

報告（出國類別：開會）

赴加拿大出席核威脅倡議（**NTI**）
核能網路安全論壇推動會議

服務機關：行政院原子能委員會

姓名職稱：洪子傑科長

派赴國家/地區：加拿大

出國期間：107年10月27日至107年11月1日

報告日期：108年1月31日

摘 要

數位網路高度發展後，工業控制系統之資通安全防護成為新興的保安議題，對核能電廠更是重要課題。美國非政府組織「核威脅倡議」(Nuclear Threat Initiative, NTI)有感於目前並沒有全球性核能資安防護技術層面的交流與合作機制，遂推動成立 Cyber-Nuclear Forum (核能網路安全論壇)，目的在提供各國核能資安防護運轉與技術專家一個可以對話、資訊交流、合作及解決問題的機制，將來可能擴大到包括政府、供應商、管制機關、非政府組織等。

本會已要求台電公司參考美國核能法規指引 RG 5.71 訂定「核能電廠關鍵數位資產資通安全計畫」並據以實施，落實核能電廠之資安防護。我國資通安全管理法已於 107 年完成立法程序，健全資安管理的法制規範。我國核子設施資通安全防護的表現獲得國際肯定，NTI 邀請我國參與核能網路安全論壇，及參加論壇推動會議，以確認優先合作項目，建立後續會議的時程草案。

10 月 30 日於加拿大多倫多進行「核能網路安全論壇推動會議」之討論，會議議程包括核設施常見/共通資通安全挑戰、現行國際和國內的合作機制回顧、國際合作優先項目的確認、研擬 2019 年論壇會議的議程，及如何使論壇永續。我國與會代表於會中發表簡報，提出我國對於成立論壇的相關意見，也表達我國希望在論壇的籌備及參與上有所貢獻。

目 錄

摘 要.....	1
目 錄.....	2
壹、目 的.....	3
貳、行 程.....	4
參、會議概要.....	5
一、緣起.....	5
二、NTI 簡介.....	7
三、上午會議概要.....	8
四、我方簡報概要.....	11
五、下午會議概要.....	16
六、Nuclear Weapons in the New Cyber Age 簡介.....	19
七、Outpacing Cyber Threats (初稿) 簡介.....	20
肆、心得與建議.....	22
附 件：	
附件一：Nuclear Weapons in the New Cyber Age 報告封面.....	23
附件二：會議議程與討論簡報.....	24
附件三：我方於會議中發表之簡報.....	29
附件四：Outpacing Cyber Threats (2018)初稿封面.....	36
附件五：Outpacing Cyber Threats (2016)封面.....	37
附 圖：	
圖一：會議成員合影.....	38

壹、目的

美國非政府組織「核威脅倡議」(Nuclear Threat Initiative，以下簡稱 NTI)有感於工業資通安全的威脅日益嚴重，而目前並沒有全球性核能資安防護技術層面的交流與合作機制，遂推動成立 Cyber-Nuclear Forum (核能網路安全論壇)，目的在提供各國核能資安防護運轉與技術專家一個可以對話、資訊交流、合作及解決問題的機制。

論壇的推動，展現全球核能工業已經體認到資安威脅的嚴重性，並願意在核能資通訊的安全與保安上善盡責任。我國身為使用核能的國家，理應將我國實施經驗與面臨問題貢獻國際社會。藉由參與推動會議及後續的大會，與各國專家交流，可以完整了解核能資通安全防護趨勢與面臨之威脅，以強化我國核能資通安全防護之管制作業。

我國參加論壇推動會議，成為論壇發起國，得以獲取核能資通安全防護技術趨勢、實務做法、面臨威脅與實際案例的第一手資料，可完整了解最新防護機制與管制措施。藉由與各國專家交流，可促進技術合作及問題解決，有助於提升我國核設施資通安全防護之強固完整性與本會之管制作業效能。

貳、行程

此次赴加拿大出席「核威脅倡議」(NTI)核能網路安全論壇推動會議，於 107 年 10 月 27 日搭機離台，當日抵達加拿大多倫多市。10 月 29 日晚上主辦單位於多倫多市區餐廳，以非正式晚宴招待各國與會專家，並進行初步討論。10 月 30 日於 Fairmont Royal York Hotel 會議室，全天進行核能網路安全論壇推動會議。10 月 31 日搭機返台。

詳細行程如下表：

日期	地點	工作內容
10 月 27 日	台北→多倫多	去程
10 月 28 日	多倫多	週日
10 月 29 日	多倫多	晚宴及討論
10 月 30 日	多倫多	會議
10 月 31~ 11 月 1 日	多倫多→台北	返程

參、會議概要

一、緣起

107 年 8 月 23 日「核威脅倡議」(NTI) 的 Page Stoutland 博士來信邀請我國參加「核能網路安全論壇」¹ (Cyber-Nuclear Forum, 以下簡稱「論壇」), 希望我國派遣一位核能電廠網路專家參加這個尚在構想中的國際組織, 以推動核能網路安全合作交流。經簽陳主任委員同意由本會核能技術處核子保安科洪科長子傑(作者)與會。人選決定後, 透過駐美代表處回復 NTI。

9 月 20 日 Stoutland 博士來信說明「核能網路安全論壇」的成立構想, 也是召開這次推動會議的緣由:

「核能網路安全論壇」成立目的在提供各國從事核設施資通安全防護、運作與技術研究層面的專家對話與合作的場合。目前並沒有這樣的機制。國際原子能總署 (IAEA) 雖有促進核能資通安全防護國際合作的機制, 但是定位在國家與政策層級。這個論壇希望聚焦在營運、操作與技術研究方面的第一線專家對話, 尤其在預防及應變對於核設施運轉系統 (Operational Technology, OT) 的資安攻擊。

論壇的目標在建立一個推動並使國際核設施資通安全防護在技術及運轉層面上可以合作的機制。因為對核能電廠控制系統一次成功的資安攻擊, 可能造成極嚴重的後果, 資安防護對於各類核設施都很重要, 尤其對於在新興國家缺乏資安防護的核設施。這個論壇和 IAEA 推動的資通安全防護國際合作是互補的, 因為 IAEA 並未聚焦在運轉及技術層面。而「世界核能發電協會」(World Association of Nuclear Operators, WANO) 著重於核能安全的合作, 對於核子保安與資通安全並沒有實質的推動。「世界核子保安協會」(World Institute for Nuclear Security, WINS) 雖然有舉辦過幾次資通安全訓練及研討會, 但並沒有常設的交流論壇。

¹本報告將 cybersecurity 譯為「資通安全」, 雖然部分文獻使用「網路安全」, 但因核能工業界的資通訊安全問題絕大部分不是透過網路造成的, 因此使用比較廣義的「資通安全」。而 Cyber-Nuclear Security Forum 仍沿用「核能網路安全論壇」名稱。

「核能網路安全論壇」的願景在提供各國核設施資安防護運轉與技術專家一個可以對話、資訊交流、合作及解決問題的機制，參與成員將來可以擴大到包括政府、供應商、管制機關、非政府組織及其他機構。論壇的推動，也展現全球核能工業已經體認到資通安全的嚴重威脅，並表達願意在核能資通訊的安全與保安上善盡責任。為支援此目標，NTI 願意提供幕僚在論壇內建立合作機制及特定的交流議題。隨著時間演進，NTI 在論壇的角色將逐漸轉換由工業界接續承擔。

論壇的發展是漸進、分階段的。初始階段，NTI 規劃在 1 年到 1 年半期間，舉辦 3 次會議。2018 年 10 月 30 日是第 1 次會議（即本次出國參加的會議），定位為小型推動會議（steering meeting），規劃約 6 到 8 位成員，目標在於確認優先的合作項目、建立在 2019 年召開更多方參與的較大型會議的時程草案。所以這個推動會議是論壇成立的第一步，希望集思廣益，建構在大會中討論的議題。目前規劃的討論構想是：

