中共以「和平崛起」掩飾實質資訊武裝的霸權

作者　陸軍司令部少將委員　柴惠珍

提　要

一、21世紀是新型態戰爭精彩演出的年代，愛沙尼亞事件與鬼網間諜活動揭開序曲；從國家戰略角度看，新興網路平台的出現卻也代表另一個全球化時代人類生存必須面對的問題 ── 資訊戰與資訊安全議題。

二、全球化3.0網路平台的演變讓傳統的國家地緣戰略延伸至資訊疆域；國家安全的戰略價值不僅有地緣戰略，資訊疆域的戰略價值更對國家存續有著無可替代的影響性。

三、中共懍於資訊科技對於國家安全戰略的影響，將資訊安全列為國家四大安全戰略之一；除在武力上要有強大的擴軍外，更要在網際疆域建立無人能敵的強大力量，以實現並保障中共的崛起；這是全世界必須面對的新霸權。

四、中共早在其國防現代化的文件中透露武裝資訊的動機，更用具體的行動趕搭資訊科技列車，藉網路突穿地域限制，在世界各國虛擬的疆土上布下深沉且難以拔除的暗樁；其和平崛起只是煙幕，爭奪新世紀霸權才是事實與真相。

五、我國防資訊戰與資訊安全在戰術以下各層級都已具相當程度的能量；然仍須秉持能安全的使用網路資源作為網際安全的目標；並思考建立完整的國家整體安全戰略，訂定我國家新的資訊戰戰略作為，才能確保全球競爭優勢。

關鍵詞：和平崛起、地緣戰略、資訊安全、網路戰、戰略性資訊戰

前　　言

21世紀是數位化時代，也是新型態戰爭精彩演出的年代。2007年的愛沙尼亞事件揭開序曲，其資訊基礎建設遭到網路攻擊，導致政府、金融等服務全面癱瘓❶；愛沙尼亞的官員無論是公開或私下均控訴俄羅斯在背後操控整體攻擊事件；但克林姆林宮卻矢口否認，並反控愛沙尼亞捏造事實；其所運用的「殭屍電腦」遍及全球世界各國。2008年俄國與喬治亞的戰爭更展示全面的網路攻擊是伴隨真正軍事行動的序曲❷。

2009年4月，正當全球20國集團在倫敦召開G20高峰會，置重點於加強全球國際金融系統的監管之際，加拿大蒙克國際研究中心（MCIS）卻公布：中共對全球103個國家至少1,295部電腦實施資訊滲透，許多政府的機密文件遭竊；諷刺的是，中共於表面上大聲疾呼全球金融整頓，私底下卻監控各國的金融機構；而控制這個「鬼網」（GhostNet）的主機幾乎全設在大陸，是目前所知最大的間諜活動；中共北京當局亦駁斥此項說法：「中國政府反對，並嚴禁任何網路犯罪行為❸。」

無疑的，資訊網路已成為國家新經濟建設的基礎，各國為提升競爭力莫不倚賴資訊科技，網路帶給全球經濟旺盛的活力與效率，瞬間讓互動的時間縮短、距離拉近，舊有的人類歷史從此進入一個跨越新世紀的巨大變革，邁入一個嶄新的平坦世界。但「水能載舟，亦能覆舟」，當全球經濟與資訊一體，網路價值躍升的同時，資訊網路也成為破壞者的捷徑與戰爭的場所；敵人為達到攻擊目的，任何資訊漏洞都有可能遭受到劫持，淪落成為黑暗世界的替身。以最近這幾個事件，我們看到愛沙尼亞慘遭不明身分者的攻擊，卻投訴無門；而中共以發展經濟與保衛國家為由，暗地裡卻擴張其黑暗世界的勢力，其真正目的是想要用非對稱武力一舉取代美國，成為新的霸權。

正視全球化中的新興威脅

美國《紐約時報》國際事務專欄作家，知名評述人湯瑪斯・佛里曼（Thomas L. Friedman）在其《世界是平的：21世紀簡史》（The World is Flat: A Brief History of the Twenty-first Century）❹一書中，描述這樣一個預料之外的科技與社會變動，夷平整個原有經濟世界的崎嶇；佛里曼所描述的夷平機制，主要乃指資訊科技在網路平臺基礎上的發展，包括

註❶：Mark Landler and John Markoff, “Digital Fears Emerge After Data Siege in Estonia”, The New York Times, May 24 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html

註❷：John Markoff, “Before the Gunfire, Cyberattacks”, The New York Times, Aug 12 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html

註❸：John Markoff, “Vast Spy System Loots Computers in 103 Countries”, New York Times, March 28 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html

註❹：Thomas L. Friedman, “The World is Flat: A Brief History of the Twenty-first Century”(U.S.A., Farrar, Straus and Giroux, 2005).

