TO: ICCL

Invited Keynote-speech in Taipei City, Taiwan

～KALMAGI(卡玫基)～

Academic Tour

(Story setting off in middle July 2008, finished in late Aug. 2008)

王旭正

July 17, 2008

1100 點吧，在忠孝復興捷運站下了車，HY 說著，「老師，在 13 號出口，你可看到我」，我回著說那有出口號碼到 13，這麼多啊。HY 說著「地圖上是這麼說的，不過那是通往東區的地下街，老師您往地下街方向走去，應該就會看到了吧!」多想無義就往那兒走吧，看到了捷運站出口只是 1~5，沒有 13(早在意料中)，然注意著東區地下街，在出口 4/5，嗯這是唯一的線索，就往那兒走吧。走著走著地下街裡裝飾著人文/藝術氣息，很有生氣/活力這是聚集人氣的地方，在東區裡這樣的投資肯定值回票價，因為柔性給人舒緩、輕鬆、解脫的感覺，想多擁有一些，駐足在那兒，多徘徊一刻，商機也跟多了一份機會，Win-Win，遊/走者有了放鬆的心靈、商/推銷者有了說服的間隙，商機活動的互動就拉上了線，地下道的營造環境，那是現代都市迎合著現代人綠色叢林生活嚮往的設計，將擁忙的生活給點輕鬆，也將多些前進的本錢，不正是緩退徐進，引柔克剛的學問/實例，盡在生活點滴裡。

踏著地下街的步伐，望著出口的號碼數 17、16、15、…我猜想 13 不再是個懷疑的數字，只是它不是捷運的出口，而是東區地下街的引道，引到中午的一個飯局，與著學生 HY 的研究討論，與應著下午 invited keynote speech 的熱身準備。在飯局裡我、不，該說是 mobile meeting one-to-one meeting with HY,

my student，談著數位證據/稽核紀錄/入侵偵測/編碼技術，說著 Merkle Tree 能否引用至數位證據與稽核紀錄的連結，那是有趣的一種概念與技術的結合。

「明君賢將所以動而勝人，成功出於眾者，先知也。先知者，不可取於鬼神、不可象於事、不可驗於度、必取於人，知敵之情者也。」有趣之至、說著、何謂先知，其實來自於情報的收集。收集的要則來自於人的善用，而非乞求於鬼神的謨拜，也非憑空的憶測想像，更非求占於日月星辰、龜卜的占筮。對於先知先覺，一直沒有很清楚的了解。總是喜歡戲謔式地說:「慢半拍的人是後知後覺、麻木不仁的是不知不覺，當然可以『洞燭先機』的就是先知先覺囉!」只是這「洞燭先機」的意義為何，實在是說不明白、講不清楚。 「不可取於鬼神、不可象於事、不可驗於度」，排除了神話/魔術的臆想，原來先知的要件在於人啊，難道人有如此神奇的魔力，可以成為先知的要件? 當然得善用謀略的操作之間，那有著因間/鄉間、內間、反間、生間、死間的運用哲學。人啊、人生戲的主角、盡在你我間，有時你是主角、我是配角; 有時我是主角、你是配角; 有時你我只是萍水相逢，在山之隅、海之角。何必相識，彼此牽伴、限制呢? 「鄉間」有著市井小民的情報平實而深刻;「內間」裡有著權力互鬥、矛盾情仇的買通情資，那深宮秘史全都漏;「反間」呢，以其人之道反制其身，本來欲試探情資反倒成了情資的提供者，豈不耐人尋味;「生間」，以親身聽聞傳達最真實的情報，欣見全身而退，圓滿達成任務。「死間」，置死地而後生，有著詐降的學問，得先取得信任再從中從事偽訊/誤信/分化造成猜忌，達成混淆情報。

庭院裡，坐上老位置，那靠椅上沾味著書論。，體會著智慧積萃，留下些痕跡。爾後時而在手卷中，瞥見整理後的文字，在生活的運用與學習，將更多徹底與踏實。不再只是口號，不再只是遙不可止，不再只是試卷中的選項，不再只是講演中的題裁，不再只是說說唱唱，卻從未踐履她。應該是要做得去做，說到

做到。總掛在嘴邊，與著家中的二個小鬼說著:「要求玩具要收好，才能看電視;要求功課要寫好才能玩玩具、騎腳踏車。」「要求要專心吃飯，才能吃糖果。」有許多的要求，也搭配著許多的誘因，做完了，當然即可享受豐美/快樂的欲望果實。那種說到做到的執著，著實得有手腕，也一直在生活/工作中踐履著。在這一天裡，正等著一群兵，從北部殺下海邊，在 KALMAEGI 肆虐後的隔天，在海邊的一隅。

