SSL/TLS 加密封包監控之法律上疑慮

林伯樺

摘要

基於網路資通安全之需要，網路通訊大幅使用SSL/TLS等加密技術進行通訊，以避免通訊中發生資訊外洩等資安事件發生。而目前 SSL/TLS 加密技術已成為網路流量主要之通訊協定，計有過半之網路通訊流量採用此等加密技術。唯加密技術之使用，亦成為駭客進行網路攻擊、病毒傳播或有心人士外洩機敏資訊之管道，亦即利用加密後通訊無法探知之特性，將病毒、網路攻擊或外洩機敏資訊藏匿於加密通訊中以規避防火牆之檢查。因此利用新型資安設備對於加密通訊內容進行檢查，已為目前資安防護所必要採行之手段。然對於加密通訊進行解密並解析，是否將有侵害秘密通訊之虞，而成立刑法上妨害秘密、妨害電腦使用罪或通保法之違法監察罪是必須要思考的問題。本文試圖由分析網路封包特性出發，就解密可能構成之刑事責任加以探討，並尋找調和資通安全與秘密通訊自由法益衝突之可能。

關鍵字：資訊安全、加密通訊、妨害電腦使用、違法通訊監察、封包、SSL/TLS

abstract

Based on the need of network security, people use SSL/TLS or other encryption technologies to encrypt network communications to avoid information leaks and other security incidents. At present, SSL/TLS has become the main communication protocol for network traffic, and more than half of the network communication traffic uses such encryption technology. On the other hand, the use of encryption technologies has also become a channel for hackers to conduct network attacks, computer virus transmissions, or confidential information leaks. Encrypted communications have important features that whose contain can't be detected, so hackers may hide the computer virus, network attacks or confidential information leaked in encrypted communications to circumvent the firewall check. Therefore, the use of new security equipment or technologies to check the encrypted communication content has become a necessary means for the current information security.

However, if the encrypted communication is decrypted and parsed, whether it will infringe on the right of secret communication and cause the crime of illegally supervising on communication or impairing the use of the computer is a problem that must be considered. This paper attempts to analyze the criminal liability of decryption according to the characteristics of network packets and finds the possibility of reconciling the conflict of information security and the right of secret communication.

Keyword: information security, encrypted communication, impairing the use of the computer, illegally supervising on communication, packet, SSL/TLS

一、前言

資訊安全為現今國家安全、社會發展所不可或缺之環節，我國更於 107 年 5 月 11 日三讀通過資通安全管理法，宣告我國資訊安全發展進入一個新的時代。然資訊安全並非僅有國家機關之重視即可，尚必要由各基礎環節普遍落實方足以維持整體資訊通訊環境之安全，而其中最為基本之步驟，即為使用適當防火牆對各種惡意程式、攻擊進行防禦，及採用加密之通訊協定傳輸資料以免資料竊取二者。根據報告指出，目前已有過半網路流量採用了 SSL/TLS 技術加密保護[1]。但原本為了增進資通安全所生之加密傳輸，卻與資通安全之間卻不可避免發生齟齬；詳言之，廣泛使用加密之傳輸協定，故可避免資料傳輸過程中發生資訊遭竊等資安事件發生，但若原本即已存在電腦中的惡意程式，亦透過加密之傳輸協定對外傳送資料，抑或外部攻擊者透過 SSL/TLS 等加密連線對內部伺服器、電腦進行攻擊時，防火牆即面臨無由發現、監控之困境。

於此困境下，技術發展使次世代防火牆等資安技術設備，具有就加密傳輸協定之封包流量進行解密之能力，進而可監控包括傳輸之流量、位置等資訊，透過對傳輸流量、頻率之分析，得以發現惡意程式、病毒之存在。但於此卻發生第二個爭議之處，防火牆或其他分析設備與資料之傳輸者屬於同一人所有時，其固然不生爭議，但倘防火牆或其他分析設備與資料傳輸人分屬不同人時，是否發生通訊保障及監察法中之違法通訊監察，或刑法中妨害電腦使用等情形？此等情形又以企業設置防火牆，對員工或其他利用網路之使用者（例如訪客）進行監控防禦最易發生。企業基於組織內部資訊之保護，因而對內部員工使用網路通訊產生監控必要，以避免惡意程式之攻擊及因企業間諜行為所致之資訊外洩事件，然此與刑法保障之秘密通訊自由、電腦使用安全，及通訊保障及監察法保障之秘密通訊自由，將發生緊張關係。

是以本文企圖由網路封包之結構與加密技術出發，以及刑法暨通訊保障及監察法之相關規定，理解就加密封包進行解密所可能涉及之法律上疑慮、爭點，希企能就此技術於資安保障與個人電腦使用安全、秘密通訊自由之保障兩者間取得平衡。

二、封包結構與 SSL/TLS 加密技術

網路為現代資訊生活中幾近不可或缺之通訊方式，而資訊欲在網路上傳輸，則必須透過各種軟體、通訊協定，將資料轉換為封包（packet）透過網路傳輸至目的端節點，再由目的端依循通訊協定及軟體規格將封包解開得到資料。目前對於通訊協議、封包格式之理解，以 OSI 參考模型與 TCP/IP 參考模型二者為主，茲簡要說明如下。

（一）OSI 參考模型與 TCP/IP 參考模型

1.OSI 參考模型

[1] Electronic Frontier Foundation, We're Halfway to Encrypting the Entire Web, 2017.02, available at: https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web , last visit at: 2018.06.19.

OSI 參考模型係 1977 年 ISO（國際標準組織）制定之概念性架構，用於設計網路標準之參考；其由下往上分別為第一層的實體層、第二層的資料連結層、第三層的網路層、第四層的傳輸層、第五層的會議層、第六層的表達層，以及第七層的應用層：而資料傳輸時，會由應用程式的應用層開始向下至實體層，經過資訊網路傳輸後，接收方的電腦再由應用層開始層層將封包解開，最後得到原始資料。[2]

2.TCP/IP 參考模型

相較於 OSI 參考模型，主要用於網際網路 TCP/IP 通訊協定者，為 TCP/IP 參考模型。TCP/IP 參考模型將網路傳輸區分為四層，由下往上分別為第一層之連結層、第二層之網路層、第三層之傳輸層，及第四層之應用層。其中第一層之連結層相對應於 OSI 參考模型之第一、二層，第四層之應用層相對應於 OSI 參考模型之第五至第七層。傳輸方電腦係由第四層開始不斷將原始資料封裝，最後於第一層連結層以「訊框」（frame）方式傳輸，而接收方電腦則是將資料一層層解封，最後得到原始資料；而其中一般習慣稱為「封包」（packet）的資料，在 TCP/IP 參考模型中是指於第三層網路層中之資料；於第二層傳輸層中的資料，則稱為資料段（segment）。[3]

而 TCP 資料段之格式，包括了 TCP 表頭（header）與 TCP 資料（payload）兩個部分，TCP 表頭係用來記載 TCP 連線的相關資訊，包括傳輸來源通訊埠、目的通訊埠、封包的序號、確認序號、檢查碼等傳輸用的資訊；而 TCP 資料則是記錄了來自於應用層的資料，亦即電腦中各種軟體使用的通訊協定所產生的原始資料。[4]舉例而言，以 BBS（Bulletin Board System）系統為例，使用者於用戶端（client）輸入之資料，會經過 BBS 軟體（如 NetTerm）轉換成符合 Telnet（遠端登入）通訊協定之資料（應用層），經過傳輸層加上 TCP 表頭成為資料段，然後於網路層加上 IP 表頭變成封包，最後以訊框的格式在連結層中進行傳輸至伺服器（server）端的 BBS 主機。

（二）SSL/TLS 加密技術簡介

一般網路上傳輸之資訊，係以 TCP/IP 參考模型封包為主，然此種封包倘若未經加密，在網路傳輸時可謂毫不設防；換言之，倘若未經過加密程序即進行傳輸，除用戶端與伺服器端外，在傳輸的網路中任何一段，只要能夠攔截到此一封包，即可觀察封包內容，不僅包括表頭的部分，亦包含其上層資料內容；且雖然欲於網路中傳輸，必須以經組譯後之二進位制機械碼方式傳送，在傳輸層的資料段或網路層的封包，則可能以十六進位制方式呈現，一般人固不能輕易理解，但透過程式反組譯還原後，即可獲得使用者輸入之原始資料。因而，為確保資訊傳輸之安全，須採用加密方式將本文（plaintext）轉換成密文（ciphertext）後再進行傳輸，接收方接收密文後，再進行解密將密文還原成本文；而目前網際網路主

[2] 陳惠貞，新趨勢網路概論，碁峯，2018.04，頁 2-2～2-3。
[3] 前揭註 2，頁 2-10～2-11。
[4] 前揭註 2，頁 12-11～12-12。

要採用之加密技術，如上揭所述，有過半採取 SSL/TLS 方式加密。

TLS（Transport Layer Security，傳輸層安全性協定）加密技術係以 SSL（Secure Sockets Layer，安全通訊協定）技術為基礎發展之技術，目前版本為 1.3，但基本的加密概念仍與 SSL 技術相同。SSL 對於網路傳輸過程，係採取非對稱式加密及對稱式加密兩種方式結合模式進行，以下就 SSL 加密技術與過程簡要說明。

1.對稱式與非對稱式加密

加密技術有所謂對稱式與非對稱式兩種，所謂對稱式加密（symmetric encryption）是由傳輸方與接收方協議一不公開的秘密金鑰（secret key），傳輸方利用此金鑰將資訊予以加密成為密文，而接收方亦利用此金鑰將密文解密獲得本文的原始資料。此種加密方式之安全性取決於秘密金鑰的保密程度，具有演算法容易取得、運算速度快速等優點；缺點則在於每對使用者均須協商該組通訊中的秘密金鑰，因而需要大量的秘密金鑰，且無法利用加密過程同時進行通訊對象身分認證，及一旦金鑰外洩通訊雙方即必須重新協商金鑰等。[5]

而所謂非對稱式加密（asymmetric encryption）則是存在一對公鑰（public key）與私鑰（private key），公鑰與私鑰是透過特定公式計算所得，以公鑰加密後僅有私鑰得解密，反之透過私鑰加密後僅有對應之公鑰得解密；而公鑰對外公開，私鑰則保持不外洩。當用戶端利用伺服器端所公開的公鑰將資訊加密後，僅有伺服器端所持有之私鑰得以將資訊解密，伺服器端以私鑰將資訊加密後，用戶端得利用其公開的公鑰將資訊解密。因此非對稱式加密所需要的金鑰數目較少，同時較易於傳播，且可同時達成認證通訊對象身分之效果。[6]

2.SSL/TLS 加密過程概念

SSL/TLS 的加密過程，簡單而言，是透過 SSL 交握協定（SSL Handshake Protocol）與 SSL 記錄協定（SSL Record Protocol）兩個階段達成。首先關於 SSL 交握協定，係指用戶端與伺服器端建立連線之過程，於其中用戶端與伺服器端會透過非對稱式加密，利用伺服器端所公開的公鑰及秘密持有之私鑰，決定專屬於此一連線的秘密金鑰；其次關於 SSL 記錄協定，則是用戶端與伺服器端正式傳輸資訊的過程，此時用戶端與伺服器端於此連線中，會透過在交握協定中所決定之秘密金鑰，將所有傳輸的資訊予以加密解密，以達成資訊傳輸之安全並確保資訊之完整性。[7] 透過加密之過程，於 SSL/TLS 傳輸協定下所傳輸之封包成為密文方式傳輸，因此於網路中即便攔截到此封包，由於欠缺交握協定所決定之秘密金鑰，因此無法對此封包進行解密，亦無從觀察此封包內容。