網景（Netscape）的興起、網路熱潮及其所引起數以百兆計的光纖纜線的投資；讓全球跨國合作得以發生的共通網路平臺和開放原始碼軟體；新興外包、海外生產、供應鏈規劃及內包（或稱委內，承接公司內部業務）等。

曾是前白宮首席評論員的佛里曼認為：這些夷平機制在2000年統合在一起運作，「架構一個平坦的世界：不受時間、距離、地理與愈來愈超越語言的限制，透過網路的平臺來進行各種知識和工作的分享」。從一般商管的角度來看，隨著網路平臺的出現，3個巨大的經濟體吸引全世界的聚光 —— 印度、中共❺和前蘇聯。就如書中所述：「30億人口原先只能袖手旁觀，現在正式踏上舞臺。」舞臺上充滿許多新奇的角色，人馬雜沓地渲染全球化後繽紛的色彩，各式多采多姿的活動呈現地球村的新生活力。

從國家的戰略角度來看，新興網路平臺的出現卻也代表另一個全球化時代人類生存必須面對的問題 —— 資訊戰與資訊安全議題❻。網路拉平世界，世界各國的人同樣地面對來自四面八方的文化；隨著30億人口的投入，我們必須面對地理上的鄰居，同時也必須面對網路平臺上，遙遠卻鄰近的敵人。資訊時代，網路使人無所遁形。這是我們生活在21世紀中首先必須要有的認知與覺悟。

一、從地緣戰略延伸至資訊疆域

在佛里曼的書中闡述近500年來，世界從全球化1.0進化到2.0（西元1492～2000年）的過程，在2000年之前，世界在邁向全球化的演變進程中，歷經工業技術革命、帝國主義興起、殖民思想氾濫及民族主義的自覺，並且經過兩次世界大戰的衝擊；全球化的過程中顯示地緣戰略的重要性。

然而在21世紀之後，全球化3.0的演變卻有重要的改變；2007年4月27日，東歐的愛沙尼亞共和國遭到來自網路上的分散式阻斷服務攻擊（Distributed Denial of Service, DDOS），國家政務，包括總統與議會的網站、政府服務網站、新聞媒體、金融、電信設施等都受到等同於癱瘓的打擊與影響；5月24日，愛沙尼亞的國防部長艾維克舒（Jaak Aavikso）接受訪談時說：「情況已經演變成攸關國家安全的大事，和重要港口遭受敵人封鎖是沒有兩樣的❼。」美國負責網路與情報整合的副助理國防部長魏爾斯也談到：「現代社會有其脆弱的一面，這場國對國新型態的網路攻擊，可視為重要的分水嶺。」

愛沙尼亞請求與號召北約與歐美各國的資安專家前往協助，經過「網路聯合防衛軍」多次的攻防與復原工作，愛沙尼亞的資訊基礎建設逐漸恢復，國家政務的操作才步入正常運作。雖然愛沙尼亞並未遭受攻擊源國家的一兵一卒侵略，甚至僅能證明：部分攻擊源來自俄羅斯，但國家的

註❺：BBC中文台，〈G20：金磚四國，中國為重〉，2009年3月31日，http://news.bbc.co.uk/chinese/simp/hi/newsid_7970000/newsid_7975400/7975414.stm