清晨仍有幾陣大雨，拍著窗旁的玻璃，劈哩叭啦做響，正在寫作，想著該會過的。KLAMAEGI 已遠離，所有事都會再回到一個自然風情。熱、盛夏，樹頭的蟬將再競鳴，海邊的潮汐將再湛藍，推漲回退裡，有著長者佇留在沙潮彎尋那原味的貝殼，也正等著一個慶祝活動，學生 PY 與 WY 已從 ICCL 結束 ICCL 該有磨練，進入忠烈祠了。PY，2006 年進來 ICCL，問要做啥? 一般的學生總回答著:「不很清楚」，只是進了一階段，得去知道下一步要怎麼做。前些時候，七月中旬吧，同事的小孩在清大資工念書，大學生念了二年說著以後要考研究所。因為現在大學生畢業生，已經是無法分出職場的勝負，到處都是，也隨著大學開放政策的導向，進大學已成了屆齡青年的全民趨勢，似乎不再有任何限制。此情此景，已截然不同於 20 年前左右的場景，維持 30-5%的錄取率，採優勝餘轉的規則。大學路裡有著基本的素質控管，其餘的，另外有技職體系工作就業的管道，採取分峰節流的做法，控管了質量，也在第一時間引導其它的青年朋友至相關專業，從事未來工作的職業教育/訓練培育。現在呢?所有的青年朋友，一股腦兒擠向同一條大學流路，不斷地擴充水道，對於其中的蝦兒/蟹兒、大魚、小魚已不再能有所掌握，無外乎只能另闢更高的進修路，學制下的研究路對於同事的憂心，似乎小孩無法理解，總嫌著長者的多心/慮。在校園裡的偶遇提了這段際會，所以帶著小孩來到 office 坐坐，喝杯咖啡吧，想必能聊點是非，也能解憂了父母心中的線愁。

Office 說著研究所的存在，其實並非同於大學四年教育的生態，那是得由學生，打從心裡的認知，從裡頭磨鍊一套邏輯訓練功法，從觀察、收集、定義、

關連、方法、實驗/分析比較、延伸、趨勢、結果，林林總總的邏輯性過程所構成的一種訓練課程/研究。跟著同事小孩說著研究所在台灣循著過去教育政策下，或許現在不可避免，大家都走在這波逐流裡。然得清楚一件事，進了研究所，若過著如同過去四年基礎教育的課程修習，意義性不大。應該要清楚這套訓練功法，為你帶來什麼，能產生什麼更大的受益，報酬投資的時間成本，才能實質反映在未來工作/生活挑戰與風格上。另一方面若暫不走入這一遭，大三/四也當涉獵不同主科的學養修習，喜加工作/生活面觀的敏感度，那或許也應了除專業外，歷史、經濟、藝術多元化的人生三樣實的精髓。多些內涵多些機會、多些契機、多所不同、好處多多。談了些經驗，給了些方向，身旁陪著的老爹類類地點頭，客氣地說著:「一席話…如沐春風之類。」倒也不至此，只是藉由這番機會對著年青人講著生活的認知，其實常常與 ICCL-member 在 office/beach/restaurant/car/anywhere meeting 聊聊一些想法，對於下午一席話，或許僅是「倒帶」的一部份罷了，自然而不假思索地移轉到這位年輕人罷了。

…

…

趨勢裡，亦令人想起 IDS(Intrusion Detection System) 的過去不可一世、現在的不可一時，未來的不可一式。因為科技已結合了生活，在生活裡有啥情事，在科技使用裡，就通通會發生，這就是電腦犯罪愈趨勢絡的來由。要能因應此趨勢，不外乎能留下任何蛛絲馬跡，使得事件的發生，能夠完全復原。對於人/事/時/地能全然掌握，那始作俑者能不「破然心驚」，而斷了歹念的企圖嗎!是的，當然是的，從事破壞/窺探者，不外乎能隱藏自己，而愚稅他人，消遙於外。使得證據說話，駐留絕對痕跡，正是一帖最好的藥方。古云裡，有一則典示，倒覺有些適切於公開證據的 power，「摩而恐之，高以動之，微而證之」。其中的微而證之，將所做的小動作，不良行為/痕跡公諸於市場，公開於輿論中，攤在陽光下，讓大家看到了，這不就有了嚇阻效果了。對當事者，對畜意者，不正是一帖驚心破膽猛藥。因為所有原委皆現了形，這是人性最虛慌的一部份，只得緊採煞車。所以趨勢裡，該是證據的存留與否的時代到了，那是早已存在的脈絡，而得釐出新興思唯，因應科技裡，拾得一份保障的作為。

在事件責任裡，總有一句話，正繞在生活/工作話題，「打太極」，影射著推拖閃躲的技倆，不來則已，一旦有著危機入侵，哇!個個的招數推打，漓灑盡致。就以資訊安全事件而言，該反著說「打太極」是渾圓，是分工，所有人皆在其中的渾圓，切出陰陽、二極現了太陽、太陰、少陽、少陰的四象，那即是分工。資

