原文出處：The UK Cyber Security Strategy-Protecting and promoting the UK in a digital world (2011/11)

英國網路安全策略-在數位世界中防護與提升英國

目錄

摘要

網路改變我們社會、經濟，人們有了新的方式聯繫與合作。成本下降後，也代表網路會更便宜、簡單取用，讓更多的英國人民與世界上的人民來使用，促進創新與生產力的‘民主化’。這般演化擴展了網路環境與網路價值。章節 1 描述網路成長背景，社經利益。

網路帶來的改變，增加了生活彈性帶來了機會也相對帶來了威脅。當網路促進開放市場與社會，如此開放性也會讓罪犯、駭客或新型惡意智慧服務找到我們更多的弱點。章節 2 描述這些威脅，只要我們對網路依賴成長也代表威脅相對的成長。

網路讓組織國家超越藩籬，網路中所發生的事件是快速與密集的(舉例說：網路中的刺探等同於實體世界中的詐欺行為，但網路罪犯卻遠端控制就可以輕易地造成工業規模大的犯罪)，儘管我們有方法管理網路風險，但無法符合這個動態與複雜的環境。所以我們需要新的傳輸程式來加強民主化與持續國際間的互動。

章節 3 條列我們 2015 年最終想達到的英國網路安全。

2015 年英國的使命是利用多樣化、有彈性以及安全的網路環境創造大量的經濟，讓我們的行為能夠建設在具備自由、公正與透明度的法規之上，加強我們的資產、國家安全並建立強壯的社會。

為了達到我們的使命，必須

(1). 解決網路犯罪，讓英國成為世界上網路貿易最安全的國家之一。

(2). 有彈性的面對網路攻擊，最好能夠保護網路利益。

(3). 讓英國塑造為一個開放性、穩定、多樣化的網路環境，能安全的運用並且支持開放性的社會。

(4). 能夠及時進行知識、技能跨區域性的修正，由上而下支援全面網路安全事件。

這也代表英國為具備以下特色的國家

(1). 為一個了解如何保護自己遠離犯罪的個體。

(2). 企業意識到自己所面臨的商業威脅、自身所擁有的缺點並且與政府合作，讓整個英國利用網路安全服務策略之下，建立一個繁榮又多樣化的市場。現今經濟趨勢之下，英國必須比以往更多辨識與探索來成長國際競爭優勢，期望網路環境就是我們的優勢之一。

(3). 政府加強法律的實施，快速回應犯罪，讓英國佔據國際間網路安全服務的優勢。激勵企業在網路安全上的成長，支援防禦國家關鍵基礎建設

免於網路攻擊，與世界上其他國家、機構、企業建立合作關係以幫助塑造開放、多樣化的網路環境來自身與跨國間的社會體系。

為了達到這些，我們準備了六十五億歐元，當作為期四年國家網路安全專案之公眾基金。

第四章節介紹政府將會做什麼，如何與機構、其它國家協同合作以達成使命。

政府即將展開之行動計畫如下

(1). 持續以 GCHQ、MOD 建立英國的主權能力，防禦與偵測高等威脅。
(2). 遵循倫敦網路環境研討會所制定的"rules of the road"，在網路環境的使用上符合國際間的準則。
(3). 與管理關鍵基礎建設資料的廠商密切合作以確保資之安全。
(4). 建立與私有機構合作關係，在網路環境下分享網路威脅資訊。
(5). 鼓勵具備知識的廠商建立已使用準則成為工業標準，也讓優良的安全廠商的資安知識成為賣點。
(6). 利用鼓勵優良網路安全產指標，幫助顧客與小廠商能夠領航市場。
(7). 與商業服務舉辦策略首腦會議，具備保險、稽合、律師以決定他們在降低網路風險上該扮演什麼角色。
(8). 結合既有的特殊法律加強在網路犯罪上，成為新的國家犯罪機構，專屬於網路犯罪，幫助制定政策。
(9). 與其它國家合作，確保可以跨國界的協同合作，謝絕罪犯。
(10). 加強法庭，對線上犯罪進行制裁。
(11). 循求線上服務提供者得的同意書，防護使用者免於惡意軟體。
(12). 利用社會媒體幫助顧客回應網路威脅成為新的正規。
(13). 在所有階級上進行教育，加強關鍵技能與 R&D。
(14). 為小型企業與公眾建立單一的授權顧問機構，幫助他們擁有安全的線上環境。
(15). 多樣化與創新網路安全區塊，包含探索新的企業與 GCHQ 的伙伴關係加強政府的專業。

因為智慧與國家安全的連結，許多政府的活動必須進行分類，這些分類在 Annex A。

1. 網路環境 成長、強大英國、世界各地社會

1.1 網路與網路技術驅動經濟成長、人民通訊以及提供新的方式溝通與偕同互助。WWW 由 1991 年崛起，直到今年度已有二十億人民在網路上活動，這已佔了幾乎三分之一的世界人口。在下一個十年將會有更大的改變。

