行政院及所屬各機關出國報告

（出國類別：其他）

2024年參加馬歇爾歐洲安全研究中心「網路安全研究計畫研討會(PCSS-S)」

服務機關：海洋委員會海巡署

姓名職稱：杜佩珊技士

派赴國家：德國

出國期間：2024年3月8日至3月14日

報告日期：2024年4月16日

摘要

本次訓練由「馬歇爾歐洲安全研究中心(The George C. Marshall European Center)」辦理，為期5天的網路安全基礎知識課程，參訓人員為各國中階軍事、政府和非政府相關人士，針對網路安全制訂或影響立法、決策或實際執行之政府(軍方)部會人員設計，互相交流網路安全戰略、政策、應變和實踐機制，提高合作夥伴網路安全能力。

本署派員自113年3月8日至3月14日赴德國參加馬歇爾歐洲安全研究中心網路安全研究計劃研討會(Program on Cyber Security Studies-Seminar,PCSS-S)，期望增加對「網路安全」及「資通安全執行策略」等議題認知，提供機關未來相關政策與執行參考，培養參訓學員對資安事件應變能力及提升國際視野，增進國際交流。

目錄

壹、訓練資訊

一、訓練目的

本次訓練名稱為「網路安全研究計劃研討會(Program on Cyber Security Studies-Seminar)」，旨在探討國內和跨國網路安全挑戰，提供一個全面性、以政策為主(非技術性)的網路安全課程，教導如何規劃最明智的網路安全政策及戰略，並學習網路攻擊威脅的性質和規模。該研討會由智庫馬歇爾歐洲安全研究中心各領域專家授課，探討網路安全對國家和國際安全的影響，並為各國不同領域學員建立聯繫和交流的機會，課程包括網路安全法規、國際組織政策框架、資安事件應變處置及網路犯罪與新興技術等。

二、訓練資格

依據美方所列參訓人員資格要求，本次訓練學員以中階軍事人員(軍餉等級04-06：相當於少校至上校)、警察、海巡、文職及非營利組織人員為主，國際學生之英文能力需達美國軍事人員英文理解能力測驗(English Comprehension Level, ECL)80分以上。

三、訓練日程

本次訓練自2024年3月8日(星期五)起至2024年3月14日(星期四)止共計5日，訓練日程表如表1：

表 1 PCSS-S訓練日程表

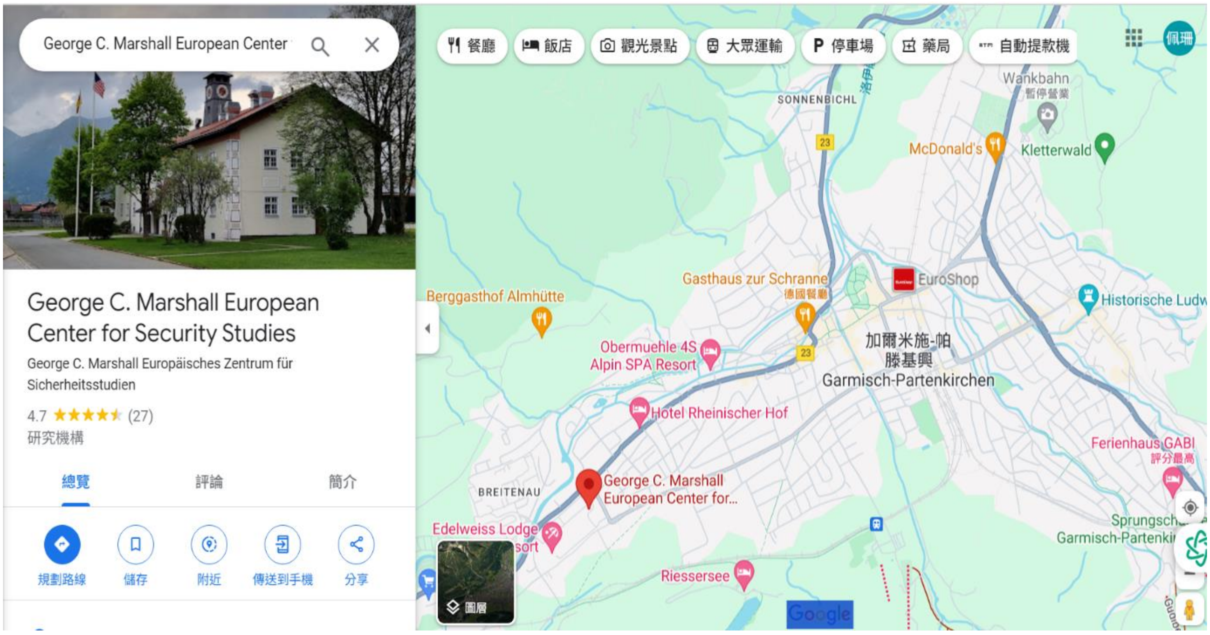
Friday, March 08, 2024		
0830-0850	Plenary Session	Registration
0850-0920		Welcome and Course Opening
0920-0930	Other	Group Photo
0930-1000		Participants’ Photos for Recognition Book
1000-1030	Coffee Break	
1030-1200	Plenary Session	Technical Cyber Foundations(網路安全基礎技術)
1200-1330	Lunch	
1330-1500	Plenary Session	Insider Threats(內部威脅)
1500-1530	Coffee Break	

