Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale in Lingue, Economie e Istituzioni dell'Asia e dell'Africa mediterranea

in Language and Management to China

ordinamento (D.M. 270/2004)

Tesi di Laurea
Magistrale

Cybersicurezza e Cina

Impatto su economia, società e politica con repertorio terminografico italiano-cinese

Relatore
Ch. Prof. Livio Zanini

Correlatore
Ch. Prof. Franco Gatti

Laureando
Federico Restelli
Matricola 882055

Anno Accademico
2021 / 2022

序言

网络安全是计算机科学的一个分支，网络安全主要研究如何保护计算机系统免受外部威胁。 网络安全最技术方面包括身份验证系统的体系结构，恶意软件分析，加密算法的设计或开发新的杀毒软件等等，其实网络安全对许多领域很重要。经济的、社会的、政治的、军事的。 对所有这些领域，网络安全是解决新的和以前未知的挑战和困难的核心。 网络安全研究的现象产生于人与信息技术之间的复杂互动。

本文的第一部分介绍计算机科学的基本概念，以便理解计算机网络的功能，比如说互联网的功能。网络只不过是连接在一起的一组计算机，这些计算机按照特定的规则相互通信，交换虚拟数据。保护者和攻击者争夺数据。计算机在当今生活中占据中心地位，互联网上或者计算机里有重要的数据：个人信息、银行密码、企业秘密知识、外交和政治机密。避免未经授权的访问这些数据是至关重要的。第二个基本需求涉及在互联网上验证人们的身份：无法签证身份，就不能使用购物或网上银行等基本服务。保证身份、保护网络通信的解决措施是密码术。因为数据保护的水平取决于加密算法的复杂性，算法设计需要高等数学知识，所以密码术是计算机安全最技术的方面。其次，加密技术用于设计几乎不能伪造的证书，以确保网站管理人员的身份。复杂的公钥系统(公钥基础设施) 使互联网成为商业、公共服务和远程通信的平台成为可能，它是基于加密算法的使用，而这种算法实际上不可能解密和伪造。这就是说，现代社会和经济背后的大部分齿轮都要归功于密码术。

在密码学中，人们找到了一种有效而灵活的方法来保证网络虚拟环境的安全。然而，网络空间中还存在其他类型的威胁，这使得网络安全专家的工作绝地必要。例如，恶意软件是危害个人用户电脑的最常用工具之一；由于无法攻击在网上传播的数据，许多网络犯罪分子试图进入毫无戒心的用户的计算机，以获取有价值的信息，有时甚至控制这台机器。从那里，他们还可以在很短的时间内感染大量的计算机，或者在一个私有网络上移动，直到它们到达所有相互连接的计算机。最危险的恶意软件是两种: “蠕虫” 和 “加密勒索软件” 。第一个具备病毒传播难以置信的能力：蠕虫病毒能够潜入用户的计算机，然后复制自己，并将自己发送到其他计算机上。它们可以在几小时内接触到数千台电脑。第二个，加密勒索软件，是一种真正的社会和经济祸害；是网络犯罪分子的主要获利手段：加密勒索软件被引入计算机系统，通过一种加密算法来屏蔽用户数据，恶意软件的创建者才知道怎么解码。当用户不能访问他们的数据时，就需要支付赎金。

许多计算机系统的攻击策略利用计算机程序和虚拟通信系统的漏洞，所以网络安全的大部分工作包括开发反病毒软件、防火墙系统、在改进加密算法等方面。总而言之，“保护”工作的一部分在于改进保护和监视技术。网络安全的另一个极其重要的部分是围绕人为因素。事实上，IT安全不仅仅是一个技术问题，还需要传播知识和培训。许多恶意软件感染和数据偷窃是因为用户被精心策划的骗局和陷阱欺骗了：虚假网站、虚假邮件、虚假账户、虚假反病毒程序等等。诈骗和欺骗的攻击名称是“网络钓鱼”，网络钓鱼是一个严重的网络安全问题。在第一章中，作者介绍一些网络攻击事件来解释网络罪犯怎么使用这些不同的工具和策略。

介绍了网络安全的核心题目以及网络信息空间的主要威胁之后，重点转向网络攻击的幕后黑手。网络空间中存在着大量的参与者，从在黑客方面经验丰富的人，到专业人员组成的真正的犯罪集团。后者称为“APT”(高级持续威胁)。后者称为“APT”(高级持续威胁)。APT 是一群极其协调的专业人员，其专业人具备丰富的资源和知识；这些组织通常会进行精心策划的网络钓鱼活动，以进入公司或政府机构的计算机系统，目的是提取具有很高经济或政治价值的特定信息。在实践中，他们是虚拟“窃贼”，他们可以策划一场长达数月的攻击，并在同样长的时间内包围目标的网络保护，寻找特定的信息。

本文最后部分分析受政治利益影响的行为群：匿名黑客、黑客行动主义和爱国黑客都是通过新技术进行政治和意识形态斗争的群组。其特点是，这些组织是围绕网络和新技术诞生和聚集的，此外，他们还使用网络攻击方法来实现自己的政治斗争目标。然后，本文介绍一些具有国际重要性的事件：维基解密和震网病毒。这些事件表明，网络安全问题是许多不同领域讨论的核心问题:在经济领域，为了使公司更好地面临新环境风险（比如说，工业间谍活动），在社会领域，为了面对小犯罪的新前沿(在线诈骗、信用卡盗窃、个人数据盗窃和勒索等等)，在政治和军事领域，网络空间构成国家竞争的新战场。

第二章深入研究中国在网络安全方面的作用和情况。事实上，值得注意的是，中国经常与网络安全相关的新闻和讨论联系在一起。主要原因是，不少针对 APT 和工业间谍的调查案件或多或少与中国有直接联系。除了这个原因意外，中国网络安全情况值得研究是因为，与西方的情况相比，中国的网络安全问题有不同独特的形式。本章第一部分包括两个方面：结构负责网络安全政策设计的分析，并国家总体情况的介绍。然后，讨论继续到网络安全相关的具体经济问题，其中有一部分专门讨论网络犯罪的地下经济。作者介绍一些中国背景下特有的文化现象，如“长城防火墙”和“红客”的现象。像论文的第一部分一样，作者也分析中国网络空间群体和运动的特点。中国专家发现，有两种类型的方面，平民和军事/国家的。为了清楚中国军方与网络

攻击案例之间的联系，本文回顾解放军的网络攻击能够，以及一些著名 APT 攻击案例。论文最后部分是词汇表，词汇包括与网络安全相关的文章和文档中的最广泛和最重要的术语。

Introduzione

La cybersicurezza o sicurezza informatica è una branca delle scienze informatiche che si occupa principalmente della protezione dei sistemi informatici dalle minacce esterne. La cybersicurezza può essere intesa nella sua accezione più tecnica e settoriale come la disciplina che si occupa di architettura dei sistemi di autenticazione, analisi dei malware, di progettazione di algoritmi di crittografia oppure di sviluppo di nuovi programmi antivirus e così via, ma in realtà i campi di rilevanza della cybersicurezza sono molto più numerosi. Economia, società, politica, disciplina militare. In tutti questi campi la cybersicurezza occupa una posizione centrale per affrontare sfide e difficoltà nuove e precedentemente sconosciute. La cybersicurezza va ad indagare i fenomeni nati dalle complesse interazioni dell'uomo con le nuove tecnologie informatiche.

La prima parte del presente elaborato si occupa di presentare i concetti di base delle scienze informatiche, utili a comprendere il funzionamento delle reti private e pubbliche, internet compreso. Le reti non sono altro che l'insieme di computer che comunicano tra loro secondo regole specifiche, scambiandosi dati virtuali. I dati sono il principale oggetto di contesa tra chi cerca di proteggere le reti informatiche e chi cerca di comprometterle. Vista la centralità dell'uso del computer per la vita di oggigiorno, tutto ciò che è di valore viene comunicato sotto forma di dati che viaggiano in rete: informazioni personali, codici di accesso bancario, proprietà intellettuale aziendale, segreti diplomatici e politici. Evitare l'accesso non autorizzato a tali dati risulta essere di fondamentale importanza. La seconda esigenza fondamentale riguarda la verifica dell'identità delle persone su internet: senza di ciò sarebbe impossibile utilizzare servizi essenziali come lo shopping o l'online banking. La soluzione per garantire e proteggere le comunicazioni in rete è stata individuata nella crittografia. La scienza crittografica rappresenta uno dei campi più tecnici della sicurezza informatica, siccome il livello di protezione dei dati dipende dalla complessità degli algoritmi utilizzati per cifrare il contenuto dei pacchetti di dati spediti su internet. Secondariamente, le tecniche crittografiche vengono utilizzate per creare dei certificati difficilmente falsificabili che servono per assicurare l'identità dei gestori dei portali web. Il complesso sistema di chiavi pubbliche (Public Key Infrastructure) che rende possibile l'utilizzo di Internet come piattaforma di commercio, servizi pubblici e comunicazioni su lunga distanza si regge sull'utilizzo di algoritmi di cifratura praticamente impossibili da decifrare e da falsificare. Ciò equivale a dire che una larga parte degli ingranaggi alla base della società ed economia moderna funzionano grazie alla crittografia.

Nella crittografia si è trovato una risposta efficace e flessibile per rendere sicuro l'ambiente virtuale di internet, ciononostante esistono minacce di altro tipo che infestano il cyberspazio e che rendono il lavoro degli esperti di cybersicurezza indispensabile. I malware sono per esempio uno degli strumenti più utilizzati per compromettere i computer dei singoli utenti; non potendo "attaccare" i dati mentre circolano in rete, molti dei criminali online cercano di introdursi nei computer degli utenti ignari per guadagnare l'accesso, a volte persino il controllo, dei dispositivi altrui. Da lì, possono anche arrivare ad infettare un numero elevatissimo di computer nel giro di poco tempo oppure muoversi in una rete privata fino a raggiungere tutti i computer connessi tra loro. I malware più pericolosi sono di due tipi: i "worm" e i "ransomware". I primi rappresentano un problema anche solo per l'incredibile capacità di diffusione virale: sono capaci di introdursi di nascosto nei computer degli utenti per poi autoriprodursi e spedirsi ad altri computer connessi in rete. Possono raggiungere anche migliaia di computer in poche ore. I ransomware rappresentano invece una piaga sociale ed economica; essi sono i principali mezzi di lucro dei cybercriminali: introdottosi nei sistemi informatici, il ransomware blocca i dati dell'utente attraverso l'utilizzo di un algoritmo di crittografia conosciuto solo dal creatore del malware. Escluso l'utente dall'accesso ai propri dati, viene poi chiesto un riscatto.