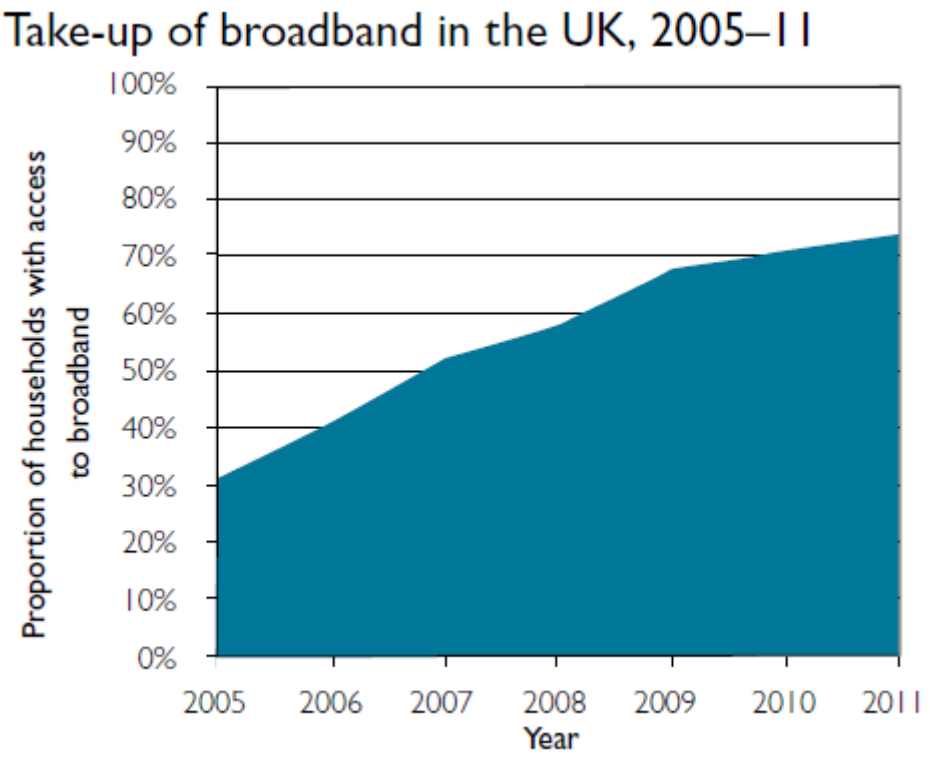
1.2 網路已經大量影響我們的生活，就像鐵路與冶煉金屬的技術都是歷史的轉捩點。

…是什麼帶領成長…

1.3 網路戲劇性的成長，網路環境讓貿易更具效率與效果，開放性的環境降低成本，行動中也能進行交易，新的商業模式提供公司較佳、低成本且更方便的服務，提供顧客跨國界購物與比價。

1.4 尤其是開發中國家更能因此加速成長，更輕易地進行電子商務、存取資訊與接受教育等。讓人們可以在全球市場盡情創新與競爭。

1.5 2009 年英國的六億筆線上交易，總金額共高達四百七十二億，2011 約 74%英國家庭存取寬頻，圖表如下：



1.6 調查中顯示，網路在開發中國家平均貢獻了 3.4%GDP，在英國則是 6%。

1.7 一樣的調查中顯示，網路在成熟國家中扮演了核心的腳色，在過去五年中提升了 21%GDP。

1.8 網路幫助很多公司的基礎建設之自動化與最佳化。

1.9 成為電話通訊與面對面會議之替代方案，更節省了成本。

…扶助開放、強壯之社會結構…

1.10 網路成為最大的知識儲存體，讓人們分享知識、表達觀點與共同解決問題。他提供新的更有效的方式來聚集大量的人們在相同的議題上互助合作，也產生了更多的創意。只要不斷地成長下去，網路環境將成為民主化的社會，讓人民更輕易地參與政府公眾事務。

…什麼將會持續成長…

1.11 從 1970 年代開始，我們已可清楚看見

1.12 網路的行動化、雲端將會對我們有更大的價值與影響

2. 改變中的威脅

2.1 網路的成長，威脅伴隨著機會來臨而且必須要對抗它。

2.2 網路成長初期並沒有太注重於網路安全上，當我們放置越多的生活重心於網路上就必須要越重視經濟、資產、私人資訊等安全議題。

2.3 越來越多利用網路竊取、佔據、破壞關鍵資料的惡徒，我們的生活就越受影響，2010 年國家安全政策〝Tier I〞就是我們最高權限的對抗行動之一。

什麼是威脅？

2.4 數位世界中，各地罪犯透過各種方式針對電腦、網路與各種服務企圖侵入英國，網路也提供了罪犯接近各處之孩童與弱點，跨各國法律管轄區導致更難打擊犯罪。

2.5 有些以英國為目標的犯罪是來自於其他國家的間諜策略以監督我國政府、經濟、資產。那些“愛國”的犯罪者入侵我國之後再散布假消息、干擾關鍵服務或在緊張的氛圍下尋求自身優勢。戰爭衝突之下，對手透過入侵降低我們軍事科技之能力，抑或是透過該技術對我方進行攻擊。