1530-1700	Breakout Session	Seminar Group Discussions(小組討論)
Saturday，March 09，2024 and Sunday，March 10，2024		
Personal Time		
Monday，March 11，2024		
0830-1000	Plenary Session	U.N. Framework of Responsible State Behavior in Cyberspace(聯合國網路空間國家責任行為框架)
1000-1030	Coffee Break	
1030-1200	Plenary Session	Geopolitical Competition in Cyberspace(網路空間的地緣政治競爭)
1200-1330	Lunch	
1330-1500	Breakout Session	Seminar Group Discussions(小組討論)
1500-1530	Coffee Break	
1530-1700	Plenary Session	Movie: “The Defenders” (影片欣賞)
Tuesday，March，12 2024		
0830-1000	Plenary Session	National Cybersecurity Laws(國家網路安全法規)
1000-1030	Coffee Break	
1030-1200	Plenary Session	Ransomware(勒索軟體)
1200-1330	Lunch	
1330-1500	Plenary Session	Emerging Technology and Challenges(新興技術與挑戰)
1500-1530	Coffee Break	
1530-1700	Breakout Session	Seminar Group Discussions(小組討論)
Wednesday，March 13，2024		
0830-1000	Plenary Session	National Cybersecurity Strategies(國家網路安全策略)
1000-1030	Coffee Break	
1030-1200	Plenary Session	Cyber Incident Response and Crisis Communications(網路事件應變與危機溝通)
1200-1330	Lunch	
1330-1500	Plenary Session	Movie: “The Social Dilemma” (影片欣賞)
1500-1530	Coffee Break	
1530-1700	Breakout Session	Seminar Group Discussions(小組討論)
Thursday，March 14，2024		
0830-1030	Breakout Session	Seminar Table-Top Exercise Scenario(兵推演練)
1030-1100	Coffee Break	

1100-1115	Plenary Session	Introduction Marshall Center Alumni Programs
1115-1145	Plenary Session	Strategic Insights and Actionable Tips
1145-1200	Plenary Session	Closing Remarks