Molte delle strategie di "attacco" dei sistemi informatici fanno leva sulle vulnerabilità dei programmi di gestione dei computer e le architetture dei sistemi di comunicazione virtuale, motivo per cui una buona parte del lavoro nella sicurezza informatica consiste nel sviluppare software antivirus, sistemi di firewall (filtraggio dei dati in entrata ed uscita dal computer), nel migliorare gli algoritmi di crittografia e così via. In sintesi una parte del lavoro di "difesa" consiste nel migliorare le tecniche di protezione e sorveglianza. Un'altra parte estremamente importante della cybersicurezza ruota invece attorno al fattore umano. Infatti, lungi dall'essere solo un problema tecnico, la sicurezza informatica necessita anche di divulgazione e formazione. Molti dei malware e dei furti dei dati avvengono proprio perché gli utenti vengono ingannati da truffe e trappole ben congeniate: finti siti internet, finte mail istituzionali, finti profili social, finti programmi antivirus e così via. I tentativi di truffa e inganno vengono raccolti sotto il termine di "phishing" e rappresentano un grave problema per la sicurezza delle reti. Nel corso del primo capitolo vengono presentati alcuni episodi di attacco informatico per spiegare come i diversi strumenti di offesa e le vulnerabilità più comuni vengono sfruttate dai criminali sul web.

Dopo aver fatto un'introduzione su cosa sia la sicurezza informatica e di quali minacce si occupa, l'attenzione viene spostato su chi si cela dietro agli attacchi informatici. Esiste una pletora di attori presenti nel cyberspazio, da singoli individui più o meno esperti di "hacking" a veri e propri gruppi

criminali di professionisti ben organizzati. Quest'ultimi prendono il nome di "APT" (Advanced Persistent Threat) e vengono analizzati per primi. Si tratta di gruppi estremamente coordinati di professionisti in possesso di elevate risorse ed expertise; tali gruppi sono soliti portare avanti elaborate campagne di phishing per ottenere l'accesso ai sistemi informatici di aziende o enti governativi, con l'obiettivo di estrarre informazioni specifiche ad alto valore economico o politico. In pratica agiscono da "scassinatori" virtuali, possono pianificare per mesi un colpo e assediare le difese del target per altrettanto tempo; essi vanno alla ricerca di informazioni specifiche e si sospetta che spesso lavorino su commissione o per conto di agenzie governative. A questo punto lo spazio viene dedicato ai gruppi di attori mossi da interesse politico: Anonymous, hacktivismo e hacker patriottistici sono tutti termini che vanno ad individuare persone o movimenti che attraverso le nuove tecnologie portano avanti delle battaglie politiche e ideologiche. La caratteristica saliente è che tali gruppi nascono e si aggregano attorno al web e alle nuove tecnologie digitali, inoltre utilizzano i classici metodi di attacco informatico per portare avanti i propri obiettivi di lotta politica. Il discorso poi viene ampliato presentando alcuni casi di rilevanza internazionale: Wikileaks e Stuxnet. Tali episodi servono per dimostrare come il problema della sicurezza informatica sia centrale alle discussioni di molti ambiti differenti: in ambito economico per meglio equipaggiare le aziende nel far fronte a nuovi tipi di rischi ambientali e spionaggio industriale, in ambito sociale per far fronte alla nuova frontiera della piccola criminalità (truffe, furti di carte di credito, furto di dati personali e ricatti…), in ambito politico e militare in quanto il cyberspazio costituisce campi di scontro tra Nazioni.

Il secondo capitolo è dedicato ad uno sguardo di approfondimento nei confronti del ruolo della Cina e della situazione cinese per quanto riguarda la cybersicurezza. Occorre infatti notare come molto spesso il gigante asiatico sia legato a notizie e discussioni aventi a che fare con la sicurezza informatica. Il motivo principale è che non pochi casi di investigazione sulle APT e sullo spionaggio industriale sono collegati in maniera più o meno diretta con la Cina. Inoltre, nel Paese le questioni relative alla cybersicurezza prendono forme differenti ed uniche rispetto alla situazione Occidentale. Per poter fare chiarezza si parte dall'analisi delle istituzioni e delle policy dedicate alla sicurezza informatica e dalla presentazione della situazione generale nel Paese. Successivamente si passa alle problematiche in campo economico specifiche del contesto cinese, con uno specchietto dedicato all'economia sotterranea dei cybercriminali e la presentazione di alcuni fenomeni culturali della cybersicurezza cinese, come il "Great Firewall" e i "Red Hacker". In seguito, come per la prima parte della tesi, si presentano i gruppi e i movimenti riconosciuti che compongono l'insieme degli attori presenti nel cyberspazio cinese. Ciò che è stato scoperto dagli studiosi e osservatori asiatici è che esistono due tipologie di attori, quella civile e quella militare/statale. Volendo chiarire i legami tra

l’esercito cinese e i casi di attacco informatico spesso citati nelle discussioni riguardo la cybersicurezza, si passa in rassegna ciò che è stato studiato della struttura dell’esercito cinese e delle capacità di cyber-offesa, assieme con alcuni celebri casi di APT a matrice cinese.

La tesi si conclude con l’elenco delle schede terminografiche per i termini più diffusi e importanti che affiorano negli scritti e nella documentazione relativa alla cybersicurezza.

Sommario

Capitolo 1

Cyber sicurezza: che cos'è

Sebbene non esista unanimità sulla definizione del termine, con buona approssimazione si può dire che la cyber sicurezza sia il campo preposto alla difesa delle reti e dell'equipaggiamento informatico, con il fine di prevenire o rimediare ai furti e alle manomissioni dei dati da parte di attori terzi non autorizzati. Fare cyber sicurezza può significare secretare la comunicazione dei dati tra utenti, impedire infiltrazioni di programmi o individui malintenzionati all'interno delle reti e dei computer di un'organizzazione, fare ricerca e analisi dei pericoli del mondo digitale ma anche ripensare l'architettura dei processi e delle strutture aziendali, o persino istruire il personale a non cadere nei tranelli psicologici dei truffatori in rete e a disimparare le cattive abitudine nella gestione dell'equipaggiamento informatico. E la lista si estende potrebbe proseguire. Il campo della sicurezza informatica non deve essere considerato un settore squisitamente pertinente alle scienze informatiche strette, per la natura e l'ampiezza dei fenomeni trattati. Tornando brevemente sulla definizione del termine, ecco come l'ex Direttore della Ricerca presso l'Agenzia Nazionale di Sicurezza degli Stati Uniti Fredrick Chang ne parla:

"La scienza della cybersicurezza offre molte opportunità di avanzamento attraverso un approccio multidisciplinare, perché, alla fine dei conti, la cybersicurezza riguarda fondamentalmente il confronto con un avversario. Le persone devono difendere le macchine attaccate da altre persone che utilizzano le macchine. Dunque, in aggiunta ai campi critici delle scienze informatiche, ingegneria elettrica e matematica, sono necessarie prospettive da altri campi." (Chang, 2012, 1–2)

Perché la cyber sicurezza è importante?

Oggi il mondo economico, governativo, militare e privato è sempre più pervasivamente informatizzato, i computer, miniaturizzati o meno che siano, svolgono un'innumerevole quantità di compiti fondamentali per il funzionamento di ogni cosa, per di più essi sono spesso collegati tra loro, formando così una rete (di reti) che copre tutto il globo, ovvero internet e tutti i suoi sistemi. Le tecnologie informatiche sono diventate linfa vitale e requisito imprescindibile per il funzionamento del mondo moderno, i processi sono diventati più rapidi, efficienti e comodi, ma assieme con i benefici si sono aperti nuovi scenari di vulnerabilità, minacce e conflitti internazionali.

Come funzionano Internet e i computer: le basi

La comprensione dei confini tematici, ma soprattutto dei termini specifici, della cyber sicurezza è subordinata alla comprensione dei principi generali di funzionamento delle reti e delle tecnologie informatiche.

Il computer

Per quanto possa risultare triviale, il primo passo consiste nel fare alcune fondamentali distinzioni riguardo al funzionamento dei computer. Con il termine computer all'interno del presente elaborato si intendono sia personal computer a postazione fissa sia i computer portatili, occorre inoltre far notare che ai fini dell' analisi sul tema della sicurezza informatica, i dispositivi come smartphone, tablet, smartwatch e via dicendo sono anch'essi considerati computer e dunque verranno indicati con lo stesso termine-cappello. I computer sono composti da hardware e **software**, ovvero da una parte fisica di componenti elettroniche e da una parte virtuale di istruzioni logiche. Il software comprende il vero e proprio **sistema operativo**, ovvero lo scheletro di direttive e regole fondamentali, di solito non direttamente accessibili all'utente di base, che non le deve conoscere per poter operare. Si tratta di un'infrastruttura digitale sommersa che permette il funzionamento di base della macchina. In realtà alla base il computer non fa altro che eseguire un numero enorme di calcoli simultanei, ovvero tutta una serie di operazioni logiche esemplificate in 0 e 1, cioè in **codice binario**. Ciò che organizza e presenta le informazioni in maniera sensata all'occhio umano è l'interfaccia utente; attraverso l'interfaccia l'utente umano può utilizzare il computer per numerose operazioni differenti. Per ogni cosa che si può fare su un personal computer (PC) esiste un'applicazione o **programma**, per esempio Word è un programma che si usa per scrivere documenti di testo, così come Outlook si usa per mandare e ricevere mail, oppure Autocad per eseguire disegni tecnici e planimetrie. Ognuno di questi programmi è pensato per eseguire una o più funzioni specifiche o molte funzioni basilari (come il sistema operativo), e vengono scritti in differenti codici o **linguaggi di programmazione** dagli addetti ai lavori (es. programmatori, software designer). Il linguaggio di programmazione o le linee di codice sono informazioni che il computer interpreta come direttive per eseguire specifiche azioni. Quando il codice di programmazione viene scritto per svolgere una specifica funzione, come per esempio un calcolo matematico, viene chiamato **algoritmo**; un algoritmo rimane comunque un