- 那些是全球共同關切的核能資通安全議題，透過國際間合作交流最有用？
- 國際間合作交流存在那些障礙？如何強化合作？需要建立什麼新機制來強化合作（例如資訊交流共同對抗資安威脅）？論壇能提供那些協助？
- 對於供應鍊議題，國際合作交流能提供那些有價值的幫助？
- 需要雙邊互助協定嗎？或成立資安事件應變夥伴關係？在這些領域，論壇應該扮演什麼角色？

後續的工作計畫和會議，會由初始階段的經驗與討論所得慢慢建構出來。等論壇發展得成熟一些，更多國家和相關機構，例如供應商和研究機構，可以加入。論壇的終極目標就是建立一個由核工業界領導，永續經營的常設組織，在協助核工業界的資通安全防護上扮演重要角色。因為核能資通威脅持續增強，攻擊與入侵技術也一直在進步，防護與應變措施更應該保持精進，走在惡意威脅之前。

NTI 將組織和召開論壇的第 1 次會議。會議議程將由推動會議和 NTI 共同決定。創始會員將由世界各國的核設施經營者和資通安全工作者開始。目前有 45 個國家

有核子設施，希望參加會議的成員是各核子設施（主要是核能電廠）的資深資安專業人員或主管，例如資安長（Chief Information Security Officer, CISO）或核電廠電算組經理等，以聚焦在資安防護運作及技術層面的交流與討論。

NTI 已經獲得幾個國家的核子設施資安首長表達意願加入論壇，這些國家包括美國、加拿大、法國、英國、南韓、荷蘭及芬蘭。其他國家尚在接洽中。

第 1 次的論壇推動會議於 2018 年 10 月 30 日召開，籌備、開會及參加會議人員的差旅規劃與費用由 NTI 負擔，而後續的論壇籌備會議參與者將自付費用。

二、NTI 簡介

「核威脅倡議」（Nuclear Threat Initiative, NTI）是一個總部設立於美國華盛頓的非營利組織，其使命為致力於防範全球遭受化生放核大規模毀滅性武器（Weapons of Mass Destruction and Disruption, WMDD）災難性攻擊而釀成的事故，包括網路攻擊。該組織成立於 2001 年，發起人為前美國參議員 Sam Nunn 及 CNN 創辦人 Ted Turner。目前兩位發起人及前美國能源部長 Ernest Moniz 博士為 NTI 的三位共同主席，Moniz 博士兼任 NTI 執行長。

2008 年 NTI 協助創立「世界核子保安協會」（World Institute for Nuclear Security, WINS），其願景是讓所有核子物料、放射性物料及核子設施都得到具專業能力人員的有效保護，並協助核子物料、放射性物料和核設施經營者以最佳做法實現永續的營運，最終達到提升國際整體核子保安的目標。該協會目前的主要業務為推動核子保安管理專業訓練及發展核子保安認證制度，並透過與其他核產業相關對象（包括國際原子能總署 IAEA、電力公司、核能電廠、管制機關及非政府組織等）的合作，逐步達到其中長程目標。該協會目前有來自 118 國約 3800 位會員，共同研商、交流及合作以達成促進核子保安的目標，其成功經驗也被拿來作為「核能網路安全論壇」創建的參考。

NTI 自 2012 年起，與經濟學人智庫（Economist Intelligence Unit, EIU）合作，

每兩年出版一次 Nuclear Security Index，評比世界各國核子保安狀況，已具有國際聲望，對促進世界核子保安與核物料管制有所助益。

三、上午會議概要

10月30日於 Fairmont Royal York Hotel 飯店 19 樓包廂會議室舉行一整天的核能網路安全論壇推動會議。

早上 8 點半抵達會議室，座位已經排定，每人桌上放著四樣文件：一本 2018 年 NTI Nuclear Security Index 報告、一本 NTI 出版的 Nuclear Weapons in the New Cyber Age（見附件一）、一份會議議程卷宗夾及一張差旅費用結報單。

早上 9 點開始開會，共有 9 人與會，除作者外的 8 位介紹如下（最後兩位為主辦單位 NTI 代表）：

姓名	職務
Tim Collier	加拿大安大略電力公司（Ontario Power）核能部門電算經理
Nathan L. Faith	美國Exelon電力公司核能部門資通安全經理
Scott Hilts	加拿大布魯斯電力公司（Bruce Power）核能部門電算經理
Anno Keizer	URENCO核燃料公司荷蘭分公司保安經理
Christophe Martin	法國EDF電力公司資通安全部門資深執行顧問
John Sladek	加拿大Lofty Perch資安技術公司資深保安顧問
Page O. Stoutland	NTI科學與技術事務部門副總裁，本次會議主席
Erin D. Dumbacher	NTI科學與技術事務部門專案經理

Stoutland 博士先自我介紹，他在 NTI 工作 8 年，工作領域在核武器與核設施資通安全、核子保安評比、大數據分析，及強化與中國大陸及俄羅斯技術合作等業務。然後簡要介紹 NTI，說明 NTI 對於核生化的威脅都做研究，再講述召開這個會議的緣由與目的（如前文所述）。近年來資通安全的議題引起相當大的關注，無論在核武器或核設施都會產生重大的影響。幾年前 NTI 開始做 Nuclear Security Index 評比，將資通安全項目納入。NTI 認為這個議題需要國際合作，而且著重在技術與操作層面的人員對話。NTI 希望成立 Cyber-Nuclear Forum，可以讓這些專業技術人士對話和合作。這個論壇

可以有很多運作模式，就是今天這個會議要討論與激發創意的。今天是論壇第 1 次起頭會議，希望 2019 年能擴大規模，召開大約 40 到 50 人的會議。

接下來主持人先請與會人士自我介紹並發表對於資通安全合作機制的意見。來自荷蘭的 Anno Keizer 認為核設施資通安全資料的分享有機敏性，但 IAEA 的資安交流則沒有。他認為資通安全合作交流和實體保安一樣，要看好處在哪裡？優先性何在？一般而言，保安和資安工作平常是看不出來績效的，如果不能說服主管資通安全的重要性，是不容易拿到經費的。

為使會議的討論依循規劃進行，聚焦於主軸，主辦單位製作一份討論題綱簡報（見附件二）。開場後，主持人依以下簡報題綱引導討論：

- 核設施常見/共通資通安全挑戰（Common Cybersecurity Challenges at Nuclear Facilities）
- 現行國際和國內的合作機制回顧（Review of Existing Cooperative Initiatives, International and Domestic）
- 國際合作優先項目的確認（Identifying Priority Areas for International Cooperation）
- 研擬 2019 年論壇會議的議程（Developing an Agenda for 2019 Forum Meeting）
- 如何使論壇永續（Making the Forum Sustainable—Building Support and Buy-in）

9 點半開始進行第一個議題：「核設施常見/共通資通安全挑戰」（Common Cybersecurity Challenges at Nuclear Facilities）的討論。主辦單位事前規劃由以下幾個方面進行討論：

1. 越來越複雜的資安威脅環境：資訊軟體與硬體進步迅速，攻擊與入侵技術日新月異；
2. 受限的資源：防禦方的資源受限，包括人力與技術難以取得；
3. 難以取得上級長官的認同和支持：資通安全沒發生事情就是績效，所以績效是感受不到的，難以說服上級投注資源；
4. 跟不上技術潮流的管制環境：主管機關的技術能力跟不上工業界和駭客的能力，卻要執行過時的管制措施；

5. 不充分的溝通協調，包括企業與政府，及企業對企業的。

經過討論，與會專家還提出其他的挑戰與困境：

1. 發展企業的資通安全文化；
2. 為了處理危機，必須在危機發生前知己知彼；
3. 管制機關的立場；
4. 同業評估的困難，例如 WANO 在核能安全扮演的角色，必須先確認業界領導者；
5. 資訊界講的「風險架構」(Risk Framework)的溝通，這和資源及預算有關。資通安全不是一個專案型的工作，做完就結束，而必需要持續不斷，有計畫，長期的實施。但是風險架構只是一個評估，難以說服上級。
6. 由前項引伸，資通安全是一個方案 (Program)，而不是一個專案 (Project)，所以需要人力、程序和計畫。
7. 最佳實務做法 (best practice) 何在？安全餘裕 (safety margin) 何在？品牌 (branding) 和資產保護 (asset protection) 的 know how 企業間都不會分享，何況是網路上？
8. 「工業標準」對比於「管制標準」，其間有落差 (gap)。
9. 論壇和 IAEA 機制的功能有何不同？差距多大？是要全公開還是組成聯盟？信任非常重要，要能長期運作。
10. 資通安全的設計基準威脅 (Cyber DBT) 為何？是可能的 (possible) 還是不曾發生但似乎合理的 (plausible)？
11. 實施上共通的弱點，例如法國由管制機關設定資通安全演練劇本，如前所述，有與現實脫節的問題。