註❻：柴惠珍，〈資訊戰組織與資訊安全整體架構〉《陸軍通信兵九十一年度軍事學術研討會論文集》，2002年，頁19-1～19-12。

註❼：同❶。

損失卻超過數千萬美元。這場攻擊備受矚目，許多軍事學家稱之為數位化時代的第一場國家層級的網路戰爭。

2008年8月，俄羅斯與喬治亞的戰爭也以類似方式呈現，在俄羅斯真正實兵攻擊喬治亞前就先發動網路戰，針對喬治亞政府與國會網站資訊進行阻斷服務破壞，在某種程度上讓喬治亞政府對外的資訊聯繫癱瘓。一些參與本次防衛的專家指出，這些攻擊的「主機」來自俄羅斯商業網路與政府網路；喬治亞政府認為網路攻擊為俄國政府所策劃，但俄國已否認與俄國政府有任何關聯。許多網路技術專家也認為：「這是第一次網路攻擊伴隨真正軍事作戰的戰爭型態❽。」這可能是第一次，但絕不會是最後一次；參與這次事件的以色列資訊安全專家Gadi Evron說：「這種型態的攻擊會隨著任何衝突或政治緊張，而很自然且立即的發生」❾。

愛沙尼亞與喬治亞等兩個戰爭為案例證明：網路平臺打破地域的限制，國家安全的戰略價值不僅有地緣戰略，資訊疆域的戰略價值更對國家存續有著無可替代的影響性。在全球化2.0的地緣戰略中，我們絕對可以劃出疆土國界，也很清楚的知道敵人何在？但進入全球化3.0的數位化世紀時，資訊網路打破國家界線，敵人在無國界的虛擬空間中，卻已悄悄地邁入國之大門；而資訊疆域不再只是一個網路平臺，更是資源與權力的所在；誰控制資訊網路的資源，誰就控制權力；而世紀的強權更是賦予那些在實體世界與資訊疆域可同時掌握優勢的國家❿。

二、全世界必須面對的新霸權 ── 中共

不可否認的，「金磚四國」的確是在新興經濟的舞臺上展現令人亮眼的成績，尤其是擁有全球最多人口的國家 ── 中共，藉由網路平臺的延伸與整合，中共在全球供應鏈上扮演極為重要的關鍵角色。

中共自1978年實施改革開放以來，社會發展平穩，經濟成長相對快速，而維持國際環境的穩定及和平，提供其經濟成長的空間，便是中共領導人的首要工作。冷戰結束之後，中共的國家安全戰略無論在形式或內容都產生巨大的改變。近年來，中共懍於資訊科技對於國家安全戰略的影響，在內部會議及論壇均積極研討，包含從國際和國內的政治、經濟、軍事、文化、資訊、人口、環境等不同角度，進行深入研討和論證。

中共在其「十五計畫綱要」中提到：「發展是解決我國所有問題的關鍵」。2002年時，中共認為國家綜合安全戰略包括經濟安全、金融安全、能源安全、糧食安全和資訊安全等項目⓫。但自2003年後，在中共的黨十六屆四中全會、六中全會中，資訊安全一躍成為國家四大安全之一，國家四大安全包括文化安全、政治安

註❽：同註❷。

註❾：Shaun Waterman, “Analysis: Russia-Georgia Cyberwar Doubted”, Space War, Aug 18 2008, http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html

註❿：柴惠珍，〈國軍資訊戰發展策略與管理〉《軍事資訊應用研討會》，空軍航空技術學校，2001年，頁11～33。

註⓫：陳立編著，《中共國家戰略問題報告》（北京：中共社會科學出版社，2002年9月）。

全、經濟安全、資訊安全。在在顯示，中共的國家戰略不僅針對經濟發展，資訊安全也是其致力建設的目標。

而今，中共除已成為21世紀新興經貿強國，美國亦在對中共軍力評估報告中，提出對中共發展資訊戰力的觀察與警示。顯然地，在此一波新興全球化經濟革命中，中共經貿的強勢力量已加速其國家軍事建設的成果，證明中共在資訊疆域發展上有極大的突破與成果。若再仔細觀察中共的國家戰略觀，則可發現其在網際空間已成為一股不可忽視的新興力量。

中共致力發展網際霸權的建設

依據中共在《2006年國防白皮書》中所述，中共制定國防和軍隊現代化建設三步走的發展戰略：預於2010年打下堅實基礎，在2020年前後將可有較大的發展，到21世紀中葉即可實現建設資訊化軍隊、打贏資訊化戰爭軍隊的戰略目標⓬。「立足打贏資訊化條件下的局部戰爭」已成為中共在21世紀初期建軍的指標，其發展的方向與作為大致如下：