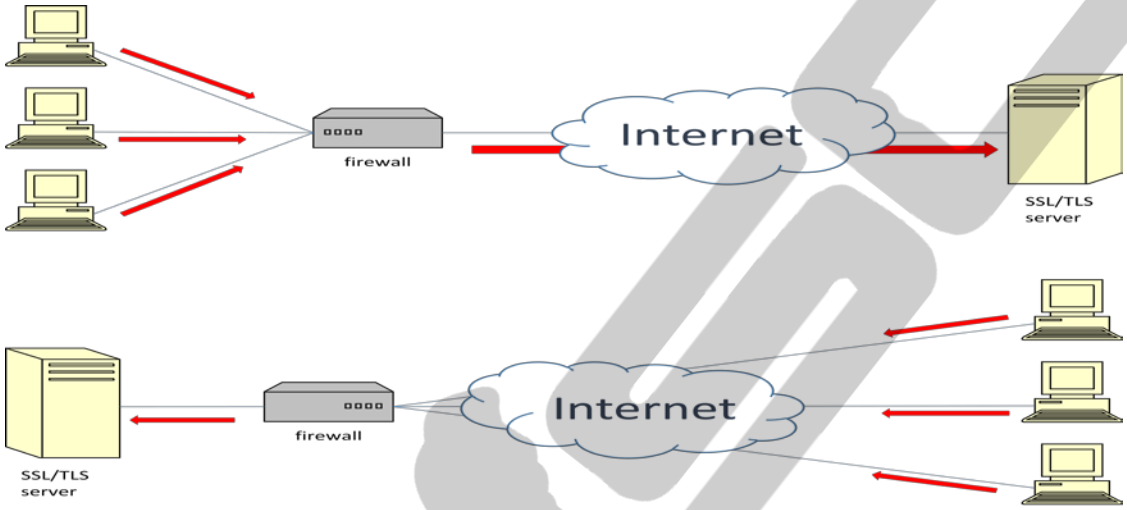
（三）針對 SSL/TLS 通訊之解密、監控

1.對 SSL/TLS 加密通訊之解密、監控之需求

於此，即出現對於 SSL/TLS 連線中封包解密之需求。在 SSL/TLS 加密連線已經過半情形下，對於加密流量無法監控時，將導致向內傳輸之 SSL/TLS 連線內藏

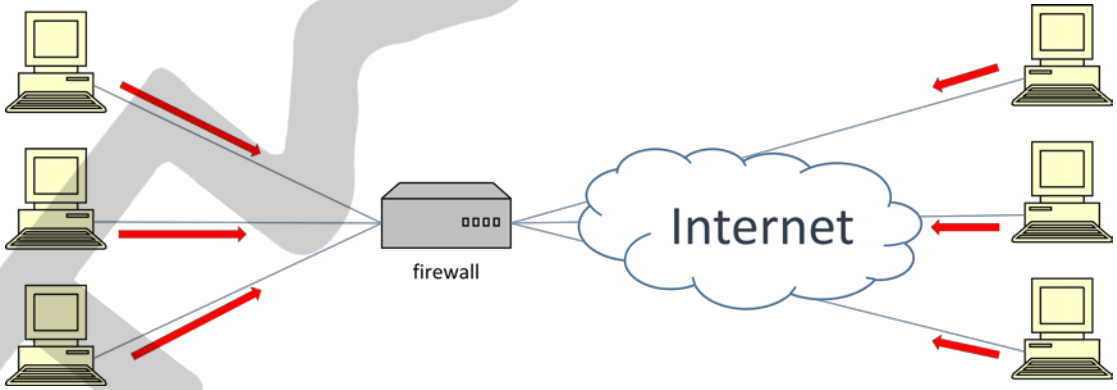
[5] 前揭註 2，頁 15-21。
[6] 前揭註 2，頁 15-22～15-23。
[7] 黃明祥、林詠章、周永振，資訊與網路安全實務，普林斯頓，2017.01，頁 81-86。

有攻擊而無從防禦，及透過 SSL/TLS 連線對外傳輸不得、不應傳輸之內容亦無從檢驗等兩種主要之困境。換言之，以伺服器的情形為例，亦即存在於外部對內部伺服器進行 SSL/TLS 加密連線，及內部網路對外部伺服器進行 SSL/TLS 加密連線兩種情形下（如下圖一），倘若攻擊行為或洩漏秘密行為隱藏於加密連線中時，傳統資通安全設備如防火牆（Firewall）因無法對加密封包進行解密、監控，致使無法確保資通安全之情勢發生。



圖一　對外、對內 SSL/TLS 連線示意圖

若考慮到企業內部用戶端非與外部伺服器端建立連線，而是直接與企業外部之其他用戶端建立 SSL/TLS 連線，用以進行資訊傳輸之情形，則會出現第三種類型（如下圖二），無論是向內部用戶端進行攻擊或向外部洩漏資訊，均無法加以解密、監控之情形。



圖二　內外客戶端 SSL/TLS 連線示意圖

2.解密技術與應用可能

目前普遍使用於 SSL/TLS 的解密技術主要有二大方向，其一是透過取得秘密金鑰（secret key）或私鑰（private key）方式進行解密，其二則是透過中間人（MITM, Man-in-the-Middle）方式進行解密。透過取得秘密金鑰或私鑰的解密方式，係透

過向 SSL/TLS 傳輸雙方中其中一方取得最後決定之秘密金鑰，或是取得伺服器的私鑰，以對加密傳輸進行解密；例如透過網頁瀏覽器等預設儲存之 SSL/TLS 金鑰日誌，取得傳輸金鑰以就封包進行解密[8]。而透過中間人方式則是於加密傳輸中，以類似於代理伺服器（proxy）之方式，建立起兩個 SSL/TLS 加密傳輸，使傳輸端的雙方認為自己正與對方進行加密傳輸，事實上則是分別與中間的代理伺服器進行傳輸。[9]

目前常用於資安防護之設備中，由於涉及各廠商營業秘密，大多均未說明其所使用之解密技術為何；但於各廠商之產品文件中，多半宣稱具有對 SSL/TLS 加密流量進行解密、分析之功能，例如 Symantec 之 SSL Visibility Appliance[10]、F5 之 Herculon SSL Orchestrator[11]、Palo Alto 之 PAN-OS[12]、A10 Networks 之 Thunder SSLi[13] 等。雖然未能從各廠商產品說明中，確實理解所使用之解密技術為何，然就其各自宣稱，至少可確認廠商對其所生產之資安設備，主張具有對 SSL/TLS 加密傳輸協定之封包進行解密、檢測之功能。進而本文以各家廠商所宣稱之解密功能確實存在作為前提，以討論、分析等對 SSL/TLS 加密傳輸協定下所進行之封包傳輸通訊，進行解密、解析時所可能涉及之法律上責任與爭議。

三、SSL/TLS 封包於法律上之定性

欲理解對於 SSL/TLS 封包進行解密並監控之行為，其法律上性質與所涉法條為何前，應先確定者在封包與加密封包於法律上定性為何。

（一）封包屬電磁紀錄

首先，最基本的定義，封包無論在加密與否之情形下，均為刑法第 10 條第 6 項所稱之「電磁紀錄」無疑。刑法第 10 條第 6 項所謂電磁紀錄者，係指「以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」而言，而網路通訊封包無論其加密與否，皆是由電腦應用軟體作成之原始資料，經過通訊軟、應體所採取的通訊協定，層層封裝而於實體網路上透過電子訊號，由各硬體設備加以處理傳輸者，因此封包應於法律上定性為電磁紀錄，故無疑問。

（二）封包是否屬「準文書」

---

[8] Jackyhwei，一個最簡單的破解 SSL 加密網絡數據包的方法，SAOWEN，2017.08.04。available at: https://hk.saowen.com/a/279fe2a510c923ddf71ddc7ea4d515e65dbe200258f867495ca658ca39c7edac , last visit at:2018.06.30。

[9] 陳琮元，SSL 代理伺服器之設計與實作，清華大學碩士論文，2005 年，頁 21-24。

[10] Symantec, “Cost-Effective, Flexible Visibility and Control of SSL/TLS Network Traffic”, available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/flexible-visibility-and-control-of-ssl-traffic-en.pdf , last visit at:2018.06.30。

[11] 李宗翰，「透視 SSL 加密流量並能與資安系統協防，F5 推出檢測分析設備」，iThome，2017.03.03。available at: https://www.ithome.com.tw/review/112440 , last visit at:2018.06.30。

[12] 李宗翰，「扛下解密流量負載，Palo Alto 新版次世代防火牆平臺登場」，iThome，2018.06.23。available at: https://www.ithome.com.tw/review/123197 , last visit at:2018.06.30。

[13] A10 Networks，「A10 Thunder SSLi：檢測網路加密資料的最佳利器」，iThome，2017.03.21。available at: https://www.ithome.com.tw/pr/112863 , last visit at:2018.06.30。

有所爭議者在於，封包雖屬刑法第 10 條第 6 項所謂之「電磁紀錄」，是否得依據刑法第 220 條第 2 項之規定屬「準文書」？按刑法第 220 條第 2 項規定，「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」亦即電磁紀錄足以表示其用意之證明者，即屬刑法上之準文書。判決亦表示，倘記載、儲存表意人之意思、思想，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，依刑法第二百二十條第二項之規定，應認係準文書之一種[14]，而問題即在於網路傳輸之封包是否存有「表示其用意之證明」之相關資訊，尤以與表意人相關之資訊。

發生此疑義之問題點有二，其一在於封包資訊內容並不僅有表意人之意思表示。網路封包結構中，僅有封包內所載的原始資料部分，可能係由表意人所作成，至於其他部分則是由通訊軟體、硬體層層封裝時所加上的資訊，並非由表意人所作成；再者，部分通訊封包係由系統自動送出，為系統運行下必然產生之結果，例如系統設定更新檢查等，與電腦使用者之意思表示並未有關。據此，網路傳輸封包能否認定其係表示表意人之意思、思想以證明使用者之用意，即生第一層次之疑問。

第二層次之疑慮在於，網路傳輸封包並不一定為完整的表意人意思表示。由於在傳輸層中將資料段封裝成為封包後，要以連結層的訊框加以傳送，因此封包大小受到訊框大小之限制，超出訊框大小時封包即必須切割（fragmentation），至目的地後再行重組（reassembly），因此封包大小即受限於實體網路的最大傳送單位（MTU, Maximum Transmission Unit）；以目前在企業、家庭或個人主要使用的乙太網路（Ethernet）為例，其 MTU 即為 1500 位元組[15]。單個經切割後的 IP 封包，並不一定具有完整的表意人意思表示，而必須經過重組後的完整 IP 封包，方可以得到表意人最初的完整意思表示。

就此二層次所生之疑慮，本文管見以為，封包仍應屬刑法第 220 條第 2 項所稱之準文書無疑。其理由在於，就第一層次而言，無論封包容是否僅有部分屬表意人之意思表示，抑或全然係電腦及網路系統所自動生成，均不影響其文書之表意性。倘封包內容僅有部分係由表意人作成時，其餘部分固然係由系統、網路自動生成，然此自動生成部分係屬電腦、網路系統處理、判讀網路封包所必要，並不影響其原有由表意人作成之部分。正如判決認定仿冒光碟為準文書之案例中[16]，著重在於仿冒光碟所呈現之內容，而不論光碟內是否存在有其他機械或電腦於判讀、處理時所必須之資訊，亦即此類資訊不致影響內容作為準文書之效果，據此封包內容中由電腦、網路等軟硬體所增加之資訊，並不會對封包內記載原始資料作為準文書之效果產生影響為是。

其次倘若封包係由系統自動產生而非使用者之意思表示而生者，亦應認為屬刑法第 220 條第 2 項之準文書為是。其理由在於，縱或由電腦系統、網路系統自

[14] 最高法院 95 年度台上字第 1705 號刑事判決。
[15] 前揭註 2，頁 9-22。
[16] 最高法院 96 年度台上字第 1387 號、95 年度台上字第 1705 號、94 年度台上字第 4791 號。

動產生之相關通訊傳輸封包，並非由使用者作為表意人進行意思表示而生，而係使用者整體使用、支配電腦系統下由電腦系統自動生成，此時此種封包仍可做為電腦使用、通訊之記錄證明，自仍應合於文書表意性為是，故仍應將此類封包視為準文書之一環。

第三就第二層次而言，封包之完整性是否應影響其作為準文書之性質？完整未經切割或已經重組之封包，承載表意人完整之意思表示，固屬於準文書無疑；而已經切割尚未重組之封包，其雖未記載表意人完整之意思表示，但其所包含之資料，仍存有表意人部分意思表示，甚至由其中即可能獲知整體原始資料核心部分，倘若因其欠缺完整性即不予準文書之保障，可能致使對文書信賴法益保障之欠缺。因此，縱然經切割尚未重組之封包未能完整的紀錄原始資料而僅有部分，仍應該視為準文書之一種。綜上所述，無論封包之完整與否，及其是否係使用者決定下所傳輸抑或是系統自動生成者，均應屬刑法第 220 條第 2 項之準文書為是。

（三）封包可能屬通訊保障及監察法「具合理隱私期待之通訊」

一般社會通念中，利用網路系統傳輸資訊故屬通訊無疑，然事實上，透過網路傳輸資訊中之封包本身，縱然非整體傳輸之資訊，亦屬通訊保障及監察法（下簡稱「通保法」）之「通訊」，試說明如下。依據通保法第 3 條第 1 項第 1 款規定，所謂「通訊」係指「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。」而所謂「有線及無線電信」，則依據通保法施行細則第 2 條第 1 項之規定，係包含「電信事業所設公共通訊系統及專用電信」而言，但對公共通訊系統及專用電信為何，通保法施行細則並未進一步定義之。

因而參酌電信法之規範，電信法對於「公共通訊系統」亦未有定義，但「專用電信」之定義，則依據電信法第 2 條第 6 款規定，係指「指公私機構、團體或國民所設置，專供其本身業務使用之電信」，因而相對於此，所謂公共通訊系統者，應為可供公共使用之電信系統，而專用電信則指非公眾使用者。進一步，依據電信法第 2 條第 1 款規定，所謂電信係指「指利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息」者。

據此，綜合上述，透過網路傳輸之封包係屬於「利用有線、無限方式，以電磁系統發送、傳輸或接收各種訊息」之電信，且存在於公眾使用之「公共通訊系統」或專用之「專用電信」上而屬有線及無線電信，因而屬於通保法第 3 條第 1 項第 1 款規定之通訊無疑。唯問題在於，縱然網路封包屬通保法第 3 條第 1 項之通訊，是否屬於同條 2 項「對其通訊內容有隱私或秘密之合理期待」之通訊？所謂合理隱私期待者，係 Katz v. United States 案中對美國憲法第四修正案所提出之判斷標準，意即當事人有無主觀上的隱私期待，再考慮此一期待是否受到社會一般性的認可為準 [17]。易言之，亦即由當事人主觀與社會一般通念對客觀事實之認定出發，決定是否屬隱私權保護之範疇；進而，網路通訊中封包傳輸是否屬具有

[17] Katz, 389 U.S. 347, 361 (Harlan, J., concurring).