休息後，10 點 30 分接著討論第二個議題：「現行國際和國內的合作機制回顧」 (**Review of Existing Cooperative Initiatives, International and Domestic**)。由於與會有三位加拿大業者，所討論的國內合作機制指的是加拿大核能電廠使用的 CANDU 反應器業者組織 (CANDU Owner's Group)；而國際合作機制方面，以 NISGS (Nuclear Industry Steering Group for Security) 為例，這是核能工業界為促成核子保安合作與交

流而組成的組織。

討論中談了許多核能及保安國際組織的合作交流做法。由於我國沒有參與大部分國際組織，對這方面沒有經驗。其中談到 INPO 及 WANO 在資通安全的技術協助相當有限。INPO 和所屬的 Nuclear Information Technology Strategic Leadership (NITSL) 每年舉辦 1 次資通安全及數位控制系統研討會 (workshop) 分享最佳實務做法 (best practice)，參加者多為資安、電算或儀控同行，可能會後仍保持聯絡交流，但是並沒有建立策略性的交流機制。也提到三哩島 (TMI) 事故後催生了 INPO，車諾堡事故後催生了 WANO，其驅動力及初始組織與程序可做為成立論壇的參考。WINS 主辦的訓練或研討會是一次性，沒有後續的交流機制；WINS 學院則有開設資通安全課程。世界核能協會 (World Nuclear Association, WNA) 對於核子保安的著墨相當有限。再討論到「核能協會」(Nuclear Energy Institute, NEI)，NEI 只在美國運作，以專案小組或合約方式進行，而且 NEI 主要致力在政策層面，或與管制機關交涉，並不在技術層面，有關資通安全的工作是成立專案小組處理管制議題。加拿大方面，CANDU 反應器業者組織是應管制機關的要求而成立，協助制訂加拿大核能國家標準，但其成員並不熟悉資通安全，也就是說，資通安全管制與技術標準與現實狀況是有落差的。Canadian Standard Association 有資源制訂新的工業標準，但還沒關注到核能資安。

主席 Stoutland 博士認為多個組織可以共同合作，但大部分核能組織都還沒有注意到資通安全對核能工業的重要性。有人認為核能資通安全需要做更多的研究開發。

與會人員的共識是目前核能資安防護領域，基本上沒有國際合作交流機制，而且也沒有著力於解決前文提出的諸多挑戰與困境。幾個國際核能組織，包括 NISGS 及 WINS 等致力於核子保安的組織，都還沒有特別關注資通安全議題。

四、我方簡報概要

作者在行前即已針對這次的會議議題，蒐集台電公司電算部門的經驗與意見，綜合本會管制立場製作一份簡報，預備在會議中表達我國希望在論壇的籌備及參與上有所

貢獻。經向主席及與會成員表達，取得同意，安排於下午時段進行簡報。

中午午餐休息後，開始進行下午的議程，先由作者自 12:45 到 13:05 進行簡報（簡報檔見附件三）。簡報前作者先聲明，簡報係依據會議議程的討論主題預先製作，今天的討論只進行到一半，但簡報中要談的已經包括全部主題，已經討論過的係再陳述我方意見，還沒討論的就先提出台灣的意見。預期與會人員對於台灣並不熟悉，所以在簡報開頭先介紹台灣核能工業現況，果然引出一些相關詢問，包括台灣地理特性等問題，均逐一回答。

接下來說明台灣 3 座運轉中核能電廠已經在原能會管制要求下，依據 NRC RG 5.71 精神從技術面、操作面、管理面等三方面落實關鍵數位資產資通安全防護。台灣的核能電廠未發生過網路或資通攻擊事件。台灣有「電腦網路危機處理暨協調中心」（CERT），也就是 TWCERT/CC，在行政院資通安全辦公室指導下運作。2018 年 5 月，資通安全管理法完成立法程序，將於 2019 年施行。依據這項法律，關鍵基礎設施應備有資通安全計畫，關鍵基礎設施發生資安事件應通報行政院資安處，TWCERT/CC 有義務協助處理。在台灣，核能電廠為一級國家關鍵基礎設施。

然後就會議議程的討論主題說明台灣的意見：

1. 那些全球共同關切事項，國際間合作交流最有用？

由於數位設備的使用增加，核設施面臨更多的資安威脅，導致資通安全計畫必須考量更多方面的威脅，例如社交工程技術、移動式數位裝置和其他創新工具。在分享處理資通攻擊的經驗上，跨國合作交流很有用，但也不應僅限於分享受攻擊的經驗。因為台灣核能電廠數位化控制系統之架構與運轉維護方式，受到來自於網際網路外界攻擊之可能性很低，所以案例不多。其他可交流的領域建議包含：

- (1).人員資安意識的強化及組織資安文化的建立。
- (2).資安防護架構與機制的強化：如網路分層管理、落實執行人員存取管制以及可攜式儲存媒體管控等。

(3).資安管理系統的建立，但要提出的問題是：

- A. 依據何種規範或標準？如ISO-27001、RG-5.71、NEI-08/09、NERC CIP V5、IEC 62433-3-3 或 NIST SP 800-82 等。
- B. 如何實施及遵循規範或標準？
- C. 如何維持管理系統的有效性？內部稽核、外部稽核或像BSI（英國標準協會）的獨立第三方驗證？

(4).採用新的防護方法（技術面或行政管制面）：運用新型的資安設備或採取新型態資安威脅的因應措施。

2. 國際間合作交流存在那些障礙，如何強化合作？論壇能提供那些協助？

業界資訊交流的障礙可能有：(1)業者擔心負面的經驗有損名譽；(2)可能洩漏營業機密，所以有些國家可能不願完全分享對抗資通安全事件的經驗或知識。論壇可以在提供收集及分享有用資訊的平台上扮演關鍵角色。以 WANO 的事件報告方案

（WANO Event Report, WER）為例，論壇可以鼓勵成員分享他們資通安全相關（如網路攻擊）的事件報告。此外，如 WANO 的「重要事件報告」（Significant Event Reports）做法，論壇也可以在成員有需要知道的「緊急議題」或「最新趨勢」上採取主動提供。

■ 就「緊急議題」而言，例如當設備廠商傳出重大軟體漏洞時，我國「行政院國家資通安全會報技術服務中心」（簡稱技服中心）除在網站上公告外，也會在第一時間發送通知信件給各單位資安連絡人，告知影響平台（如何種作業系統）、影響等級、建議措施、參考資料等。不過技服中心發佈的是一般性的資安警訊，論壇則可專注於工業控制系統（ICS）設備或相關系統。

■ 就「最新趨勢」而言，論壇可根據成員回報自身所經歷的資安事件加以分類並歸納統計，也可以透過論壇的協調整合，收集其他資通安全組織所發布的統計資料，定期彙整成趨勢分析報告，例如最近一季或最近半年以來業界工業控制系統設備曾遭受到的攻擊或威脅之相關資訊，可讓論壇成員及早因應，採取適當的管制措