一、戰略方向 ── 戰略機遇期的把握和利用⓭

戰略思維的改變是中共在面對21世紀資訊世代時最大的調適。中共曾多方論證如何推進共軍資訊化建設，為維護國家發展重要戰略機遇期提供安全保障。觀察綜整中共近年在資訊化建軍大致為：

㈠強調「以劣勝優」的資訊戰概念

資訊戰是作戰的「戰力倍增器」，也是不對稱作戰、非接觸作戰的重要一環；成本小、效益大，也是用以剋制歐美等先進但高度依賴資訊化之國家的最好打擊武器。

㈡強化「跨越式成長」的軍事轉型

規劃有關機械化和資訊化複合發展，取法美軍先進的建軍優點，跳脫逐步實現共軍由機械化、半機械化向資訊化的轉型，快速成長實現軍隊火力、突擊力、機動能力、防護能力和資訊能力整體提高。

㈢推行「積極防禦」的軍事戰略

主張軍事戰略首先必須主動預防、化解危機，俾堅決遏制危機的爆發和升級。因此，必須強化積極的能量與作為，調整軍兵種的戰略，除陸、海、空軍的戰略目的轉型成「積極」的外向作戰外，也規劃有關「網軍」的編組與實驗。

㈣宣傳「和平崛起」的國家政策

透過各式文宣，營造有利於國家和平發展的安全環境、宣稱「和平崛起」不等於「積極發展」，使亞洲國家不致感到其軍備擴張的威脅，而世界各國轉而注目於其經貿市場的成長，塑造和平的形象而達成其軍力成長的實質目的。

二、戰術作為

註⓬：國務院，《2006年中共國防白皮書》（北京），2006年12月。

註⓭：中共在十六大報告中提出戰略機遇期的概念，在2020年前是一個必須緊緊抓住且可以大有作為的重要戰略機遇期。其包括確定與不確定的戰略機遇，對確定的機遇，如信息化、全球化等趨勢構成的全球新戰略環境，必須抓住這些機遇來豐富中共發展戰略；對不確定的機遇則發展戰略框架進行調整。中共中央黨校鄧小平理論研究中心，〈全面建設小康社會：中國發展的新戰略〉《人民日報》，2003年08月20日，http://www1.peopledaily.com.cn/BIG5/guandian/1035/2025976.html

配合戰略指導，共軍提出許多，諸如「網電一體戰」、「陸海空天電網多維一體」等作戰概念。並聚焦於密切結合其資訊戰建設現況，探尋資訊戰的「非對稱」發展方略。發展具中共特色之資訊化建設，主要目標如下：

㈠研發網路作戰之關鍵工具與手法

突破現有的技術關卡，置重點於發展網路作戰的新概念資訊戰武器裝備，鑄造資訊領域的「殺手鐧」。

㈡成立資訊戰網軍部隊

規劃建設資訊實驗部隊，集中建設戰略戰役資訊戰部隊，形成打贏未來戰爭的「拳頭」力量，包括兩支隊伍：網路戰專業部隊及非專業部隊，培植網軍能量。

㈢發展毛式網路人民戰爭的戰術

依靠人民群眾建設和鞏固國防，是中共的真正優勢和力量所在。其規劃軍民結合、寓兵於民、信息民兵的編制，在各省及軍區納編於軍事演訓行動；另有高達近30萬名各式網路公安及監察（看）員，負責監控其網內各式活動，以維護保障其網路安全；另外還有較為專屬而引人爭議的是駭客部隊，中共內部對網路之箝制與管控極其嚴格。

諷刺地是，在中共的網路上仍存在為數極多的駭客網站及駭客群；這種荒謬與矛盾，就如同在警察管區內，成立許多小偷及搶匪的集結地，並且明目張膽教人如何偷盜及搶劫的方法一樣。何以警察容許這些盜匪在轄區內公然活動？

2008年3月，美國CNN曾訪問廈門的某個駭客團體，其領導人承認曾接受中共軍方委託而攻擊美國國防部，並在攻擊成功後獲取夠量的酬勞⓮。事後雖然受訪人承受壓力過大而予以否認，但由此可見中共官方仍可掌握境內的駭客團隊。