隱私權期待之範圍，即應思考通訊當事人主觀與社會通念對於此等客觀事實之認定為何。

1.非公開信息之封包應為有隱私期待之通訊

而行為人主觀上對網路傳輸未加密信息是否具有隱私權期待，管見以為應該依據其所使用之方式、模式加以區分討論。固如前揭所述，未經加密之信息在網路設備端或網路資訊流經任一點，可透過抓取封包觀察其內容無疑，但此等客觀事實與行為人使用網路傳輸未經加密信息時是否存在有隱私權期待並不一致。舉例而言，倘行為人使用通訊軟體，諸如早期的 MSN 或現在通用的 Skype、Line 等，或行為人使用電子郵件系統傳輸信件、檔案，無論電子郵件軟體或網頁郵件頁面，一般行為人於此類信息傳輸狀態下，對於自身信息內容應存有隱私權期待；易言之，此類非公開信息模式中，即使因未經加密而可透過解析每一個封包，加以觀察整體信息之內容，然行為人認知中係與相對人為通訊，並無憑任意第三人觀覽之意思，因此係存在隱私權期待。

問題在於此等未經加密信息行為人主觀上具備之隱私權期待，可否進一步解釋為對個別未經加密封包之合理隱私期待？本文認為於此情形下，應區分二層次進行觀察，第一層次在於一般網路使用者對於網路傳輸信息與封包概念之理解。對於一般網路使用者而言，並不會清楚信息與封包之間的關係；換言之，縱然在資訊安全、網路安全概念已然如此盛行的現在，大多數使用者仍僅是知其然而不知其所以然，或者說，一般使用者對網路資訊安全之認識，僅停留在使用層面而不包括網路技術原理層面。例如以對國中生使用網路素養之研究為例，其認為學生在網路知識、安全兩項目中均略高於平均分數，僅有智慧財產權項目低於平均分數，顯示學生之網路知識與安全意識有不錯之表現[18]；但事實上參酌該研究問卷內容[19]，不論網路知識或網路安全之提問，與網路技術原理並不相關而多為網路使用、應用層次。又若另一研究指出，受測對象學生在網路安全素養方面呈現正向積極狀態[20]，但參酌其問卷內容[21]，仍可以發現僅包含使用層面而不包括技術層面。在此一認知下，社會大眾對網路傳輸封包事實上係欠缺認識者，或者說係將網路封包理解為傳輸信息之一部分而加以認識，亦即並非將封包視為一種獨立存在之個體，而是觀察到自身所傳輸的信息整體，封包只是一種組成成分，甚至對於此種組成成分並不甚理解。於此則進入第二層次之問題，倘若並不理解作為成分之封包，則對於信息本身的隱私期待得否合理推展至做為成分之封包？

就權利本質而言，本文認為對於信息之隱私期待，應擴及至封包本身；其理由在於對信息之隱私期待，係期望信息內容不被公眾所探知而保留在私領域狀態下，而封包作為信息成分倘被公共所探知，部分內容即有外洩遭公眾探知之可

[18] 黃俊捷，雲林縣國中學生網路使用現況、網路素養與網路態度相關之研究，南華大學碩士論文，2013 年 5 月，頁 42。

[19] 前揭註 18，附錄三，頁 142～143。

[20] 陳佩佩，台南市國民中學學生網路使用行為與網路素養之研究，台灣師範大學碩士論文，2011 年 6 月，頁 77。

[21] 前揭註 20，附錄三，頁 142。

能，與原始對信息之隱私期待相悖。此與其他權利之性質相當，諸如所有權之權利及於物之全體，物之成分縱然與原物分離，所有權原則上依然屬於原權利人；著作權之權利及於著作之全部，縱然係著作之片段、成分，著作權人仍對其保有著作權，不因分割而喪失。據此，使用者在傳輸未公開信息的模式下，其信息縱然未經加密，其構成封包亦應該屬當事人有合理隱私權期待，而屬通保法第 3 條第 2 項所指具有隱私權期待之通訊；進而依據舉輕以明重之法理來看，未經加密之未公開信息的組成封包，當事人對之已有隱私權期待，則經加密之未公開信息的組成封包，當事人更應有隱私權合理期待，亦屬通保法所指具隱私權期待之通訊。

2.公開信息之加密封包

進一步的問題在於，倘若使用者係以公開模式傳輸信息，但傳輸協定係採用 SSL/TLS 等加密協定，此時該封包是否仍屬於具有合理隱私期待之通訊？管見以為，雖然採取 SSL/TLS 等加密通訊協定時，使用者可以理解其傳輸之信息於網路傳輸過程中，將受有保密傳輸之保障而不被駭客等非法方式探知，因而即便其係採取公開模式之傳輸訊息，在我國現行網路非採取言論管制、實名制管制，而採取自由網路環境的運作模式下，當傳輸協定採取加密模式時，使用者之個人資料即可獲得部分保密之效果，因此難謂毫無合理隱私期待可言；舉例而言，使用者於網路論壇上公開發文，雖然係採公開傳輸信息模式，但因透過加密傳輸，使用者除網路代號（ID）外之其他個人資料，仍有保持私密不被任意第三人所探知之可能性，因此不能說完全沒有隱私期待可言。

換言之，於公開使用方式下，倘若使用者其傳輸之信息沒有任何隱私期待，亦無任何不欲人知的資訊於其中時，其本來透過非加密傳輸模式進行網路資訊傳輸即可，並無使用 SSL/TLS 等加密技術對網路傳輸進行加密之必要；此時倘使用者利用加密模式進行傳輸，即便係網站或系統預設且使用者並不理解封包加密過程，但只要使用者對網路使用具有基礎認識，確知 SSL/TLS 係用於傳輸加密，亦不能謂使用者對此加密傳輸過程之所有部分均無隱私期待，亦即使用者仍應有部分之合理隱私期待為是。

縱上所述，由於非公開之信息傳輸，與公開但加密之信息傳輸，使用者均應對其傳輸中之封包具有合理之隱私期待；而公開且未經加密的信息傳輸過程中，使用者對於其所傳輸之信息不存在有合理隱私期待，進而對構成信息之封包，亦不存在有合理隱私期待；縱或使用者主張其對未經加密之公開傳輸信息有隱私期待，但由於其係公開信息之使用方式，再加以未經加密之傳輸協定下，網路封包傳輸經過的任一點均可觀察此傳輸內容，亦難謂其主觀隱私期待係屬合理。因而封包不全然屬通保法第 3 條第 2 項所謂之具有合理隱私期待之通訊，必須依據封包所存在之通訊協定及使用者之使用方式決定之。

四、對 SSL/TLS 封包解密之法律上定性與法律上疑慮

（一）SSL/TLS 封包解密行為之法律上定性

1.是否屬電磁紀錄之「取得、刪除或變更」

(1)電磁紀錄之「取得」

依前所述，網路封包固屬電磁紀錄之一，則透過 SSL/TLS 技術加密之封包亦屬電磁紀錄無疑，則透過設備對加密封包進行解密，是否屬刑法 359 條所謂「取得、刪除或變更電磁紀錄」？所謂取得電磁紀錄之行為，與一般動產之取得不同，動產之取得在於阻斷原持有人之持有狀態，而重新建立起新的穩定持有狀態；但電磁紀錄與動產不相當，可透過複製之方式建立起多份內容相同之電磁紀錄，亦即可複製性。由於電磁紀錄可輕易複製之特殊性，行為人取得電磁紀錄一事，並不必然影響原持有人對於電磁紀錄之持有狀態，而係透過複製該電磁紀錄方式為之，判決亦云「…稱取得電磁紀錄罪，係指複製電磁紀錄於行為人所能支配之附著媒體…」[22]等語。因此對於傳輸封包加以複製至解密之硬體中進行解密，係透過複製原有電磁紀錄之方式，將內容相同之電磁紀錄複製至解密設備中加以解密、解析，雖不影響原始封包透過網路設備向外傳輸，實與電磁紀錄之取得行為中，係以複製方式獲得與原始電磁紀錄內容相同之複製品行為並無二致。

(2)電磁紀錄之「變更」

另外，除電磁紀錄之取得外，針對 SSL/TLS 封包加以解密之行為，是否會構成對於電磁紀錄之變更，亦有其必須思考之處；倘進行解密係將使用者所傳輸之原始加密封包加以複製至解密設備中加以解密解析，而原始加密封包不加變動逕以傳輸至通訊相對方，固然非對電磁紀錄加以變更而僅涉電磁紀錄之取得。然上揭解密技術中倘採中間人模式，接收使用者原始封包後另行建立與相對之通訊並傳輸經加密後之封包，或將原始封包進行解密解析完畢後再加密並進行傳輸，則必須思考此是否涉及封包電磁紀錄之變更。

學說謂變更者，係指電磁紀錄之內容組成遭到改變而言[23]，然問題在於此等內容組成之範圍包括何者？如前揭所述，網路通訊封包架構中，僅有最原始的資料部分是使用者有意傳輸之部分，其餘表頭等資料係網路架構中不斷封裝增加而生之資料，此時將使用者所傳輸之原始封包加以解密並解析後，另行加密送出時，縱或原始資料部分未生任何變動，然表頭等資料是否亦完全無變動則有疑問存在。尤其若以中間人方式進行解密防護，對外端的 SSL/TLS 連線中係以防護設備作為通訊之一方，表頭資料一定與對內端的通訊內容不相同，縱或原始資料部分並未加以變動，但網路封包表頭部分以與內部用者傳輸至防護設備之原始封包有所不同；由於封包表頭資料事實上係有其存在之價值，其係用於表彰封包傳遞之網路過程，因而以封包之整體概念加以觀察，對於表頭部分資料之變更亦應認為屬於對封包進行變更之行為。

2.是否屬準文書之「開拆或其他方式窺視」

電磁紀錄於刑法之評價上，基於其記錄資訊之功能，故屬於準文書無疑，此於刑法第 220 條第 2 項規定中，將電磁紀錄於刑法各章節中皆準用文書之規定可明知。則對加密封包加以解密之行為，是否屬於刑法第 315 條之「開拆」或「開

[22] 新竹地方法院 95 年度易字第 121 號刑事判決

[23] 盧映潔，刑法分則新論，新學林，2015.07 十版，頁 797。

拆以外之方法，窺視其內容」？所謂開拆者係針對封緘之實體信件而言，電磁紀錄並無法以開拆之方式加以侵犯，因而必要思考封緘之本質，進一步解釋對於電磁紀錄之開拆意義究竟為和。「封緘」行為在性質上係以排除他人任意拆閱的方式宣示其應秘密的屬性，以電子郵件為例，電子郵件在使用上可認為「封緘」者，應係電子郵件透過帳號及密碼設定之方式來保護電子郵件之秘密內容，而電子郵件之開拆封緘行為，則是非法輸入帳號、密碼之行為[24]。據此，則加密封包之「封緘」行為，即係透過公鑰、私鑰或金鑰將封包內容由本文轉為密文，而開拆封緘行為即係非常規的利用公鑰、私鑰或金鑰將封包予以解密，而直接使用程式或其他方式破解加密演算法將封包進行解密，則應為刑法第 315 條所定之「開拆以外之方法」。