施或採購合適的設備予以防範。例如台灣行政院技服中心定期發布的監控月報，就是一種具體的趨勢分析報告。

3. 對於供應鏈議題，國際合作交流能提供那些價值？

從正面的方向看，因為資通安全是一直在演進的議題，數位設備供應商最了解這些威脅，也具有豐富的經驗。讓供應商參與論壇，不僅可以提供強化安全與解決問題的方法，也可直接了解用戶端的問題與需求，可說合則雙利。但是從負面的方向思考，極少部分的供應商是懷有惡意或是疏忽造成漏洞來源（例如台積電事件）。是否數位設備的檢證（並建立具公信力的檢證系統）與資訊交流是可行的呢？實際上，工業控制系統設備的網路資安檢證（或驗證）是可行的，例如目前國際上已有 **NSS Labs**、**ICSA Labs** 等具有公信力的機構專門針對網通安全產品如防火牆（**firewall**）、入侵防範系統（**Intrusion Prevention System, IPS**）等進行檢測，甚至連物聯網安全及隱私（**IoT Security & Privacy**）也可以檢證。目前台灣政府機關採購網路安全設備應該都會要求廠商提出產品通過 **NSS** 或 **ICSA** 檢證的證明文件，例如共同供應契約已加入以下規格要求：「原廠 **IPS** 技術能力須獲得 **NSS (Network Security Services) Group** 或 **ICSA (International Computer Security Association) Labs** 對於 **IPS** 產品類別之技術能力證明文件，以確保 **IPS** 產品之防禦能力，並提供相關檢測認證證明文件以供審查」。

4. 互助協定或夥伴關係對於資安事件應變有效益嗎？在這方面，論壇應該扮演什麼角色？

對於互助協定，論壇必須明確定義雙邊有限的權利義務關係，供論壇成員遵循。讓缺乏資安防護技術的論壇成員，可以得到協助。另一方面，分享的資訊是機敏且為商業機密，必須遵守保密規定。有嚴謹的規範，論壇成員才願意揭露及分享其經驗及技術，從而強化資通安全防護能量。所以論壇要研擬全體成員能接受的權利義務協定，如果有利益衝突，論壇必須扮演仲裁者的角色，這也需要有明確的規範。

思考論壇成員間可能做攻防演練嗎？或是類似 WANO 的 Peer Review？攻防演練由於攻擊方可能會窺探到防守方的詳細資安防禦部署，除非雙邊互助協定能有非常嚴謹的保密協約，而且論壇能確保落實保密協約，否則攻防演練應該不太容易被論壇成員所接受。WANO Peer Review 的確是一種比較可行的做法，但 Peer Review 是以績效目標為導向的評估活動，有一套嚴謹而且被核能業界認可的績效評定標準（Performance Objectives and Criteria, PO&C）供所有成員遵循，論壇若要參考 WANO Peer Review 的做法，可能要先建立類似 WANO PO&C 的標準規範。

WANO 還有一種提供會員服務（Member Support Mission, MSM）的制度，其前身是 TSM (Technical Support Mission)，這種制度可供論壇參考，亦即由論壇成員提出支援需求（可以是技術面或管理面的），由論壇協調找出成員中的專家組成一個團隊，至需求方進行訪談及討論，讓需求方可在短期內吸收到其他成員成功的技術及經驗，而且講授內容由專家自行決定，不致有機敏資訊外洩的疑慮，因此 MSM 方案應是技術交流較為可行的做法。

簡報最後提到台灣對於論壇的建議及預期效益。在討論議題的方面，因為台灣運轉中的核能電廠都已營運超過 30 年，電廠重要的控制系統早期大多屬於較舊型的類比式設計，雖然有部分控制系統更新為數位化控制，但架構上還是維持原有類比式的獨立運作方式。論壇成員中像台灣這種型態的電廠，其採取何種策略建立重要數位設備的資安防護，是值得相互交流的議題。因此建議論壇成立討論群組，可就運轉已久的部分數位化核能機組的資安防護經驗與技術，進行交流分享。另外，也建議論壇可比照一般研討會型式，邀請幾位專家擔任主講人（keynote speakers），針對工業控制系統網路資安新知或重大趨勢進行演講，其餘時間則可以依主題安排不同的 session，由廠商或論壇成員介紹並進行討論。

簡報結束後，與會專家提出幾個問題，簡述如下：

1. 所謂資安文化的推動是指組織或個人？回答：兩者兼顧。
2. BSI 是什麼？回答：British Standards Institution。

3. 台電公司曾經申請 WANO PO&C 的資安協助嗎？回答：有。台電公司是 WANO 的會員，隸屬 WANO 東京中心，如果有任何支援需求，就向東京中心提出申請，東京中心會根據需求內容，轉達給 WANO 其他中心或亞洲地區的會員，請他們提供協助。台電公司 2016 年曾提出「關鍵數位控制系統資安防護技術支援 (MSM)」要求，特別希望獲得美國同業的經驗分享，但是不巧美國只有亞特蘭大中心一位專家可以去，東京中心則邀請日本島根電廠的資安專業人員參與。也因此得知日本核能業界目前重點在強化機組安全設計改善，爭取電廠重啟再運轉，當時尚未著力於關鍵數位化控制系統的資安防護計畫。依據台電公司說法，那次 MSM 基本需求有達到，但認為若有實務經驗比較豐富的美國電廠人員參與，其成果將更顯著。

五、下午會議概要

下午進行第三個議題討論：「國際合作優先項目的確認」(Identifying Priority Areas for International Cooperation)，其實討論範圍不限於國際合作，只要是核子設施尋求外力支援的都算。

主辦單位預規劃幾個可以討論的技術主題：

1. 降低複雜度：如(1)確認數位化帶來的保安利弊得失；(2)限縮未知的因素；(3)減少互聯的系統；(4)透徹了解系統特性並加以評估；(5)旁通數位監視和控制的可行性。
2. 建立主動防護：如(1)從靜態防護到主動防護；(2)全時防護；(3)網路監視和應變；(4)緊急事件應變計畫；(5)在防護技術和緊急應變能量上的投資。
3. 將資通安全意識植入於設施的文化及程序：如(1)管理和團隊；(2)跨企業的功能和協調；(3)建立資通安全文化；(4)採取持續改進的做法。

與會者在這個主題的討論中，提出幾個可以深入討論的議題，包括：

1. 共通的關鍵績效指標 (KPI)；
2. 建立與強化資通安全文化；
3. 為資安營運和資安文化發展任務計畫 (mission scheme)；

4. 合理且可溝通的風險架構及風險評估；
5. 如何設定技術議題小組，或是結構上的分組；
6. 組織管理（因為有些機構太龐大），包括管理系統和能量，這部分 IAEA 有相關文件；
7. 建立分享機敏資訊的模式；
8. 供應鍊管理：(1)合約條款；(2)標準化（如同核能安全）；
9. 技術議題：(1)雲端；(2)系統單晶片（SOCs）；(3)可攜式媒體；(4)二極體等；
10. 緊急尋求支援與協助的管道；
11. 系統評估方法。

歸納出幾個大主題：就是資安文化、管理，和技術。

下一個主題是「研擬 2019 年論壇會議的議程」(**Developing an Agenda for 2019 Forum Meeting**)。經過討論，要有充足的討論時間，原則為 3 天會議，人數約 40 人（IAEA 的供應鍊會議約 120 人），由 NTI 挑選，使世界各地區都有代表參加，成熟使用核能的國家和新興國家都應該有代表，以兼顧多樣性（Diversity）。除了專業技術人員外，也應包括管理階層。不提供同步口譯。會決定 8 到 9 個論壇主題，剛開始用大主題（General Topics），以後再決定須深入探討的特定主題。

最後一個討論主題是關於「如何使論壇永續」(**Making the Forum Sustainable—Building Support and Buy-in**)，也就是尋求財務支援。請各與會者（大都來自電力公司）思考以下問題：

1. 如何讓你所屬的組織支持你或你的同事繼續參加論壇？
2. 什麼資源或服務是一個協調組織者（coordinating body，指 NTI）必須提供？
3. 為何 NISGS 的資通安全分組在 2016 年後未被合併？
4. 可向那些管道尋求財務支援？
5. 你會在公司內部和外部對論壇作宣傳嗎？