linguaggio di programmazione che impartisce alla macchina delle istruzioni da eseguire, di solito si distingue dal termine “codice” perché viene utilizzato per risolvere uno problema molto specifico. Le informazioni, che invece impartiscano o meno ordini al computer sono conservate sotto forma di **file** digitali, ovvero contenitori di dati, i quali poi possono essere letti dai uno o più programmi per essere mostrati all’operatore umano. Foto, video, audio, documenti digitali o programmi eseguibili sono tutti esempi di file. I file sono conservati in **database** all’interno del computer, che possono essere intesi sia come supporti fisici di memorizzazione (banche di dati, hard disk), sia come luoghi virtuali, ovvero l’architettura logica di organizzazione dei dati. I dati possono anche essere archiviati in supporti esterni di memorizzazione come **chiavette USB** o **hard disk** portatili, ma anche conservati in remoto in ciò che viene chiamato “cloud storage” (cioè dati salvati su server di aziende che mettono a disposizione lo spazio di archiviazione delle loro macchine agli utenti, che possono accedere ai propri dati ovunque vadano finché hanno una connessione internet; si dicono “in cloud” perché invece di essere presenti sul proprio computer sono “online”, in realtà ben lungi dall’essere conservati “nell’etere” sono semplicemente salvati sui computer di altre aziende). La presente spiegazione, per quanto rudimentale, serve per sottolineare alcuni punti chiave: 1) parte di ciò che succede all’interno di un computer, nel suo spazio virtuale si intende, non tra i suoi cavi, microchip e transistor, avviene “dietro le quinte”, solitamente l’utente medio non ne è consapevole; 2) tutto ciò che è presente nello spazio virtuale di un computer è sotto forma di informazioni basilari (binarie), che poi possono essere presentate in forme più complesse come immagini, suoni o interfacce appetibili alla percezione umana 3) alcune informazioni possono essere interpretate dal computer come istruzioni da eseguire, se presentate in un certo linguaggio (di programmazione).

Le reti, la comunicazione tra computer e Internet

Il passo successivo è comprendere come i computer si possono collegare tra loro e come comunicano. È ormai risaputo che Internet è nato dal progetto militare americano degli anni ‘60 ARPANET, così chiamato perché finanziato dalla “Advanced Research Projects Agency” (ARPA). In un periodo in cui i computer cominciavano a diffondersi tra le istituzioni militari e di ricerca, si cercò un modo per sfruttare la nuova tecnologia e ottenere un vantaggio strategico sul resto del mondo; ciò a cui si pensò fu di facilitare la comunicazione tra differenti centri di ricerca collegando tra loro computer che risiedevano a grande distanza: in questo modo nacquero le prime reti o **network** informatici. Una rete informatica è essenzialmente un collegamento tra più dispositivi informatici, realizzata attraverso connessioni via cavo, radio, fibra ottica o satellite. È interessante notare come nello stesso periodo cominciano ad avvenire, con la diffusione dei computer e dei collegamenti tra di

essi, le prime prese di coscienza che porteranno poi allo sviluppo della cyber sicurezza come disciplina. Secondo le ricerche di Warner sui rapporti degli ufficiali e i teorici militari americani, già nel 1960 era chiaro che "i computer possono disperdere dati sensibili e devono dunque essere sorvegliati" e nel 1970 che "i computer possono essere attaccati e le informazioni rubate" (Warner 2012, 3), dunque ben lungi dall'essere un cruccio di epoca moderna, le domande fondamentali della sicurezza informatica cominciarono ad essere poste ben prima dello sviluppo di Internet. Con l'abbassarsi del costo delle tecnologie informatiche, negli anni 80 e 90, iniziò la diffusione dei computer tra la popolazione civile; a questo punto fu necessario l'intervento del settore privato per commercializzarli capillarmente. L'ultimo passo per la creazione dei sistemi di telecomunicazione odierni fu quello di allargare la connessione tra computer alla popolazione su larga scala: è così che nacque Internet. Infatti, così come un network consiste in una rete di computer, allo stesso modo **Internet** è in essenza una rete di reti (Singer and Friedman 2014, 17-20).

Come comunicano i computer tra loro?

Nella creazione di un'infrastruttura di rete globale, la sfida davanti a cui si trovarono gli esperti e gli ingegneri informatici fu quella di trasmettere le informazioni attraverso diversi tipi di collegamenti, su cui viaggiano diversi tipi di segnali (si pensi alle onde radio o alla trasmissione via cavo telefonico, o ad oggi la fibra ottica che trasmette impulsi luminosi) per di più su linee non sempre stabili. Nel 1973 Vint Cerf, professore alla Stanford University e Robert Khan dell'ARPA ebbero l'idea di far comunicare le diverse macchine secondo uno stesso protocollo, una serie di istruzioni condivise secondo cui stabilire una connessione, segmentare il messaggio, spedirlo sulle linee di comunicazioni più stabili e ricomporlo all'arrivo. Ciò che oggi si usa per la connessione Internet deriva da tale intuizione iniziale: il **protocollo TCP/IP** (Transmission Control Protocol/ Internet Protocol).

Come funziona dunque la comunicazione tra computer attraverso il protocollo TCP/IP? In sintesi, funziona per trasmissione di pacchetti di dati. Le informazioni sono divise in segmenti più piccoli che possono essere consegnati in modo indipendente e decentralizzato. Pacchetti di informazioni provenienti da fonti differenti possono condividere la stessa linea senza interferenze e possono viaggiare sulle linee dove la connessione risulta più stabile e veloce, senza perdere l'interezza del messaggio, perché una volta arrivati a destinazione vengono riconosciute come provenienti dalla stessa fonte (dallo stesso PC) e ricombinate nell'ordine corretto. I pacchetti possono viaggiare per strade molto diverse e ricombinarsi all'arrivo senza apparente perdita di connessione; il protocollo TCP/IP risulta in questo modo essere un'architettura efficace e resiliente. Per fare chiarezza, se per ogni computer che desidera mettersi in connessione si dovesse riservare un'unica "strada" esclusiva,

sarebbe molto difficile gestire il traffico enorme di dati che caratterizza Internet e in caso di problemi di linea ci sarebbe un'interruzione della comunicazione. In questa maniera invece i dati possono trovare la strada migliore per evitare di sovraccaricare le reti e di incappare in vicoli ciechi dovute al malfunzionamento di una linea.

C'è un ultima invenzione che ha dato forma ad Internet come è conosciuto al giorno d'oggi, il protocollo HTTP. L'HyperText Transfer Protocol (HTTP) è un protocollo usato per trasmettere e presentare le informazioni che arrivano da un altro computer in una rete, per gestire la richiesta di dati da un server e presentarli poi come un insieme di documenti collegati tra loro (una pagina web), fu inventata da Tim Berners-Lee nel 1990, mentre lavorava come ricercatore per il centro di ricerca europeo CERN in Svizzera, assieme con un sistema per identificare i documenti collegati tra loro, chiamato **Uniform Resource Locator (URL)**. Il collegamento tra due (o più) file viene chiamato **Hyperlink** o collegamento ipertestuale, in gergo "link".

Come funziona la navigazione su Internet?

Dati alcuni concetti di base, può essere utile fare un esempio di cosa realmente succede quando si "visita" una pagina Web, per rendere più chiaro il meccanismo alla base del funzionamento di Internet. Per esempio, se uno studente decidesse di visitare il sito internet dell'Università Ca' Foscari, dovrebbe per prima cosa "cliccare" sul link www.unive.it, ovvero sull'indirizzo URL indicante la serie di documenti virtuali che compongono il sito internet dell'Università Ca' Foscari. I documenti in questione sono conservati all'interno di specifici computer destinati alla conservazione e trasmissione dei dati, chiamati "**server"**. I server sono siti in diversi luoghi in tutto il mondo, i server che ospitano la pagina dell'università veneziana (assieme con molte altre) sono localizzati in Italia. Dunque, quando l'utente immette o selezione l'indirizzo URL, per prima cosa il computer cerca l'accesso alla rete globale, ad internet. Il punto di accesso ad Internet è un dispositivo chiamato "**router"** o Modem. Il modem indirizza la richiesta all'**Internet Service Provider (ISP)**, ovvero alle infrastrutture informatiche dell'ente responsabile per l'erogazione dei servizi di connessione alla rete globale (per esempio Telecom, Fastweb, Wind…). Gli ISP posseggono numerosi server per gestire le richieste dei propri clienti, tali server conservano tra le altre cose le informazioni per poter rintracciare i siti desiderati. Come si fa a rintracciare uno specifico sito nella vasta marea di pagine web che esistono al mondo? In sintesi, i siti web sono associati ad un codice numerico univoco, l'indirizzo IP. L'architettura virtuale che permette di collegare nome di un sito ad un preciso indirizzo numerico è chiamata Domain Name System (DNS). Nel caso del sito www.unive.it l'indirizzo IP è 157.138.7.88 . Una volta che il DNS ha individuato il server che ospita il sito internet, esso invia una

richiesta HTTP per ottenere i dati da inviare al computer di partenza (allo studente). Ricevuti i dati, il computer presenta le informazioni in maniera coerente ed organizzata attraverso il **browser**, ovvero l'applicazione che fa da interfaccia per la navigazione web e appunto legge e riorganizza i dati. In questo modo sullo schermo del computer dello studente appare finalmente il sito universitario sotto forma di pagina web.