3.是否屬通訊之「監察」

如前所述，網路封包一旦加密，即應屬有合理隱私期待之通訊，則對於此等封包加以解密解析，是否屬通訊保障及監察法所稱之通訊監察？依據通保法第 13 條第 1 項規定，通訊監察之監察行為，包括有「截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法」，立法理由謂「監察通訊之方法宜隨科技進步而改變，除予以例示外，並予概括現定，以切合實際需要」[25]，據此可知通訊「監察」之方式不限於條文所明示列舉方式，唯仍應與列舉方式具有相當程度與性質上之相類似，方可謂「其他類似之必要方法」。

則對加密封包之解密並解析之行為，是否與通保法第 13 條第 1 項所列舉之各種監察行為，於性質上相同或程度上相當之本質？本文管見以為，對加密封包之解密並解析，係具有相當於通保法第 13 條第 1 項所列舉行為之本質的；其理由在於，首先，對封包之解密並解析，本文認為與刑法第 315 條所指開拆以外方法，其與該條之「開拆」具有本質上相似之狀態，則自然亦與通保法第 13 條 1 項之開拆具有相當之價值為是。其次，網路傳輸中關於加密封包解密過程中，其大致可以區分為將原有封包解密解析完畢再行加密傳輸，或複製原有封包後針對複製封包進行解密解析二種方式，而於第二種方式中，雖所解密者為複製封包，然係針對原有封包複製而來，其亦相當於錄影、錄音之性質，與一般針對通話之通訊偵察，將原有對話以錄音方式加以複製無異。綜上所述，針對加密封包予以解密並解析之行為，應屬於通保法所規定之監察行為無疑。

（二）SSL/TLS 封包解密行為之法律上疑慮

於就 SSL/TLS 封包解密加以法律上定性後，進一步，應思考該行為是否具有構成各種刑事犯罪之可能。

1.刑法 359 條妨害電腦使用罪

針對 SSL/TLS 封包加以解密解析之行為，該當於刑法第 359 條中的「取得」及「變更」兩種行為如前揭說明故無疑問，則企業針對網路通訊中加密封包進行

[24] 士林地方法院 102 年度訴字第 200 號刑事判決

[25] 立法院議索關條文書院總第 1407 號-政府提案第 4235 號之 1，立法院，1999.04，頁討 555。available at: https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcbcfcecfc7cfcdc5cacdcad2cac8cb ，last visit: 2018.08.01。

解密，是否構成刑法第 359 條之犯罪？依刑法第 359 條之規定，實行行為為「無故取得」、「無故刪除」或「無故變更」三者，犯罪客體為「屬於他人電腦或相關設備之電磁紀錄」，並以「生損害於公共或他人」作為結果要件[26]，於此前提下，進一步對使用防護設備就 SSL/TLS 封包加以解密並解析之行為，依照不同之類型進行分析。

(1)對內部伺服器連線之加密封包進行解密

首先，第一個類型，對「向內部伺服器連線之 SSL/TLS 加密傳輸」，基於防護之需求而進行解密並解析者。此類型下，針對 SSL/TLS 加密連線進行解密解析，應不生刑法第 359 條之妨害電腦使用罪之疑慮；其理由在於，企業、機構（下簡稱組織）甚或個人倘若為防護內部伺服器，而就向內部伺服器傳輸之 SSL/TLS 加密傳輸進行解密時，設置防護設備如次世代防火牆、加解密設備者，係與伺服器之所有者為同一人，或為伺服器所有者所允許、授權者，因此對於加密封包之取得、變更係得同意而取得、變更，亦即得到電磁紀錄接收者及該伺服器所有者之同意，或解密之行為人本即為電磁紀錄接收及該伺服器所有者者，因而並非無故為之而屬「有故」，於構成要件層次之行為部分即不該當而無構成犯罪之可能。

再者，就客體而言，由於進行解密之防護設備與伺服器同屬組織或個人所有，因此於其中將封包複製至伺服器之取得電磁紀錄，抑或採取中間人模式進行解密而產生封包變更之變更電磁紀錄，均非取得、變更「他人電腦或相關設備」之電磁紀錄，而係取得、變更「自己電腦或相關設備」電磁紀錄，於構成要件客體層次亦不該當而無成立犯罪之可能。

(2)對內部其他使用者之 SSL/TLS 封包加以解密解析

①構成要件層次

除上揭對於組織之伺服器所進行之 SSL/TLS 加密傳輸所進行之防護目的之解密解析外，使用解密技術之另一目的常在於預防組織內員工或其他使用者之電腦或相關設備遭受攻擊，或避免內部人員故意、過失向外洩漏機敏資訊，或因遭植入惡意程式而對外洩漏機敏資訊等。關於此類型，於構成要件層次應有數項不同爭議，其一在於，組織基於防護資通安全及內部秘密資訊，對於使用其網路設備之通訊加以解密，是否為刑法上之「無故」；其二在於倘組織由所屬網路設備中複製內部使用者利用網路所傳輸之網路封包，是否仍屬刑法第 359 條由「他人電腦或相關設備」取得電磁紀錄之行為？若採取中間人模式加以解密又復加密，是否屬變更「他人電腦或相關設備」電磁紀錄之行為；其三則在於究竟對於內部使用者之封包加以解密解析，是否造成公眾或他人之損害。

(a)是否屬「無故」？

關於第一層次，必須思考刑法關於「無故」之定義。刑法上所謂無故者，依據實務見解係指無正當理由而言[27]，有論者謂此處正當理由不以法律明文者為限

[26] 前揭註 23，頁 797～798。

[27] 臺灣高等法院 85 年上更（一）第 1190 號判決

[28]，亦有認為前說之「正當理由」概念範圍不明有違法律明確性要求，因而應限於構成要件層次以法益處分權人之同意，或違法性層次之阻卻違法事由為限，亦即具有雙重機能之要素 [29]；又或有主張認為「無故」係屬一「語感」，僅用以表示一般社會通念下多數人不會為之的意思 [30]。本文認為於此首要解決之爭議，即在於刑法第 359 條所稱之「無故」之真正意思為何；本文認為此三說事實上具有相同之疑慮，即在於混淆構成要件要素與違法性要素，詳言之，針對第二說有學者指出，犯罪各階層各有其須審查之要素，鮮有要素跨越數階層存在 [31]，而當案件事實中存在阻卻違法事由時，阻卻違法事由亦會構成第一說中之「正當理由」，及第三說中之社會通念下的「非無故」，均屬於各自學說中之構成要件要素；因而無論採取何說，都會使得「無故」的意義擴張及於違法性要素之阻卻違法事由，而生混淆構成要件要素與違法性要素之疑慮；另外，第三說以社會一般通念作為標準，此與第一說相同者即為範圍不明確，亦生違背法律明確性原則之虞。

在此考慮下，若為避免構成要件要素與違法性要素之混淆而採取「無故」係指未獲得同意 [32]之見解，雖似可避免此等階層混淆之疑慮，但卻另有違背文義解釋之虞。詳言之，為避免混淆不同階層要素而將無故之「故」解釋為當事人同意下，行為人未獲同意且未有其他阻卻違法事由時，取得、變更或刪除他人電腦或相關設備中之電磁紀錄者，即為無故取得、變更或刪除而該當於構成要件之行為要素；而倘行為人僅係未得當事人同意而另有阻卻違法事由，依前揭理論下，行為亦於構成要件層次該當於無故取得、刪除或變更電磁紀錄，而必須待違法性層次方得阻卻違法；此等結論於社會一般通念下，實與「無故」之語意有所齟齬，可謂過度限縮文義解釋範圍。例如行為人持法院開立之搜索票對嫌疑人之電腦搜索取得其中之電磁紀錄，固然持搜索票搜索係屬於依法令之行為得阻卻違法而不構成犯罪，但依前揭理論之結果，將行為人持搜索票搜索之行為判定為「無故取得」，實難為一般社會通念所接受。

據此，本文認為「無故」一語之解釋上，包含同意及其他法律上依據、阻卻違法事由等則失之過寬，若僅包含當事人之同意則又過度限縮失之過嚴，因而由立法論之角度觀之，無故二字應修正為「私自」或「未經同意」以呈現其未獲同意、未經授權之本質方屬妥適；然修正前仍須就「無故」一語加以解釋適用。本文對此之發想認為，或可採折衷說之觀點，亦即認為「非無故」之範圍包含當事人之授權同意或行為人本身即具有之法律上權限，亦即阻卻違法事由中之依法令行為二種類，而其他阻卻違法事由之審酌則回歸違法性層次。其理由在於，相對於其他阻卻違法事由而言，依法令行為較為單純，純以行為人之行為是否具有法律上依據為準，不同正當防衛必須確認不法侵害是否發生，緊急避難則涉及須確認違難是否發生等要素，其判斷標準相對明確而不至於違背構成要件明確性之需

[28] 甘添貴，體系刑法各論Ⅰ，2011.09 修正再版，頁 267。
[29] 盧映潔，侵入住宅罪之「無故」判斷，月旦法學教室 19 期，2004.05，頁 25。
[30] 前揭註 29。
[31] 前揭註 29；前揭註 23，頁 576。
[32] 前揭註 23，頁 576～577。

求。其二在於相對於其他阻卻違法事由而言，依法令之行為較無社會一般通念上之爭議，具有法令上之依據時在社會觀念下應多認為屬於「有故」之情形，較合乎構成要件之文義解釋範圍。以此標準，組織對於內部使用者之加密通訊加以解密解析，倘取得內部使用者之同意，則其應為「有故」無疑，真正核心問題在於，無法取得或未取得同意情形下，組織是否具有權限或其他法律上依據，對內部使用者所傳輸之加密通訊封包進行解密、解析。

此處有兩種不同的思考進路，第一種思考方向係朝向組織作為網路系統的所有者所生之權限而發想，其二則係尋求有無其他法律上依據。第一種進路，無論終端設備係屬組織抑或內部使用者個人所有，只要連結組織所設置的網路，必然無疑的利用組織所有之網路系統傳輸封包；此時組織針對網路系統內之封包加以加密、解析，可否認為基於網路系統資通安全必要，網路系統「所有者」具有此等權限而屬「非無故」。本文認為以資通安全的角度觀察，倘區域網路之終端設備遭受駭客或惡意程式攻擊，則該區域網路系統設備亦會產生相當程度之風險，反之亦然[33]；換言之，利用組織網路系統的電腦或智慧型手機等終端設備，倘遭駭客攻擊或病毒感染，對於網路系統中由組織所有之網路設備如路由器、交換機等，亦會產生受攻擊或感染之風險，至少亦會產生網路系統頻寬受到影響之結果；反之，當網路系統設備受到駭客攻擊或惡意程式感染時，網路內的終端設備亦有遭到攻擊或感染之風險，網路系統與終端設備之資通安全可謂一體。在此風險作為前提下，可否得到組織等網路設備所有者，對內部使用者所進行之 SSL/TLS 加密傳輸具解密、解析權限之結論？則須回歸刑法第 359 條之規範目的思考。

依據學說見解表示，刑法第 36 章妨害電腦使用罪章，其係在保護電腦使用安全，並兼顧個人財產、秘密及公共信用之安全[34]，以此目的觀之，其所保障之法益在於使用者使用安全法益，亦即電磁紀錄之使用者、擁有者對於電磁紀錄不受他人取得、變更之安全性，而非電腦或相關設備之所有權人之權利。據此，雖然組織對於網路設備具有所有權，甚至就網路系統上的終端設備具有所有權，內部使用者僅為網路之利用者，但刑法所保障者正是電磁紀錄利用者之使用安全，仍不能謂組織即獲得電磁紀錄取得或變更之合法權限。

第二層次的思考進路則在於，倘不能基於網路設備之所有權限使組織產生取得、變更之合法權限，是否有其他可能獲致法律上正當依據。我國於 2018 年 5 月 10 通過，同年 6 月 6 日公布之資通安全管理法，或許為可思考之方向。依據資通安全管理法第 3 條第 2 款規定，所謂資通服務係指「與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。」依據此定義，組織對內部使用者所提供之網路服務，係屬於資通服務之一種無疑。而又依據同條第 3、4 款規定，資通安全係指「防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及

---

[33] 參照林妍溱，「路由器漸成為 APT 攻擊的最愛，防毒公司警告，威脅僅次於 CPU 漏洞」，iThome，2018.04.13，available at: https://www.ithome.com.tw/news/122403 ，last visit: 2018.08.02。