中共「和平崛起」的事實與真相

一、事實

㈠和平崛起須以武力為後盾

中共對於國家戰略作為一直遵循毛澤東的指導：「你打你的，我打我的」。雖然鄧小平曾經在國家戰略指導：「冷靜觀察、穩住陣腳、沉著應對、韜光養晦、善於守拙、決不當頭、有所作為」，但在中共的解釋其中「韜光養晦」是策略，「有所作為」則是目的，因此「中共要綜合地運用武力和非武力方式實現崛起，綜合使用多種手段，其效果必然高於使用單一手段」、「中共要實現和平崛起就得加強國防。當我國國防力量強大到足以遏制別人不敢於用戰爭來遏制中共崛起時，我們和平崛起就有了安全保障」⓯等說帖。

從中共的和平崛起的策略中可以得到一個邏輯：中共若單靠強大的武力欲達成實現「崛起」目的是必要的，但顯然不足；因此，透過其他非武力手法，綜合交織運用，則要實現中共「崛起」目的的效果較佳；要獲得「崛起」的保障就要有強大到無人可以遏制的國防力量。

我們不難獲得推論是：中共除在武力上要有強大的擴軍外，更要在網際疆域大建立強大到可以遏制他人來遏制中共的

註⓮：John Vause, “Chinese Hackers: No Site Is Safe”, CNN, Mar 11 2008, http://www.cnn.com/2008/TECH/03/07/china.hackers

註⓯：閻學通、孫學峰等著，《中共崛起及其戰略》，北京大學出版社，2005年12月。

力量（即無人能敵），以實現並保障中共的崛起。

㈡各國網域遭到有系統的攻擊

美軍在2006～2008年間對中共軍力報告書中⓰，對中共的資訊作戰能力即保持相當程度的看法。無獨有偶，除臺灣自1999年開始陸續遭到中共來自網路的攻擊外，部分國家也有類似的經驗，例如：2004～2005年，美國遭到所謂的「泰坦雨」攻擊；2006～2007年，英、美、德、法、紐、日等國也陸續報導其軍事或政府機敏網路均曾遭到有系統、有組織的駭客團體或強或弱的攻擊；美國國防部更在2008年11月下令禁止使用任何外接儲存設備的政策，包括軟碟、快閃記憶體，或是可攜式硬碟等USB儲存設備，除非已確定其中無任何惡意程式⓱。

而2009年加拿大蒙克國際研究中心（MCIS）在受西藏流亡精神領袖達賴喇嘛辦公室的請託，開始監測他們的電腦時發現：中共對全球103個國家至少1,295部電腦實施資訊滲透，許多具高機敏性的外交部、大使館、國際事務、新聞媒體、非政府組織（NGO）等機構的機密文件遭竊；遭入侵的電腦包括伊朗、孟加拉、拉脫維亞、印尼、菲律賓、汶萊、巴貝多與不丹等國外交部的電腦，此外還在印度、南韓、印尼、羅馬尼亞、賽浦勒斯、馬爾他、泰國、臺灣、葡萄牙、德國與巴基斯坦等國駐外使館的電腦中發現駭客軟體，是目前所知最大的間諜活動。這個「鬼網」具有超強的監控能力，不但能偷竊資料外，還能讓被滲透的電腦自動打開攝影機與錄音功能，以便作室內環境監視；而控制鬼網的主機幾乎全設在中國大陸；中共北京當局亦駁斥此項說法：「中國政府反對，並嚴禁任何網路犯罪行為⓲。」

許多國家逆溯追蹤攻擊源到中共後，便毫無下落；如若詢問中共，獲得的答案除「毫無所悉」外，就是「拿出證據來」、「外國勢力炒作中共威脅論」等字眼。一個擁有近30萬名網路公安，24小時監看網際網路（互聯網）的國家，面對諸多國家異口同聲質詢時，居然無法將境內大規模的駭客攻擊予以破獲，並繩之以法，究竟是對駭客的包庇縱容或是有所隱瞞？還是上述各個國家簽訂秘密協議，一起誣陷擁有強大貿易市場的中共呢？