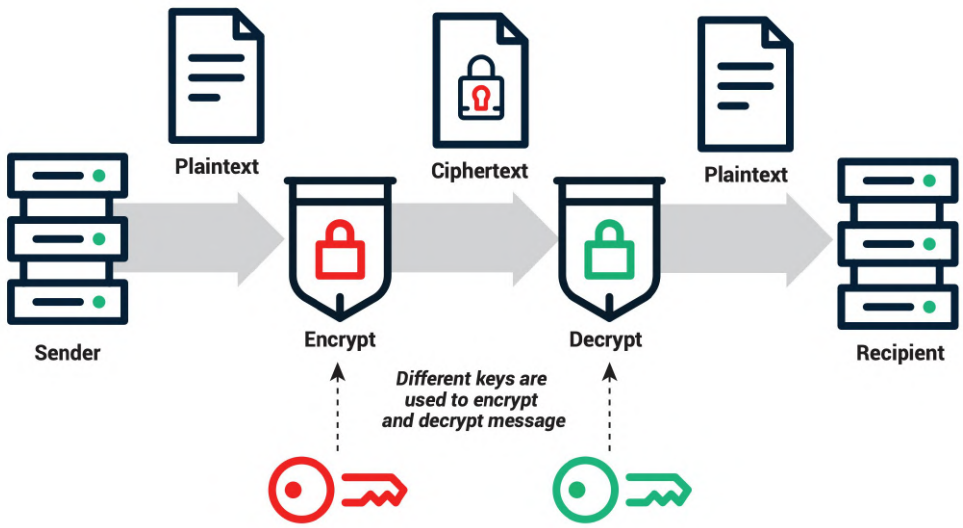
Il punto della spiegazione è che Internet è formato dall'insieme di computer collegati tra loro e da tutte le infrastrutture che permettono il suo funzionamento, in estrema sintesi da altri computer addetti all'elaborazione di dati; dunque navigare su internet significa scambiare dati che viaggiano da computer a computer: internet non esiste nell' "etere", ma è frutto dello scambio di informazioni via computer e server. Lo scambio di informazioni su internet può consistere in una visita ad un sito web, un messaggio di mail virtuale o un download di un file o di altro ancora; essenzialmente quello che avviene è un trasferimento di informazioni da un altro computer e come visto sopra (pag. 2, applicazioni, file) le informazioni possono essere immagini, documenti virtuali ma anche istruzioni da impartire al calcolatore. Ne conseguono due considerazioni fondamentali: 1) ogni connessione alla rete è una connessione a due vie, 2) le informazioni ricevute dall'esterno possono contenere istruzioni "maligne" per il computer. Quel che è peggio è che le istruzioni perniciose possono essere scaricate senza che l'utente se ne renda conto e si possono fare notevoli danni senza sollevare grandi segnali di allarme (nel dettaglio più avanti). La terza considerazione da fare è che i dati in viaggio sulla rete portano con sé informazioni sensibili, oltre al contenuto (che potrebbe essere di natura confidenziale), anche indirizzo virtuale del mittente e del destinatario, orario e frequenza delle comunicazioni, si può persino individuare con buona approssimazione l'area geografica di residenza del mittente. In pratica i dati che viaggiano in rete lasciano tracce, possono essere intercettati, manomessi o addirittura usati per carpire informazioni sensibili riguardo all'utente.

La crittografia

La scienza della **crittografia** può essere considerato una sezione del campo della sicurezza informatica, soprattutto quando si parla di reti e delle loro **vulnerabilità**. La scienza crittografica si occupa di secretare i dati virtuali in modo da prevenire l'accesso di utenti non autorizzati. Si tratta dunque sia di utilizzare matematica avanzata come strumento di protezione delle informazioni sia di architettare complessi sistemi di sicurezza a tutto tondo, per questo motivo parlare di crittografia spesso implica parlare di sicurezza delle reti e dei sistemi informatici, ovvero nella cyber sicurezza (Schneier et al. 2010, 3). In nuce, crittografare un testo significa cambiare le informazioni contenute

in modo che non sia possibile risalire al significato originale per chi non possegga la **chiave di crittografia**, ovvero il metodo con cui il testo è stato cambiato. La chiave di crittografia consiste in una serie di numeri usati per secretare e de-secretare i dati, le chiavi sono create da algoritmi che cercano di assicurare la maggiore casualità e unicità possibile; si tratta di formule matematiche complesse (Johansen 2020). Il testo codificato secondo pratiche crittografiche viene chiamato "testo cifrato" (cyphertext in inglese) (Sectigo 2020).

Fig.1 (Sectigo 2020)



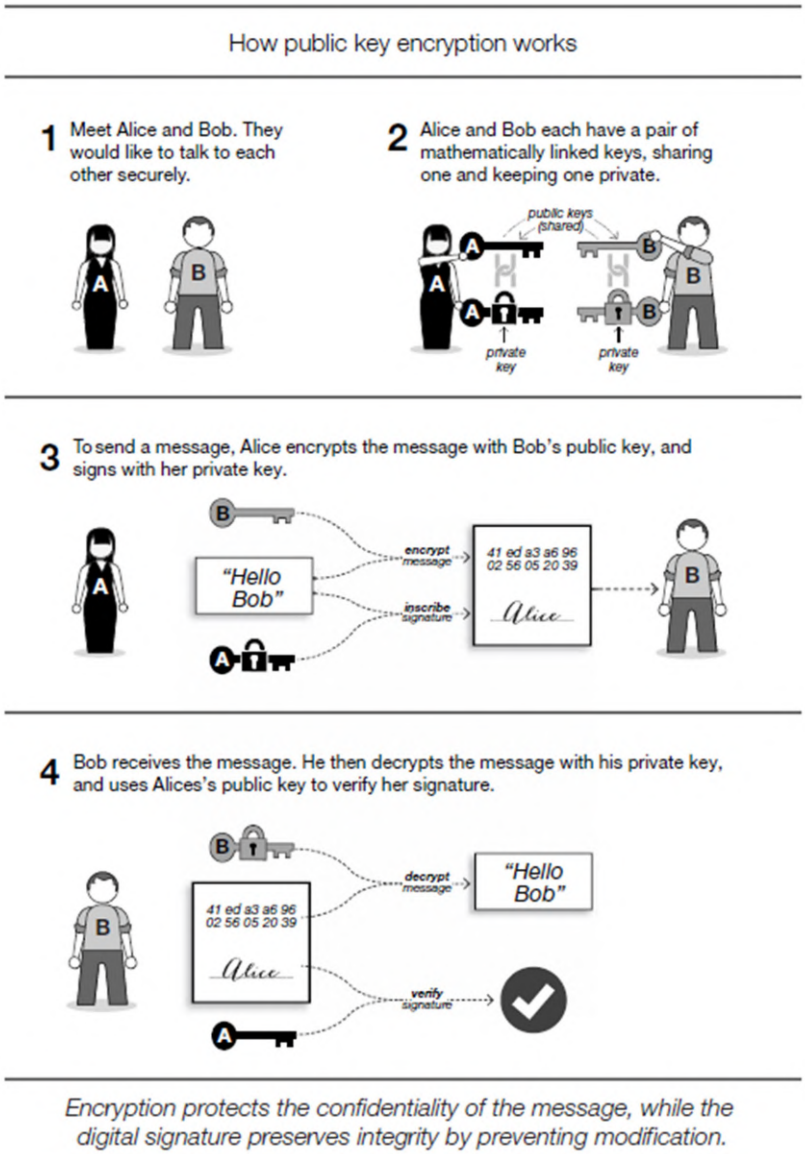
Nonostante esistano numerosi principi e tecniche di crittografia, ai fini del presente elaborato è sufficiente delineare la differenza tra crittografia simmetrica e asimmetrica, in particolare quest'ultima risulta particolarmente importante in quanto sostegno fondamentale all'impalcatura dell'odierna comunicazione su internet.

Crittografia simmetrica e crittografia asimmetrica

Quando mittente e destinatario condividono la stessa chiave per decriptare i messaggi, si parla di **crittografia simmetrica**. Il mittente scrive un messaggio, lo modifica secondo la logica di una chiave crittografica e lo manda al ricevente. Il ricevente, possedendo la stessa chiave può ritradurre il messaggio secondo il significato originale. Il problema nell'era di internet è evidente: come si può comunicare con un recipiente sito dall'altra parte del mondo se non lo si è mai incontrato prima d'ora? Il codice segreto che permette la decodifica della comunicazione non può essere inviato via web (perché potrebbe essere intercettato e diventare dunque inutile, anzi dannoso), né è immaginabile di recapitarlo a mano. Con l'avvento dei servizi bancari via web, dell'e-commerce, dei

servizi online al cittadino, il problema di poter comunicare in maniera sicura con gli sconosciuti in rete è diventato particolarmente rilevante. La soluzione? Un sistema di chiavi pubbliche e private, enti certificanti e certificati d'identità. La **crittografia asimmetrica** consiste nell'utilizzare una chiave pubblica ed una privata per assicurare la protezione, l'integrità e la provenienza del messaggio (Singer and Friedman 2014, 47-49). Il funzionamento del sistema di crittografia simmetrica può essere spiegato con un semplice esempio: Alice e Bob sono due utenti che non si conoscono ma vogliono comunicare online tra di loro; Alice possiede due chiavi, una chiave pubblica A ed una chiave privata A, così come Bob possiede una chiave pubblica B ed una privata B. Alice desidera scrivere a Bob, dunque prende la chiave pubblica B (che è appunto visibile a chiunque), codifica il proprio messaggio secondo tale chiave e lo manda a Bob. Assieme con il messaggio codificato, Alice allega una "firma" digitale creata con la propria chiave privata A. Bob cosa vedrà ricevuto il messaggio? Innanzitutto Bob sarà l'unico a poter decodificare il testo siccome possiede la chiave privata B, secondariamente prenderà la firma di Alice e la confronterà con la chiave pubblica A: siccome le due tipologie di chiavi (pubblica e privata) sono matematicamente imparentate tra loro, potrà confermare che il messaggio proviene effettivamente da Alice (figura 1, tratta da Singer and Friedman 2014). Infatti utilizzando la chiave pubblica B è possibile cifrare il testo, ma non è possibile decodificarlo; ciò succede perché le chiavi pubbliche sono costruite tramite formule matematiche apposite che non rendono possibile decifrare il messaggio dopo che è stato secretato con esse.