[34] 前揭註 23，頁 795。

可用性。」而資通安全事件則是指「系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。」據此於組織內發生駭客或惡意程式攻擊，以及部分資訊外洩事件等，均應屬資通安全事件無疑。再者，復依據同法第 10 條第 1 項、第 16 條第 2 項及第 17 條第 1 項規定，公務機關、關鍵基礎設施提供者，及關鍵基礎設施提供者以外之特定非公務機關（下簡稱「特定非公務機關」），均有「符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫」之義務。同時又依據第 12、13 條、第 16 條第 3 項、4 項，及第 17 條第 2、3 項規定，上揭單位均有提出資通安全計畫實施情形及受上級機關或中央目的事業主管機關稽核之義務。

綜合上揭所述，在資通安全管理法之規定下，既然公務機關、關鍵基礎設施提供者及特定非公務機關均有防止資通安全事件之義務，是否可認為必要時採用特定安全防護設備對於內部網路使用者之 SSL/TLS 加密傳輸加以解密並解析，係符合資通安全管理法所定應採取之資通安全防護計畫，屬遵守法令之行為得以阻卻違法？本文認為，資通安全有其特殊性質，隨技術之發展推移，無論在攻擊或防禦方面均會隨時變化，法律相對於此較穩定不變，因而不適宜也不可能就各項資通安全技術為實質的、列舉式的規範，因而即便在資通安全管理法中未能有明文授權組織使用相關解密設備對於使用者封包加以解密解析，並不能謂使用解密解析 SSL/TLS 傳輸即非屬資通安全管理法之容許範圍，而須考慮此方式是否合乎資通安全管理法之規範目的，倘合乎資通安全管理法之規範目的時，組織使用此等資通安全防護措施，即應得據以認為係屬合乎法令之行為而予以阻卻違法。

SSL/TLS 幾已成為主流通訊協定之狀態，倘不採取對加密流量進行解析之方式進行資安防護，將有過半之網路通訊流量處於無法解析的狀態，亦無法預防藏匿於其中之駭客或惡意程式攻擊，及利用加密通訊協定進行資訊洩漏之情形。就此觀點觀察，利用解密設備對於 SSL/TLS 加密通訊協定之網路封包進行解密，可謂符合資通安全管理法第 1 條所稱之「建構資通安全環境」，亦符合第 4 條所謂之「提升資通安全」；進而，雖使用資安防護設備對 SSL/TLS 等加密傳輸協定中封包加以解密解析之行為，未能獲明文規範於資通安全管理法內，但仍係符合資通安全管理法之精神之防護措施，屬合乎法令之行為進而係屬構成要件層次之「有故」而非「無故」；唯此種模式僅得解決部分爭議，其理由在於資通安全管理法之適用對象僅限於公務機關、關鍵基礎設施提供者及特定非公務機關，此等身分以外之組織並非資通安全管理法要求必須實施防護計畫之對象，能否類推適用資通安全管理法規定，即非毫無疑義可言。雖刑法理論上有認為對行為人有利部分仍有類推適用之空間之說，唯此等學說並非全然無爭議之通說見解，在刑法禁止類推適用之基本原則下，似不能逕此主張而仍須尋求其他出路。

(b)是否為他人電腦或設備

倘不能由「無故」之環節種尋找解套方案，另個可思考的爭點在於究竟係由

他人之電腦設備或自己之電腦設備，取得或變更電磁紀錄。其理由在於，電磁紀錄在網路傳輸的狀態下，並非「動產」之一種，其本質上係透過電能、光能或電磁波所傳遞的「能量」波動變化，當使用者由所使用的電腦送出封包後係於網路設備中以能量波動變化方式傳遞，此時倘網路設備所有者由設備中複製此段能量波動變化，是否仍該當於由「他人之電腦或相關設備」複製之取得概念？或僅是對自己所有之網路設備中能量波動變化加以紀錄複製而取得之行為？要解決此一疑問，必須由電磁紀錄之特性及傳遞方式加以觀察；電磁紀錄本身係以電力、磁力或光學方式，於特定儲存媒介上儲存以供電腦或相關設備處理之用，在儲存的狀態下，以硬碟為例，係在碟片上的磁粉以帶電與不帶電方式表示 1 與 0 的二元機械碼[35]，而在傳輸時，則係依照傳輸設備之特性，以電流、光學方式傳送能量波，由另一方接收後再轉換於處理設備中加以處理或儲存。所以在傳輸過程中，電磁紀錄本身並未有所移動，仍然存在於原有設備之儲存或處理單元中，僅係在傳輸設備以電流、光學方式傳送。因此網路傳輸過程中複製取得封包一事，並非是針對封包加以複製而生，而應係透過記錄傳輸過程中電流、光之變化，將資料予以還原為電磁紀錄之狀態。

比較接近此種行為的，應是對於無線電或廣播的截收，亦即針對能量流動變化予以記錄並加以還原，但並不因此使能量傳輸過程中斷。在這樣的理解下，進一步可以思考，於組織所屬之網路設備上，「截收」使用者所發送之封包並加以解密解析，究竟係於自己（組織）之電腦設備上取得、變更，抑或是於他人（使用者）之電腦設備上取得變更電磁紀錄。從這樣的角度觀察，本文認為縱然組織係從自己的網路硬體設備中記錄取得加密封包，但仍應係屬於由他人電腦及相關設備中取得電磁紀錄之情形。其理由有二，其一，由傳輸方式可知，發送方使用者將封包向接收方發送時並非將完整封包交給網路設備，而係將封包轉換為電子訊號於網路設備中傳送，由此可知使用者並沒有將封包交給網路設備所有人之意思。由最簡單的網路架構可以更明顯的看出這個特徵，最簡單的網路架構下，由兩台終端電腦與相連接的網路線即可構成網路，電腦間傳輸電子訊號並不會產生將封包交給「網路線」之意思。

其二在於，刑法第 359 條或者說第 36 章所要保障者在於使用者使用電腦相關設備之安全，若此，網路傳輸之封包係屬使用者所有，倘若一旦經由網路傳輸而於傳輸階段即不屬使用者控制範圍，即會使對於使用者之保護出現漏洞。亦即倘若認為網路傳輸階段係使用者將封包交給網路設備所有人，則於此時網路設備所有人對處在網路傳輸階段之封包加以修改、變更，則接收此封包之接收方必然無法獲得正確之結果，若此情形不加以規範，則無法獲致刑法第 359 條所要保障之電腦使用法益之安全。

於類似的狀態中亦會獲致上揭結論。與目前網路封包傳輸之截收解密解析最為類似而又有明確法律加以規範之情形，大概以電信監聽最為類似。目前電話通

[35] 參照凌威科技，硬碟基本原理，2014.12.16，available at: http://www.linwei.com.tw/article/ins.php?index_id=22 ，last visit:2018.08.02。

信主要採取數位電話交換機的方式加以交換，在此情形下對電話進行通訊監察，亦會將電話線路上傳輸的封包加以複製並轉換為聲音，但並不影響原有的封包傳輸至受話方。在相同的結構下可參照電信法相關規定，依據電信法第 6 條第 1 項規定，電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密；復依據第 56 條之 1 第 2 項規定，電信事業之負責人或其服務人員亦為第 6 條所規範之對象；據此，倘若電信封包有交給電信業者之意思，即使用者對於電信業者並無合理之隱私期待，電信業者及無有妨害秘密通訊構成之可能，反之，既然條文認為電信業者及服務人員亦有構成妨害秘密通訊之可能時，即代表使用者對於電信業者仍有隱私期待，電話通信封包並未移轉予擁有電信設備之電信業者為是。據此相同之概念，於企業組織內部使用者利用企業之網路設備進行網路通訊時，倘若未經使用者與組織之明確協定，並不能說使用者有將通訊網路封包對組織開放之意思，亦不能認為使用者將網路封包之所有權移轉予組織；進而，組織利用資安防護設備於所屬網路設備中複製取得使用者之封包，或變更其封包部分內容，仍應屬於他人之電腦或相關設備中取得、變更電磁紀錄為是。

(c)是否造成損害

綜上所述，公務機關、關鍵設施提供者及特定非公務機關得以透過遵守資通安全管理法之規定，以遵守法令之行為而係屬「有故」，對內部使用者與外部之 SSL/TLS 加密網路連線封包加以解密解析，唯此等身分以外之組織並不能為此等主張；進而，僅得依據構成要件中之結果加以思考，亦即是否造成公眾或他人之損害。刑法第 359 條係以「致生損害於公眾或他人者」作為結果構成要件，且本罪並不處罰未遂，因而倘使用資安設備對於 SSL/TLS 加密連線封包加以解密，並不會生損害於公眾或他人時，即構成要件不該當而不成立犯罪。則問題在於究竟刑法第 359 條所稱之「損害」其範圍究竟如何？依據本條立法理由說明四，刑法第 359 條與第 339 條之 3 不同處在於刑法 339 條之 3 需取得他人財產獲得財產上不法利益，而 359 條並無此限制因此規範範圍較廣，且因未涉及金融秩序之危害，故刑責較輕[36]；就此觀之，似 359 條所謂之損害並非限於財產之損害，且其所造成之損害應較刑法第 339 條之損害為輕。但對照刑法第 360 條之立法理由，即會產生相當嚴重之疑義；刑法第 360 條干擾電腦或相關設備罪立法理由之說明二表示，又 360 條處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為[37]；而說明六表示「干擾尚未達到毀損之程度，且通常是暫時性，排除干擾源後，電腦系統及網路即可恢復運作，故可罰性較刑法第 359 條略低」[38]，則顯示刑法第 359 條之可罰性應於 360 條之上，其行為應較「產生重大影響之干擾行為」為嚴重，亦即損害應較第 360 條為嚴重為是。

---

[36] 立法院議案關條文書院總第 246 號-政府提案第 8862 號之 1，立法院，2003.05，頁討 19-討 20。available at: https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcacfcccecdcfcdc5cdc8c6d2cccfcb ，last visit:2018.08.02。

[37] 前揭註 36，頁討 20。

[38] 前揭註 36，頁討 21-討 22。

若依據上揭立法理由說明，立法者應認為刑法第 339 條之 3、359、360 條之罪之輕重，應為 339 條之 3 重於 359 條，而以 360 條為最輕，由三條文之刑度來看亦是如此；則在此理解下，進一步以台積電機台中毒事件來檢視這樣的預想，就該事件本文不另加以詳述[39]，唯本文認為該事件之客觀因果歷程上，係接近電磁程式干擾電腦設備之情形，亦即電腦病毒感染台積電之生產機台造成停工損害，偏向刑法 360 條所描述之情形[40]，其損失為新台幣 76～79 億元[41]，試問有什麼情形是高於此等損失而又低於刑法第 339 條之 3 的損失？由此可知當年電腦犯罪立法歷程中，對於各類行為之理解並不全然正確，至少在時代變遷後電腦犯罪所能造成之損害並非立法當年所能預想者。因此對於刑法第 359 條之「致生損害於公眾或他人」中究竟「損害」應當如何解釋，實有重新思考之必要。

倘若由本罪之法益出發，或可獲致不同於傳統見解之損害之觀點。第 359 條法益依據立法理由說明係以個人之使用安全、秘密、財產法益為主，兼顧社會法益之社會信用，然學說見解以為本罪係以個人法益作為判斷之第一關卡，而以公眾或他人利益是否受損，作為社會法益之侵害是否達到值得以刑法加以規範的程度之判斷標準[42]，亦即認為本罪係以社會法益作為其保護之對象[43]，而該社會法益之內容，學說主張係為「對於電腦或網路使用上的安全秩序的公眾或多數特定他人的信賴」為具體的法益內容[44]。若此，刑法第 359 條所謂之「損害」應當是指稱「足以動搖公眾或多數特定人對於電腦、網路使用之安全秩序信賴」之損害為是。依據此標準，此等損害必然不至於過小，輕微的損害雖然造成行為客體（電磁紀錄）之持有當事人可能之各種損害，並造成他人之財產或非財產之損失，但不足以動搖社會大眾對於電腦或網路安全之信賴；巨大的財產損害亦不必然導致社會信賴之動搖，諸如前揭提及台積電中毒受害之案例，但由於行為係因為工程師過失所致，且並未透過網路向一般社會大眾擴散蔓延，因此也未產生社會大眾對於電腦與網路使用安全信賴之受損。因此，刑法第 359 條所稱之「損害」，本文認為，無論其造成之損害大小、性質為財產或非財產之損害[45]，重點應在於其「擴散」或「非特定」之性質，亦即向其他尚未受害但有可能作為潛在受害者之人擴散，或非特定使用者均可能成為行為對象之性質，此特性下方能動搖一般社會大眾對電腦使用、網路安全之信賴。換言之，因行為人取得、變更或刪除電磁紀錄之行為可能透過網路等方式擴散，例如木馬病毒取得檔案資料、個