經討論，認為有以下幾個理由（也就是論壇的價值），必須為論壇籌措永續的財務

支援，以讓論壇永續發揮功能：

1. **尋求並保持核能資通安全防護的技術領先管制機關。**管制標準不同於工業標準或最佳實務做法，也就是不能依賴管制機關的作為讓業界免除資安威脅。國際合作交流是一種「自我管制」的做法，意即業者自主提升自我防護技能，才能超前部署，走在威脅之前。這樣的超前防護思維，比起被動回應新的管制要求，或在發生資安危機或事故時才採取應變措施，都要節省經費與資源；
2. **為潛在的資安危機作準備。**全球的核能資安專家都應該有機會彼此認識，互相幫忙，為未知的潛在資安危機做好準備。核能資安危機的問題不是會不會發生，而是何時發生。WANO 和 INPO 都是在核災發生後才成立，但是現在核能工業界應該更主動，不要等到重大的資安事件發生才第一次合作解決；
3. **交流最佳實務做法，增進全球核設施的資通安全。**核能資通安全做得好，有助於提升核能的良好專業形象。以當前的國際社會與媒體資訊快速交流的環境，如果一個國家發生核能事故，全世界核能工業界都會受到負面影響。如果論壇發揮功能，提升整體核能資通安全技術品質，整個核能工業界都會因此受益。

至此，完成會議規劃的議題討論，結束論壇推動會議議程。NTI 的 Dumbacher 女士宣布，會議議程簡報檔將寄給與會專家。她也向作者索取發表的簡報檔，表示將寄給每位與會人員參考。

會議後作者詢問主持人為何本次會議亞洲只邀請台灣參加？他回答亞洲主要使用核能的國家中，NTI 有邀請韓國，但因韓國代表另有要務而不能前來；曾考慮邀請日本，但因一些理由而決定不邀，所以這次只有台灣代表出席。

會後與 Dumbacher 女士談到 NTI 近期在核能資通安全的研究工作，她說目前在撰寫一份報告，名稱為 **Outpacing Cyber Threats**，對核能工業界的資通安全威脅進行研析，並提出概念性及規範性的建議，然而報告尚未完成，他將手邊的初稿紙本送給作者，並承諾會將初稿檔案寄給與會人士參考。

下午 4 點 30 分結束會議，於會議室外合影（見圖一）。

六、Nuclear Weapons in the New Cyber Age 簡介

關於 NTI 致贈出版之 Nuclear Weapons in the New Cyber Age（新網路時代的核武器）（附件一），內容簡介如下。

NTI 在 2018 年出版此報告，作為網路-核武研究小組（Cyber-Nuclear Weapon Study Group）第一期研究成果報告。Stoutland 博士為作者之一。這個小組在 2016 年成立，成員包括退休的政府高階官員及軍事將領、資通訊專家、核武專家及核能專家等。小組的任務在探討核武系統的網路資通弱點，並提供建議以減少弱點及降低遭受網路攻擊的後果嚴重度。第一期研究聚焦在美國的核武系統，其他國家的問題將在第二期進行。

如同核設施，核武系統如果遭到成功的網路入侵或資通攻擊，將造成災難性的後果。例如，成功的網路入侵或資通攻擊，可能造成核武指令、控制與通訊系統不可信賴，產生假的攻擊警報，而採取錯誤的反擊行動，引發大規模的軍事行動。

研究小組以下列 4 個情境探討核武系統的資安風險，並研究發生這種情境的可能性，從而思索如何加以防範：

1. 發生危機時，預警系統提供假的核武攻擊警報；
2. 資通攻擊摧毀指揮官和核武系統操作者間的通訊系統，以及與他國的通訊；
3. 有心人士透過供應鍊將缺陷或惡意程式植入核武系統，破壞系統功能；
4. 有心人士以網路入侵或破壞保安裝置的方式，未經授權而操控核武器。

本報告的結論之一是，即使核武系統的資通安全防護措施非常重要，也必須很嚴謹，但是對於關鍵系統並無法提供足夠的資安防護，因為不法人士的心思縝密且入侵技術持續進步，因此建議必須裝置多重多樣的（包括非數位）控制與通訊系統，以降低資安風險。

七、Outpacing Cyber Threats (初稿) 簡介

關於會議後 NTI 的 Dumbacher 女士致贈之 Outpacing Cyber Threats (先一步防範資通安全威脅) 初稿 (附件四), 內容簡介如下。

此報告作者為 Stoutland 博士及 Dumbacher 女士, 尚未正式出版, 目前提供的是初稿。

NTI 在 2016 年也出版過一份同名報告 (附件五), 對核產業界提出 4 個概念性的優先建議, 如果核設施實施這 4 個概念, 其防護和技術就可以超越資安威脅, 有效保護設施免於資通安全攻擊。這 4 個優先建議是:

1. 資通安全防護制度化: 建構堅實的資通安全設備與程序, 並執行品質管理方案。
2. 採取主動式防禦: 防護措施與應變計畫必須跟上趨勢, 與時俱進, 人員訓練與跨機構合作也是必要的。
3. 降低複雜度: 核設施數位系統太複雜會增加保安困難度, 重要設備可考量使用非數位控制系統。
4. 追求轉型: 資安威脅為新型威脅, 以前的數位系統沒有資安考量, 且太複雜造成防護不易, 應以兼顧防護功能轉型建構資安系統。

新版報告 (初稿) 將這些行動建議轉化為規範性的行動。提出三個原則:

1. 降低複雜度:
 - (1) 權衡數位化的好處 (可靠、精確、功能、效率等) 和保安風險;
 - (2) 了解數位系統, 辨識關鍵組件, 簡化設計, 減少未知之處;
 - (3) 減少互連系統數目;
 - (4) 嚴謹地分析與評估系統;
 - (5) 讓數位監視及控制系統可以旁通, 或建構監視及控制系統異質多樣性。
2. 建立主動防禦:
 - (1) 從靜態防衛轉型到主動防禦;

- (2) 持續防禦；
- (3) 網路監視和應變；
- (4) 建立緊急應變計畫。

3. 將資通安全認知融入於設施組織文化的與程序中：

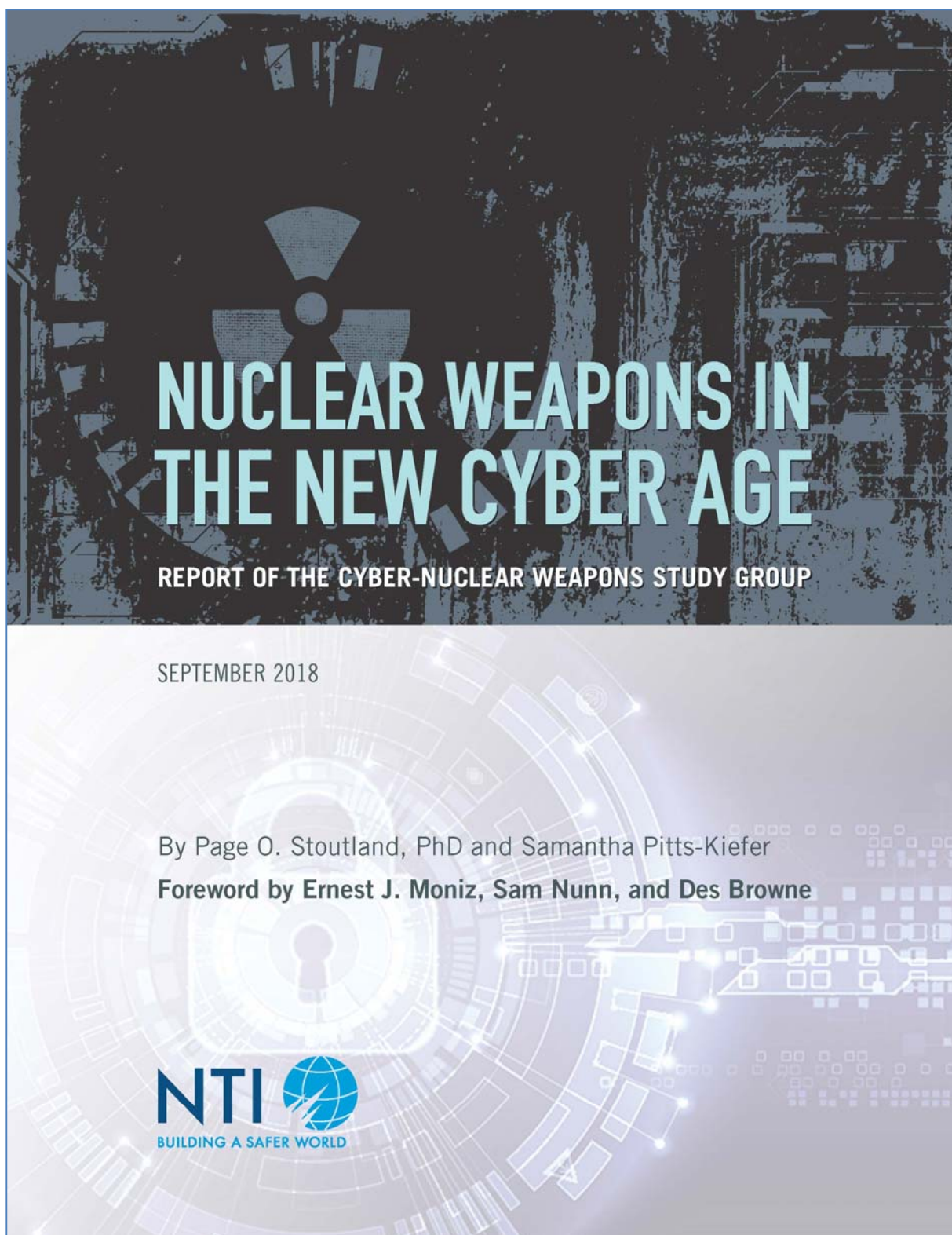
- (1) 建立管制與規定；
- (2) 機構間的協調；
- (3) 建立資通安全文化；
- (4) 評比和聯盟；
- (5) 激勵和維持資安認知；
- (6) 採取持續改善的做法。