Fig.2 (Singer and Friedman 2014, pag. 48)



Encryption protects the confidentiality of the message, while the digital signature preserves integrity by preventing modification.

Con tale sistema il messaggio risulta illeggibile per chiunque altro al di fuori di Bob, ma non solo, dovesse una terza parte riuscire ad intercettare il messaggio, anche riuscisse in qualche modo a decodificarlo, non potrebbe falsificare la firma di Alice, perché non possiederebbe la chiave privata A, dunque sarebbe evidente l'intromissione; è per questo motivo pure l'integrità del messaggio originale è assicurata. Il funzionamento del sistema di crittografia è invisibile all'utente in realtà, viene usato soprattutto per le connessioni sicure via web ed è gestito automaticamente dal software del computer. Le chiavi pubbliche sono conservate in registri virtuali (su server) e mentre le chiavi private sono salvate sul computer dell'utente. Ma chi si occupa di fornire ed assegnare le chiavi pubbliche e private?

Le certificate authorities

Le **certificate authorities** (CA) sono enti pubblici e privati strettamente controllati e supervisionati, che si occupano di assegnare le chiavi di crittografia pubbliche e private, ma anche di una fondamentale operazione di verifica dell'identità online delle altre organizzazioni; in rete è facile impersonare qualcun altro, ed è particolarmente pericoloso se sconosciuti malintenzionati cercano di spacciarsi per una banca, un portale governativo o un sito di un'azienda. Le CA verificano che la presenza online di un'organizzazione sia effettivamente gestita dai proprietari legittimi, assegnando certificati digitali (certificati SSL/TLS) che vanno rinnovati periodicamente e sono difficilmente falsificabili. (Crane 2020) I certificati digitali sono delle strutture di dati elettronici che possono assicurare la provenienza di un determinato sito web, programma informatico o firma virtuale ad una specifica organizzazione, aumentando così la sicurezza dell'ecosistema di internet. Il sistema di crittografia asimmetrica, le CA con le relative chiavi e certificati digitali fanno parte di quella che viene chiamata **Infrastruttura a Chiave Pubblica (ICP)**, ovvero l'insieme di politiche, procedure e tecnologie che permettono tutto il sistema di crittografia pubblico e di verifica delle identità online sopra descritto (Perlman 1999).

Esiste un ulteriore implementazione crittografica da menzionare, ovvero la crittografia end-to-end. Quando più sopra si è spiegato l'esempio di Alice e Bob, si è voluto tralasciare un'imprecisione della spiegazione: i dati codificati non sono consultabili solo dai due partecipanti, in realtà è comune che quando i dati passano sui server dell'azienda fornitrice del servizio di comunicazione, essi siano decodificabili e "in chiaro" (non crittografati). Questo significa che ad un ascoltatore esterno all'azienda e diverso da Alice e Bob, i dati apparirebbero comunque incomprensibili, ma i gestori del servizio hanno comunque accesso ai contenuti delle conversazioni. Per evitare problemi di privacy e per quietare l'opinione pubblica, la maggior parte dei servizi di telecomunicazione ora incorporano la funzione di **crittografia end-to-end** (Coldewey 2013): i dati vengono codificati attraverso chiavi generate al momento sui due (o più) dispositivi in conversazione, così facendo anche viaggiando sui server dei proprietari del servizio di comunicazione, essi non possono essere letti da terze parti (Vienazindyte 2020).

Crittografia in transito, a riposo, in uso e i sistemi di autenticazione

La crittografia può dunque essere usata per creare canali sicuri attraverso far passare le informazioni, in gergo ci si riferisce alla crittografia "in transito". I dati possono essere rubati anche quando sono

conservati sull'hard disk di un pc e/o utilizzati dagli utenti mentre lavorano: per questo si fa distinzione tra crittografia in transito e "a riposo" o "in uso" (Privacy365EU 2019). Spesso infatti si è necessario proteggere le informazioni contenute su un computer, ancora prima che inizino a spostarsi in rete. Spesso assieme con la crittografia di tutti i file sensibili e si istituisce un sistema di accesso limitato alle informazioni: solo chi viene riconosciuto dal sistema può accedere ai dati in maniera leggibile; chiunque altro invece si troverà davanti un incomprensibile testo cifrato. I sistemi a metodi di autenticazione prevedono l'utilizzo di un nome utente e una **password** da parte di chi vuole accedere alle informazioni protette da tale sistema. Il nome utente e password si dicono anche **credenziali**, non sono altro che una stringa di lettere, simboli e numeri che il sistema verifica siano presenti sull'apposito database creato in precedenza, ovvero viene verificato che l'operatore in questione sia effettivamente autorizzato ad accedere ai dati. Effettuare il **login** nel sistema significa inserire le credenziali per avere l'accesso. Siccome nome utente e password possono essere perse, dimenticate, divulgate senza autorizzazione, rubate o indovinate, si sono sviluppati diversi metodi di autenticazione come per esempio il metodo One Time Password (OTP), dove, solitamente attraverso un dispositivo elettronico, si generano password ad uso singolo ogni volta che serve effettuare l'accesso. Un altro sistema consiste nell'autenticazione a più fattori (Multifactor Authentication, MFA), dove viene richiesto un ulteriore conferma dell'identità dell'utente anche dopo aver inserito le credenziali corrette (Marioni 2019).

La crittografia è infallibile?

A giudicare dal fatto che l'intero sistema di economia digitale, si parli di servizi bancari o in generale di pagamenti online, si basi sulla fiducia nelle transazioni sicure via web, ovvero sulla sicurezza delle comunicazioni crittografate tra utenti e la validità dei certificati virtuali delle CA, sembrerebbe che la crittografia sia un metodo sicuro al 100%. In linea di massima è così, le strategie di crittografia offrono un alto grado di sicurezza, ci sono però alcuni caveat da fare. Quali sono le possibili vulnerabilità della sicurezza tramite crittografia?

Gli attacchi di forza bruta

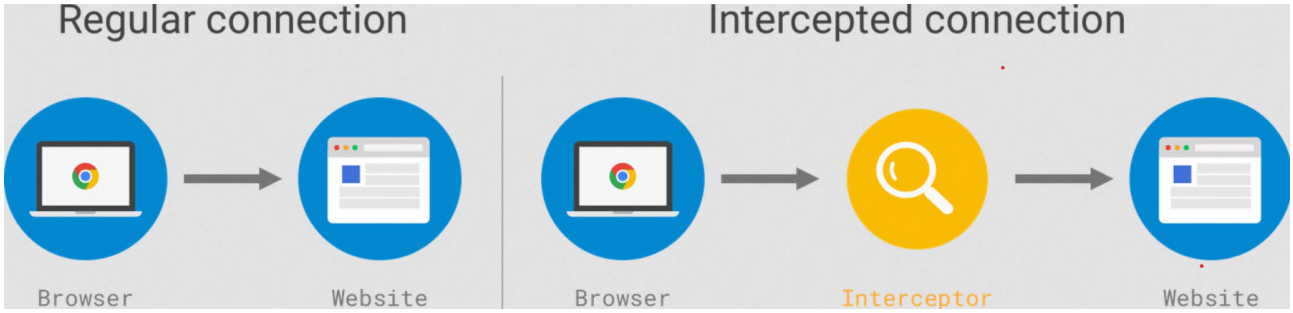
Le chiavi di crittografia sono generate da algoritmi, significa che con la giusta matematica è possibile cercare di trovare le regole che hanno governato la codifica del testo cifrate. Inoltre molti sistemi di crittografia sono associati ad uno di credenziali (come spiegato precedentemente). Chi volesse "rompere" la codifica di un testo potrebbe cercare di calcolare la formula matematica originaria che

ha fornito la chiave di crittografia, oppure per poter accedere ad un sistema di autenticazione potrebbe tentare di indovinare nome utente o password. Perché chiamarli "**attacchi di forza bruta**" dunque? Perché la tecnica di decodifica o di accesso senza password prevede un numero altissimo di calcoli o di tentativi casuali. Per esempio, avendo una password di 10 caratteri ci sono 171,3 quintilioni ($1{,}71 \times 10^{20}$) di possibilità da indovinare. Un computer in grado di processare 10,3 miliardi di combinazioni al secondo, impiegherebbe circa 526 anni per trovarla (Khali 2014). Un altro esempio è l'"**attacco dizionario**", che consiste nell'utilizzare dizionari integrali da cui attingere le parole per i tentativi in sequenza (Craig 2016). Un altro esempio: le chiavi crittografiche utilizzate per codificare le informazioni si dicono misurate in bit, per semplificare molto una chiave a 256 bit (tipo di chiave diffusa), richiederebbe 2^{256} tentativi per essere individuata, detta in un'altra maniera una chiave a 256 bit ha 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.40.564.039.457.584.007.913.129.639.936 possibili combinazioni; per quanto un computer possa eseguire calcoli rapidamente, il tempo e l'energia richiesta per elaborare un numero così alto di operazioni sarebbe eccessivo anche per i calcolatori più potenti (Nohe 2019). Gli attacchi di forza bruta hanno dei limiti evidenti, per esempio si possono costruire sistemi in cui non è possibile effettuare più di una manciata di tentativi e si possono costruire algoritmi particolarmente complessi da crittografare (Schneier et al. 2010, 306), ma rimangono degli strumenti ancora largamente utilizzati oggi, soprattutto perché non tutti gli utenti utilizzano password sicure (lunghe e complesse).