四、訓練中心介紹

馬歇爾歐洲安全研究中心(Marshall Center)位於德國加爾米施-帕滕基興（Garmisch-Partenkirchen），屬於美國國防部(Department of Defense, DoD)之防衛安全合作局(Defense Security Cooperation Agency, DSCA)全球 6 處區域研究中心之一，餘 5 處分別為「尼爾·K·亞太安全研究中心(Daniel K. Inouye Asia-Pacific Center for Security Studies)」、「威廉佩里西半球防衛研究中心(William J. Perry Center for Hemispheric Defense Studies), Perry Center)」、「非洲戰略研究中心(Africa Center for Strategic Studies),ACSS」、近東南亞戰略研究中心(Near-East South Asia Center for Strategic Studies),NESA」及「泰德史蒂芬北極安全研究中心(Ted Stevens Center for Arctic Security Studies),TSC」。



五、校友互動機制

每位參訓學員完成各項課程後，均可順利結業並獲頒結業證書(Course Certificate)及取得校友身分(Alumni Status)，並建立校友帳號提供交流管道，馬歇爾歐洲安全研究中心迄今已有來自 160 國家、超過 15,000 名校友，目的在全

球建立值得信賴的安全合作關係，密切聯繫結業校友之連結，強化資訊共享和人員交流互動。

貳、訓練過程

一、學員組成

本次參訓學員共有來自 29 個國家，共計 42 位學員，參訓人員除軍人外，大多數為政府部門文職官員，分別來自國安、國防、外交、警察、經濟與金融等領域部門，另有部分為學界或法律專長專家，各代表國家及人數如表 2(依國家英文字母順序排列)。

表 2 PCSS-S 參訓學員組成一覽表

編號	國家	人數
1	阿根廷（ARG）	1
2	亞美尼亞（ARM）	1
3	巴西（BRA）	1
4	保加利亞（BGR）	1
5	蒲隆地（BDI）	1
6	捷克（CZE）	2
7	德國（DEU）	3
8	喬治亞（GEO）	1
9	瓜地馬拉（GTM）	1
10	克羅埃西亞（HRV）	1
11	伊拉克（IRQ）	1
12	日本（JPN）	1
13	拉脫維亞（LVA）	2
14	馬來西亞（MYS）	1
15	摩爾多瓦（MDA）	1
16	蒙特內哥羅（MNE）	2
17	北馬其頓共和國（MKD）	1
18	莫三比克（MOZ）	1
19	奈及利亞（NGA）	5
20	科索沃（XXK）	2
21	羅馬尼亞（ROU）	1
22	塞爾維亞（SRB）	2
23	斯洛伐克（SVK）	1

24	波士尼亞與赫塞哥維納（BIH）	1
25	臺灣（TWN）	1
26	土庫曼斯坦（TKM）	2
27	烏克蘭（UKR）	3
28	模里西斯（MUS）	1
29	葉門（YEM）	1

二、課程內容

「網路安全研究計畫研討會(PCSS-S)」以應對跨國網路安全挑戰為主軸，本梯次課程為期 5 天，分為共同課程(Plenary)、小組討論(Seminar)及兵推演練(Table-Top Exercise)等三類。

(一)共同課程(Plenary):

全體學員於會議室統共同參加（約 90 分鐘），包含兩堂影片欣賞，討論網路攻擊與社交軟體帶來成癮與隱私衝突問題，其他 9 門課程，均為非技術性網路安全議題課程，相關課程簡介如下:

1. 網路安全基礎技術 (Technical Cybersecurity 101):

   介紹互聯網、資訊與通信科技技術、網路架構和管理的基礎知識，並解釋美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）的網路安全框架（Cybersecurity Framework, CSF），包括：政府(Govern)、辨識（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）和復原（Recover），組織應依據業務需求及框架層級，評估網路安全威脅程度，並整合現行風險管理實務做法，強化資訊安全治理能力，降低網路的資訊安全風險。

2. 內部威脅 (Insider Threats):

   當前資安的風險已經由單純外部攻擊轉向利用內部人員來達成滲透，且比外部威脅更難偵測，本堂探討「內部人員(Insider)」和「內部威脅(insider threat)」所帶來不同的風險，並分享內部威脅實際案例，例如內部人員惡意資料竊取、間諜或破壞等，並討論國家、地區或國

際政府可以採取的策略，以保護自己及其關鍵基礎設施免受內部網路威脅的影響。

3. 聯合國網路空間國家責任行為框架 (U.N. Framework of Responsible State Behavior in Cyberspace)：

   瞭解聯合國網路空間國家責任行為框架在網際網路間的概述、背景、發展和要素，包含國家主權原則、不干涉其他國家內政原則等均適用於網路空間，並且同意負責任國家行為規範，建立信任措施，另探討由非國家行為者及代理人所發動之網路攻擊與國際法適法性問題。

4. 網路空間的地緣政治競爭 (Geopolitical Competition in Cyberspace):

   網際網路雖然被視為一個虛擬的無邊界世界，但實際上許多網路出現的許多問題與國家政治和地緣互相關聯，瞭解大國Great Powers(GP)在國際領域，包含政治、經濟、社會、國防及科技等層面對較小國家的合作與競爭關係，其中分享烏俄戰爭和中國的智慧城市等例子，突顯地緣政治對於社會、經濟的嚴重影響，探討每個大國在網路空間中的地緣政治動機以及他們所面臨的政策問題。

5. 國家網路安全法規(National Cybersecurity Laws):

   討論國際法如何在網際網路的應用，包含聯合國在制訂國家網路安全法規扮演角色，及政府、軍隊、民間社會和工業不同組織所關心的議題，但各國對網路安全和資訊安全之間的概念差異，影響網路安全法規接受程度不同，為建立國家網路安全法規的主要挑戰。

6. 勒索軟體(Ransomware)：

   介紹勒索軟體相關的基本術語、歷史演變和潛在攻擊目標，以及當前趨勢和不同種類攻擊手法，並討論防禦勒索軟體的基本方法，如定期備份資料、軟體更新、加強人員教育訓練等，如何在國家法規面、技術面與國際組織合作下，發展有效的防禦策略。

7. 新興技術與挑戰 (Emerging Technology and Challenges):

瞭解新興技術相關的具體風險和威脅，其中探討因人工智慧技術的普及，已影響生活的所有領域，透過四因素分析，探討對國家經濟、政府機構、國家安全和社會的影響，並預測該領域可能走向並提出應對或防禦的方式，幫助國家或組織制訂網路安全策略。

8. 國家網路安全策略 (National Cybersecurity Strategies)：

講述國家網路安全策略的生命週期流程，評估在網路空間面臨的威脅後，確認網路安全策略的整體目標，例如保護關鍵基礎設施、提升網路韌性、打擊網路犯罪等，制訂法規、具體的行動計畫或與其他國家組織共同合作應對，持續監控策略實行狀況並適當調整，以實現國家網路安全策略的目標。

9. 網路事件應變與危機溝通 (Cyber Incident Response and Crisis Communications):

定義網路事件應變和危機溝通的基礎概念，解釋資安事件應變生命週期，分別為準備(Preparation)、偵測與分析(Detection and Analysis)、遏制、根除和復原(Containment, Eradication and Recovery)、事後檢討(Post-Incident Activity)等程序，除建立資安事件應變計畫，當下識別和分析潛在資安事件性質、影響範圍和風險等級，並通知利害關係人進行危機溝通，瞭解主要參與者和關聯組織的角色和責任，採取適當措施防止事件惡化，以減輕事件的影響並恢復正常運作，事後記錄應變過程或對應變計畫滾動修正，防止類似事件再次發生。

(二)小組討論(Seminar)

該中心依據國籍和專長領域將學員分成 4 組，每小組約 10 名學員，於每日下午課程結束後至專題討論室進行小組討論，每組均由歐洲馬歇爾安全研究中心派 2 員專家學者擔任導師共同帶領，就當日共同課程拋出議題引導學