此外，新版報告特別強調針對工業控制系統(ICS)的資安攻擊，這是前版沒有的。

新版報告提到更多攻擊案例，顯示敵方的技術日益進步。

肆、心得與建議

- 一、這是一個集思廣益的會議，針對核能資通安全議題，聆聽各國專家的說法，提出自己的看法，腦力激盪，獲致共識。基本上是提出問題，還沒有解答，因為解答在後面幾次會議中，要靠所有參與者的合作與交流解決。各國與會人士有參與核能國際組織的豐富人脈及經驗、資通安全專業知識和希望這個領域更好更安全的熱情。經過一天的會議，深感收穫良多。
- 二、基於研究結果，NTI 感受到核能資通安全的重要性且長期被忽視，針對目前的國際組織交流合作機制的不足，設定論壇參與成員為第一線營運、技術及研發人員，使合作交流奠基在專業技術層面。建議後續的論壇會議，除了本會能繼續派員參加外，台電公司、核能電廠或研究單位資通安全或電算相關人員亦能出席，共同強化我國核設施的資通安全防護。
- 三、由於我國國際處境困難，無法參加聯合國-IAEA 體系的核能國際組織。在核能資通安全領域，管制方面主要和美國核能管制委員會（NRC）交流，台電公司主要從 WANO 尋求技術支援。將來若能加入論壇，不僅增加一個與國際同儕交流的管道，且因論壇聚焦於專業技術層面，免除政治的干擾。建議我國應持續爭取參與論壇後續會議與活動之機會。
- 四、由主辦單位 NTI 的整理，及與會專家的討論，清楚呈現核能資通安全防護的重要性，以及面臨的挑戰與困境。我國近年來重視核能電廠關鍵數位資產資通安全防護之執行與效能，已經納入核子保安之管制與視察。近年來邀請美國能源部國家核子保安局（DOE/NNSA）專家來台辦理兩次核子設施網路資通安全課程，成效良好。我國核子設施資通安全防護的表現已獲得國際肯定，但仍應持續強化精進，就如這次會議揭示的目標：技術水準要跑在資安威脅的前面（Outpacing Cyber Threats）。



附件二、會議議程與討論簡報



Cyber-Nuclear Forum
Planning Workshop
Tuesday, October 30 2018

NTI 
BUILDING A SAFER WORLD

1

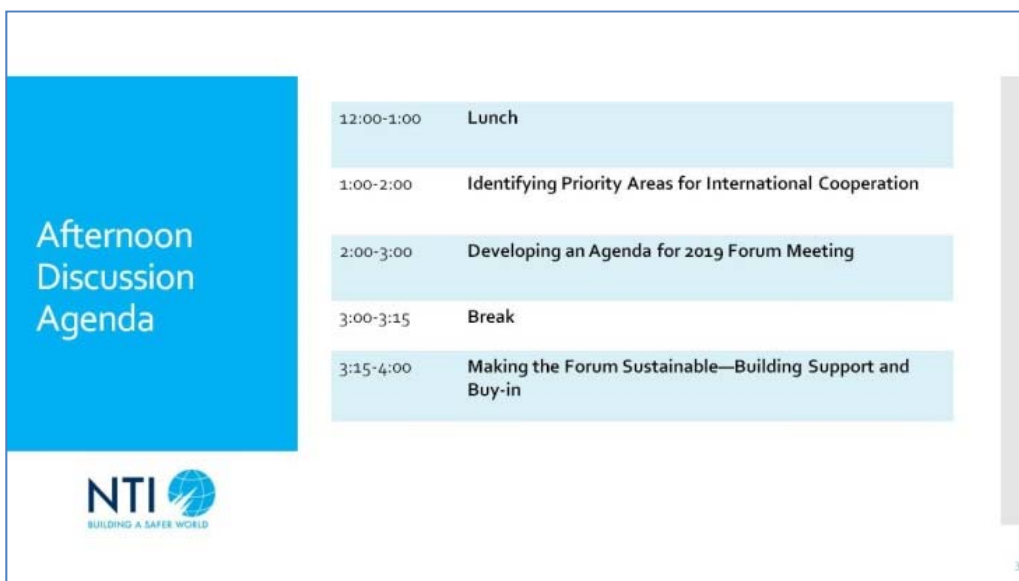


Morning Discussion Agenda

9:00-9:30	Welcome and Introductions
9:30-10:30	Common Cybersecurity Challenges at Nuclear Facilities
10:30-10:45	Break
10:45-12:00	Review of Existing Cooperative Initiatives, International and Domestic


NTI 
BUILDING A SAFER WORLD

2

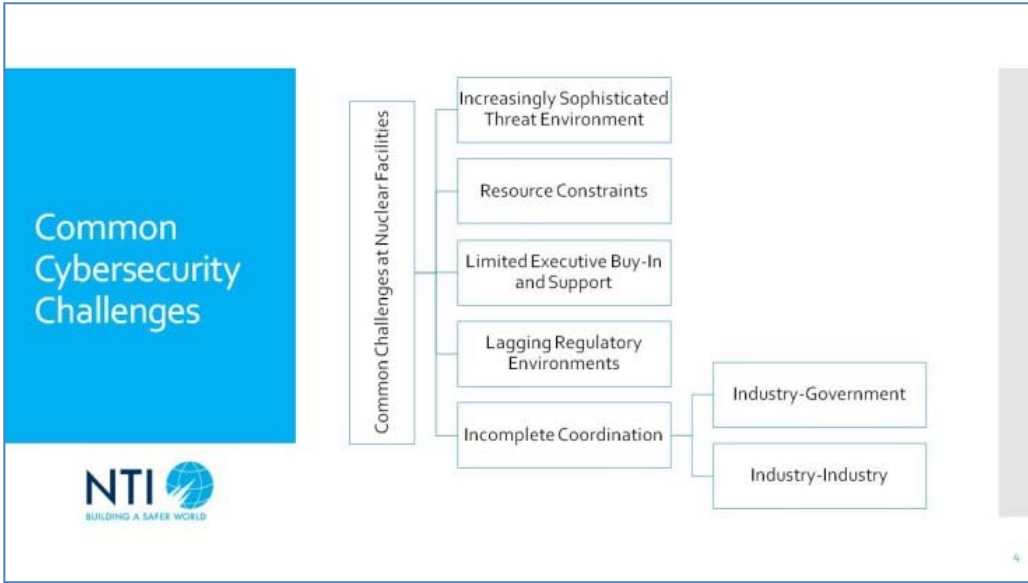


Afternoon Discussion Agenda

12:00-1:00	Lunch
1:00-2:00	Identifying Priority Areas for International Cooperation
2:00-3:00	Developing an Agenda for 2019 Forum Meeting
3:00-3:15	Break
3:15-4:00	Making the Forum Sustainable—Building Support and Buy-in