Gli attacchi Man-in-the-middle

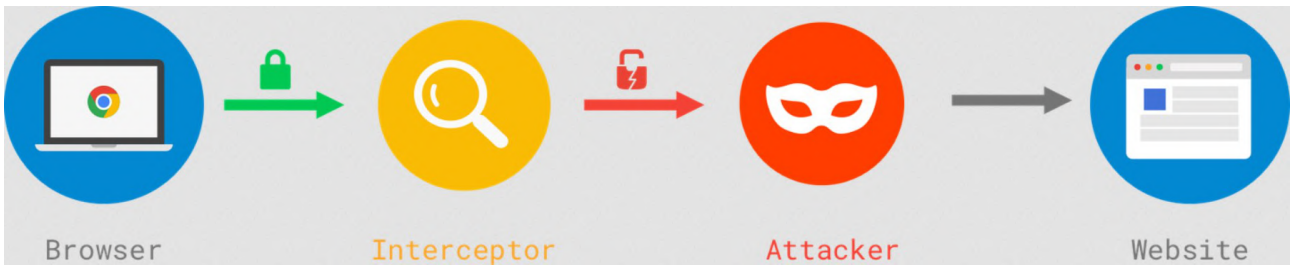
Il sistema di crittografia asimmetrica assieme con i certificati digitali SSL/TLS permettono di aprire una connessione sicura tra utente e sito web, tramite cui scambiare i dati. Si potrebbe definire come l'apertura di un "tubo" tramite cui spedire i messaggi; la connessione sicura è come un tubo che impedisce a terze parti di vedere all'interno. Uno dei metodi usati per aggirare il problema è inserirsi tra mittente e destinatario, re-direzionando la connessione sicura verso la terza persona, che agisce da proxy, cioè da tramite per i messaggi. In questo modo il proxy viene incluso nella connessione sicura e riceve i messaggi che può leggere, modificare o bloccare, da qui il nome **man-in-the-middle** (Bursztein 2017).

Fig.3 (Bursztein 2017)



Intrufolarsi nelle conversazioni altrui non è semplicissimo, per esempio bisogna compromettere il computer dei partecipanti in precedenza oppure i server attraverso cui fluiscono le informazioni, ma è senz'altro fattibile. L'intercettore però non è sempre malintenzionato. Molti programmi per la sicurezza filtrano la comunicazione con il fine di rilevare minacce nel traffico dati, gli stessi Internet Service Provider (vedi sopra) effettuano controlli del genere. Anche quando l'intenzione è quella di tutelare gli utenti internet, la verità è che la cattiva architettura dei processi di gestione dei dati può portare a delle vulnerabilità inaspettate; per esempio molte delle intercettazioni dei dati avvengono perché i processi di crittografia sono mal pensati: l'intercettore (a fin di bene) filtra i dati e nel rispedirli al mittente non ricodifica le informazioni in maniera protetta; i dati vengono rispediti in chiaro, a libera disposizione di chi voglia rubare o manomettere i contenuti. La causa di solito risiede in una cattiva implementazione dei sistemi di crittografia (vengono progettati e "scritti" male) (Bursztein 2017).

Fig.4 (Bursztein 2017)



Furto delle chiavi di firma digitale

Nonostante le CA siano aziende strettamente controllate, i cui standard di settore richiedono un altissimo livello di professionalità e sicurezza, le chiavi digitali utilizzate per creare i certificati possono essere rubate. Chi riesce ad entrare in possesso delle chiavi di una delle aziende certificatrici,

può impersonare portali web e organizzazioni, può sorvegliare indisturbato e senza lasciare tracce il traffico da e per computer, siti, infrastrutture di dati cloud (in remoto) e dispositivi mobili (Brown 2016). Non solo, si possono anche firmare programmi dannosi come fossero provenienti da una fonte affidabile, facendo sì che passi i sistemi di sicurezza di un computer senza destare nessun allarme (Brown 2016) (Singer and Friedman 2014, 49). Come verrà spiegato più avanti con il caso Stuxnet, il furto delle chiavi digitali da una CA può avere implicazioni particolarmente gravi, fortunatamente ottenere le chiavi digitali dei certificati è estremamente difficile.

I metadati

Visto che una delle falle del sistema di comunicazione sicura sul web potrebbe essere causato proprio da chi dovrebbe gestire la connessione in modo sicuro o da attori che riescono ad appropriarsi dell'autorizzazione a leggere i dati, appare ancora più evidente come la strategia di crittografare i dati end-to-end sia una buona soluzione alle falle già menzionate: una crittografia basata su solidi algoritmi matematici, difficili da rompere ed un canale sicuro che esclude qualsiasi intermediario nella comunicazione tra due utenti. La crittografia end-to-end rappresenta effettivamente un esempio di buona pratica di sicurezza della comunicazione, ma anche in questo caso non si può parlare di sicurezza e protezione assoluta. Le informazioni che viaggiano su internet o i file che vengono conservati su un computer, contengono dati aggiuntivi che non riguardano necessariamente i contenuti, sono in pratica dati riguardo ai dati: i **metadati**. Per esempio, secondo la normativa italiana i file conservati in un database devono includere metadati descrittivi, metadati amministrativi/gestionali e metadati strutturali. "I primi sono funzionali all'identificazione e al recupero dei documenti stessi (…); i secondi sono utili alla loro gestione all'interno dell'archivio e comprendono quindi anche informazioni di natura tecnica (ad. es. quelle sui formati, le procedure di creazione, l'ambiente tecnologico); la terza categoria comprende le informazioni necessarie a descrivere l'articolazione interna e le relazioni fra le parti che compongono gli oggetti digitali" (Archivi Biblioteche 2019). La normativa statunitense invece individua altre tre categorie: i metadati delle app, che vengono aggiunti al file attraverso il programma usato per creare il documento. Per esempio si tratta di dati che riguardo agli interventi dell'utente sul file, tra cui il registro delle modifiche e i commenti. "I metadati di sistema includono il nome dell'autore, il nome del file e le dimensioni, le modifiche e altri dati di questo genere. I metadati incorporati (o embedded) sono in genere formule di Excel, link e file associati. I metadati di tipo EXIF, che sono tipici dei file immagine, appartengono a questa categoria di metadati" (Kuksov 2017). Anche quando i file sono protetti da crittografia, i metadati possono rimanere fuori dalla protezione in codice e rivelare dettagli cruciali

riguardo al contenuto nascosto (Kuksov 2017); tornando alla questione della crittografia end-to-end, sebbene essa protegga il contenuto della conversazione, non può nascondere informazioni come luogo di provenienza, tempistiche e volume delle comunicazioni destinatario dei messaggi; tutti questi sono metadati allegati alle comunicazioni secretate (Coldewey 2013).

In conclusione, la crittografia permette la creazione di sistemi di comunicazione sicura e di certificazione virtuale, che a loro volta costituiscono le colonne portanti di un sistema di fiducia condiviso: internet si sorregge sulla ragionevole certezza di poter parlare con la propria banca senza che i dati della carta di credito siano rubati da qualcuno mentre sono in transito, o che quando si effettua una transazione monetaria essa arrivi effettivamente ad un esercizio commerciale lecito e non ad un truffatore che sta imitando ad arte il sito web di un'altra azienda. La crittografia, pur non essendo infallibile, è un metodo piuttosto sicuro per proteggere i dati online e offline; gli algoritmi di cifratura sono in grado di creare protezioni difficili da "rompere", mentre "falsificare" i certificati virtuali è quasi impossibile. Ciononostante ci sono alcuni modi per aggirare la protezione dei dati (ex. man-in-the-middle). Difatti, siccome rompere la protezione crittografica dei dati può essere molto difficile e dispendioso, spesso si preferisce carpire i dati quando ancora non sono in movimento e dunque sono conservati sul computer del bersaglio in chiaro.

Le minacce

Il problema della sicurezza sul web ruota attorno alla protezione dei dati, siccome sono le informazioni sensibili a rappresentare del valore sia per chi le vuole proteggere sia per chi le vuole rubare. Il modo più semplice per mettere le mani sulle informazioni, dunque sui dati, è quello di infestare il dispositivo che li contiene, piuttosto che cercare di carpirli mentre sono in movimento (come spiegato prima). I **malware**, o "malicious software" (programmi maligni), sono i mezzi più utilizzati dagli operatori esterni che intendono introdursi senza autorizzazione nei sistemi altrui. I malware sono programmi disegnati apposta per compiere azioni dannose per i sistemi in cui riescono ad introdursi; solitamente chi li produce e utilizza mira ad ottenere un guadagno di qualche tipo, ma non è sempre il caso, alle volte il fine è semplicemente quello di creare scompiglio sul web. Nel linguaggio comune, chi sfrutta i malware per infiltrarsi su un computer viene definito "**hacker**" e le azioni a danno degli altri utenti web a fine di lucro o guadagno personale in senso lato vengono indicate con il termine "**cyber crimini**", proprio per individuare un tipo particolare di atti illegali portati avanti attraverso le tecnologie digitali.

I malware più diffusi

Virus

Normalmente i malware vengono definiti “virus informatici”, come termine cappello dell’intera categoria, ma i virus sono in realtà solo una parte dei programmi nocivi esistenti; essi hanno la caratteristica di non potersi riprodurre e diffondere da soli, vanno scaricati e eseguiti manualmente dall’utente. Ciò è possibile perché spesso sono camuffati da altri file come messaggi di testo, immagini, video o altri programmi.