2.6 網路已被恐怖份子用來宣傳、激活潛在支持者以便聚集討論計畫、募集資金，並可能在其發現英國基礎建設之弱點後進行攻擊。

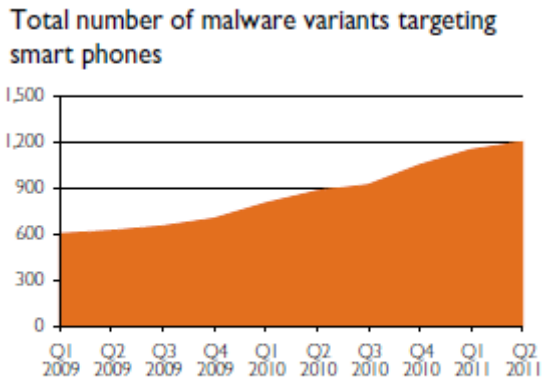
2.7 以英國為攻擊目標的團體是真的存在的，針對公/私英國線上服務的攻擊也越來越普遍。

2.8 罪犯、恐怖份子、競爭軍隊等為重要議題，但是網路的匿名性與無國界導致辨別對手之意圖更加困難。

對商業影響

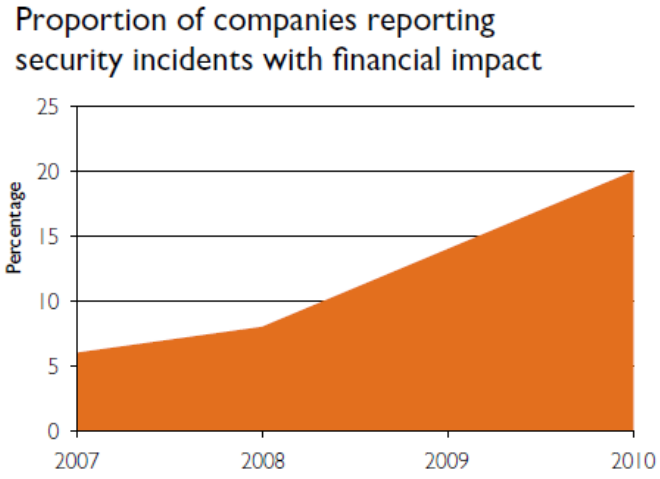
2.9 組織總是不容易注意到網路為他們所帶來的漏洞，智慧資產或是私密資訊可能就是吸引駭客的目標。英國政府將此視為不容忽視的一環。

2.10 服務數位化讓個人與企業線上連結大增，意外事件有可能發生在個體與企業間的此環節，學者建議英國每年應撥出 270 億歐元來維護網路安全，下圖為智慧型手機所帶來的網路安全議題



Source: data from McAfee, as cited in *The Economist, October 2011*.

2.11 下圖為資安事件對財政的影響



Source: *Pricewaterhouse Coopers. Global state of information security survey, 2011*

2.12 在網路上要明哲保身必須要付出很多的心力與金錢，如果沒有分享弱點與威脅的機制，任何的防護都不夠用。

對安全的影響

2.13 網路空間成為了工業(水、電、交通等關鍵基礎建設)或軍事策略優勢的策畫領域，近乎三分之二的關鍵基礎建設公司發現惡意軟體在攻擊他們的系統。

2.14 並肩既存的安全防禦能力，必須要保障國家在網路上的利益。

對個人與社會的影響

2.15 讓人民有信心以網路為基礎來改變自身生活方式，就必須要降低風險取得人民信任，任何造成信心衰退的事件都會導致英國社會經濟之傷害。

2.16 必須要以自由、平等、透明度為基礎的法則來保護國民網路使用的安全

性。

2.17 公約與法規處於制定中狀態，這會導致責任歸屬的不確定性與不穩定，模糊的界線導致個人與企業生存在更多的風險下。

2.18 強化國家安全的過程中必須要符合人權，像是言論自由、隱私權等。

2.19 這不是專屬英國的議題，而是世界各地擁有數位科技國家的共同擁有的問題，一些國家甚至妄想控制與限制網路領域之建置，而英國只會與那些有共同想法的國家合作，一起享受網路所帶來的利益與共同解決問題。

