因此，對於未來所有軍規的感測裝置，必須要考慮其使用的介面，而國軍未來在籌建物聯網系統的過程中，必須要注意所有感測器的介面、軟體與硬體受否能夠完全相容，若是委託一般民間企業進行物聯網系統的建置，也必須在研發過程，提出相關的需求，以利未來系統的運行順利。

五、建立彈性規範

目前國內許多國防科技研究單位，無論在進行武器系統的自主研發、委外研究或裝備採購，其相關的規定都相當的嚴格，因此也限制許多優良的民間企業及學術研究單的共同研究合作或委託研究合作。舉例而言，目前與國防科技研究單位的研發成果或是委託研究的成果，通常都歸屬於國防科技研究單位所有，而非屬於合作的民間企業或學術研究單位。因此，經常衍生許多的研發成果歸屬權糾紛，造成民間企業與學術研究單位，多不願意與國防科技研究單位進行合作，以確保其研發成果歸屬於民間企業與學術研究單位本身。以物聯網系統而言，由於牽涉的技術與系統非常廣泛與龐大，未來國軍在研發的過程中必須要與民間企業或學術研究單位進行合作，才能縮短研發的時間與減少研發成本。若是依照現行的規定做法，將不利於民間企業、學術研究單位與國防研究單位的合作，因此有賴國內各國防科技研發單位，能夠從新檢討相關的規範，建議依照不同的研發技術與專案，制定不同的規範，或制訂更有彈性的規範，藉此吸引外部民間企業與

學術研究單位，願意與國內科技研究單位進行共同研究合作與委託研究合作。

六、列入建軍構想

我國國防部應該仿效許多國外國防單位，將物聯網系統，列入建軍構想或戰略規劃中，並編列相關的科研預算，以利國防科技研發單位進行研發。例如，美國在 2008 年底，IBM(International Business Machines Corporation)提出智慧地球的概念=物聯化+互聯化+智慧化，受到美國總統歐巴馬的高度重視，2009 年 1 月將其納入國家級戰略規劃中。目前我國國防科技研發單位，皆會依據國防部的建軍構想或戰略規劃，當作國防科技研發的主要目標與方向，以此進行科研計畫的建案，以強化我國的國防自主研發能量。由於建構軍用物網系統，所需投資的先期研究預算金額非常高，因此需要政府研發資金的協助。許多的研發科技，都需要建構在日積月累的研發成果基礎上，並非一蹴可幾，需要依照規劃，按部就班，才能及早完成軍用物聯網系統的研發與建構工作，並將其應用於國防科技領域與國內各軍種單位。

結論

目前全世界都在關注物聯網系統的發展與應用，雖然物聯網並非全新發明的單一技術，而是將感測技術、網際網路與智能分析等技術，進行整合與應用。許多國際知名的產業研究機構都預測，聯網物件每年都會大幅增加。至2020 年前，全世界大約會有 300 至 500 億個物件與網路進行連結，除了可以進行感測與資料收集之外，也可以進行數據的分析與行動規劃，更可以透過網路進行物件與物件的連結，進而下達正確的指令與動作，其龐大的商機不言可喻。未來，物聯網非常有潛力可以應用在政府部門、軍事國防、健康管理、倉儲管理、交通運輸、資通連結與能源開採、產品製造與運送等領域，每年全球可以創造的商機可高達數十兆美元。尤其，後續分析所獲得的數據，除了當作管理與供應的參考之外，更可衍生出許多創新服務與商業模式。雖然，軍用物聯網所面臨的困難與挑戰比企業物聯網高，但是許多國家仍在積極規劃布局，以提高軍隊作戰能力，減少人員傷亡。國內由於 3C 與電腦資訊產業的發展蓬勃，電子與半導體技術分工與垂直整合完善，先天具有發展軍用物聯網的優勢，可參照國外目前發展物聯網遭遇的困難與挑戰，初期也可考慮以後勤補給與軍隊管理為主。朝此目標進行規劃布局與研究開發，相信不久的將來，軍用物聯網可以很快的在國內軍隊實施與運用。

參考文獻

一、https://en.wikipedia.org/wiki/Internet_of_Things, 2015/11/20.

二、http://www.trentonsystems.com/applications/machine-to-machine/, 2015/11/20.
三、Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswamia, “Internet of Things (IoT): A vision, architectural elements, and future directions,” http://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf, 2015/11/20.
四、http://www.w3.org/WoT/, 2015/11/20.
五、http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081, 2015/11/20.
六、http://blog.claricetechnologies.com/wp-content/uploads/2014/03/clarice_Iol_predictions_20201.jpg, 2015/11/20.
七、Joe Mariani, Brian Williams and Brett Loubert, “Continuing the march: The past, present, and future of the IoT in the military,”http://dupress.com/articles/internet-of-things-iot-in-military-defense-industry/, 2015/11/20.
八、http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf, 2015/11/20.
九、http://www.afcea.org/content/?q=defense-department-awakens-internet-things, 2015/11/20.
十、http://eecatalog.com/military/2014/05/09/the-military-internet-of-things/, 2015/11/20.
十一、http://www.defenseinternetofthings.com/wp-content/uploads/2014/09/MIOT_C_fl14.pdf, 2015/11/20.
十二、https://www.boozallen.com/content/dam/boozallen/documents/2014/12/Internet_of_Things.pdf, 2015/11/20.
十三、Denise E. Zheng and William A. Carter, “Leveraging the internet of things for a more efficient and effective military,” http://csis.org/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf, 2015/11/20.