Worm

I **worm** sono malware in grado di diffondersi autonomamente senza l’intervento dell’utente, non hanno bisogno di essere eseguiti dall’operatore (a differenza dei virus e trojan) (Tiwari 2021). I worm spesso sono nascosti dentro altri file, messaggi di posta o di chat istantanea, possono quindi essere scaricati automaticamente senza che l’utente se ne accorga. Una volta scaricati essi si attivano, spesso con le istruzioni di replicarsi ed auto-spedirsi a più computer possibile. I worm possono raggiungere un numero molto elevato di computer nel giro di poco tempo, sono difficili da individuare e come detto sopra, spesso si scaricano automaticamente ed involontariamente, motivo per cui possono rappresentare una vera e propria piaga del web. Per esempio, nel 2003 un worm chiamato “SQL Slammer” infettò 75.000 vittime in soli 10 minuti, mentre nel 2017 “WannaCry” riuscì a raggiungere 230.000 computer in un solo giorno (Belcic 2020). Gli obiettivi dei worm possono essere differenti, ma uno degli impieghi più comuni è quello di creare una rete di computer infetti che possono essere controllati da remoto da un utente, anche definito una rete di **botnet** (crasi di robot e network). Chi tiene le redini del sistema di terminali infetti può sfruttare la loro potenza di calcolo combinata per i propri scopi, come per esempio un attacco di forza bruta, oppure può organizzare quello che viene definito **attacco DDoS**, Distributed Denial of Service. L’attacco di “Denial of Service” o negazione di servizio viene effettuato sovraccaricando i canali di comunicazione verso un server per bloccare il traffico di dati, in questo modo impedendo di fatto l’accesso ad uno o più siti web (Singer and Friedman 2014, 208). Un singolo computer può essere facilmente bloccato se fonte di eccessivo traffico comunicativo, ma quando viene utilizzata una botnet di centinaia o migliaia di computer è difficile evitare la paralisi del server. L’attacco DDoS è un esempio di sabotaggio o ritorsione tramite mezzi digitali. Una botnet viene anche utilizzata per nascondere identità e

provenienza degli autori di attacchi informatici; se un hacker ha avuto accesso ad un gruppo di computer dall'altra parte del mondo, può tranquillamente sfruttarli per lanciare offensive difficilmente riconducibili a lui. Nel 2008 il worm informatico "Conficker" infettò 7 milioni di terminali formando una delle botnet più grandi del mondo; impressionati dalla diffusione spropositata del malware, diverse università, ISP, aziende di sicurezza e software si misero ad investigare l'origine dell'attacco. La dimensione della rete di computer infetti rese quasi impossibile capire l'esatta origine del programma, alcuni ipotizzarono provenisse da Russia e Cina all'inizio, finché non si scoprì un dettaglio nel codice di programmazione di una delle prime versioni: l'applicazione, subito dopo aver infettato un computer, aveva l'ordine di controllare la tipologia di tastiera impostata sul PC, in caso questa fosse in ucraino, avrebbe dovuto disattivarsi (Singer and Friedman 2014, 72). Fu solo grazie a questo dettaglio che poi nel 2011 furono individuati e fermati tre cittadini ucraini ed uno svedese, anche se non esistono documenti che ne comprovino la prosecuzione ufficiale da parte del governo locale (Conficker, Wikipedia). Dunque i worm, grazie alla loro diffusione virulenta, sono molto usati per creare reti di terminali infetti e dunque associati agli attacchi DDoS, ma essi possono avere diverse funzioni e a seconda del loro scopo vengono chiamati in maniera differente; per esempio un worm dedicato a monitorare le attività online di un utente può essere definito "**spyware**" (spy software), così come moltissimi **ransomware** utilizzati per ricatti economici (vedere sotto) sono essenzialmente worm, siccome si diffondono a macchia d'olio come da caratteristica di tale malware. Con il termine worm si va a definire una macrocategoria di programmi che si auto-propagano in rete, ma poi esistono diversi tipi di worm che si differenziano per la funzione a loro associata. Occorre anche notare che non sempre le etichette aderiscono in maniera stretta al tipo di malware a cui sono associate, per esempio Conficker pur essendo un worm in realtà era un insieme di programmi nocivi che sfruttavano vulnerabilità differente. Come spiegato in precedenza (vedere pag. 1) i programmi non sono altro che informazioni interpretate come ordini da parte di un terminale, ma se le istruzioni sono scritte nella maniera giusta (o i sistemi interni scritti nella maniera sbagliata) il computer non è in grado di discriminare tra ordini "buoni" ed ordini "cattivi". Alla stessa maniera i malware si differenziano più per il fine per cui vengono utilizzati e per alcune caratteristiche particolari (come metodo di propagazione) piuttosto che per natura intrinseca: rimangono sempre programmi virtuali.

Trojan

I **trojan** prendono il nome dal cavallo di Troia dell'Odissea e non a caso: il programma spesso si camuffa da altro, come un'altra applicazione legittima per esempio e una volta scaricato e avviato

dall'utente esso fa partire le istruzioni nocive per il dispositivo; spesso viene utilizzato per aprire una **backdoor**, ovvero una porta segreta di accesso, per introdurre altri utenti o malware nel sistema. I trojan come i virus hanno bisogno di essere scaricati a mano dall'utente, motivo per cui vengono travestiti da programmi legittimi come per esempio programmi antivirus (vedere sotto), ciò detto esistono anche worm in grado di aprire backdoor di accesso al sistema (Belcic 2020).

Rootkit

I rootkit sono malware pensati per prendere il controllo di un computer da remoto, di solito aprendo una porta backdoor per introdurre programmi appositi per lo scopo. Il nome deriva dal come viene chiamato l'amministratore di sistema nei sistemi operativi Linux, l'utente principale è detto "root". I rootkit si insediano ad un livello del sistema operativo profondo che rende molto difficile individuarli. I rootkit possono contenere moduli di codice in grado di registrare ciò che viene digitato sulla tastiera del pc, chiamati **keylogger**, possono anche salvare ciò che avviene a schermo e disabilitare i sistemi di sorveglianza e sicurezza di un computer. La funzione principale rimane comunque quella di consentire il controllo da remoto del dispositivo da parte di un operatore non autorizzato. L'accesso di questo genere può essere totale e dunque estremamente pericoloso, siccome l'operatore avrebbe il potere di leggere e modificare ogni tipo di file sul computer infetto. Tale caratteristica assieme con la difficoltà di individuazione ed eradicazione rendono i malware rootkit estremamente pericolosi (Malenkovich 2013).

Bombe Logiche

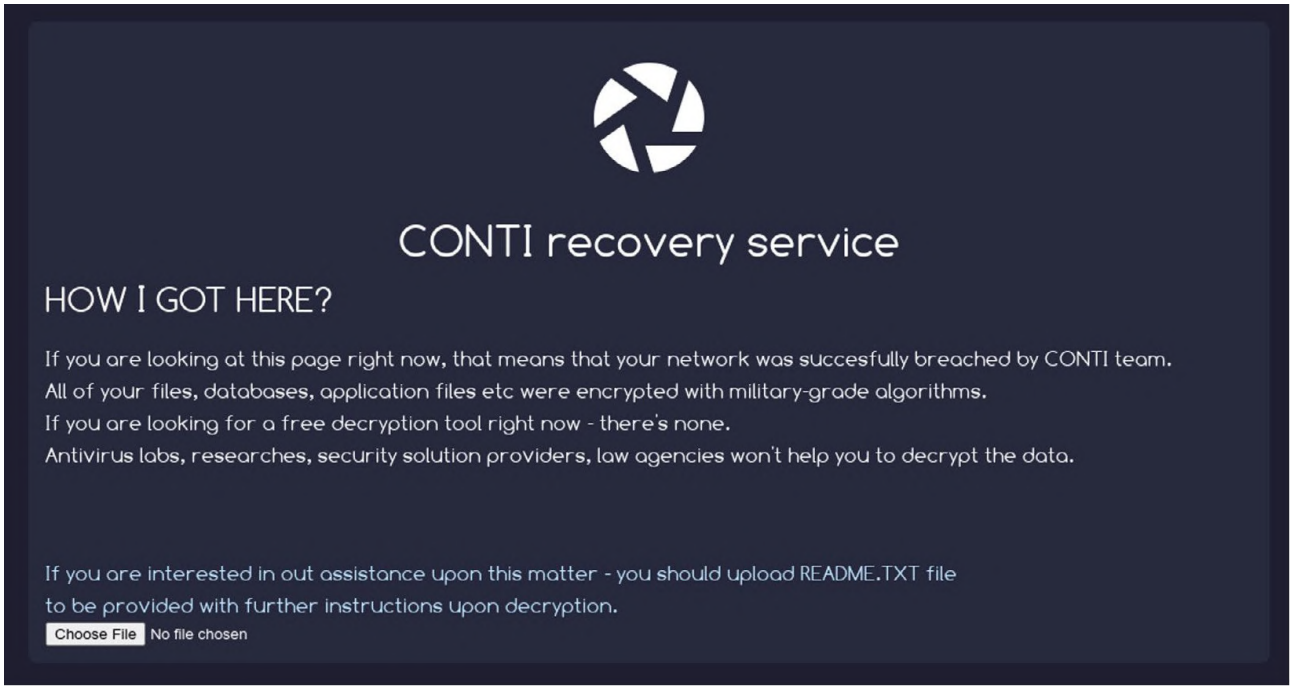
Una **bomba logica** è un codice malevolo inserito in altri programmi di nascosto. Il compito di una bomba logica è quello di attivarsi quando si verifica una data condizione; le condizioni di attivazione possono variare, può essere necessario che passi un numero preciso di giorni, può servire che il computer si colleghi alla rete o si metta in comunicazione con altri dispositivi, insomma i parametri possono essere tanti. Una volta attivata l'istruzione, l'effetto può anch'esso variare: alle volte vengono usate per cancellare i dati su un sistema, altre volte per auto-terminare il programma malevolo o attivare altri malware (Razzini 2019).

Ransomware

Ad oggi uno dei metodi più diffusi per lucrare sfruttando le vulnerabilità di sicurezza dei sistemi informatici privati ma molto più spesso, aziendali. La crittografia viene utilizzata come mezzo di offesa invece che di protezione, i ransomware escludono gli utenti dall'accesso ai proprio dati; una

volta introdotto il malware sul computer, esso cifra tutti i file nel sistema e lascia un avviso su come recuperare i file: pagare un riscatto o perdere per sempre le informazioni criptate (da qui la crasi "ransom software").