一個複雜的影響

2.20 遽增的網路應用與連結技術造成了快速改變與複雜的環境也帶來了挑戰

- 網路被大量的商業化應用，全球化的成長。
- 網路元件封裝、組合、複雜、多方資源提供者與多階層合約商。
- 預測與了解網路將會被如何使用是困難的，畢竟有太多創新與應用的方式了。
- 新的弱點與風險不斷湧現。
- 事件層出不窮導致防禦方式顯得緩慢與不足，複雜的網路環境也使歸類罪犯之屬性是困難的。
- 隱蔽威脅的文化也導致公眾與企業低估網路所帶來的風險。

目前迎接挑戰的能力

2.21 我們私人部門、關鍵政府單位、學術單位在網路環境中具備領導世界的優勢，而我們必須將這些優勢聚集起來共同迎接挑戰

- 英國擁有強力的國際聯盟可以共同分享價值與利益。
- 我們健全的國家框架與監督環境讓英國有基本回應網路犯罪的能力，而我們必須讓這樣的能力國際化。
- 英國已經具備與民間機構交換網路安全資訊的方式，只要風險出現就能夠與民間機構共同解決問題。
- 專精於網路特殊技術的專家會幫忙英國達到資安目標。
- 特殊機構 GCHQ 有著世界級的處理技能。
- 我們已擁有一些商業網路資訊安全上的優勢。
- 資訊確保已扮演重要的角色來降低網路環境的弱點。

2.22 但是政府的這些能力並不足以應付網路時代的變動，我們的法律仍然太過

分散，罪犯仍然將網路環境視為高利益低風險的投資選擇。

2.23 一些企業了解這些風險所帶來的衝擊，而一些較小型、中等的企業則仍沒有能力保護他們自己，我們必須更有效的控管、了解各領域之風險。

2.24 確保公眾安全地存取他們所須的資訊與技能，政府與私人機構的協同合作是必要的。

2.25 必須與其他國家適用的網路環境共同準則。

2.26 雖擁有了良好的網路技術，但是罪犯屬性與行為的改變才是偵測的關鍵。

2.27 網路改變生活，利益帶來威脅，持續變動的環境需要一個新的解決方案。

3. 2015 年英國網路安全之使命

3.1 為了確保網路所帶來的經濟與社會利益，以下章節將介紹英國依照目標來執行自身該進行的工作並拓展國際安全專案來確保達成使命。

2015 年英國的使命是利用多樣化、有彈性以及安全的網路環境創造大量的經濟，讓我們的行為能夠建設在具備自由、公正與透明度的法規之上，加強我們的資產、國家安全並建立強壯的社會。

為了達到我們的使命，目標如下

(1). 解決網路犯罪，讓英國成為世界上網路貿易最安全的國家之一。
(2). 有彈性的面對網路攻擊，最好能夠保護網路利益。
(3). 讓英國塑造為一個開放性、穩定、多樣化的網路環境，能安全的運用並且支持開放性的社會。
(4). 能夠及時進行知識、技能跨區域性的修正，由上而下支援全面網路安全事件。

我們的準則

以風險為基礎的方法

3.2 全球化的網路世界中，系統總是有著弱點，攻擊總是難以偵測，所以我們將提出仍會有風險的方法來優先列出該有的回應

…合作夥伴…

3.3 如此規模所帶來的挑戰，必須要有國家強力領導的後盾，而具備這些能力的專家通常存在於私人機構中，為了跟緊威脅的腳步，合作通常是商業導向的。

3.4 再來網路是跨國界的，並不是所有的基礎建設都是英國所建置，所以必須尋求國際合作夥伴。

…具備自由與隱私的安全環境…

3.5 我們國家所追求的網路安全政策必須要保障個體的隱私、自由與個人價值。

3.6 我們會持續建置確立合法安全網路行為之法規

- 政府的法律必須不違背國際法律
- 每個人必須有能力、技術、信心與機會來存取網路。

- 網路使用者必須要尊重、容忍不同的文化、語言與想法。
- 確保網路的開放、創新與源源不絕的資訊。
- 必須尊重個人隱私權，鞏固智慧財產權。
- 必須允許我們收集網路中犯罪行為以便解決威脅。
- 確保網路競爭環境中擁有公平的投資報酬率。

腳色與責任

3.7 網路環境個人、私人機構、政府人人有責，才能共享網路所帶來之利益

個人

3.8 有秩序的人民於食、衣、住、行上均能夠在安全的網路環境下。

- 人民了解基本對抗威脅之方法，隨時得到關於自身所處之威脅的最新資訊，並瞭解如何對抗。
- 人民必須注意放在網路上的個人資料，小心電子郵件之附件或超連結，並不要輕易下載不了解的檔案。
- 每個人都能夠幫助上載、分享威脅資訊。
- 個人身處於企業與政府之間之角色，必須保護個人密碼、即時更新軟體與作業系統，並切記要安裝防毒軟體。
- 人民必須了解網路環境等同於現實生活，我們也必須要為自己在虛擬環境中的行為負責任。