NTI 
BUILDING A SAFER WORLD

3



Morning Discussion Agenda

9:00-9:30	Welcome and Introductions
9:30-10:30	Common Cybersecurity Challenges at Nuclear Facilities
10:30-10:45	Break
10:45-12:00	Review of Existing Cooperative Initiatives, International and Domestic

NTI BUILDING A SAFER WORLD

5

Existing Cooperative Initiatives

<u>Domestic</u>	<u>International</u>
e.g., CANDU Owners Group	e.g., NISGS

NTI BUILDING A SAFER WORLD

6

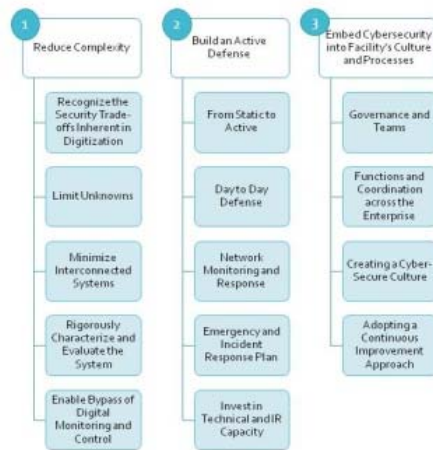
Afternoon Discussion Agenda

12:00-1:00	Lunch
1:00-2:00	Identifying Priority Areas for International Cooperation
2:00-3:00	Developing an Agenda for 2019 Forum Meeting
3:00-3:15	Break
3:15-4:00	Making the Forum Sustainable—Building Support and Buy-in



7

Priorities for Facilities— Opportunities for Mutual Assistance?



8

Afternoon Discussion Agenda

12:00-1:00	Lunch
1:00-2:00	Identifying Priority Areas for International Cooperation
2:00-3:00	Developing an Agenda for 2019 Forum Meeting
3:00-3:15	Break
3:15-4:00	Making the Forum Sustainable—Building Support and Buy-in



9

Open Discussion

Planning for a 2019 Meeting



10

Afternoon Discussion Agenda

12:00-1:00	Lunch
1:00-2:00	Identifying Priority Areas for International Cooperation
2:00-3:00	Developing an Agenda for 2019 Forum Meeting
3:00-3:15	Break
3:15-4:00	Making the Forum Sustainable—Building Support and Buy-in



11

How Can We Make the Forum Sustainable?

1. What would motivate your organization to support your or a colleague's ongoing participation?
2. What resources/services would a coordinating body need to provide?
3. Why did the NISGS cybersecurity group not coalesce after 2016?
4. What sources of funding have been/could be explored?
5. What would be your internal or external "pitch" for the Forum?



12

Outstanding Items



33

Thank you!



34



Discussion Material on Nuclear-Cyber Security Forum


Tze-Chieh HORNG
Atomic Energy Council, Taiwan
2018/10/30


行政院原子能委員會
 Atomic Energy Council
精安核安 民衆心安 日新又新 專業創新


Outline

- Nuclear Energy in Taiwan
- NPP Cyber Protection
- National Cybersecurity Framework
- Draft Response to the Potential Areas of Interest
- Taiwan's Opinions and Interests

2


行政院原子能委員會
 Atomic Energy Council
精安核安 民衆心安 日新又新 專業創新

Nuclear Power Plants in Taiwan



Plant	Capacity/Type	Operating License
Chinshan	1804 MWt/unit GE BWR4 X 2	Unit 1:1978.12.06 Unit 2:1979.07.16
Kuosheng	2943 MWt/unit GE BWR6 X2	Unit 1:1981.12.28 Unit 2:1983.03.15
Maanshan	2822 MWt/unit W PWR X2	Unit 1:1984.07.27 Unit 2:1985.05.18
Lungmen	3926 MWt/unit GE ABWR X2	Unit 1: <u>Deferred</u> Unit 2: <u>Suspend</u>

3

行政院原子能委員會
Atomic Energy Council
精安核安 萬眾心安 日新又新 專業創新

Nuclear Energy in Taiwan

Chinshan NPS
GE BWR-4 636 MWe × 2
Commercial Dec-1978 Unit1
Jul-1979 Unit2

Maanshan NPS
Westinghouse PWR
951 MWe × 2
Commercial Jul-1984 Unit1
May-1985 Unit2

Kuosheng NPS
GE BWR-6 985 MWe × 2
Commercial Dec-1981 Unit1
Mar-1983 Unit2

Lungmen NPS
GE ABWR
approximately 1,350 MWe × 2
Construction Suspended

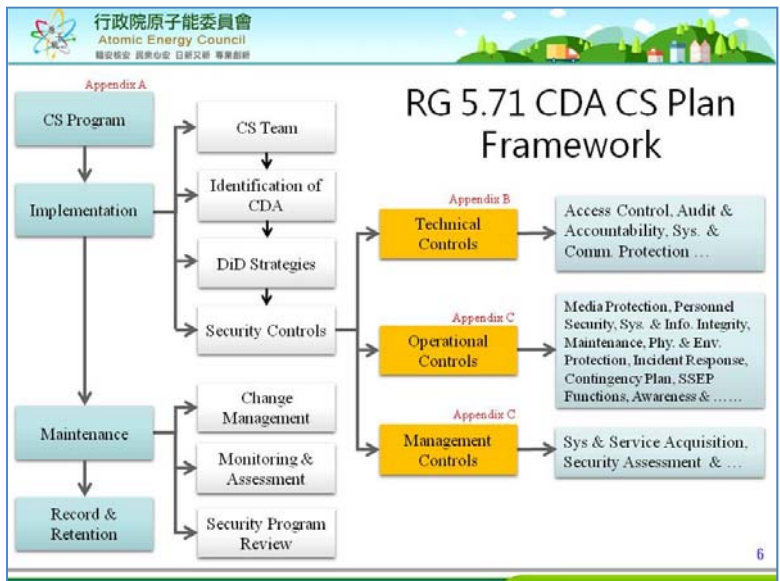
台湾电力公司

行政院原子能委員會
Atomic Energy Council
精安核安 萬眾心安 日新又新 專業創新

NPP Cyber Protection

- Under AEC's request and regulation, Taipower's 3 operating NPPs are implementing cybersecurity protection framework according to NRC RG 5.71
- Taiwan's NPPs have no cyberattack case

5





National Cybersecurity Framework

- Taiwan has a CERT -- TWCERT/CC, operated under the supervision of the Executive Yuan
- Cyber Security Management Law has been completed the legislative process in May, 2018, and will put into force in 2019
- According to the law
 - Critical infrastructure should have a Cyber Security Plan
 - The cyber emergencies at critical infrastructure should be reported to the Executive Yuan, and TWCERT/CC has a mandate to respond

7



Draft Response to the Potential Areas of Interest

8



1.Cooperation to Common Concerns (1/3)

- Nowadays, many nuclear facilities have much more cyber threat exposure due to increasing use of digital systems
- Cyber security program should take into account that the threat vector has shifted from physical plan attacks to attacks via third parties, social engineering techniques and other innovative methods
- Cross-border cooperation might be useful to share experiences on dealing with cyber-attacks, but not limited to

9



1.Cooperation to Common Concerns (2/3)

- Areas of potential experience sharing:
 - Improvement of personnel cyber sense
 - Fostering organization-wide cyber-culture
 - Enhancements of cyber protection framework and mechanism, such as
 - ◆ Hierarchical network management
 - ◆ Assess control
 - ◆ Portable media control