二、真相

追查來自網際空間攻擊的證據確實很困難；透過全球化的平臺，任何一點都可能是嫌疑犯，但要密集地集中在中國大陸地區似乎也不容易。雖然中共可以閃爍其詞，但從其處理資安事件的心態便可以看出，中共在處理全球化與資訊安全的事務上，赤裸裸地呈現「自卑」又「傲慢」的心態；自卑心態以民族主義表現，即「外國勢力炒作中共威脅論」為號召，召集國內網民團結一致對抗外侮；傲慢心態則以霸權主義展示，即「毫無所悉」、「我說

註⓰：USA DoD, “Annual Report to Congress: Military Power of the People’s Republic of China”, 2009, http://www.defenselink.mil/pubs/china.html

註⓱：Noah Shachtman, “Under Worm Assault, Military Bans Disks, USB Drives”, Wired, Nov 19 2008, http://blog.wired.com/defense/2008/11/army-bans-usb-d.html

註⓲：University of Toronto, “Tracking’ GhostNet’: Investigating a Cyber Espionage Network”, Mar 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

沒有就是沒有，拿出證據來」等字眼應付外國的指責。

所以我們看到以下的事實：中共境內有大量公開的駭客教學網站、大量的駭客工具與活動、中共會傲慢地反對國外針對網路犯罪的追查、中共還會用民族主義團結所屬的網民；如果可以依據犯罪心理學的推論，我們是否可以得出一個真相：中共是網際恐怖分子的培訓大本營呢？

總之，中共外表不管是經濟或是武力其本質都是掩飾其霸權，其在經濟上的動員不僅收買全世界，也順利的征服其內部矛盾不安的民心；事實證明，人民已妥協於民生，六四天安門事件的民主英雄早已被世人遺忘；經濟讓中共僥倖鞏固其領導的機會，這點中共並不否認，在其「十五計畫綱要」中提到：「發展是解決我國所有問題的關鍵」。

在G20會議上中共已向外表態展露出其意圖領導世界經濟上的野心。另一方面，中共毫不在意加拿大公布其向世界103個國家實施滲透與監視等令人羞惡的事件；事實上，中共早在其國防和軍隊現代化的文件中透露其武裝資訊的動機，更用具體的行動以資訊打造出第二座萬里長城，媲美秦始皇才有的霸氣；絕無僅有、傲慢的心態顛覆國際網路的原始精神和趨勢，而反進化的作為，推翻佛里曼書裡描述的文明，又締造一個崎嶇不平的內部世界；中共和平崛起只是煙幕，爭奪新世紀的霸權才是事實與真相。

結　　論

當諸多的地緣戰略之學者仍汲汲辯論，互相探討驗證中共水面武力威脅是否突破第一島鏈、第二島鏈時，中共的新興力量早已搭乘資訊科技列車，藉網路突穿地域的限制，在世界各國虛擬的疆土上布下深沉而難以拔除的暗樁。

面對全球安全環境的變革，網際安全（Cyber-Security）才是各國所面臨最嚴重的經濟與國家安全挑戰。美國蘭登公司在上個世紀所提及的「戰略性資訊戰」（Strategic Information Warfare ）已於本世紀初，在愛沙尼亞、喬治亞的國土上實踐；每一個國家都應體認到：傳統的地緣戰略與武力戰爭的時代已經過去，「在網路世界，戰爭已經開始」⓳；而戰爭方式已演變成運用戰略性資訊戰結合軍事武力來達成國家目標，新型態戰爭方式已儼然形成。

我國防資訊戰與資訊安全，在這幾年持續不斷的努力，在戰術以下各層級都已具相當程度的能量；然仍須秉持國軍以往不只取得最佳網際安全防衛，而是以能安全的使用網路資源作為網際安全的目標；並且思考如何師法本世紀每場資訊網路戰之精髓，從國內與國際觀點建立完整的國家整體安全戰略，訂定我國家新的戰略作為；國防部則應依政府所訂定之國家戰略作為，結合包括戰規司、聯二、聯三、聯六等多方投入，共同訂定軍事上整體資訊戰與作戰安全等作為，才能有效支持國家整體戰略目標之達成，協助我國在本世紀仍保有全球的競爭優勢。

註⓳：Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency,” (Center for Strategic and International Studies, Washington, DC, December 2008). http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf