# 調　查　報　告

壹、案　　由：國內部分中小學近期傳出疑遭殭屍網路攻擊致教學活動受阻，知名資安公司Check Point亦指出，2021年10月至2022年3月間，臺灣教育及研究機構平均每週遭到多達4,730次攻擊，為所有產業最多；究我國中小學及教育主管機關之資安資源配置是否允當？聯防機制是否有效？相關法令遵循及通報應變是否落實等情，均有深入調查之必要案。

貳、調查意見：

本案經調閱教育部及基隆市政府等機關卷證資料，並於民國(下同)112年9月27日赴花蓮縣、9月28日赴臺東縣、10月6日赴高雄市及臺南市、11月9日分別於基隆市及本院辦理現場履勘及訪談基層教師共56人與相關機關人員，已調查完畢，茲臚列調查意見如下：

**一、基隆市教育網路111年12月發生殭屍網路資安事件，導致網路瞬斷，嚴重影響全市教育網路及教學活動，依照「資通安全事件通報及應變辦法」，應確實執行通報應變及復原；惟基隆市教育局於事中之通報時效及事件等級、事後之根因查明及復原等環節核有明確違失；又臺灣學術網路危機處理中心未能善盡本案資安事件等級審查職責，主管機關教育部亦有檢討改進空間。**

(一)「資通安全事件通報及應變辦法」(下稱通報應變辦法)涉及本案規定如下，另教育部亦訂有「臺灣學術網路各級學校資通安全通報應變作業程序」供地方主管機關及學校遵循，依該等規定內容顯示，資安事件之等級、通報及復原時效，主要取決於「受影響業務是否屬於核心業務」以及「受影響之嚴重程

度」兩項因素，合先敘明：

1、第2條第1項：資通安全事件分為四級。

2、第2條第2項：公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：

（1）非核心業務資訊遭輕微洩漏。

（2）非核心業務資訊或非核心資通系統遭輕微竄改。

（3）非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

3、第2條第3項：各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：

（1）非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

（2）非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

（3）非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4、第2條第4項：各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：

（1）未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

（2）未涉及關鍵基礎設施維運之核心業務資訊或

核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

（3）未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓,於可容忍中斷時間內回復正常運作。

5、第4條第1項: 公務機關知悉資通安全事件後，應於1小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

6、第5條第1項：主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並**得依審核結果變更其等級**。

7、第6條第1項：公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：

（1）第一級或第二級資通安全事件，於知悉該事件後72小時內。

（2）第三級或第四級資通安全事件，於知悉該事件後36小時內。

8、第7條第2項：主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。

(二)摘錄基隆市教育網路中心(下稱教網中心)依「通報應變辦法」填報之通報單重要內容如下：

1、事件發生時間：2022年12月20日14時39分30秒。

2、確認為資安事件時間：2023年1月9日17時42分57秒。

3、事件分類：INT-殭屍電腦(Bot)

4、破壞程度：影響本市教育網路及學術網路無法正常運作。

5、事件說明：12/20發生網路連線無預警瞬斷，造成全市網路無法正常運作，經查，發現全市連線(session)數不正常，從平常每秒25萬筆暴增到每秒800萬筆。處置說明：將防火牆設定自動封鎖規則阻擋災情擴大。

（1）確定受到感染(Botnet.CNC)

（2）Session數超過2000筆/每秒(PC正常值約為200筆/每秒)，開啟自動封鎖。

6、資通安全事件影響等級:

（1）機密性衝擊-1級-非核心業務資訊遭輕微洩漏。

（2）完整性衝擊-1級-非核心業務資訊或非核心資通系統遭輕微竄改。

（3）可用性衝擊-2級-非核心業務之運作受影響或停頓,無法於可容忍中斷時間內回復正常運作,或未涉及關鍵基礎設施維運之核心業務或和核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

7、資安事件綜合評估等級:2級。

8、影響範圍及損失評估：影響本市教育網路及學術網路無法正常運作。

9、是否需要支援:否。

10、緊急應變措施：已中斷網路連線，待處理完成後再上線。

（1）解決辦法:

〈1〉將防火牆設定自動封鎖規則阻擋災情擴大。

〈2〉請各校將受感染裝置恢復正常後，來信教網中心申請解除IP封鎖控管。

（2）解決時間：2023年1月9日17時41分37秒。

(三)另據基隆市政府查復[1]事件經過並經本院綜整如下表，其他重要查復內容一併臚列如下：

1、本案大事紀如下表9：

表1　本案大事紀

| 時間 | 處理進度 |
|---|---|
| 111/12/20 | 基隆市教網發生網路連線無預警瞬斷，造成網路不穩定情形（並非直接斷網），教網中心立即召集中心機房防火牆及core switch 的廠商調查發生原因及討論後續因應做法。 |
| 111/12/21 | 發現全市連線(Session)數不正常，從平常每秒25萬筆爆增到每秒800萬筆，再深入調查發現是BotNet(殭屍網路）攻擊，立即將外部1,600多個Botnet.CNC黑名單的IP進行封鎖，封鎖後攻擊並無下降。 |
| 111/12/22 | 先行手動封鎖35個內部學校IP。 |
| 111/12/23 | 發現市內攻擊擴散到496個IP，再進行人工封鎖阻擋，並於處務公告1,776通知各校因應。公告內容略以：「因近期發生大量網路攻擊事件，嚴重影響基隆市教育網路及學術網路正常服務，為維護其他使用者正常使用之權益，自111年12月26日19時起，基隆市教網中心將開始針對受感染設備進行自動封鎖，遭到封鎖之IP將無法進行上網.....」等語。 |
| 111/12/25 | 狀況仍未改善，災情擴散已無法以人工方式阻擋，並可能造成防火牆崩潰全市所有學校斷網，在與防火牆原廠工程師及資安顧問緊急開會決議，以下列兩條件設立自動封鎖規則阻擋災情擴大。<br>● 確定受到威染(Botnet.CNC）。<br>● Session數超過2,000筆/每秒(PC正常值約為200筆/每秒，單一網頁約40-60筆/每秒)，開啟自動封鎖。 |
| 111/12/26 | 成功阻止殭屍網路擴散，網路連線恢復平常每秒25萬筆，故上簽教育處長官通報事件處理，並於19:00將 |

[1] 112年5月24日基府教學壹字第1120225055號函

| | |
|---|---|
| | 原本封鎖歸零，之後有感染行為才加入封鎖清單。 |
| 111/12/26 | 處務1788號公告該市各校後續因應作為，內容略以「因近期發生大量網路攻擊事件,將擴大設備封鎖範圍.....」等語。 |
| 112/1/9 | 經過整體評估及確認災損範圍後,教網中心至教育機構資安通報平台自主通報本次事件 |
| 112/1/30 | 第一階段清理，封鎖IP數量為552個 |
| 112/2/23 | 第二階段清理，封鎖IP數量為272個 |

2、此次事件主要是終端載具受感染後對外發起攻擊，若設備為校內公用載具則權責在各校，各校的資訊組長將其設備進行掃毒或重灌等相關作業後，回報教網中心即解除IP鎖定；然而若為私人載具則權責在設備所有人，若載具所有人未進一步處理，仍會因其設備的網路攻擊行為而被鎖定IP，避免其對外攻擊其他正常設備，影響基隆市整體網路正常運作。

3、受感染IP裝置大多為未更新之公用或私人windows電腦或筆電。如為公用財產，則屬於各校資產盤點項目之一；私人載具則不在資產盤點項目中。

4、教網中心核心業務之一為「維持基隆市學術網路整體運作正常」。111/12/20發生教育網路連線無預警瞬斷情形，造成網路使用不穩並非直接斷網，經基隆教網中心緊急應變處置後，教育網路已於111/12/26 恢復正當運作，各校均可使用教育網路進行教學不受影響，核心業務已回復正常運作。

5、本次資安事件發生當下，大多數的教學設備與載具均可正常運作，並不影響教學進行。且在教學場域中，網路只是輔助教學的工具，即使網路無法運作,仍可進行其他教學活動,例如書本閱讀、課堂討論、教師講解……等。此外，基隆市每個

班級都配有觸控大屏及各校公用載具亦可採用已安裝好的軟體與教學內容離線使用，因此並無因電腦或載具IP被封鎖而影響教學一事。

(四)至於殭屍網路之攻擊手法及威脅，根據法務部調查局102年3月清流月刊「殭屍網路與進階持續性威脅」[2]有簡要說明如下，其主要係駭客運用各式手法滲透系統或裝置，取得控制權，再透過惡意中繼站之連線，指揮受控制之系統或裝置協助其進行各式資安攻擊(如DDoS、挖礦及竊資等)，而其手法迄今仍不斷推陳出新，包括資安網路媒體112年12月16日報導[3]「由Cisco、DrayTek、Fortinet 和NETGEAR的防火牆和路由器組成的新殭屍網路正被利用為APT攻擊行為者的隱匿資料傳輸網路，其中包含先前曾對美國關島電信系統發動攻擊的中國駭客組織伏特颱風(Volt Typhoon)」等語，顯見殭屍網路病毒仍為資安重大威脅之一：

1、在針對性的攻擊行動中，常可見到透過殭屍網路進行資訊的竊取或是大規模的攻擊活動，當攻擊者選定攻擊的對象或目標後，將會採用多種不同的攻擊手法，針對特定目標進行長期且持續性的攻擊，不擇手段以達成攻擊的目的。許多受駭的電腦在不自覺的情況下，參與了駭客所發起的攻擊行動，而殭屍網路所使用的惡意程式，大多針對該目標被發掘的弱點進行客製化的開發。

2、殭屍電腦為了能穿透防火牆等資訊安全設備的防禦，大多採用一些在防火牆上允許通過的協定與通訊埠，也改變了傳統的資訊安全防護機制。

---

[2] 蔡一郎，殭屍網路與進階持續性滲透攻擊趨勢，清流月刊102年3月

[3] https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10859。「伏特颱風」又來？新殭屍網路鎖定邊緣設備為攻擊鋪路。

以往大多將內部的網路視為安全等級較高的區域，而外部的網路則是安全等級較低的區域，在存取的管制上，較高安全等級的區域預設就能夠連線到較低安全等級的區域，因此許多受到惡意程式感染的殭屍電腦，能夠自由地進出防火牆等資安設備，而不會受到阻擋，這也是造成殭屍網路大規模擴散與感染大量電腦主機的原因之一。

3、網管單位或是遭到惡意程式感染的系統，往往很難察覺這些通訊行為的存在；尤其當殭屍網路仍在潛伏期，除了與中繼站或駭客的控制平台保持微量的通訊外，在傳統網路流量的統計方式上，並無法有效掌握這些微量的通訊行為。

4、殭屍網路與傳統電腦病毒、木馬程式或是網路蠕蟲最大的差別在於前者除了對我們的系統造成影響之外，也配合中繼站或是中央控制站角色，提供了殭屍網路更有效的管理方式，受害的殭屍電腦會主動與這些中繼站或中央控制站進行連線，並隨時等待來自攻擊者所下達的指令，一旦接獲攻擊的指令，便能在最短的時間內依據指令的內容進行惡意攻擊，改變傳統攻擊者必須自行下達指令予分散各地的受駭主機模式，除了更有效率的管理外，也能在較短的時間內進行針對式的攻擊活動。

(五)惟按「通報應變辦法」第2條第4項第3款「未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作」之第3級事件構成要件觀之，基隆市教網中心通報本次資安事件為第2級事件有所低估，確有違失，茲臚列證據及分析如下；至於基隆市政府所稱「本次事件並未對資通系統產生影響，僅造成教

育網路使用不穩」、「受影響設備僅占少數」等說詞尚非可採：

1、**首先該府自承教網中心核心業務之一為「維持本市學術網路整體運作正常」，符合上揭辦法前段條文所稱:「未涉及關鍵基礎設施維運之核心業務或核心資通系統」甚明**，至於該府於本院履勘時稱「本次事件受影響範圍為本中心防火牆運作，而防火牆屬非核心業務」難稱有據，原因在於本案防火牆因殭屍網路瀕於負載極限，與學術網路整體運作正常與否，密不可分，不應切割看待。

2、其次，依據基隆市政府資安事件通報單內容，資安事件之破壞程度已達「**影響本市教育網路及學術網路無法正常運作**」；此外該府於12月23日及26日公告均陳述略以「……大量網路攻擊事件，**嚴重影響**本市教育網路及學術網路正常服務」，**已符合第3級事件構成要件後段條文所稱:「核心業務或核心資通系統之運作受影響或停頓」**；再經本院向基隆市基層教師查證，證實資安事件發生期間，行政作業網路確實曾有無法使用情形，益證**本案嚴重程度超出基隆市政府所稱第2級事件。**

3、最後，基隆市政府於111年12月20日發現網路異常開始排查，直至12月25日狀況(即自動封鎖IP數量未降，且防火牆接近全負載)仍未改善，似未構成該府資通安全維護計畫所稱「最大可容忍中斷時間」1至3個工作天之情形；但仍屬於通報應變辦法中第3級事件「……無法於可容忍中斷時間內**回復正常運作**」之情形，綜合研判，該府認定為第2級事件確有低估。

4、在可用性之影響方面，該府所稱「**即使網路無法運作，仍可進行其他教學活動，……教學內容離線使用，不影響教學進行**」，等語，**並未考量故障或資安事件通常屬於突發事件，也未體察基層資訊組長面對教師立即之教學需求及家長質疑而產生之壓力**，例如某教師證稱遭遇資安事件「一節課40分鐘有25分鐘在排除問題」、「老師已經習慣數位教學，碰到設備故障通常很急著修」等語，該府說詞與教學現場嚴重脫節，本院容難參採。

5、小結：為達資安聯防效果，資安事件發生單位應確實依照通報應變辦法相關構成要件進行適當等級之通報；況事件通報等級之高低，與事發單位責任或懲處並無直接相關，事發單位實無以高報低之必要，本案凸顯部分事發單位仍有大事化小之心態，有待主管機關教育部進一步宣導。

(六)此外，「通報應變辦法」設計事件等級審核單位之目的，亦係避免事發單位隱匿災情而造成災情進一步擴大；在本案中，臺灣學術網路危機處理中心(下稱TACERT)為教育網路資安事件通報對象，於本案負責資安事件等級審核等作業，然而TACERT竟認可基隆市教網中心將本案列為2級事件，其審查標準難稱妥適，亦有檢討改進空間；另查，行政院技術服務中心(下稱技服中心)早在112年1月改制為資通安全研究院，但TACERT網頁迄本院112年9月28日履勘臺東縣時，仍將技服中心連結置於首頁，其資安風險雖然偏低，惟經本院當場提示，卻迄113年1月6日止尚未修正(如下圖7所示)，其網站及內部管理顯有疏漏，難為聯防體系表率，主管機關教育部亦有檢討空間。


圖1　TACERT網頁仍將改制之行政院技服中心至於首頁連結

(七)次查，本案在通報時效亦有缺失；按通報應變辦法第4條第1項規定:「公務機關**知悉資通安全事件後，應於一小時內**依主管機關指定之方式及對象，進行資通安全事件之通報」，而依基隆市政府查復，該府111年**12月21日即已發現**造成防火牆瀕臨崩潰之原因為「BotNet（殭屍網路）攻擊」，在23日之公告亦敘明「發生大量網路攻擊事件」，該府卻**遲至112年1月9日始通報資安事件，至少延宕19日**，在通報時效上明顯違反法令規定，違失至為明確。

(八)再查，在事後復原方面，基隆市政府在111年12月20日發現資安事件後，至111年12月26日始初步控制災情，112年1月9日完成通報，至1月30日第一階段清理時，封鎖IP數量仍為552個；而該府資安事件通報單卻在「是否需要支援」一欄填報為「否」，復經本院向基隆教育網路架構上層單位台北第二區網中心查證，該中心證實未曾收到基隆市教網中心之通報或請求支援；經檢視該府於本事件所展現之處理能力，與處理效果顯不相當，若能及時向上請求支援，則應能有效縮短殭屍網路衝擊時間。

(九)另查，本次資安事件迄今未曾究明第一個遭僵屍病毒入侵的是哪個學校？哪部設備？如何入侵？如

何擴散？擴散程度(學校、系統、終端)？等等問題，尤以12月20日殭屍網路爆發時，已影響教育網路運作，可見其橫向移動擴散已有一段時間，主管機關教育部亦認資安事件之管理和應對不僅止於事態控制，應注重深入的根本原因分析和持續改進。爰此，基隆市教網中心所稱「評估本次事件已處理完畢，並查明清楚事件發生之根因，故不需送數位鑑識」，容難參採。質言之，本案未究明網路擊殺鏈並針對漏洞防堵，將導致風險持續未受控管，無法降低類案發生機率，基隆市政府做法確有違失。

(十)綜上，基隆市政府教網中心處理112年12月20日爆發之殭屍網路資安事件，在事中通報時，其事件等級及通報時效不符「資通安全事件通報及應變辦法」規定；在事後復原方面，未申請上級單位支援，導致資安事件衝擊時間拉長；在根因調查方面，並未究明本案技術手法及橫向移動模式，導致風險持續未受控管，無法避免類案肇生，均有明確違失；又TACERT除未善盡資安事件等級審核職責外，內部管理亦未臻嚴謹，長期將已改制機關之連結置於首頁而不自覺，主管機關教育部亦有檢討空間。

**二、教育機關為我國資安聯防體系之一員，連線學校達4,000餘所，使用者高達數百萬，而教育部在積極建構資安聯防體系、要求法遵及推動數位化教學之餘，卻未正視國中小兼辦資訊業務基層教師之困境；經本院訪查56位第一線教師顯示，基層存在減授課嚴重不平等、缺乏資安事件高發時期支援機制、事件通報與教學不能兼顧、專業匱乏及職務混淆等五大問題，以至於基層教師僅處理日常排查及維護即已分身乏術，遑論處理資安事件，顯見學術網路資安實有末端麻痺之虞，教育部應確實檢討並研謀精進措施。**

(一)教育機關為我國資安聯防體系之一員，並受「資通安全管理法」及其子法之規範；據TACERT簡報顯示，全國共計4千餘所學校，連線使用者高達數百萬，網路使用範圍廣大，潛在資安風險相對提高，教育部為強化資訊安全，依據「臺灣學術網路各級學校資通安全通報應變作業程序(核定版)」進行資安情資分享，共成立A-ISAC、TACERT、NA-SOC、SA-SOC 及Mini-SOC計5個聯防組織，其中A-ISAC及Mini-SOC由逢甲大學團隊負責，TACERT由中山大學團隊負責，NA-SOC由臺灣大學團隊負責，SA-SOC由國家高速網路電腦中心團隊負責，目前運行架構如下圖8，顯見整體架構尚稱完善，而本案所涉國中小資通安全屬於聯防體系末端。

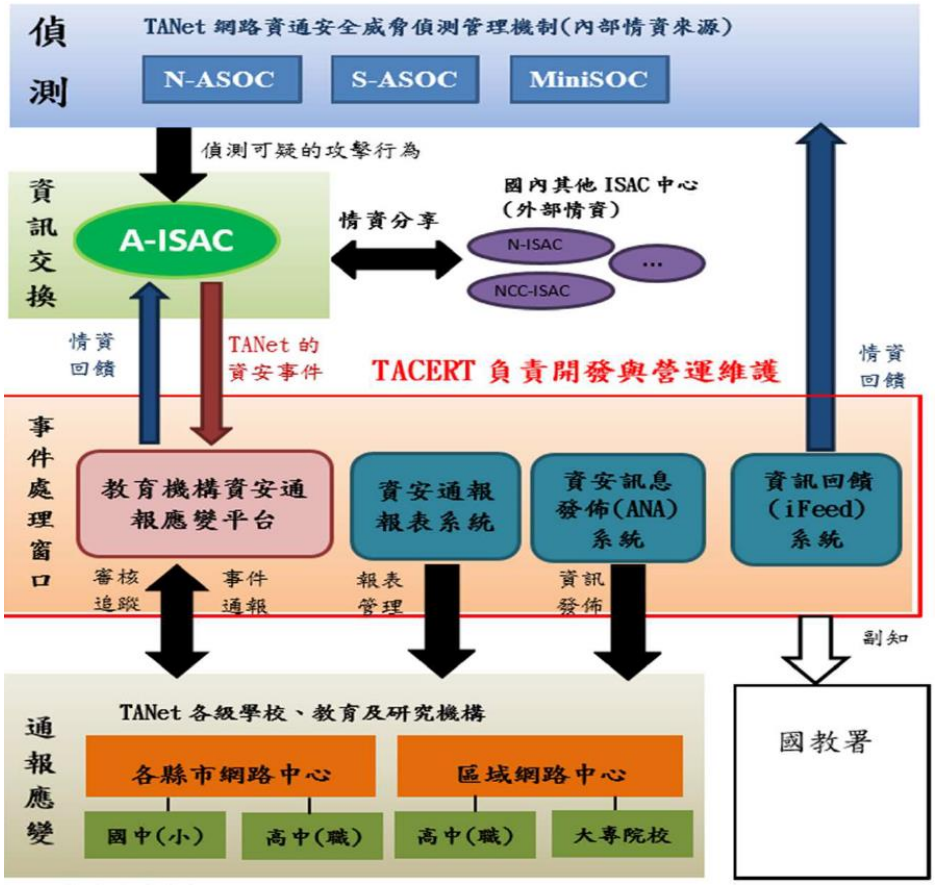


圖2　臺灣學術網路聯防架構

1、有關國中小資訊組長編制之推動過程，據該部查復：有關中小學設置資訊組長係依國民教育法第20條：「(第1項)學校為辦理教務、學生事務、總務及其他事務，應視規模大小，分別或合併設一級單位或二級單位。(第2項)前項各單位之一級單位置主任一人，二級單位置組長一人，各置職員若干人。公立學校主任由校長就甄選且儲訓合格之專任教師聘兼之，組長由教師兼任、職員專任或兼任之，職員由校長遴用之，均應報直轄市、縣(市)主管機關備查。(第3項)學校應設人事及主計單位。規模較小未設專責單位之公立學校，得由直轄市、縣(市)人事及主計主管機關(構)指派所屬機關(構)、學校之專任人事、主計人員或經有關機關辦理相關訓練合格之職員兼任之；其員額編制標準，依有關法令之規定」。

2、復依前開規定授權訂定，112年12月18日修訂之「國民小學與國民中學班級編制及教職員員額編制準則」(以下簡稱編制準則)明定國民小學各組及其他二級單位置組長一人，得由教師兼任、職員專任或兼任；國民中學部份，六十一班以上者，學生事務單位及輔導專責單位得共置副組長一人至三人，得由教師兼任。並依編制準則第7條規定：「(第1項)直轄市、縣(市)主管機關得就教職員員額編制，另定**優於本準則**之規定。(第2項)直轄市、縣(市)主管機關得依學校分布情形或學生人數多寡，視財政狀況及實際業務需要，於不違反相關法律規定下，就職員員額編制另定有關規定，並報中央主管機關備查，不受第三條及第四條規定之限制」。

(二)在通報應變架構方面，則可分為三線架構，第一線

為連線單位，如本案之國中小；第二線為區、縣(市)網路中心，主責為審核與追蹤連線單位的資安通報、協助與支援連線單位資安通報處理等；第三線則為TACERT及教育部，TACERT主責審核連線單位的資安通報等，教育部之任務則包括監督下屬機關資安通報處理、指揮重大資安事件的處理、協助跨部會的溝通協調，其通報應變架構如下圖9。

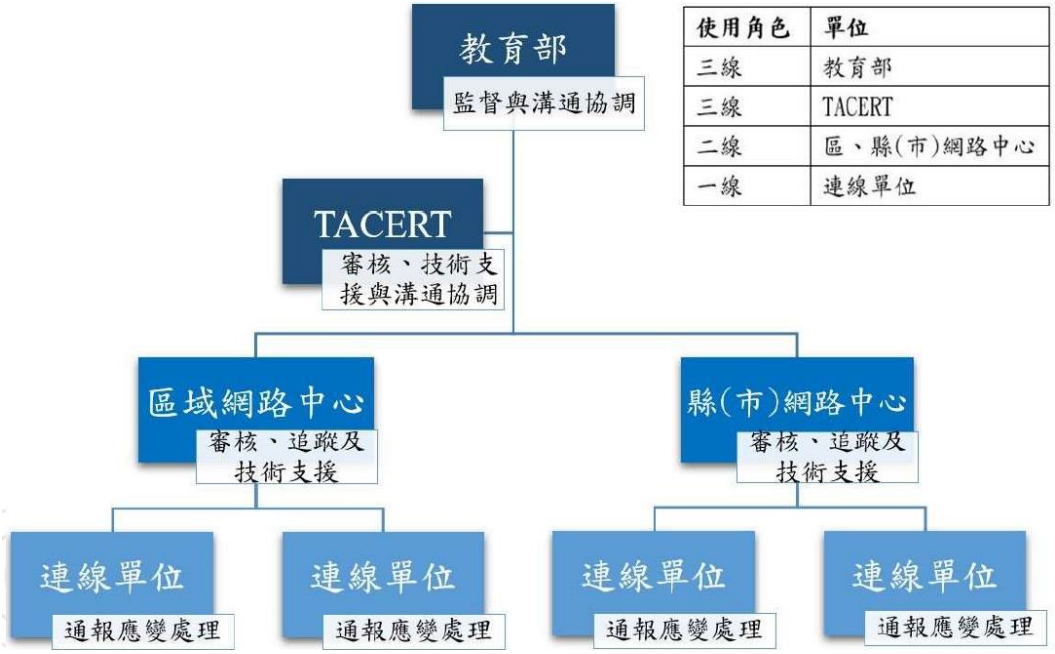


圖3　臺灣學術網路通報應變架構

(三)惟查，為掌握國中小資安業務實際辦理情形及面臨挑戰，本院分於112年9月27日赴花蓮縣、9月28日赴臺東縣、112年10月6日赴高雄市及臺南市、11月9日於本院及基隆市訪談承辦資安業務之第一線基層教師，共計56所學校，並將基層教師意見已去識別化方式臚列如下表10，經本院綜整其面對資訊業務之挑戰，**教師除普遍反映資安或資訊業務人力不足之外，其他為教育體系所特有之問題則包括減授課嚴重不平等、缺乏資安事件高發時期支援機制、事件通報與教學不能兼顧、專業匱乏及職務混淆等六**

**大問題**，茲逐一分析如後。

表2　本案訪查56位基層資訊組長之所屬學校及其意見彙整表。

| 區域 | 學校 | 區域 | 學校 | 區域 | 學校 |
|---|---|---|---|---|---|
| 東部 | 國風國中 | 南部 | 延平國中 | 北部 | 三民國中 |
| | 海星中學 | | 復興國中 | | 士林國小 |
| | 明廉國小 | | 崇學國小 | | 大安國中 |
| | 明禮國小 | | 土城國小 | | 永安國小 |
| | 嘉里國小 | | 進學國小 | | 西湖國小 |
| | 水源國小 | | 博愛國小 | | 辛亥國小 |
| | 長橋國小 | | 安佃國小 | | 長春國小 |
| | 吉安國小 | | 楠西國中 | | 溪口國小 |
| | 玉里國中 | | 麻豆國中 | | 麗山國中 |
| | 富里國中 | | 玉井國中 | | 重慶國中 |
| | 春日國小 | | 新化國小 | | 明德國中 |
| | 高寮國小 | | 玉山國小 | | 中正國中 |
| | 東里國小 | | 深坑國小 | | 百福國中 |
| | 東竹國小 | | 勝利國小 | | 武崙國中 |
| | 瑞穗國小 | | | | 仙洞國小 |
| | 寶桑國中 | | | | 港西國小 |
| | 新生國中 | | | | 中興國小 |
| | 仁愛國小 | | | | 仁愛國小 |
| | 三仙國小 | | | | 南榮國小 |
| | 嘉蘭國小 | | | | 三民國中 |
| | 富岡國小 | | | | |
| | 美和國小 | | | | |

資訊組長減授課及勞逸不均議題

- 我是專任資訊老師，18堂課之外還要負責網管。
- 如果整棟大樓斷網，我要花一個中午時間去找到原因。
- 我是網管，我是代理教師，每週20節課，因為全校只有我一個資訊背景。

- 年長教師碰到問題都會找我，我覺得很難負荷。
- 我們遇到很多人力不足，然後現在又要做很多的事情。
- 人力問題在於一般都認為年輕老師比較會管網路，但其實這個技術是要去學習的。
- 老師40分鐘上課就花25分鐘在排除故障。
- 我急需人力處理，我們有1500個學生，只有我一個資管。
- 我除了資訊相關，還兼總務處主任，也沒有任何組長，沒有文書事務。
- 我沒有資訊背景，我也不知道為什麼找我接資訊，只要跟電腦有關的問題都會找我。
- 老師年齡偏大資訊能力落後，數位落差很大都需要協助。
- 班班都有設備，管理難度大增
- 碰到的問題都差不多，我兼學務組長，包括10幾種業務，減到12堂，還有設備容易損壞的問題。老師已經習慣數位教學，碰到設備故障通常很急著修。
- 今年接資訊組長是第22年，因為沒有人，沒有人要接，每次校長都說拜託我嘛。
- 小學像他們資訊組長幾乎每一年都在換，因為國小其實大部分是教育系對嘛，師院就是教育系，他們本身不是資訊專長的。

通報、排查與教學無法兼顧問題

- 我們資安通報限定一小時覺得很趕，如果我不在當地或正在開會，就很難處理。
- 如果碰到要資安通報，我科任老師就要臨時找人代班。
- 通報時一小時是真的很趕。
- 我在上課的時候，突然出事或者是行政老師電腦或網路出現問題，但我自己有班級的課程，我不能拋下小朋友。
- 如果是很緊急的狀況，我可能就是先安頓好我的班級，然後再來趕快去拿我的筆電，然後再先把教室裡有問題的電腦先做斷線處理。
- 我在上課，那現在發生資安事件了，那我是要先處理資安事件，還是我要先上課? 資安演練他的規定是一個小時之內要通報,可是我上課如果是連續三節課呢?那我怎麼去處理通報的問題?
- 這個1小時的時間可能會對我比較有壓力
- 確定這個是資安問題了以後，你就要做立即的處理，比如說拔掉電源啊，或者是鎖IP，還是需要佔一點上課的時間去處理啦。
- 老師使用到一半的話學生不能上網,那我們就要馬上去處理,就是在處理這些雜事

資安事件高發時期支援機制問題

- 我是贊成開口契約
- 資訊教師不足的原因主要是非專業被委任成專任，碰到狀況他可能不會處理，我建議國教署可以採共聘，大校則專任技術面的人員。
- 去年接資訊的是代理老師完全不會電腦，碰到問題只能找工程師。
- 除了行政職，一般老師都身兼三職，碰到問題都無法及時處

| |
|---|
| 理，資安事件也只能做最基本的判斷。<br>● 國立高中職有資服中心可以處理，但國中小真的很難，例如好幾個學校共聘一個也好。<br>● 有沒有可能我們在國小端有專職或專責的人員，可以來負責協助處理。如果沒有專責的人駐守在學校，那至少他可以用分配的，就是不一定要固定時間，他可以是一個一個禮拜來一次<br>● 蠻需要有一個專責這方面的一個人力來協助我們第一線教學現場來去協助 |
| 業務範圍與人力配套問題<br>● 經常接到必須立即處理的資訊問題，和教學很難兼顧，我還必須處理很多設備使用方面細節問題。<br>● 只要幾乎有關電的設備，都是我們在管理，設備量大概上千，小校也有幾百台設備<br>● 只要任何資訊設備問題，我必須要立即去支援，那我在上課的時候真的就沒有辦法。<br>● 以前都是黑板不會壞，但現在都換大屏，這個東西就變成全部都是資訊組的。<br>● 教室裡面有一臺大屏突然故障要排除，這中間來來回回不要講3分鐘，我們中間只要1分鐘的話，就會影響到老師的教學的精神，然後班級的管理都會出問題。<br>● 我們就是隨時都要stand by，壓力是很大。<br>● 這個年代什麼東西都會用到電腦，什麼東西都會用到網路，所以其實我們這業務越來越多。<br>● 像是數位學生證，本來學生證是學務處的業務，當多了一個數位之後，好像就變成了資訊業務，還有電錶就變成數位電錶，也變成是我們的業務，這就是為什麼我們資訊為什麼業務好像越來越多 |

(四)經查，有關教師除普遍反映資安或資訊業務人力不足之問題，經訪查結果彙整，主要係因教育部近年積極推動數位化教學政策，包括國民及學前教育署之「推動中小學數位學習精進方案」及「高級中等學校智慧網路環境暨學術網路提升計畫」等，資安法遵亦逐年增加，另因疫情因素，遠距及視訊需求暴增，然而相關**人力配套卻未同步成長**；據部分基層教師反映，以「生生用平板」政策為例，一校數百台平板設備之故障排除及電源管理實係極為繁瑣之工作，復以欠缺實益之開機連網率作為績效指標，已**造成日常資訊網管業務及資安業務之嚴重排擠**，均待教育部提出具體有效之紓解措施，以避免

資訊及資安成為基層教師避之唯恐不及之業務。

(五)次查，有關減授課嚴重不平等一節，本院訪查結果顯示，**部分教師兼辦資訊業務卻未獲減授課，一週仍需授課達18到20節(滿堂)，部分卻一週僅需授課4節，其勞逸不均程度極為嚴重**，部分基層教師甚至稱「排查設備問題忙到沒有時間上廁所」；對此，教育部查復所稱：「為給予學校彈性因應多元化業務之裁量空間，各校得自行評估業務負荷，酌予減授協助行政之教師每週基本教學節數」云云顯未正視，容難參採；事實上教育部所提供校長之裁量範圍，根本無法協助實際需要適當減授課之基層教師；此外，教育部查復之全國數據，竟無超過16節(即減授課低於4節)之情形，此與本院實地訪查東部地區縣市即至少有兩位基層教師單週超過18節課之情形有相當出入，由此可見教育部在減授課部分之掌握與教育實況已有脫節，有待積極檢討，而教育部國教署既已承諾另案函請個案轄管之地方主管機關瞭解並予以調整，即應持續追蹤至改善為止；茲將佐證臚列如下:

1、依據「國民中小學教師授課節數訂定基準」(105年4月8日修訂):

（1）第2條規定，國民中小學專任教師之授課節數，依授課領域、科目及學校需求，每週安排16節至20節為原則，且不得超過20節之上限。專任教師授課節數應以固定節數為原則，不宜因學校規模大小而不同。

（2）第4條規定，專任教師兼任行政職務，其**減授節數之基準由各該主管教育行政機關訂定之**。

（3）第7條規定，各該主管教育行政機關應訂定不同規模國民中小學之行政組織層級、單位及人

員配置，發揮總量管制效益，合理調配專任、兼任及部分時間支援教學之人力，以維教學品質。

2、經教育部調查，資訊組長授課節數比率如下表，另有關兼辦資訊業務之教師尚非屬資訊組長之編制，爰該部國教署將另案函請各地方主管機關全盤檢視協助行政（包括資訊業務）之教師減授課時數情形，並請各地方主管機關督導學校調整減授課情形。

表3　教育部調查全國國中小資訊組長授課節數分佈

| 授課節數 | 國中 | 國小 |
|---|---|---|
| 0-4 | 37.07% | 3.25% |
| 5-8 | 54.09% | 43.00% |
| 9-12 | 8.84% | 43.00% |
| 13-16 | 0% | 10.75% |
| 合計 | 100% | 100% |

(六)又查，在缺乏資安事件高發時期支援機制部分，本院訪查多數基層教師均表示，目前縣市政府教育網路中心多數雖有群組聯繫及非制度性之支援機制，惟量能仍不足以因應平時故障或資安通報排查所需，如遇本案基隆市之大規模資安事件爆發，則教網中心亦分身乏術，無暇支援國中小排查駭侵事件，將導致事件衝擊規模及時間擴大；對此，教育部則正面回應，有關短期進駐團隊規劃一節，該部現有相關聯防組織及各區網中心皆可提供必要協助，因6都與16縣市之資源與需求各自不同，該部將召集22縣市研討，尋求適合作法，以縮短是類事件發生時處理時效。茲將重要調查內容節略如下

1、其中臺北市政府教育局因應學生人數、高度數位化教學及設備管理繁雜等因，在資訊組長之外，

另設有「系統管理師」一職，能有效支援資訊工作及資安事件排查，如在經費許可範圍，值得教育部及其他縣市參採。

2、另查臺南市政府教育局在網路架構方面高度向上集中，且防火牆配置合理先進，基層教師表示可大幅節省平時管理成本。

3、綜前，資安講究「security by design」(安全始於設計)，本院經由訪查不同縣市結果顯示，無論資源是否豐沛，各縣市教育局及國民中小學教師均感資訊或資安人力不足，部分縣市亦因網路架構設計未臻完善，而必須使基層教師疲於奔命；惟欲利用有效率之網路及防火牆架構節約人力，仍有賴教育部爭取經費並挹注資源有限之縣市。

(七)再查，在事件通報與教學不能兼顧部分，按「通報應變辦法」第4條規定:「公務機關**知悉**資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報」，其關鍵在於「知悉後」通報，而非「發生後」通報；惟經本院訪查56所國中小，發現基層教師普遍將資安事件「知悉」後通報，誤解為「發生」後通報，以致經常發生教學及應變處理無法兼顧情事；對此，教育部正面回復已規劃透過各種管道，如教育訓練，加強宣導「知悉」後通報之涵義，而非「發生」後通報，或經由通報應變演練機會，讓學校資訊組長在合理的時間內進行相應的處理和回應。透過這些改進措施，應可提高資訊安全通報機制的效能，同時減少誤解和不必要的錯誤。此外，針對基隆市政府於本院履勘簡報稱:「即使網路無法運作，仍可進行其他教學活動，……教學內容離線使用，不影響教學進行」云云；然而實務上，資訊組長遭遇老師及家長反映設

備問題或教學受到影響，不可能如此回應而必須儘速予以排除，再再顯示前述強調支援人力及改善網路架構之重要性。

(八)另查，在專業匱乏部分，本院訪談發現，第一線資訊組長為資訊本科或自然科學背景者偏低，於承辦資訊或資安業務自然事倍功半，復經教育部協助普查如下表12，在國小部分，約有半數具資訊或自然科學背景；在國中部分則較佳，有72%資訊組長具資訊或自然科學背景；顯示在國小部分，教育部仍應持續推動資訊背景教師之進用，或提供非專業背景之資訊組長額外支援；此外，在東部場次訪談亦有教師反映，非專業背景資訊組長縱有心進修，仍因反映地處偏遠不易參加資安相關講習，此有待教育部及縣市政府教育局處設法克服，以提升基層學校整體資安素養。

表4　教育部調查全國國中小資訊組長專業背景及其比率表。

| 資訊組長畢業科系 | 國中 | 國小 |
|---|---|---|
| 資訊相關科系(含科技教育、資訊教育、管理、工程等相關學系) | 39.01% | 29.18% |
| 數學及自然科學相關科系(含自然科學教育、數理教育等相關學系) | 33.41% | 21.95% |
| 教育相關科系(含特殊教育、幼兒教育、技職教育、成人教育等相關學系) | 8.19% | 17.34% |
| 心理諮商相關科系 | 0.86% | 0.54% |
| 史哲相關科系(含歷史、地理、哲學、生死、社會教育等相關學系) | 2.37% | 6.59% |
| 財經、法政相關科系(含企業管理、休閒管理、公共事務等相關學系) | 3.88% | 8.22% |
| 語文相關科系(含中文、英語、日語或其他外國語言等相關學系) | 4.74% | 6.78% |
| 藝術相關科系(含美術、藝術教育、音樂、大眾傳播等相關學系) | 4.31% | 5.33% |
| 體育相關科系 | 1.72% | 2.71% |
| 其他 | 1.51% | 1.36% |
| 合計 | 100% | 100% |

(九)至於在職務混淆一節，經本院訪查，不少教師反映兼辦網管及資安之外，尚須承辦任何名為智慧及網路相關之業務，訪談中即有教師反映**「只要幾乎有關電的設備，都是我們在管理，設備量大概上千，小校也有幾百台設備」**，而例如「智慧電錶」、「網路監視器」及「數位學生證」等，在未資訊化之前應係總務或學務業務；而資訊化後卻必須由分身乏術之資訊組長兼辦，實非合理，教育部宜就資訊組長之職務設計及範疇予以檢討並強化宣導，俾使資訊組長專注於持續擴張的資訊及資安業務。

(十)綜上，快速成長的資安法遵及業務數位化導致人力窘迫，並非教育體系單獨之挑戰，而係公私立部門普遍面臨之嚴峻問題；然而在教育體系，特別是聯防體系之末端-國中小學，經本院調查確有其特殊之問題及需求，包括減授課嚴重不平等、缺乏資安事件高發時期支援機制、事件通報與教學不能兼顧、專業匱乏及職務混淆等，已導致基層學校根本無暇，也無充分能力處理資安事件，致使學術網路有末梢麻痺之虞，有待中央及地方教育主管機關積極研謀改善。

**三、資安鑑識之目的在於究明事件根因並加以防杜，避免再遭類似手法駭侵；惟本案基隆市教育網路資安事件，對於殭屍網路大規模爆發所用漏洞或橫向移動途徑等技術手法迄今仍未究明，將難以降低教育網路發生類案之風險，教育部及基隆市政府允宜加以檢討。**

(一)資安鑑識工作在事後復原階段有重要意義，以資通安全研究院為例，其在通報應變中心轄下設有「鑑識處理組」；在國家資通安全發展方案(110年至113年)，亦將「提升資安事件溯源追蹤能力：持續拓展資安鑑識能量，自主研發現場取證工具，並強化情

資分享及技術交流，分析比對策動攻擊之來源與駭客組織，以達溯源目的」納入推動策略中。另外，資通安全署112年9月份「資通安全網路月報」[4]並敘明略以：「……**發生資安事件時，應進行事件根因分析**，據以完成漏洞修補、強化作為及改善措施，若因設備儲存空間不足而無法確認事件發生原因，除強化設備安全防護措施與偵測機制外，亦建議宜擴增日誌儲存空間(如另建置Log Server)、加強檢視日誌或清查網通設備等防護措施，以利後續調查事件發生原因，降低重複遭入侵的風險。」已足徵資安鑑識作業在事後亡羊補牢之功能及重要性

(二)次據教育部108年4月訂頒「臺灣學術網路各級學校資通安全通報應變作業程序」涉及本案規定如下，顯示本案未檢具調查報告之原因，在於本案僅被審核為2級事件，然而於事後復原部分，仍需進行原因分析：

1、第3章通報作業第7點：「4」、「3」級資安事件依本項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於1個月內將調查、處理及改善報告函送本部，由本部彙送主管機關。

2、第4章應變作業：各連線單位應建立資安事件之「事前安全防護」、「事中緊急應變」及「事後復原」作業之具體機制，並至少包含下列各項……，包括：

（1）事中緊急應變：

〈1〉……並保留被入侵或破壞相關證據。

〈2〉……如發生重大(「4」、「3」級)資安事件，

[4] https://moda.gov.tw/ACS/press/report/8493。

應主動提供相關設備系統日誌予所屬區、縣（市）網路中心及通報應變小組，俾提供相關協助。

（2）事後復原：

〈1〉在完成復原重建工作後，應將復原過程之完整紀錄（如資安事件原因分析與檢討改善方案、防止同類事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料),予以建檔管制，以利爾後查考使用。

〈2〉全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。

(三)經查，基隆市教網中心查復說明「本中心評估本次事件已處理完畢，並**查明清楚事件發生之根因**，故不需送數位鑑識」，惟經本院詢問教育部及基隆市政府有關本案第一個遭僵屍病毒入侵的是哪個學校？哪部設備？如何入侵？如何擴散？擴散程度(學校、系統、終端)?等等有助於於釐清網路擊殺鏈之問題，該府教網中心卻無法具體回應，顯見該府作法不能稱為妥適之根因分析；而TACERT率爾認定本案為2級事件，更是使該府不需依照「臺灣學術網路各級學校資通安全通報應變作業程序」進行調查報告的主要原因之一，再次證明調查意見一所陳，基隆市政府教網中心與TACERT缺失至臻明確；換言之，本案既未查明殭屍網路之技術手法及橫向擴散方式，則該漏洞可能依舊存在，而有導致下一次相同樣態之大規模資安事件之虞；教育部既函稱本案處理仍有改善空間，則應督同所屬聯防體系以本案為鑑，核實認定事件等級並適時啟動鑑識溯源作

業，茲說明如下：

1、教育部查復如下：

（1）在事故發生之初，初判為新購防火牆設定問題，後續處理過程中發現實為轄下學校集體爆發僵屍電腦網路攻擊所致，由於未接獲轄內學校資安通報，實無法判斷事件初發點，囿於處理人力不足，決定採快速復原策略，並未對轄下數十所學校設備進行資安鑑識。

（1）對此事件發生處理仍有改善的空間，例如強化轄內學校資安通報避免大規模事態、請求上層資安機構協助等。資安事件的管理和應對不僅止於事態控制，應注重深入的根本原因分析和持續改進。有助於建立更健全的資訊安全體系，將經驗分享給其他機構，以降低是類資安事件生機率。

2、在資通安全管理方面，一般雖著重於防禦面，然而由攻擊面檢視擊殺鏈，亦可達成主動式防禦之效果，根據資安院110年第2季資通安全技術報告，國際及業界一般以MITRE ATT&CK[5]描述攻擊者行為之知識庫框架，讓企業組織與資安產業對於攻擊者能有共同之行為樣態描述:

（1）MITRE於105年提出ATT&CK描述攻擊者行為之知識庫框架，讓企業組織與資安產業對於攻擊者能有共同之行為樣態描述，該框架彙整眾多駭侵組織攻擊行為，並建立共通描述語言，涵蓋攻擊前、中、後之入侵戰略、技術及流程(Tactics,Techniques,and Procedures,TTP)，讓企業組織與資安產業都受益，進而知己知彼，以

[5] Adversarial Tactics, Techniques and Common Knowledge

強化資安防護。

（2）MITRE更於109年提出「MITRE Shield」，用以描述主動式防禦之知識庫框架，使企業組織與資安產業能進一步防護攻擊者行為。該框架參考ATT&CK知識庫，提供防護、欺敵及交戰行動之參考準則，讓企業組織與資安產業可依據攻擊者行為，進行偵測、擾亂及阻擋等防護措施，而制敵機先以完備資安防護方案。

（3）109年10月發布ATT&CK Version 8最新版，主要為完整呈現網際攻擊狙殺鍊(Cyber Kill Chain)，整合原先PRE-ATT&CK，增加偵查(資訊蒐集)與資源開發(工具開發)，並汰除不夠精確與重複之技術項目。相較於原版本之技術(Technique)涵蓋範圍與執行細節不一致，新增子技術(Sub-technique)項目，可更細緻化描述各式攻擊技術之實行方式，並提供防護建議。