私人機構

3.9 私有企業使用大部分的網路資源，他們將會更加創新來對抗威脅

- 公司已意識並使用各種保護方法保護顧客資料、智慧財產與私有資料。
- 私人機構間互助合作，政府與法律分享資訊與資源到這些機構中。
- 企業必須不斷成長、創新、健全的網路安全服務。
- 加強網路，投資與創造優秀的網路安全技能已符合未來需求。

政府

3.10 政府必須負責達到所有目標

- 建置強大的能力來偵測與防禦高等威脅。
- 幫助塑造國際間網路行為法規之共同意識。
- 降低政府系統與關鍵國家基礎建設之弱點。
- 擴展網路安全專業幹部。
- 強壯網路安全法律之實施與處理網路犯罪。

- 提倡防禦與喚起公眾意識。
- 喚起企業警覺心。
- 把握與產業、學術機構合作機會以強壯網路安全市場，讓英國成為一個電子商務安全的環境。

3.11 接下來的內容將會提出我們如何與合作夥伴共同達到使命。

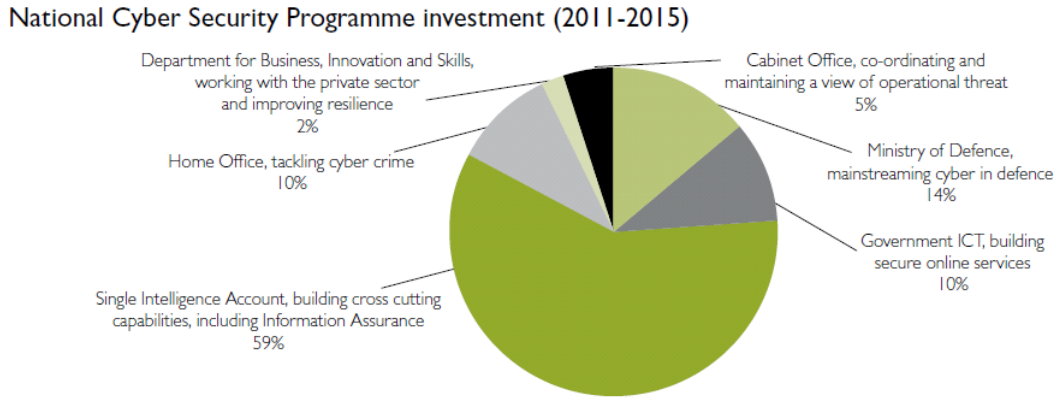
4. 把握機會，面對威脅

4.1 2010 年策略防禦與安全回顧其中一個結論，讓政府投資六億五千萬，四年的國家安全防禦專案，這項資金加強政府回應網路威脅，運用在各關鍵部門與機構。

4.2 國防部與情報機構必須複雜加強大眾了解與降低漏洞，這是 GCHQ 必須要更加付出心力於此，國家內閣辦公室都得到資金以加強資安防禦。

4.3 NCSP 為內閣辦公室負責管理與協同網路安全，也可以在專家的建議之下對分配進行調整。

4.4 與企業、夥伴、社會與國際間，NCSP 會依照優先序分配並依規定定期回報。以下為基金分配圓餅圖



行動優先序

4.5 以下將更加強化英國既有的優勢

- 加強國家關鍵基礎建設與國際系統之威脅偵測與分析。
- 匯集企業知識與適當與企業間夥伴建造國家安全回應。
- 加強能力對抗高階、國家級的威脅並且預防這些技術被非國家級人員所運用。
- 國際間合作共同訂制法則避免誤解與降低風險。
- 英國已批准了布達佩斯公約並會追求其他國家制定相容的法律，讓打擊網路犯罪能夠無國界。
- 我們會保持有效合法的框架與實施能力以破壞並起訴網路犯罪。更簡易的回應犯罪並將情報推播給大眾。
- 塑造政府網路安全系統的最佳實務，並制定標準給合作廠商。
- 加強專家之技能，保持一定的水準以確保能持續創新解決方案。

- 防禦是關鍵，全民與企業都必須加強危機意識與教育來保護自己。80%的攻擊行為只要透過定期更新防毒軟體就能夠抵擋。
- 我們將會創造一個繁榮的網路安全市場，讓英國成為一個安全的環境，讓全球無憂地與英國進行商業貿易。