員討論、交換不同觀點和分享個人實務經驗，並鼓勵每人均提出個人觀點，平衡每位學員發言狀況，以增進學員對課程之瞭解。

(三)兵推演練(Table-Top Exercise)

最後一天上午實施兵推演練，中心為學員提供了模擬情境:假想國在關鍵基礎設施被破壞，並且有潛在鄰國網路攻擊威脅情景下，政府如何執行應對策略及迅速恢復社會功能運作為本次演練重點。本次演練採用DIMEFIL模型，提供一個多方面角度來分析情況，包含外交、資訊、軍事、經濟、金融、情報和執法等全方位範疇，因策略制定需要跨部門的合作和深入理解不同領域知識，以確保能夠有效地評估災害和減輕網路攻擊風險，加強政府和企業之間關鍵基礎設施防護措施，強化政府部門應變能力。(兵推演練情境如附件)

參、心得及建議

一、參訓心得

本次研討會主要以觀念性角度講述網路安全實務面共同遇到的問題與風險,並透過有效的資通安全政策和風險管理策略克服這些挑戰，在第一堂課「網路安全基礎技術」講師提到一個重要觀念，所有的網路威脅有 90%是人為造成的(90% of cyber vulnerability is based on human error)，因網路攻擊手法日趨複雜且持續改變，政府或企業如何面對有組織的計畫型攻擊活動，除傳統防禦型模式建立資安防護架構外，更要確保執行政策與實務契合及提升組織人員的資安意識。

另訓練期間全程落實查塔姆守則 (Chatham House Rule)，即與會者可自由使用所收到的資訊，但不得透露發言者或其他與會者身分或從屬關係，鼓勵學員自由、誠實發言，也可以對其他與會者發言提出異議，進而討論帶有爭議性問題與論點，增加討論開放性與自由度；本次研討會也藉小組討論時機，向其他學員分享中國對我國網路攻擊與資訊操縱(假消息)現況，說明我國政策立場及應變機制，有助增進同組各國學員瞭解與認同，同時促進友好交流及爭取國際支持。

二、培養外語能力，擴展國際視野

本次研討會與來自 29 個國家不同領域專家一同培訓，由訓練單位馬歇爾歐洲安全中心提供一個自由、相互尊重以及開放的討論環境，讓學員分享各自面臨的網路安全問題或各國推行政策，不僅有跨領域專長交流機會，更能提升外語能力並建立國際人脈。外語能力為拓展國際視野重要基礎，建議積極培養外語專長人員，培訓具備國際觀人才，參與各項國際培訓活動與各國專家合作交流，提升本署在國際合作中的角色和影響力。

三、未來可向 AIT/T 就未來遴選參訓學員提供回饋意見

此次網路安全研究計畫研討會(PCSS-S)，提供技術面「網路安全基礎知識」，瞭解網路空間和網路安全的技術面向、概念和術語，並研討法規面「國際法網路安全框架」及政策面「制訂資通安全策略」等課程主題。

本次薦派「網路專長人員」受訓，增進對網路安全領域的深入理解，為持續培育網路安全人才，強化本署應對網路威脅的能力，建議未來持續爭取受訓名額，薦派人員參與相關課程；另可增派其他政府部會有關領域人員，有效推動國家資通安全政策及制訂有效的網路安全戰略，以確保我政府選派參訓人員符合課程需求，未來可向 AIT/T 就未來遴選參訓學員提供回饋意見。

PCSS-S Table Top Exercise
2024-03-13

Exercise Description (Seminar Leaders Only)

This tabletop exercise provides an opportunity for participants to simulate a government's strategic/policy response to a complex cyberattack scenario involving critical infrastructure and potential state actor involvement. The exercise aims to improve understanding of the interdependencies in critical infrastructure between governments and corporations, their readiness to respond effectively to complex incidents, and improve considerations of the broader implications of state-sponsored cyber threats.