(四)綜上，資安事件根因分析、鑑識或溯源，目的在防堵漏洞並防範類案再生，而本案囿於基隆市政府教網中心通報及TACERT審核認定為2級事件故無需提交調查報告，然依「臺灣學術網路各級學校資通安全通報應變作業程序」規定，仍必須進行根因分析；惟基隆市教網中心僅了解本案為殭屍網路攻擊，技術手法及橫向擴散方式卻不得而知，因此不能稱為根因分析，爰有明確違失；教育部既函稱本案處理仍有改善空間，則應督同所屬聯防體系以本案為鑑，核實認定事件等級並適時啟動鑑識溯源作業。

**四、資通安全稽核目的在於改善並強化機關資通安全防護工作之完整性及有效性，惟查本案受殭屍網路感染學校雖均曾辦理資安稽核，但稽核報告所列缺失多為欠缺文件，並未發現資安事件高發樣態(如殭屍網路)**

**之潛在風險，以至於相關風險直至感染爆發時仍未受控管，對照本案最高500餘個IP被感染之災情，顯示稽核作業已有流於形式之虞，且基於稽核作法及標準大致雷同，本案恐非個案，教育部允宜會同「資通安全管理法」主管機關本於資安聯防精神研謀改善措施，俾使稽核作業發揮應有功效。**

(一)根據「資通安全管理法」主管機關(目前為行政院，修法草案為數位發展部)112年3月所頒佈之「112年資通安全稽核計畫」，資安稽核之目的有二，其中之一為「經由外部稽核各機關資通安全維護計畫實施情形，改善並強化機關資通安全防護工作之完整性及有效性，以持續精進管理政府整體資安風險」，換言之，稽核必須具備改善機關資安防護工作有效性之功能；此外，稽核結果依所發現之缺失，依照ISO27001標準，依嚴重程度分為「主要缺失」、「次要缺失」及「觀察事項」等三類，其中「主要缺失」、「次要缺失」必須加以追蹤改善，核先敘明。

(二)經檢視基隆市教網中心之稽核情形，該中心每年配合基隆市政府執行第三方稽核，109年迄今共3次(110/3/4 、111/4/13 、112/3/10)皆已通過ISO/IEC 27001:2013驗證，並取得證書，其稽核發現臚列如下，包括110年有1項次要缺失、6項觀察事項，111年有2項次要缺失、3項觀察事項，112年有2項觀察事項；由該三年稽核發現，除了111年次要缺失「校務行政系統之密碼原則未依組織要求設定。如：變更密碼時輸入1234567被系統接受」屬於帳密強度問題，較可能被利用為殭屍網路入侵管道之外，該3年竟查無殭屍網路可能滲透管道，對照本案最高有500餘個IP所屬裝置被感染，已顯示資安稽核之有效性有待商榷。

(三)次查，在學校層級的資安稽核方面，基隆市教網中心於110至112年已執行共4次第二方稽核(110年2月、110年11月、111年11月、112年4月)，共完成32所學校第二方稽核，茲將稽核發現摘要綜整如下表13，該4次學校層級稽核不符合事項計21項，觀察/建議事項計192項，合計213項；其中**所列缺失多為欠缺文件**，可能造成殭屍網路入侵之稽核發現僅有2項，且均為帳密強度問題，尚無其他與殭屍網路有關之主要或次要缺失；而教育部雖然說明稽核發現部分學校有「未及時更新 Windows 作業系統」的情況，易成為殭屍網路之漏洞；惟並未列為主要或缺失，以至於追蹤管考強度有限，再次顯示資安稽核未能發現資安事件高發樣態(如殭屍網路)之潛在風險，稽核作業已有流於形式之虞。

表5　基隆市國中小資安稽核情形綜整

| 稽核年度 | 稽核學校 | 稽核發現 | | | 與殭屍網路相關之主/次缺 |
|---|---|---|---|---|---|
| | | 不符合事項(主/次缺) | 觀察/建議項目 | 合計 | |
| 109 | 中正國小 | 0 | 4 | 4 | 無 |
| | 中興國小 | 0 | 5 | 5 | 無 |
| | 和平國小 | 0 | 4 | 4 | 無 |
| | 建德幼兒園 | 0 | 5 | 5 | 無 |
| | 暖西國小 | 0 | 6 | 6 | 無 |
| | 正濱國中 | 0 | 4 | 4 | 無 |
| | 銘傳國中 | 0 | 1 | 1 | 無 |
| | 隆聖國小 | 0 | 5 | 5 | 無 |
| 110 | 八斗國小 | 0 | 7 | 7 | 無 |
| | 建德國中 | 0 | 8 | 8 | 無 |
| | 德和國小 | 0 | 4 | 4 | 無 |
| | 暖暖高中 | 0 | 7 | 7 | 無 |
| | 武崙國中 | 2 | 6 | 8 | 帳密強度問題 |
| | 深美國小 | 1 | 5 | 6 | 無 |
| | 百福國中 | 2 | 8 | 10 | 無 |

| | | | | | |
|---|---|---|---|---|---|
| | 碇內國中 | 0 | 10 | 10 | 無 |
| 111 | 五堵國小 | 0 | 4 | 4 | 無 |
| | 仁愛國小 | 1 | 8 | 9 | 無 |
| | 堵南國小 | 1 | 5 | 6 | 無 |
| | 成功國中 | 1 | 6 | 7 | 無 |
| | 成功國小 | 5 | 11 | 16 | 無 |
| | 武崙國小 | 0 | 3 | 3 | 無 |
| | 忠孝國小 | 3 | 8 | 11 | 無 |
| | 尚仁國小 | 1 | 7 | 8 | 無 |
| 112 | 建德國小 | 0 | 5 | 5 | 無 |
| | 七堵國小 | 2 | 7 | 9 | 未設定帳密 |
| | 八堵國小 | 0 | 5 | 5 | 無 |
| | 碇內國小 | 1 | 8 | 9 | 無 |
| | 西定國小 | 0 | 3 | 3 | 無 |
| | 南榮國中 | 1 | 5 | 6 | 無 |
| | 中正國中 | 0 | 8 | 8 | 無 |
| | 信義國小 | 0 | 10 | 10 | 無 |
| 合計 | | 21 | 192 | 213 | |

(四)綜上，資安稽核為資通安全管理中，重要之事前防範作業，然而由稽核報告內容參照本案資安事件，稽核似乎未能事前揭露資安風險，其有效性值得進一步加以強化。對此，教育部雖已承諾透過行政協助，建議基隆教網稽核時，應從策略面、管理面及技術面多方考量，以提高稽核有效性；然ISO27001稽核作業標準化程度極高，換言之，其他機關之稽核亦可能存在有效性問題，教育部宜會同主管機關通盤加以考量，以全面提升資安稽核之有效性。

參、處理辦法：

一、調查意見一、三、四，函請基隆市政府確實檢討改進見復。

二、調查意見一至四，函請教育部督同所屬確實檢討改進見復。

三、調查意見送數位發展部資通安全署參處。

調查委員：賴鼎銘

王麗珍

葉宜津