---

[39] 參照王宏仁，台積電產線中毒大當機事件簿(Day1~Day4 時程懶人包)，iThome，2018.08.10，available at: https://www.ithome.com.tw/news/125118 ，last visit:2018.08.12。

[40] 筆者註：本文之所以認為係類似於刑法第 360 條之客觀行為因果歷程，而非該當於刑法第 360 條之罪，主要係因事件中係由於工程師之過失所致，而刑法第 360 條不處罰過失犯。

[41] ETtoday 財經中心，台積電遭病毒攻擊　損失 76 億、報廢上萬片晶圓，ETtoday 新聞雲，2018.08.06，available at: https://www.ettoday.net/news/20180806/1228606.htm#ixzz5Ota8FkEW ，last visit:2018.08.12。

[42] 李茂生，刑法新修妨害電腦使用罪章芻議（中），台灣本土法學雜誌 55 期，2004.02，頁 253。

[43] 前揭註 42，頁 256。

[44] 李茂生，刑法新修妨害電腦使用罪章芻議（上），台灣本土法學雜誌 54 期，2004.01，頁 246。

[45] 筆者註：刑法第 359 條之法益應包含財產法益及金融秩序為是，亦即對於金融秩序、財產法益利用電腦與網路處理之安全的信賴為是。參照，前揭註 42 文，頁 255。

資，或行為人之行為係向非特定人為之，例如銀行行員將多數客戶帳戶中小數點後金額轉帳，使得多數非特定人均有成為潛在受害者可能時，方會致使社會大眾對於網路及電腦使用安全信賴之動搖。

以此標準觀察，企業機構對於內部網路使用者之加密通訊進行監控檢測過程所生之取得、變更電磁紀錄行為，理論上應難造成一般社會大眾對於電腦與網路之使用安全信賴遭受動搖或侵害，甚可認為對此類通訊加以監控、解析，反是為了確保電腦與網路之使用安全而生。退萬步言，縱不採上揭主張以社會法益作為刑法第 359 條之保護對象之說，而以立法目的之個人電腦使用安全作為保護法益，倘組織僅對使用者傳輸之加密封包加以解密、解析，以確認有無電腦病毒、網路攻擊之存在，對使用者可能發生之損害，應僅有隱私權或秘密通訊自由之侵犯問題；但一般而言，對於病毒或網路攻擊之比對，多係透過電腦系統自動比對完成，倘封包中部分內容與特定程式碼特徵相符合，即代表其中藏有病毒或攻擊，此時由程式對該封包或收發該封包之程式加以標示並提出警示，反之倘收發之封包安全無虞，並不會將該封包內容予以揭露或記錄，因此可謂對使用者之隱私侵害極輕微，甚或無侵害之存在。因而，較有疑慮者應在於，使用者於收發加密封包內容中涉及夾帶組織內部機密，而組織透過解密設備對此進行檢查是否有機敏資訊，方可能致生使用者之秘密通訊自由遭受侵害之疑慮。

對使用者傳遞訊息是否涉及內部機敏資訊之監控，由於其傳遞消息內容、方法的多樣性之故而欠缺固定的特徵模式，倘要採取機械化、自動化比對，以目前的人工智能（AI）技術發展顯然尚有難度，或許將來發展可能可透過 AI 進行自動化比對，但目前應仍透過人工加以比對、監察。在此情形下，當組織透過解密 SSL/TLS 連線對使用者所傳遞之訊息加以監察並檢視有無洩漏機敏資訊時，即會發生將通訊內容直接的暴露於負責比對、監察人員面前的情形。此時縱或負責比對、監察之人就內部使用者之通訊內容未加以任何之更改，往往社會大眾亦不因此而生對於電腦使用之安全疑慮而無社會法益之侵害，但對內部使用者之隱私權及秘密通訊自由已生侵害，縱可要求負責人員承擔此際之保密義務，然未有法律授權或當事人同意情形下，仍係為秘密通訊自由之侵害，而有刑法第 359 條立法理由中所涉個人秘密法液之侵害存在。

綜上所述，組織對內部網路使用者與外部網路間 SSL/TLS 加密連線封包解密解析行為，倘未取得內部使用者同意，亦非資通安全管理法所規定之公務機關、關鍵基礎設施提供者或特定非公務機關時，即屬無故取得、變更他人電腦或相關設備電磁紀錄之行為；若此解密解析行為係針對病毒或資通網路攻擊之防禦，尚屬無造成損害於他人或公眾而構成要件不該當，然倘此解密解析行為係針對內部使用者是否有對外洩漏機敏資訊之監察行為，即造成內部使用者之秘密通訊自由法益受損，屬刑法第 359 條之構成要件該當行為。

②違法性層次

倘組織對內部網路使用者之 SSL/TLS 加密連線解密、解析行為，係屬刑法第 359 條構成要件該當行為，由於本文主張依法令行為係為「有故」而阻卻構成要

件，是以應進一步確認是否具有依法令行為以外之其他阻卻違法事由存在。

(a)關於正當防衛

首先得加以考慮者，即為是否存有正當防衛之可能。由於組織使用解密設備對 SSL/TLS 加密連線封包進行解密、解析，係為預防電腦病毒、網路攻擊及內部機敏資訊的外洩；依照本文上揭主張，組織使用設備對內部使用者加密通訊傳輸封包加以解密，倘係為預防病毒、網路攻擊而生，應為構成要件不該當之行為；是以本文所討論情形中，刑法第 359 條之構成要件該當行為，應為組織對於內部使用者訊息內容加以檢查，亦即對機敏資訊外流所為之預防行為；此時得否主張係對違法侵害（洩密行為）所為之正當防衛行為而阻卻違法？本文認為，除少數情形外得主張正當防衛外，大多數情形仍不得主張正當防衛阻卻違法。依據通說見解，正當防衛要件包括現在不法侵害、防衛意識及防衛行為三者，其中防衛行為即為構成要件行為，於本文所討論情形中即為對內部網路使用者之 SSL/TLS 加密連線予以解密、解析之行為。於此情形下，可能作為正當防衛要件中之現在不法侵害者，即為使用者對外傳輸組織機敏資訊之行為；此等行為所涉及者，可能構成刑法第 342 條之背信罪、營業秘密法第 13 條之 1 之妨害營業秘密罪，甚或是著作權法第 91 條侵害著作權等關於智慧財產權之保護等，雖可能得為正當防衛要件中之不法侵害，然組織解密之行為時點是否均存有此等不法侵害，即非無疑。

倘組織已鎖定特定使用者之特定傳輸機敏資訊行為，就該次傳輸予以解密、解析並封鎖，確可認為係屬對不法侵害之防衛行為無疑；然即便組織已經鎖定特定涉嫌外洩機敏資訊之使用者，但未鎖定其特定洩密傳輸行為，即對該使用者所有加密傳輸封包均予以解密、解析，勢必亦將對該使用者非用於洩密之通訊進行解密、解析，此時即不能稱之為對現在不法侵害之正當防衛行為；舉重以明輕，尚未鎖定特定使用者即對所有使用者之加密通訊予以解密、解析，自然亦非正當防衛。換言之，本文認為僅有在特定使用者且特定洩密通訊傳輸之情形下，組織使用解密設備對加密傳輸封包進行解密、解析，方有成立正當防衛之空間，除此之外之情形均不能成立正當防衛。附帶說明者在於，倘組織未能鎖定特定使用者之特定洩密通訊，僅係剛好發現使用者之洩密行為，此時應為偶然防衛情形，亦非正當防衛行為而不能阻卻違法。

(b)關於業務上正當行為

另一思考方向係得否以業務上正當行為阻卻違法，亦即組織委任資安人員，使用相關設備對內部網路使用者所傳輸之 SSL/TLS 加密封包進行解密、解析之行為，係屬資安人員執行組織資通安全業務之正當行為，亦為組織維護自身資通安全之正當業務之一環，進而阻卻行為之違法性。若要採取此觀點，必須探究使用相關設備對於 SSL/TLS 加密連線封包進行解密、解析行為，是否屬資通安全業務之正當、正常範圍。依學說見解主張，業務上正當行為之實質標準在於可容許之風險 [46]；或謂基於社會生活需求，該業務行為具備社會有益性，雖會造成法益侵

[46] 黃榮堅，基礎刑法學（上），元照，2003.05，頁 167。

害或侵害危險，但基於利益衡量所得之優越利益原則，進而阻卻違法[47]。據此，其爭點即應為利用設備對於組織內部使用者所傳輸之加密通訊封包進行解密、解析之行為，在利益衝突下是否具備優越利益而得認為屬業務上正當行為。

在此思考下，我國政策認為資通安全係屬國家安全之一環[48]，對於資安維護之要求固然應屬社會重要法益之一，並涉及國家法益；唯爭議者在於，得否因資通安全法益保障之需求，侵犯利用組織設備的使用者之個人隱私權及秘密通訊自由。本文認為此情形中個人隱私權及秘密通訊自由，係與資通安全社會法益為一體兩面，亦即倘無整體資訊通訊安全之保障，個人隱私權與秘密通訊自由將無所附麗，反之，倘無個人隱私及秘密自由之保障，亦不能謂社會已充分實現資通訊安全；因而於此情形下，不能僅以單純的個人隱私權、秘密通訊自由與社會整體資通安全進行取捨，而應更進一步細緻的比較、思考此等行為是否造成不必要之權利侵害。本文管見以為，為求維護資通安全，事實上仍有許多其他不侵害組織內部使用者隱私與秘密通訊自由法益之方式可採行，諸如管制可攜式儲存媒體、對特定網路位址禁止連線、內外部網路實體隔離，及使用者同意後之解密 SSL/TLS 加密連線等，均足以確保資通安全且不侵害使用者之隱私及秘密通訊自由；據此，採取不經同意而直接就 SSL/TLS 加密通訊封包加以解密、解析之行為，其雖看似能確保資訊通訊安全，但對使用者隱私及秘密通訊自由顯造成不必要之侵害，進而當使用者隱私及秘密通訊自由持續受到此等不必要侵害時，解密行為所要確保之資訊通訊安全目的亦會在使用者對於通訊秘密之信賴瓦解下受到侵擾，而無法繼續確保資通安全法益之穩定。

綜上所述，未經同意也無其他法律依據時對組織內使用者 SSL/TLS 加密通訊封包之解密、解析行為，本文認為雖短期看似有益於資通安全之保障，然長期卻造成不必要之隱私及秘密通訊自由侵害，最後無益於整體資通安全之發展，不合乎前揭社會有益性而生之利益權衡法理，不能認為屬業務上正當行為之一種。據此，倘若無其他個案中之阻卻違法事由或阻卻責任事由，組織利用相關設備對於 SSL/TLS 加密連線封包進行解密並解析之行為，原則上應由決策採取解密設備之組織負責人，與實際進行加密封包解密之人員為行為人，構成刑法第 359 條妨害電腦使用罪。

2.刑法 315 條妨害秘密罪

(1)犯罪之構成

其次討論是否構成刑法第 315 條妨害秘密罪，其依然聚焦於組織未經同意對內部網路使用者與組織外連線之 SSL/TLS 加密封包解密、解析行為。依前所述，網路封包係屬電磁紀錄之一種，而電磁紀錄依據刑法第 220 條第 2 項規定，於刑法各章節之罪係為準文書。又復依據前揭說明，本文認為組織針對內部使用者 SSL/TLS 加密連線封包加以解密、解析之行為，係為刑法第 315 條中之「其他方

[47] 吳耀宗，刑法之解釋方法與業務作為阻卻犯罪成立之要素，月旦法學教室 No.45，2006.07，頁 44。

[48] 國家安全會議，國家資通安全戰略報告，2018 年 9 月，頁 6。

法」加以窺視；進而，倘此時內部使用者已有授權組織進行解密、解析，抑或有其他法律上之依據，故非「無故」而構成要件不該當，此外情形係屬刑法第 315 條之構成要件該當行為，而組織對內部使用者加密連線之解密行為又非業務上正當行為，在無其他阻卻違法或責任事由下，應成立刑法第 315 條之妨害秘密罪。