This exercise employs the DIMEFIL model to provide a comprehensive framework to analyze the multifaceted dimensions of the situation and guide decision-making. By considering the full range of diplomatic, informational, military, economic, financial, intelligence, and law enforcement elements of government power, senior policymakers can develop a well-rounded strategy that addresses both the immediate and longer-term implications of state-sponsored cyberattacks on critical infrastructure.

Background (All)

PowerUp is a prominent multinational corporation responsible for the operation of critical power generation and distribution systems in the country of Eldoria, a technologically-advanced nation known for its economic prosperity and stable infrastructure. The company's infrastructure plays a crucial role in supplying electricity to homes, businesses, hospitals, and other essential services. The efficiency and reliability of PowerUp's services has contributed significantly to Eldoria's growth and development.

Eldoria has a neighboring country named Veridia that has a history of tensions and conflicts with Eldoria. The relationship between Eldoria and Veridia is characterized by territorial disputes, ideological differences, and occasional border skirmishes. Veridia is known for its assertive foreign policy and has been involved in regional power struggles with Eldoria for years.

Eldoria is a constitutional monarchy with a parliamentary system of government. The monarch's role is largely ceremonial, while the government's day-to-day operations are carried out by elected representatives who are accountable to the parliament and the electorate. This political system allows for a blend of historical continuity and democratic decision-making.

Veridia is a unitary presidential republic. Veridia's unitary presidential republic political system provides a framework for centralized decision-making and governance. Veridia has been ruled by the same president for 24 years. Veridia’s energy systems are fully owned and managed by their government.

Eldoria and Veridia are members of United in Peace, an international organization, which has two working groups on the peaceful use of cyberspace. One of the groups is chaired by Eldoria and is presently working on norms and best practices for securing critical infrastructure. Diplomats from Veridia observe the Eldoria-chaired working group.

Briefing

The day started like any other, but chaos quickly ensued when PowerUp's monitoring systems alerted its Information Technology (IT) Security Team about unusual activities across their operational technology networks. As the IT Security Team responded, they rapidly discovered that a cyberattack had apparently been launched against the company's control systems, compromising critical components of the power generation and distribution infrastructure.

The attack had multiple dimensions:

Disruption of Power Generation: The attackers managed to infiltrate and manipulate the control systems of several power generation plants. As a result, power output was disrupted, causing localized outages in different regions of Eldoria. The blackout had far-reaching consequences however, impacting hospitals, emergency services, transportation systems, and the daily lives of citizens.

Data Exfiltration: Simultaneously, the attackers exfiltrated sensitive operational data from PowerUp's systems. This data included technical specifications, schematics, and proprietary software code that, if in the wrong hands, could pose serious threats to the stability and security of the power infrastructure. The attackers also moved laterally from operational technology systems to IT systems to access personnel data. An open-source intelligence company shared information privately with PowerUp executives that some of this data may soon be made available for sale on the dark web.

Sophisticated Malware: Initial analysis revealed the presence of a highly advanced and previously unknown malware strain. Its complexity and evasion techniques suggested that this was not the work of a typical cybercriminal group. This raised concerns that a well-resourced and skilled threat actor might be behind the attack.

Potential State Actor Involvement: Further investigation revealed patterns and techniques consistent with state-sponsored hacking groups known for targeting critical infrastructure. The attackers' tactics, techniques, and procedures (TTPs) were reminiscent of state-sponsored campaigns documented in previous cybersecurity research reports.

Geopolitical Rivalry

The presence of geopolitical rivalry adds another layer of complexity to the scenario. It raises the possibility that Veridia could be involved in the cyberattack on Eldoria's critical infrastructure as part of a larger political agenda. Veridia has a history of utilizing cyber hacking groups as a tool for exerting influence and gathering intelligence, so the involvement of state-sponsored hacking groups from Veridia could be considered for this new incident.