建置防禦對抗高等威脅的能力

4.6 北約(NATO)里斯本首腦會議中點出網路環境顯著已成為新的風險與機會之地，對聯盟來說重要的策略觀點如下：

> *利用 NATO 規劃程序建置我們的預防、偵測、防禦以及回復網路攻擊的能力，集中化的防禦與整合能力，加強 NATO 成員協同合作、共同保護網路安全之能力。*

4.7 為了達到 NATO 策略概念以及符合國家安全委員會，NCSP 持續投資確認仍採取機動性的方式處理網路威脅。

4.8 國防部確認任軍事網路與設備能夠對抗網路威脅，聯合司令部隊從 2012 年四月開始伴演防禦與整合之領導的角色。

4.9 我們將會成立新的防禦網路運籌組織以利跨各層級的防禦，該組織將會包含 GCHQ 中各聯合單位，設立新特徵、技術與規劃軍事效能，並在未來考慮徵收具備網路知識與技能之預備役。

4.10 國防部長近來將會開設新的全球運籌安全控制中心，專注於加強網路之軍事力量，位於此運籌中心的聯合網路單位將會使用新的技術破壞威脅所帶來之資訊安全議題。

4.11 國防部也會強壯聯盟國家與產業，共同收集網路威脅、弱點與事件。

4.12 6 億 5 仟萬的一半將會使用在此單位之 GCHQ 以偵測、計算網路攻擊。此部分之細節必須要再仔細分門別類。

致力於跨國網路共識

4.13 跨國間合作制定網路行為準則。

4.14 英國以國際間政府之網路行為必定是適當的且符合國際法，包含了智慧財產權與各種基本的人權。

4.15 在 2011 年 11 月的倫敦會議中已有初始的擬定，並且聯合國與各國際協會仍會共同制訂網路可接受之行為法規，必須清晰定義所有開放式、值得信賴與穩定的網路環境。

4.16 同時英國將會與聯合國、各地之 OSCE 建立信任，避免非預期之事件造成

國際間之風險與誤解。

2011年2月 將網路行為之法規稱為‘rules of the road’，制訂網路相關的利益個體之相關法規

11月1-2日 倫敦會議中，各國部長、政府高階官員與網路技術代表團體齊聚一堂，總共七百個成員來自六十個不同之國家，一同制訂網路行為大綱並且此會議將會持續進行下去，2012年與2013年將各在匈牙利與南韓舉行

降低政府系統與關鍵基礎建設之弱點

4.17 政府 ICT 將會制訂政府如何保護關鍵資料與系統安全，與產業共同建置 ICT 產品與服務之嚴謹的網路安全與 IA 標準，尤其是供應商所提供之商品必須要符合防禦裝置之標準，正如我們已經提出實體安全需求給合約商，仍有人朝著竊取資料而來，於是國防部正著手策劃 ICT 策略與程序管理政府資訊之風險。

4.18 政府所制訂之‘數位化’、雲端運算策略的確幫助我們生活更有效益，但我們必須確保這類服務能夠免於詐欺與網路攻擊，我們將會設定關於系統更新、補釘之目標。NCSP 正著手於值得信賴、堅固之方式於辨識身分等相關配套措施。

4.19 當然大部分的政府系統是發包給私人機構，CPNI(Centre for the Protection of National Infrastructure)則著手於確保合作公司是採用正確的步驟來保護系統與資料。

4.20 政府現在則會將規模擴大到沒有共同合作之公私機構，也許這些公司尚未與現今之關鍵基礎建設相關，但是仍是威脅企圖取得利益與智慧財產之地，具有造成重大經濟損失之可能性，CPNI 則將會協助 NCSP 此類相關對外事務。

4.21 網路安全〝樞紐〞將會被建立以被用來確立更多團體能夠了解並處理網路威脅。

2011年2月 英國首相與英國經濟領域高階級之公司主管共同討論網路威脅與利益共享之權利。從那之後，政府與公司共同建立了以下創新方法：

- 即時交換網路威脅資訊，強化回應網路事件之能力。
- 分析、辨識新的威脅與機會。
- 強化分享網路安全能力之連結。

聯合公/私之樞紐會蒐集各種威脅資訊再推播到各關鍵節點，幫助他們辨識他們該做什麼事與分享最佳實務給各關鍵公司遵守。首試於五種企業領域(防禦、財政、通訊、醫藥與能源)，先導實驗所帶來之心得將會被參考在未來更多領域之實行，我們也將會確立中小企業是否意識到威脅以及了解網路安全樞紐所帶來

之益處。

激勵網路安全專家

追緊威脅的腳步是必須的，可是政府跨企業間深度了解網路與建置網路的專家相當稀少，政府的訓練與教育必須加強，維持英國的專家資源並鼓勵有道德的駭客社群來確認我們國家的網路是否被良好保護：