10



1.Cooperation to Common Concerns (3/3)

- Areas of potential experience sharing:
 - Establishment of cyber management system
 - ◆ Which criterion or standard, such as ISO-27001, RG 5.71, NEI08-09, NERC CIP V5, IEC 62433-3-3 or NIST SP 800-82?
 - ◆ How to implement and follow the criterion?
 - ◆ How to maintain effectiveness of management system?
 - Inside audit, outside audit, or independent third-party verification (like BSI)
 - ◆ The adoption new protection measures, technical and/or administrative
 - Using new hardware or new measures to deal with cyber threats

11



2.Mechanisms to Enable Cooperation (1/3)

- Hurdles of information sharing
 - Concerns of incurring ill reputation
 - Leak of operation secrets
- Facilities choose not to disclose the experiences and/or knowledge on fighting against cyber incidents
- The Forum can play a key role in offering a platform for collection and sharing of valuable information among members

12



2.Mechanisms to Enable Cooperation (2/3)

- E.g. WANO Event Report (WER) program
 - Encourage members to share cyber security-related event reports in response to cyberattacks
- E.g. WANO significant event reports
 - Release relevant information on the urgent issues or latest trends to follow, the Forum may take the initiative

13



2.Mechanisms to Enable Cooperation (3/3)

- Urgent Issues
 - E.g. Major software defects
 - E.g. The issues CERT will notify entities' cybersecurity contact points
 - The Forum can focus on threats to ICS and related systems
- Latest Trends
 - The Forum collects, categorizes and analyzes incident or statistical reports, and compiles them into Trend Analysis Reports, and issues periodically
 - E.g. CERT Monitoring Monthly Reports

14



3.Supply Chain Issues (1/2)

- Cyber security is a continuously evolving issue. Suppliers of digital equipment are aware of the related threats.
- With the participation of suppliers, they can not only demonstrate their solutions to enhance cyber security but also realize the demand from customers with abundant field experiences.
- Both suppliers and the Forum members may benefit from each other.

15



3. Supply Chain Issues (2/2)

- Cybersecurity certification of ICS equipment are possible
 - E.g. NSS Labs and ICSA Labs issue certificates for firewall and IPS (Intrusion Prevention System), and even IoT Security & Privacy
 - Taiwanese government requires that supplier shall present NSS or ICSA certificate of IPS technical ability in the purchase contract of cybersecurity equipment, to demonstrate the defense ability of IPS products

16



4. Mutual-aid Agreements / Partnering (1/3)

- With mutual-aid agreements, it is clear to define limited obligations and privileges for each the Forum member to follow
- Shared information might be confidential and cannot be released outside the Forum
- Members will be willing to disclose their experiences and expertise to each other and thus strengthen their capabilities to enhance cyber security

17



4. Mutual-aid Agreements / Partnering (2/3)

- In this area, the Forum should clearly define acceptable agreements and let members realize their obligations and privileges. When there is a conflict of interests, the Forum has to act as the arbitrator according to the agreements
- Is Red Team Test possible for the Forum members?

18



4. Mutual-aid Agreements / Partnering (3/3)

- If the Forum is willing to build a mechanism like WANO peer review, a standard criterion like WANO PO&C (Performance Objectives & Criteria) should be established
- Is WANO MSM (Member Support Mission) suitable for the Forum?
 - No concern of sensitive material release

19



Taiwan's Opinions and Interests

- The operating NPPs in Taiwan are more than 30-year old. The most of important control systems are analog-type design, even some have upgraded to digital
- Proposal: Establish a discussion group dealing with cybersecurity concerns for partly digital-upgraded aged NPPs
- Proposal: In the larger conference, invite keynote speakers to give speeches:
 - New knowledge and trends of ICS cybersecurity

20

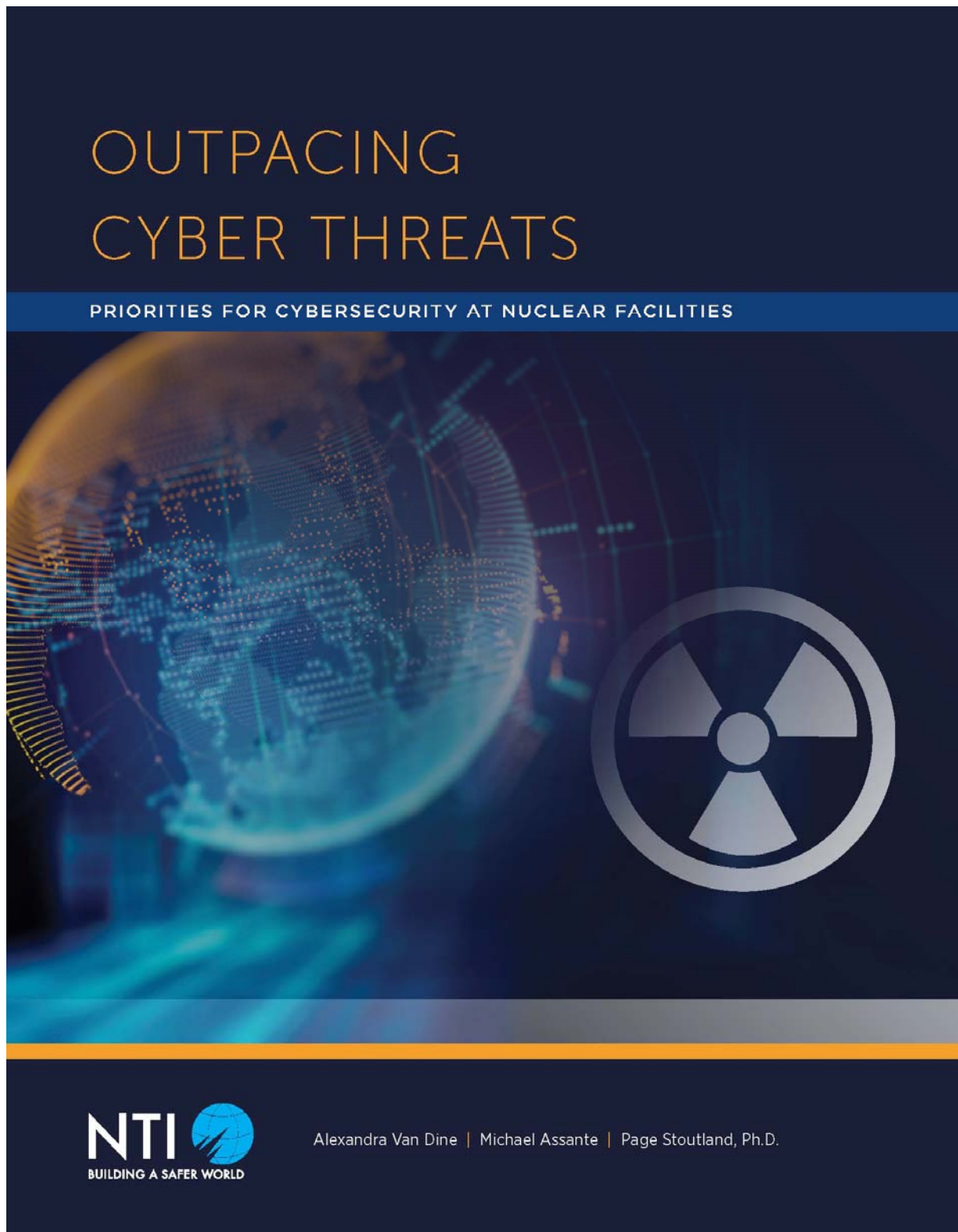


Nuclear Threat Initiative

Outpacing Cyber Threats

Essential Next Steps for Cybersecurity at Nuclear Facilities

Page Stoutland, PhD and Erin D. Dumbacher
11-1-2018



圖一、會議成員合影



會議後合影，自右而左為 Anno Keizer、Page Stoutland、Tim Collier、Christophe Martin、John Sladek、Nathan Faith 及作者，攝影者為 Erin Dumbacher，Scott Hilts 已先行離開