(2)犯罪之競合

其次問題在於刑法第 315 條與第 359 條間之競合關係。以構成要件而論，本文討論行為係該當刑法 315 條以開拆以外之其他方法窺視封緘信函、文書或圖畫，而刑法第 359 條係無故取得、變更或刪除電磁紀錄，一般情形下，兩者之構成要件行為往往難以相容、相關；但在電磁紀錄之情形下，兩要件間會發生交互之關係，換言之，對封緘─亦即加密─之電磁紀錄以開拆外之其他方式窺視，往往會涉及電磁紀錄之取得、變更。詳言之，倘若於自己的電腦相關設備中開啟他人電腦相關設備之加密電磁紀錄，必然首先涉及電磁紀錄之取得，縱然不以儲存媒體將電磁紀錄複製至自己的電腦設備，而係透過網路、遠端等方式開啟，亦會將該電磁紀錄複製至自己電腦的記憶體中進行作業，是以必然先涉及電磁紀錄之取得。其次，將加密電磁紀錄予以解密之行為，則係將電磁紀錄予以解密還原，縱或於窺視完後將該電磁紀錄復又加密，此時縱或一般自然人難以或無法察覺，但已然使得該電磁紀錄發生變動（至少存取時間已經變動過），因而涉及電磁紀錄之變更。

而於本文所示情形中，組織透過解密設備就內部網路使用者對外 SSL/TLS 加密連線進行解密時，會依據其解密方式而發生不同情形；倘組織透過設置取得通訊協定中的秘鑰，並就內部電腦設備與外部之加密通訊封包，複製至解密設備中解密而不影響原有封包之傳輸時，其行為係取得封包後，並以開拆以外之方式窺視封包內容。由於原封包已對外傳輸，而遭解密者為原封包之複製品，雖涉及取得、窺視電磁紀錄之行為，但不存在就原封包變更之行為。反之，倘組織採中間人方式加以解密，此時代理伺服器獲得封包係在使用者不知情的狀態下，亦構成電磁紀錄之取得，進而將封包解密窺視後又復加密對外傳輸，對外傳輸之封包以與原始封包有所不同，係為電磁紀錄之變更。因而無論組織採取的解密方式為何，均會涉及刑法第 315 條與第 359 條間的競合問題。

要決定上開行為如何競合，首要決定其究竟為行為單數或行為複數，依據行為單數理論，上開行為並非自然意義的一行為，應考慮上揭行為可否認為屬自然的行為單數或構成要件之行為單數，抑或應為數行為而以與罰前後行為或數罪實質競合之關係存在。由行為單數之觀點觀察，其判斷標準學者認為其與行為理論之行為觀點應為一致 [49]，因而依 Welzel 之目的行為論，所謂行為者係為人類目的性活動的實現 [50]；依據國內通說之社會行為論，所謂行為者則為由意思支配或可支配，且於外界引起社會重要性結果之人類舉止 [51]；進而，本文認為所討論案

[49] 柯耀程，刑法競合論，元照，2000.12，頁 97。
[50] 林鈺雄，新刑法總則，元照，2014.09 四版，頁 118。
[51] 前揭註 50，頁 119。

例中，組織之資通安全人員使用相關解密設備取得或變更電磁紀錄，並就電磁紀錄之內容予以窺視等數個舉動、行止，均係基於「就組織內部網路使用者之加密封包加以檢查」之目的所為的各種活動，且社會一般生活經驗中，應將此等解密並窺視之活動視為整體行止，同時此等活動在各種網路設備上操作時其時間、空間均係密接相連，因而認為其應屬一個整體行為，亦即德國法院實務之主觀上具備同一行為意思，客觀上時空關係緊密，且一般社會經驗認為係屬整體行為[52]之自然的行為單數類型。

倘組織對於內部使用者加密封包之取得並解密之行為，係屬一個整體行為，應思考者在當同時構成刑法第 315 條之妨害秘密罪與第 359 條之妨害電腦使用罪時，兩罪間究竟為法條競合或想像競合。依據學說見解表示，刑法第 315 條係保護被害人之個人隱私，意即被害人個人之生活秘密[53]，而依據前揭說明，刑法第 359 條所要保障者，在於被害人個人之電腦使用安全並兼顧個人財產、秘密及公共信用之安全，若此則第 315 條與第 359 條同時均有個人秘密法益之保障，且第 359 條尚包含電腦使用安全、財產法益及公共信用安全等，於構成要件上第 315 條又為概括構成要件，第 359 條則為特定個別構成要件，二者關係自應為特別關係之法律單一[54]，第 359 條優先於第 315 條為適用。但若依據前揭介紹內少數說觀之，刑法第 359 條所保障者，係以社會法益之公眾對於電腦使用安全之信賴為主，個人之損害僅為刑法發動之條件時，此時第 359 條與第 315 條所保障之法益不同，係為一行為侵害不同法益之情形，則應以想像競合加以決定競合之結果；第 315 條之法定刑為「拘役或三千元以下罰金」，第 359 條之法定刑為「五年以下有期徒刑、拘役或科或併科二十萬元以下罰金」，因此應以刑法第 359 條從重處斷。因此無論依據法條競合或想像競合，刑法第 315 條與第 359 條之行為於本文所示情形中發生競合時，其均應適用刑法第 359 條加以處斷。

3.通訊保障及監察法第 24 條違法監察罪

(1)犯罪之構成

關於通保法第 24 條違法監察罪之成立，參照前揭說明，經 SSL/TLS 加密之電磁封包係屬具有隱私權之期待無疑，而對於其解密並解析之行為，亦為通保法第 13 條所規定之監察行為；有疑義者在於，第 24 條所規範之對象是否僅包含具有法定行使通訊監察職權之公務員而排除一般民眾？依據臺灣高等法院檢察署研究意見認為，通保法之規範對象，應係指依法有權行使監察權之公務員，係處罰此等公務員故不依法執行監察之行為，而不含非具備公權力之一般民眾；然法務部研究意見表示通保法之規範對象不限於有權執行通訊監察之公務員，尚包含一般不具備公權力之民眾在內[55]。學者意見表示，通保法之規範意旨除有通訊監察之程序規定外，尚有保障國民秘密通訊自由之意涵，依據第 1 條之立法目的觀

[52] BGHst 10, 230。
[53] 前揭註 25，頁 605～606。
[54] 參照林山田，刑法通論（下），作者自行出版，2008.01 增訂 10 版，頁 334。
[55] 法務部 89 年法字第 000805 號函。

之，不僅限於公權力機關之規範，尚即於一般民眾為是[56]。最高法院亦採取此說，其見解表示，「…任何人監察他人之通訊，若無該法第二十九條所定不罰之情形，復據被害人合法提出告訴，自應依該法第二十四條第一項違法監察他人通訊罪論處。」[57]係認為通保法之規範對象，應包含不具備公權力之一般民眾為是。

本文認同上揭學者意見與最高法院實務見解，其理由在於通保法所保障者在於國民之秘密通訊自由，而並非僅有國家公權力會致生國民秘密通訊自由之侵害，一般民眾往往亦生對他人秘密通訊侵害之可能，倘若通保法規範對象不及於非公權力之一般民眾，則一般民眾所為之竊聽等行為，僅得依據刑法第 315 條之 1 加以處罰，於此產生刑度上之差異係為刑罰公平性之違背；其次，倘通保法之規範對象僅限於有權行使通訊監察之公務員，則其所謂之違法通訊監察，應係指此等公務員執行通訊監察時故不依法執行，亦即此等公務員執行職務上之違法行為，此時應構成通保法第 24 條第 2 項假借職務或業務上權利機會方法違法通訊監察之罪，致使第一項規定形同具文。

據此，通保法第 24 條之規範效力，應非限於具有執行通訊監察公權力之公務員而尚包含一般民眾，因而組織對於內部使用者經 SSL/TLS 加密通訊之封包加以解密、解析時，仍應考慮通保法之規範。進而依據前揭說明，組織內使用者使用組織網路進行非公開通訊，抑或進行經 SSL/TLS 等方式加密通訊者，其通訊本身與組成之封包均應為具有合理隱私期待之通訊，對於其解密解析之行為亦為通保法所規範之監察行為，此時倘若未經使用者之同意而依據通保法第 29 條第 3 款免責時，係通保法第 24 條第 1 項違法通訊監察之構成要件該當行為。

此時倘若組織具有資通安全管理法中所定之政府機構、特定非政府機構或基礎關鍵設施提供者之身分時，參酌前揭關於刑法第 359 條中無故之說明，使用資通安全設備對組織內網路使用者加密連線封包進行解密、解析之行為，尚可謂符合資通安全管理法之要求而屬於符合法令之行為，進而阻卻違法而不構成犯罪；除此以外之情形，倘若無其他阻卻違法或阻卻責任事由時，對於組織內使用者加密連線封包進行解密、解析之行為，由決策解密、解析之負責人與實際進行解密、解析之資安人員作為行為人，成立通保法第 24 條之違法通訊監察之罪。

(2)犯罪之競合

於成立通保法第 24 條之罪時，本文所示情形，亦成立刑法第 315 條及第 359 條之罪，而前揭說明刑法第 315 條及第 359 條之罪兩罪間，應以法條競合或想像競合（端視所採取學說）適用第 359 條之規定，於此應處理者為通保法第 24 條與第 359 條間競合關係。於通保法第 24 條與刑法第 315 條之關係上，學者主張應依據特別法優先普通法而適用通保法之規範[58]，其理由在於通保法規定在後且法定刑度較重，則是否於通保法第 24 條及刑法第 359 條間亦可採取此理？本文於此採取保留之態度，首先以立法時間觀之，通保法第 24 條制定於 1999 年，而

[56] 蔡蕙芳，網路監聽可能涉及刑罰規定之介紹，資訊安全論壇 19 期，2004.09，頁 40。
[57] 最高法院 94 年度台上字第 5802 號刑事判決。
[58] 前揭註 56。

刑法第 359 條則增訂於 2003 年；其次，法定刑度上刑法第 359 條之法定刑度，上限較通保法為重（併科二十萬元以下罰金）而下限較通保法為輕（拘役），是以不能單純以立法時間與法定刑度及決定兩者間之競合關係，而應該回歸兩者間構成要件與保護法益之關係為是。

就此議題，本文於結論上認為，應依照想像競合適用刑法第 359 條為是。其理由在於，首先，以法益之觀點觀察，雖刑法第 359 條以電腦使用作為保護法益時兼有個人秘密法益之保障，而通保法第 24 條係以個人秘密通訊自由作為保障法益亦為個人秘密之一環，兩者之間雖有關連性但實則係屬不同；再者，倘若以少數說主張之社會對電腦使用安全之信賴作為刑法第 359 條之保障法益，則更彰顯兩者法益之區別。其次就構成要件上而言，雖於本文所例示之情形中，組織利用設備對於內部網路使用者之加密封包予以解密時，會同時構成刑法第 359 條與通保法第 24 條之行為，但兩者之構成要件上僅是具有交集關係，而無法產生特別關係；亦即刑法第 359 條之取得行為，屬於通保法第 13 條中的監察行為之一種，而通保法之有隱私期待之通訊，於本文所例示情形中，係為刑法第 359 條電磁紀錄之一種，除此之外，無故變更或刪除均非通保法所規定之監察行為，電磁紀錄中除部分係屬於通保法第 3 條所保障之具有合理隱私期待之通訊外，其餘部分亦不一定屬於通保法所保障之通訊種類，因而刑法第 359 條與通保法第 24 條，僅得稱之為具有交集關係之條文。

既然刑法第 359 條與通保法第 24 條，僅係具有交集關係而不能形成特別關係，加之以法益之不同，本文據以認為於所討論之情形中，應係一行為同時於二犯罪中構成要件該當，且侵犯二不同法益之想像競合行為。於此，兩者之法定刑係以刑法第 359 條之法定刑刑度較高，競合時應適用刑法第 359 條之規定為是。另外的情形在於，本文見解認為於刑法第 359 條規範下，倘若組織就封包進行解密解析係透過系統進行病毒碼、攻擊碼之比對，此時應認為未造成損害而不成立刑法第 359 條之罪。然此時組織之行為仍然係屬於刑法第 315 條無故以開拆以外方式窺視電磁紀錄，且仍然成立通保法第 24 條之違法通訊監察，此係蓋因無論刑法第 315 條或通保法第 24 條，均未有具體結果之規定，只要行為著手時即應成立犯罪；此時兩者之競合如同前揭學者主張應適用通保法第 24 條之規範，本文支持此一見解。

五、結論

（一）釐清加密連線封包之監控行為法律爭議之必要

國家安全會議國家資通安全辦公室於 2018 年九月發表國家資通安全戰略報告，以「資安即國安」作為標題，顯示國家對於資通安全之重視，亦彰顯資通安全對於國家之重要性。而資通安全之兩大基礎課題，即為資通攻擊之防禦以及機敏資訊外洩之預防，而 SSL/TLS 加密技術之運用，正是要面對資通攻擊及資訊外洩的基本措施。但水能載舟亦能覆舟，於 SSL/TLS 加密通訊已經全部網路流量過半的當下，潛藏於加密通訊中之網路攻擊及資訊外洩等侵害資通安全行為，亦開始成為資通安全防護中的一大隱憂。因而對於各種加密連線之檢查，避免潛藏之