訊人員責任在那，電腦使用人又該如何正確操作，的確是全民有責的太極!此太極之合，完全不同於卸責之話題太極。

最後，說到「服務何之有」。其實服務是種感受，在現代人的工作型式與社會價值觀，已略不同於過去台灣較農村社會的型態。在生活水平已獲實質提升的都市化生活裡，消費型態已併入服務的附加價值，產品的購買，不只考慮外在的價值，也究竟內在/長遠的品質與服務。這已經脫離傳統的「便宜又大碗」的思維，但有可能是殘缺不耐用的夢魘。因此服務已成為資訊安全推銷，亦或各式科技產品得費心耕耘的無形價值競爭力，誰做得好，這塊餅就是誰的。因此多些巧思在售後服務的經營，在推銷資訊安全硬體/軟體機制的同時，必得併入服務品質的保證，以多些外在有形價值換取內在穩定可靠的功能恆久運作，是創造無限價值的支點桿槓原理的服務觀現實版!

站在三樓陽台頂，望向遠方的天際，夜裡星光皎潔，一輪明月高掛在夜空，圓的。屈指一算，那七月下旬當一伙結束了 BBQ 走在北埔車進站的路上，Sajal 指著那正圓的明月對我說著，在印度若月圓所許下的願望的各種故事。在海堤 BBQ 至今，八月近下旬已快一個月了，場景由台西的海岸小屋，換至東北蘭陽平原。山邊一隅，我的故鄉。在這裡將完成 KALMAEGI 的故事。坐在椅上，風不大，拉著延長線，用著電風扇，藉著人工的電力，來感受自然風的吹拂，也免了夜裡飛蟲的侵擾。突想到當蚊蟻叮咬那一瞬間，總有著莫名火湧上心頭，在古云裡亦有著一段話，說著:「夫播糠眯目，則天地四方易位矣；蚊虻噆膚，則通昔不寐矣。夫仁義憯然乃憤吾心，亂莫大焉。吾子使天下無失其朴，吾子亦放風而動，總德而立矣！」我想，此時該心有威威焉。在電力輔助下，風扇取代了自然風，吹走了干擾的蟲蚊，正寫下那尾幕，這個夏暑假期快近尾聲。小鬼們正在趕工那暑假作業，大人們盤算著新學期的施力點，開始佈局/佈樁，為了讓路更平順，

under expectation set!排了一些時程，北上、中部、南下，近來行程，聊聊夢想，在「出走」裡，該有些眉目!

從主機到系統　層層防護建構安全堡壘

強化數位資產安全專家分享秘訣

過往資訊安全都是從網路安全的角度出發，但是目前的攻擊型態與方式已經逐漸改變，從原先以名為主變成以利為主，攻擊者不再是以入侵為目的，而是以竊取機密或高價資料為主。在這種狀況之下，單純的網路防禦已經不足以因應層出不窮的攻擊事件，同時員工的高機動性也讓相關設備一直暴露在不安全的環境中，也讓資訊安全防護更加困難。為了提高資訊的安全性，不但需要強化閘道端的各項網路設備，同時也需要保障主機部分的安全，同時更要建立周延的管理架構才能確保防禦的健全性。

許多資訊安全專家都在呼籲，目前駭客的攻擊方式與目標已經有所改變，企業需要重新思考新的防禦方式及架構。但是對於企業而言，卻並不清楚究竟該如何防禦，防禦那一塊目標，自然也沒有辦法改善現有的防禦架構。

中央警察大學資訊管理學系及研究所 教授 王旭正

因此在本次網管人雜誌主辦的「企業數位資產安全管理論壇」中，便邀請到中央警察大學資訊管理研究所教授王旭正博士，探討企業IT新威脅時代的資訊安全策略，並由台灣二版、趨勢科技、奕瑞科技與精品科技等廠商的技術顧問說明不同技術在不同環節上的防禦措施與功效。

破除資安防護迷霧

王旭正博士在開場之時便引領在座學員重新回顧2007年的資安威脅，讓大家更為清楚現在真正造成威脅的並不是過去常講的駭客或是病毒，而是相反地，由垃圾郵件、間諜程式等惡意軟體及網路釣魚等方式入侵並竊取資料。

其實在2007年資安威脅中，我們就可以發現透過網路釣魚的攻擊方式持續增加，同時網頁應用程式與瀏覽器也是攻擊最主要的標靶。電腦或儲存裝置遺失則是造成資料外洩的主要原因，因遭受入侵而竊取資料的事件反而較少。

不過潛在威脅著資訊安全則是殭屍電腦的問題，截至去年為止，估計中國大陸約有29%的電腦是殭屍電腦，病毒早已入侵，只是不知道什麼時候會爆發。前不久才發生的大量SQL隱碼攻擊事件，就是如此產生的，而其關鍵點在於如何防範電腦遭受入侵且受控制。