- 2012年3月建立專業訓練認證程序加強資訊深度技能。
- 持續參與網路安全競賽，以加強技能專業度。
- 強化研究生教育，加強網路深度知識拓展專家資源。
- 建置連貫跨領域的網路研究綱要來強化英國學術基礎。
- 向GCHQ領取預算兩百萬歐元，為期3.5年專案建立網路安全研究機構。
- 分類出各私人機構之網路安全技能需求的範疇、特徵與文化。

網路犯罪與法律實施

4.23 確認網路安全犯罪，讓法律實施機構能夠處理網路犯罪。

4.24 網路環境允許罪犯跨國界，我們會致力於布達佩斯法案制訂相容的法律框架。

4.25 英國強力推廣稱為‘24/7 Network’法案 ，只要緊急事件被確認合作夥伴就可以與英國合作解決問題。

4.26 我們也必須確認英國是否有能力回應威脅，我們會不斷地審視電腦濫用法案以確保是否仍適應最新的改變，只要有需要修正的地方就會盡速送審。

4.27 電腦可以在具備搜查允許的狀況下被監督與存取流量，政府也必須確認在犯罪發生時執法單位是否有真正保護到大眾安全。

4.28 司法部與國土局會建置處理事件之順序，利用‘網路標籤(cyber-tags)’標誌各違反網路正常使用行為之狀況並自動通知警察與處刑服務。

4.29 當我們擴展了處置的權利，也幫助了法律的實施機構加緊了他們的操作回應。身為國家犯罪機構的一部分，我們會創造新的國家網路打擊犯罪能力，SOCA 與警視廳中央電子犯罪單位將近期發生的網路犯罪繪成拓樸。新的單位將會針對 NCA 的四個面向(國界、組織犯罪、經濟犯罪以及孩童剌探與線上保護-Child Exploitation and Online Protection–CEOP) 給予協助。

4.30 此單位將會具有國家級能力處理國家級之網路犯罪，也會共同回應主要國家安全事件。NCA 會持續協助 SOCA 以及警視廳打擊犯罪，畢竟這是屬於跨國界與司法之議題，我們也會使用網路技術來破壞組織網路犯罪。

4.31 NCA 也會支持政策在英格蘭與威爾士之實施，像是訓練網路議題之法律

實施、研究欺凌與孩童刺探之相關以期更廣的網路犯罪處理能力。關鍵點在於政策實施與 NCA 之資訊流通能力。政府會更著手於執行部隊如何執行之智慧(像是 CEOP 所提供的孩童威脅)以及執行後所帶來之結果，然後法庭能得到最佳回應以建立對威脅之正確回應。必須在政策、企業與社群間建立強壯的關係，我們會鼓勵這些群體交換技術。警視廳的中央電子犯罪單位已將特殊政策將相關技能做關聯進行開創性的使用以幫助處理網路犯罪:我們將會鼓勵警察使用'網路特殊(cyber-specials)'，我們會邀請外界法律專家幫忙處理網路犯罪組成 NCA 網路犯罪單位。

4.32 遽增的電子商務，使用網路技術進行網路交易給了罪犯更多的吸引力，企業在其中成為了關鍵的角色。我們將會從 UKCCIS(UK Council for Child Internet Safety)學習成功處理網路威脅之經驗，我們將會介紹相似的協會進行跨區塊的網路犯罪之合作，這協會能幫助釐清網路犯罪，建立網路安全的最佳實務，有效預防更層級之商業網路犯罪。

4.33 同時我們也必須確認回報網路犯罪的方式對同仁來說是簡單且直觀的。

4.34 透過整合的網路犯罪回報工具，過半的警察已能有效回報網路犯罪。我們將會協助警察辨識好的實務讓他們完善的線上回報犯罪。

4.35 人們也已被鼓勵回報詐欺，只要透過網路使用行動詐欺工具就可以上傳至相關單位，我們將會將此動作設計得更加簡易操作以增加它的可存取性與功能性。犯罪回報已可在 30 分鐘內完成，我們更期望未來可以再削減一半的時間。

4.36 更好的回報可以幫助國家詐欺智慧情報局建置智慧圖像以辨識犯罪個體，增加執法資源與犯罪預防建議。

預防與犯罪意識

4.37 預防是關鍵，大部分的網路事件都可以透過相當簡單的 '衛生網路(cyber hygiene)'來預防。GCHQ 估計 80%或更多的成功攻擊都可以透過簡單的最佳實務來預防，像是定期更新防毒軟體。

4.38 為了幫助人們保護自己，我們將會：

- 幫助顧客回應網路威脅，像是利用社交媒介來提供威脅資訊。
- 在各階層實施網路安全教育。
- 與網路公司合作為線上攻擊制訂線上制裁。
- 與 ISP 合作(Internet Service Providers)幫助個體辨識自身電腦是否遭受攻擊以及如何防禦攻擊。