網路攻擊與資訊外洩行為，係為現代社會資通安全防護之基本要求。

然資通安全亦不能無限上綱，不能以資通安全之要求作為理由，無限制的侵害個人於資訊網路上之隱私權，而必須透過法律給予適當的規範，及為維護資通安全而必須限制個人基本權利時所應採取之正當程序；是以釐清加密連線之監控行為於法規上可能之法律責任，係為釐清對於加密連線監控行為界限之首要步驟，進而方得以發現法規對於此等行為規範不足或窒礙難行之處。

（二）對加密連線封包監控行為之法律責任

本文認為，當對於加密連線封包進行監控時，首應區分其所監控之連線方向與性質，其中組織使用解密設備進行監控時，倘若係針對外部網路向組織內部之伺服器進行連線者，此部分之監控行為由於解密設備與伺服器同屬組織所有，進而不構成違法行為，因而討論之核心應在對組織內部網路使用者向外加密連線封包，利用設備加以解密解析之行為，且針對未經內部網路使用者同意之解密行為。

1.特定機關之免責

關於此部分行為，本文認為倘若係屬資通安全管理法所規定之「公務機關」、「關鍵基礎設施提供者」或「特定非公務機關」時，其利用設備對於組織內部網路使用者向外加密連線進行解密解析時，應認為係屬於具有法令授權依據之行為，而不構成刑法第 315 條或 359 條之「無故」，進而構成要件不該當而不成立此二條之犯罪；同時亦為依據法令之行為而阻卻違法，依據通保法第 29 條第 1 款之精神，不成立通保法第 24 條之犯罪。

2.刑法第 359 條妨害電腦使用

(1)對病毒、網路攻擊之防禦

除上揭資通安全管理法所示機關外，本文認為，其餘組織利用解密設備對內部網路使用者之加密連線封包進行解密解析時，倘若其係採取系統自動比對病毒碼、攻擊指令之方式為之時，無論立法者立法理由所示抑或少數說下，此行為均係為對整體資通安全防護之提升，有助於社會大眾對於資通安全、電腦使用安全之信賴之行為，應認為並此行為未造成實質損害。由於刑法第 359 條係屬造成公眾或他人損害之實害犯，因而在未造成損害情形下，係屬構成要件不該當之行為而不成立犯罪。

(2)對於機敏資訊外洩之檢查

其餘組織利用解密設備對內部網路使用者向外加密連線封包進行解密解析，而其目的或解密之行為係在進行機敏資訊是否外洩之檢查時，本文以為由於現行技術尚需要以人工方式進行最終查驗，無法完全依賴系統自動完成，於此情形下係侵犯內部網路使用者之秘密通訊自由，尚難稱之為無損害之行為，是以此情形時當為刑法第 359 條之構成要件該當行為；且此等檢查之行為除非係已掌握特定洩密對象之特定洩密通訊，否則不能稱之為正當防衛而阻卻違法；第三，由於機敏資訊外洩之預防措施方法眾多，甚至包括禁止對外連線之實體網路隔絕等方式，因而亦不能稱此等行為為業務上正當行為而阻卻違法，此時應以行為決策之負責人與實際上操作解密檢查之人員為行為人，成立刑法第 359 條之妨害電腦

使用罪。

3.刑法第 315 條開拆封緘文書罪

由於電磁紀錄係屬準文書之一種，而對於連線封包進行加密係屬於與封緘具有相同價值效力之行為，是以對於已加密之連線封包進行解密並解析之行為，係該當於以開拆以外方式窺視電磁紀錄之內容，倘未經連線之當事人同意或如資通安全管理法等其他法律上依據時，應構成刑法第 315 條之開拆封緘文書罪。由於本罪係屬行為犯之規定，一經違犯即構成本罪，並未有前揭第 359 條實害之規定，因此無論採取解密、解析行為係屬自動化比對病毒、攻擊或人工檢查內容，均應有本罪之適用。此外，當本罪成立同時又成立刑法第 359 條之罪時，兩者間之關係依據所採取之法益觀點不同，可能為法條競合或想像競合，但無論採取何者競合之結果均應適用刑法第 359 條之罪為是。

4.通訊保障及監察法第 24 條違法監察罪

組織內部網路使用者對外之加密通訊封包，係屬通保法第 3 條所稱之具有合理隱私期待之通訊，而對於採取解密、解析之行為，係為通保法第 13 條所稱之監察行為。是以在未得內部網路使用者同意，亦非前揭說明依據資通安全管理法之要求情形下，就其對外加密連線封包加以解密解析之行為，係構成通保法第 24 條所稱之違法通訊監察之罪；且應注意者在於，通保法第 24 條所規範之違法通訊監察罪並未規定結果之構成要件，是以無論基於何種目的對於內部使用者之加密連線進行解密，均會成立本罪。於成立本罪情形下，倘同時亦成立刑法第 359 條之妨害電腦使用罪時，應依據想像競合適用刑法第 359 條之罪為是。

倘僅透過系統自動比對病毒碼、攻擊碼，未造成損害致使行為不成立刑法第 359 條之妨害電腦使用罪時，仍有通保法第 24 條與刑法第 315 條之適用空間，此時應依據想像競合適用通保法 24 條之規範。

（三）關於資通安全需求之回應

1.取得使用者同意

綜上所述，組織對於內務網路使用者與外部之 SSL/TLS 加密連線，基於資通安全防護之需求，採用各式設備加以解密、解析之行為，本文認為僅有基於資通安全管理法之要求，具備公務機關、關鍵設施提供者或特定非公務機關之身分，必須建構安全的資通安全環境時，此時得據以主張依法令之行為阻卻構成要件或阻卻違法性，使得未經內部網路使用者同意而逕行就其對外 SSL/TLS 加密連線封包加以解密、解析之行為不成立犯罪，其餘情形下，非經使用者之同意均有上揭各罪之適用空間為是。進而各企業、機構於著重資通安全防護之同時，應注意對於內部網路使用者—無論其所使用之終端設備所有權歸屬—之隱私權及秘密通訊自由之保障。組織於採用相關解密設備、技術時，應以獲得網路、通訊使用者之同意作為前提。此等同意就組織內固定成員，或可以勞動契約等方式為之，但就非固定成員而有使用網路之使用者，可能需要透過連線時之告知並同意的方式加以解決；且本文認為基於組織對於網路設備之所有權，或可採用不同意被監控即無法連線等方式進行，但不應以繼續使用即視為同意之告知方式為之，以確保

獲得當事人之真摯同意。

2.單純病毒、攻擊之防禦應修正放寬

另方面，於刑法第 359 條之規範下或可透過解釋，使單純以系統自動化處理比對病毒碼及攻擊指令部分之加密連線解析行為，免於犯罪之成立，但此部分仍有通保法第 24 條與刑法第 315 條之適用。問題在於，病毒及網路攻擊之防禦可謂資通安全之基本要求，且此類行為僅係透過系統自動化完成，通常不會由人工擷取出通訊的內容，此時仍構成通保法 24 條與刑法第 315 條之罪，顯然對於資通安全防護、國家安全之建設具有嚴重重大的影響。是以本文認為就此類設置系統、設備進行比對處理之行為，理應修法將之排除於刑法第 315 條與通保法 24 條之適用範圍，以利於資通安全防護措施之採行。

3.進一步放寬之可能

最後係必然構成刑法 359、315 條及通保法 24 條等罪之行為，亦即不具備資通安全管理法身分，在未經使用者同意下就其加密連線封包予以解析、解密，並以檢查其訊息內容以防止機敏資訊外洩之行為。就此部分而言，本文認為現行技術下進行機敏資訊外洩防止，或部分可採取系統比對方式進行，但最終可能仍需要人工之判定，此時無疑會侵害當事人之秘密通訊自由權益，倘若未經當事人之同意即進行，其侵害實過於重大而仍應該成立犯罪為是。然本文亦保留對於此部分法規放寬可能性之意見，亦即透過技術之進步，於機敏資訊之比對可委由電腦系統、人工智慧完全獨立的完成，而無須再由自然人加以判定時，或可能進一步修法放寬上揭限制，以利於資通安全之維護及促進資通安全技術之進展。

政府文件

立法院議案關係文書院總第 1407 號-政府提案第 4235 號之 1，立法院，1999.04，available at: https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcbcfcecfc7cfcdc5cacdcad2cac8cb 。
立法院議案關係文書院總第 246 號-政府提案第 8862 號之 1，立法院，2003.05，available at: https://lis.ly.gov.tw/lgcgi/lgmeetimage?cfcacfcccecdcfcdc5cdc8c6d2cccfcb 。
國家安全會議，國家資通安全戰略報告，2018 年 9 月。
法務部 89 年法字第 000805 號函。

外國法規暨政府文件

BGHst 10, 230。
Katz, 389 U.S. 347, 361 (Harlan, J., concurring).

學術專書

甘添貴，體系刑法各論Ⅰ，2011.09 修正再版。
林山田，刑法通論（下），作者自行出版，2008.01 增訂 10 版。
林鈺雄，新刑法總則，元照，2014.09 四版。
柯耀程，刑法競合論，元照，2000.12。
陳惠貞，新趨勢網路概論，碁峯，2018.04。
黃明祥、林詠章、周永振，資訊與網路安全實務，普林斯頓，2017.01。
黃榮堅，基礎刑法學（上），元照，2003.05。
盧映潔，刑法分則新論，新學林，2015.07 十版。

期刊論文

吳耀宗，刑法之解釋方法與業務作為阻卻犯罪成立之要素，月旦法學教室 No.45，2006.07，頁 34-46。
李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌 54 期，2004.01，頁 235-247。
李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌 55 期，2004.02，頁 243-256。
蔡蕙芳，網路監聽可能涉及刑罰規定之介紹，資訊安全論壇 19 期，2004.09，頁 35-43。

盧映潔，侵入住宅罪之「無故」判斷，月旦法學教室 19 期，2004.05，頁 24-25。

學位論文

陳佩佩，台南市國民中學學生網路使用行為與網路素養之研究，台灣師範大學碩士論文，2011 年 6 月。
陳琮元，SSL 代理伺服器之設計與實作，清華大學碩士論文，2005 年。
黃俊捷，雲林縣國中學生網路使用現況、網路素養與網路態度相關之研究，南華大學碩士論文，2013 年 5 月。

新聞報導

ETtoday 財經中心，台積電遭病毒攻擊　損失 76 億、報廢上萬片晶圓，ETtoday 新聞雲，2018.08.06，available at: https://www.ettoday.net/news/20180806/1228606.htm#ixzz5Ota8FkEW 。
王宏仁，台積電產線中毒大當機事件簿(Day1~Day4 時程懶人包），iThome，2018.08.10，available at: https://www.ithome.com.tw/news/125118 。
林妍溱，「路由器漸成為 APT 攻擊的最愛，防毒公司警告，威脅僅次於 CPU 漏洞」，iThome，2018.04.13，available at: https://www.ithome.com.tw/news/122403 。

產品文件

A10 Networks，「A10 Thunder SSLi：檢測網路加密資料的最佳利器」，iThome，2017.03.21。available at: https://www.ithome.com.tw/pr/112863 。
Symantec, “Cost-Effective, Flexible Visibility and Control of SSL/TLS Network Traffic”, available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/flexible-visibility-and-control-of-ssl-traffic-en.pdf 。
李宗翰，「扛下解密流量負載，Palo Alto 新版次世代防火牆平臺登場」，iThome，2018.06.23。available at: https://www.ithome.com.tw/review/123197 。
李宗翰，「透視 SSL 加密流量並能與資安系統協防，F5 推出檢測分析設備」，iThome，2017.03.03。available at: https://www.ithome.com.tw/review/112440 。

法院判決

最高法院 94 年度台上字第 5802 號刑事判決。

最高法院 95 年度台上字第 1705 號刑事判決。
最高法院 96 年度台上字第 1387 號刑事判決
最高法院 94 年度台上字第 4791 號刑事判決
臺灣高等法院 85 年上更（一）第 1190 號刑事判決
士林地方法院 102 年度訴字第 200 號刑事判決
新竹地方法院 95 年度易字第 121 號刑事判決

網路文章

Electronic Frontier Foundation, We're Halfway to Encrypting the Entire Web, 2017.02, available at: https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web .
Jackyhwei，一個最簡單的破解 SSL 加密網絡數據包的方法，SAOWEN，2017.08.04。available at: https://hk.saowen.com/a/279fe2a510c923ddf71ddc7ea4d515e65dbe200258f867495ca658ca39c7edac .
凌威科技，硬碟基本原理，2014.12.16，available at: http://www.linwei.com.tw/article/ins.php?index_id=22 。