As PowerUp deals with the aftermath of the cyberattack against Eldoria’s critical infrastructure, the question of potential attribution to a state actor becomes even more critical, and understanding the motivations and intentions of neighboring countries like Veridia becomes an integral part of the discussion. The implications of this situation extend beyond cybersecurity, potentially affecting diplomatic relations, national security, and regional stability.

Response

As PowerUp's Incident Response Team (IRT) and IT Security Team worked tirelessly to contain the attack and restore power, the organization faced difficult decisions. After its initial notice of an adverse event, PowerUp notified Eldoria’s CERT of the cyberattack. Eldoria’s CERT quickly swung into action, meeting with PowerUp’s security and executive teams. The question of state actor involvement became a central concern. If indeed a nation-state was responsible, the implications extended beyond cybersecurity to diplomatic and geopolitical realms.

Given the severity of the incident, the potential attribution to a state actor, and the far-reaching impact on critical infrastructure, PowerUp needed to ensure a comprehensive and coordinated response. The organization needed to address not only technical aspects but also legal considerations, stakeholder communication, and engagement with government agencies.

As PowerUp navigated this challenging scenario in Eldoria, they recognized the need to collaborate effectively with government, engage with external experts, and make strategic decisions that balanced the restoration of services with the pursuit of accountability and resilience in the face of cyber threats with potential state involvement.

Guided DIMEFIL Discussion (All)

The DIMEFIL model is a framework used by intelligence and security analysts to consider the various dimensions and factors that influence a geopolitical situation. It stands for Diplomatic, Informational, Military, Economic, Financial, Intelligence, and Law Enforcement. Let's apply the DIMEFIL model to the tabletop exercise scenario involving the cyberattack on critical infrastructure and the potential involvement of state actors.

Take 15 minutes per DIMEFIL dimension to discuss the questions below. At the end of the exercise, please be prepared to present three key takeaways from the exercise.

Diplomatic:

- How can we leverage diplomatic channels to communicate with the potentially involved state actor and seek a de-escalation of tensions?
- Are there international forums or organizations where we can raise awareness about the implications of state-sponsored cyberattacks on critical infrastructure? What might be done through those channels?

Informational:

- How should we manage the dissemination of accurate and timely information to the public, media, and stakeholders while safeguarding national security interests?
- Can we collaborate with international partners to share threat intelligence and enhance our understanding of state-sponsored cyber threats?

Military:

- Are there military or cyber defense units that can provide technical assistance in analyzing the attack, identifying its origin, and potentially attributing it to a state actor?
- What contingency plans should we have in place in case the situation escalates and requires a coordinated response involving military forces?

Economic:

- What economic consequences might arise from a prolonged disruption of critical infrastructure services due to the cyberattack?
- How can we assess the potential impact on our nation's economy and develop strategies to mitigate these effects?

Financial:

- Are there financial implications associated with the potential involvement of a state actor? For example, could sanctions or financial restrictions be imposed?
- How might this incident affect our nation's financial stability and banking systems?

Intelligence:

- How can we enhance intelligence-sharing among national intelligence agencies to gain insights into the intentions and capabilities of the potential state actor involved?
- Can we collaborate with international intelligence partners to gather more information about the cyber threat landscape and state-sponsored activities?
- How would the level of belief or confidence on attribution affect Eldoria's decision-making to take actions in response to this situation (e.g., diplomatic, informational, military, financial, law enforcement actions)?

Law Enforcement:

- What international legal frameworks and national legal authorities that could apply to this situation, and how can we ensure compliance with relevant international laws, agreements, and statutes?
- Are there legal avenues to pursue accountability if the attack is indeed attributed to a state actor?

Report Out

Each group should nominate an individual from their seminar to report their findings, paying attention to the interplay between technical, legal, diplomatic, and strategic aspects when responding to a cyberattack with potential state actor involvement. Did you uncover the need for effective collaboration, comprehensive preparedness, and a multifaceted approach to mitigating the impact of state-sponsored cyber threats on critical infrastructure?