- 提供清楚的網路安全建議，讓人們了解如何使用自己身處的網路環境。
- 促進人民購買具備‘kitemarks’認證的安全產品，BIS 將會與社會、歐洲、全球以及商業標準組織合作制定資訊安全產品的標準並刺激資訊安全產品之市場以確保各層級都能得到正確與良好的防護。

4.39 取得線上安全(Get Safe Online)已以一個平台的形式存在，我們將會資助合作夥伴、網路公司、零售商與 ISP，讓它更具互動性並且更加完善；創造持續性的意識活動；讓大眾得到更多資源；透過 ‘kitemarks’幫助顧客分辨一般幫助產品、進階產品與偽防毒軟體‘scareware’之差別。新的一年將會組成一個聯合行動計畫。

取得線上安全為聯合公/私領域之活動，主旨為喚起大眾線上安全意識，主要針對一般大眾與小型企業，給人民信心與知識安全地使用網路，利用綜合性網站結合了行銷與關係管理給予即時更新的資訊、工具與準則。贊助來源為政府、微軟、HSBC、Cable & Wireless、Ofcom、趨勢、Gumtree、Verisign、賽門鐵克與 Paypal。

喚起企業意識

4.40 當我們與客戶交易時，我們必須喚起企業相關威脅之危機意識，像是企業聲望、營利、智慧資產。

4.41 企業是網路犯罪與經濟間諜最大的犧牲者，政府與私人機構必須共同負起責任，擁有資產與商業決策的私人機構都必須加強自身網路安全。我們已進行許多喚起威脅危機意識活動，然而最終的重點仍需要企業行為上真正的改變。

4.42 先前提過的聯合公/私人機構網路安全樞紐就是幫助辨識與管理威脅資訊之關鍵角色。

4.43 取得安全線上提升危機意識也提供建議給個人與中小型企業，但仍需要更多的方法來督促那些尚未行動的企業。我們將會利用數位頻道與網路媒介像是線上導覽。

4.44 為了保護商業關鍵資訊，政府相信網路安全漏洞資訊的透明度與歸檔是重要的。BIS 將會出版 2013 綜合研究揭露英國企業網路安全漏洞，同時，BIS 將會透過既存現行之研究來更加了解風險。

4.45 安全產品之市場較難刺激小型企業，所以 BIS 刺激產業級的標準與準則來幫助顧客辨識適當的產品，BIS 也會開創一個新方法，讓產業效能更佳的產業級安全軟體標準。BIS 將會與這些個體合作(社會大眾、英國本國、國際間)來制

定適當的標準。

4.46 提供服務給企業的供應商也扮演了喚起危機意識重要的角色之一，BIS 將會與專業企業服務提供者合作以確保企業流程中每一個環節之風險並且能夠有效的管理這些風險，BIS 會舉辦研討會邀請專業企業服務提供者(律師、保險業、稽核商)來討論如何安全地實施服務。

4.47 政府將會與零售工業合作處理威脅所帶來的挑戰。英國擁有世界上最大的零售經濟，在 2009 年評估約有 1000 億歐元的線上交易，英國的線上購物比率比起其他方式都來的高。為了保護這驚人數量的線上零售商，政府建置了零售網路安全協會來處理此類關鍵議題，包含有效回報與資訊分享。政府將會與線上零售商協會合作討論此安全議題。

4.48 透過 ISP 與顧客的關係可以辨識與預防網路攻擊，所以我們必須建立 ISP 與政府間關係，我們將會合作共同設計一連串適用的準則，這些準則必須包含 ISP 提供使用者處理惡意行為之協助、建立協同合作的方法分享資訊與辨識威脅亦或是 ISP 提供顧客方法處理他們被攻擊的電腦與保護自身免於網路攻擊。

孕育商機

4.49 為了讓私人機構可以把握機會，英國將會孕育一個全球化的網路安全領域。

4.50 GCHQ 是國際級網路安全專家孕育之地，政府將會探索更多的方法讓專家幫助經濟利益成長卻不受網路威脅所害，相關如下：

- 與私人機構合作開發潛在商機應用。
- GCHQ與BIS合作，技術策略委員會以及程與科學研究協會一起策畫將產業、學術與政府結合創造共同的網路安全方法。
- 政府贊助風險資產模型解開中小企業網路創新模式。

4.51 正如我們所言，我們企劃有更嚴謹的網路安全標準讓大眾服務網路相關的ICT產品有個準則，為確保小型企業可以產出更多創新，我們將會更進一步提出成長回顧草案幫助中小型企業能夠得到大眾利益。為了網路安全，政府將會創造25%價值的合約提供給中小企業，或將合約分成到各子中小企業，內閣將會監督各部門之透明度，確保所有中小企業之合約分配是否適當。