Fig.5 (Ransomware Task Force 2021, 11)



Tale tipologia di attacco risulta particolarmente pericolosa per le aziende, siccome spesso e volentieri i contenuti dei database aziendali contengono importantissime informazioni riguardo i clienti, documenti fondamentali per la gestione dell'organizzazione e così via. Una buona parte delle aziende preferisce pagare il riscatto invece di bloccare l'intera attività e chiamare degli esperti esterni per provare a recuperare i dati. Il processo può richiedere addirittura mesi, e come spiegato in precedenza, non è sempre possibile de-crittografare un testo cifrato bene. L'esortazione a pagare inoltre ha molto più effetto quando la vittima non vuole che i propri dati vengano resi pubblici, ovvero voglia evitare il "**leak"** (fuga di notizie) di dati sensibili come proprietà intellettuale (IP) cruciale per la competitività nel mercato, segreti imbarazzanti o per evitare l'uscita in anticipo di contenuti multimediali di intrattenimento (si pensi alla celebre serie "Il Trono di Spade" distribuita da HBO che subì un attacco del genere e vide le puntate della propria serie rilasciate in anticipo, proprio per non aver pagato i criminali; Glaser 2017). Dunque un'altra componente di rischio di un attacco ransomware risiede proprio nel fatto che non sempre i file vengono cifrati, alle volte si tratta di esfiltrazione dei dati verso operatori esterni (Ransomware Task Force 2021), che poi possono minacciare di pubblicarli al grande pubblico o alla comunità hacker, inserendo i dati su server

chiamati “data lake” (lago di dati) (Cimpanu 2021). Nei data lake si riversano grandi quantità di informazioni che poi verranno riordinate ed analizzate. I data lake vengono anche utilizzati per scopi legittimi come analisi di mercato, se la raccolta dati da parte di aziende private può essere considerata legittima ovviamente, ma è risaputo che vere e proprie comunità hacker raccolgano i dati rubati per metterli a disposizione di altri malintenzionati, per esempio per sfruttare le stesse vulnerabilità dei sistemi di sicurezza o per provare a trovare collegamenti fruttuosi: con abbastanza pezzi di informazioni private di un utente è molto più semplice eseguire truffe online (vedere più avanti “Phishing”).

Come si entra in contatto con i malware?

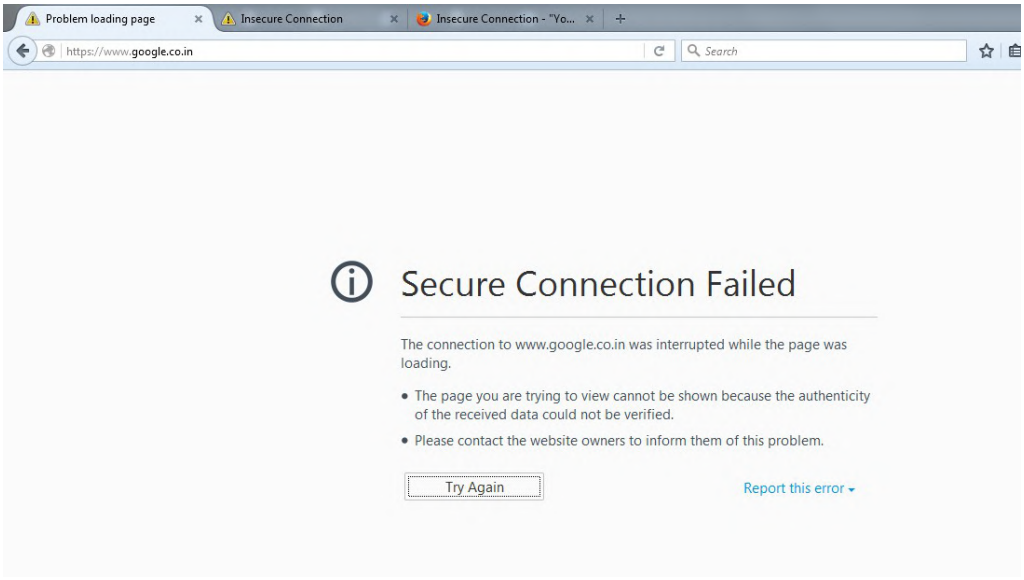
I malware possiedono diversi sistemi di propagazione , ma sorprendentemente nella maggior parte dei casi è necessaria una certa collaborazione da parte dell’utente stesso per introdurli in un sistema. Il primo ammonimento da fare infatti è quello di evitare siti web poco affidabili e download provenienti da fonti sconosciute. Solitamente è buona prassi non fidarsi di tutti quei siti che offrono download gratis di prodotti a pagamento, così come siti di cui non si conosce l’origine e l’entità che li gestisce. Davanti ad un sito internet di dubbia natura, bisogna dubitare di tutto ciò che si scarica dall’esterno, soprattutto se il file è un’applicazione eseguibile (file con “.exe” come formato); con buona probabilità si tratta di trojan o virus. Purtroppo non sempre i siti web pericolosi sono quelli chiaramente truffaldini.

I dati che si ricevono navigando sul web provengono da server esterni (cfr. infra pag.3), dunque la prima cosa da tenere a mente è che i server possono essere infettati da operatori malevoli per diffondere malware. Un tipico attacco di propagazione malware è l’attacco “**drive-by**” o “drive-by download”: l’utente ha la sola colpa di finire su un server precedentemente infettato, quando viene inviata la richiesta di connessione o si scaricano dei file, i programmi malevoli sfruttano le vulnerabilità del browser per depositarsi sul computer. Anche se la pagina web visitata risulta perfettamente legittima e certificata, alcune falle nella sicurezza potrebbero aver permesso in precedenza l’intromissione da parte di altre persone. Alle volte vengono sfruttati siti web visitati da specifici gruppi di individui per colpire obiettivi ben definiti: in un caso un gruppo di hacker ha cercato di raggiungere i computer dei dipendenti di una compagnia americana di difesa, compromettendo il sito web di una celebre rivista aerospaziale che molti degli utenti leggevano, riuscendo ad infettare centinaia di computer in un giorno solamente (Singer and Friedman 2014, 44).

Un tale tipo di attacco drive-by prende il nome di attacco "**watering hole**", dall'idea del cacciare le prede quando si riuniscono in uno stesso luogo come erbivori ad una fonte d'acqua.

Dunque come si fa a sapere se è sicuro visitare un sito internet? La risposta sono i certificati virtuali (cfr. infra pag.7). I certificati esistono apposta per assicurare la sicurezza di una connessione web e di ciò che si scarica dalla rete. Quando un utente approda su sito web non sicuro viene solitamente avvisato dal proprio browser:

Fig.6



Allo stesso modo, quando si riceve un file dall'esterno, soprattutto quando si tratta di programmi eseguibili, si può sempre verificare la fonte controllando le proprietà del file, anche in questo caso i certificati assicurano la provenienza del "pacchetto" da aziende legittime. Sfortunatamente anche se non appaiono avvisi di sicurezza, non significa che il sito web sia per forza sicuro. È sempre necessaria un'abbondante dose di cautela e buonsenso mentre si naviga; quando un sito appare poco chiaro, sarebbe meglio non scaricare nulla ed evitare addirittura di visitarlo, mentre bisogna usare estrema cautela quando si ricevono file di ogni tipo dall'esterno.

Un altro modo in cui i malware possono diffondersi è tramite posta elettronica e messaggistica istantanea; è molto comune che i worm, una volta insediatisi dentro un terminale, inviino automaticamente messaggi a tutti i contatti che riescono a trovare, di solito amici, colleghi e parenti dell'utente. I messaggi possono contenere un allegato o un link che se aperti scaricano il programma malevolo; alle volte basta anche solo aprire il messaggio (Belcic 2020), motivo per cui gli esperti di cyber sicurezza consigliano di stare sempre molto attenti ai messaggi strani che potrebbero arrivare

dai propri contatti. Anche senza possedere un indirizzo di posta elettronica o un profilo sui social network (i quali a loro volta possiedono sistemi di messaggistica integrata), essere connessi ad internet significa avere una porta di comunicazione a due vie; esistono per esempio tipologie di malware che prima generano indirizzi IP casuali e poi si spediscono ai malcapitati utenti: è il caso del worm "SQL Slammer" citato in precedenza. Essere connessi ad internet significa essere potenzialmente rintracciabili. A tal proposito occorre citare un altro pericolo del web: il **doxing** (Singer and Friedman 2014, 79). L'indirizzo IP associato al proprio computer può essere usato per delimitare con buona approssimazione l'area geografica dove è sito, assieme con le informazioni che volontariamente si mettono in rete (foto, video, post sui social network) è possibile scoprire l'identità, la residenza, le abitudini e a volte gli imbarazzanti segreti di un utente. Spesso non ci si rende conto della delicatezza delle informazioni che si rilasciano online, tramite un'accurata ricerca si può arrivare a conoscere anche dettagli molto personali di qualcuno, esponendolo dunque a rischi inaspettati.

In ultimo, i malware possono essere spostati da un computer all'altro condividendo i file, anche quando non si utilizza internet. I supporti di memoria esterni (chiavette usb, hard disk portatili, CD…) possono rappresentare dei vettori di contagio se precedentemente sono stati collegati a computer infetti. È buona norma non utilizzare dispositivi di archiviazione di cui non si conosce l'origine o le abitudini d'uso. In una storia che ha dell'assurdo, nel 2008 in una delle basi americane in Medio-Oriente un soldato raccolse dal parcheggio una chiavetta USB abbandonata, per poi inserirla in un computer della base per verificarne il contenuto. L'attacco informatico che ne seguì prese il nome di "Buckshot Yankee", richiese un anno e due mesi di lavoro per rimuovere il worm dai sistemi e per controllare i danni effettuati (Singer and Friedman 2014, 64). Chiaramente in questo specifico caso il dispositivo fu scientemente collocato nel parcheggio dai servizi segreti di una nazione antagonista, cionondimeno non è mai una buona idea fidarsi di chiavette usb sconosciute o utilizzate su tanti computer diversi.

Phishing

Come già detto in precedenza, cercare di aggirare i moderni sistemi di sicurezza è molto più conveniente che affrontarli direttamente. Il **phishing** consiste nel tentare di ingannare un utente col fine di fargli fornire informazioni personali sensibili. Solitamente un attacco phishing sembra una semplice mail da parte di un collega, un familiare o un ente di fiducia (come la propria banca, ad esempio), il quale chiede al destinatario del messaggio di fornirgli dati come carta di credito o le credenziali di accesso al sistema. Così facendo l'autore del messaggio fraudolento può accedere

indisturbato al sistema, vedere tutti i dati in chiaro, farne copia e magari effettuare pure delle modifiche. Non importa quanto raffinato è il tuo sistema di crittografia se poi l'utente dà via login e password di accesso ad uno sconosciuto. L'autore del messaggio può arrivare a metterci molto impegno per simulare l'aspetto e lo stile dell'ente o individuo che sta impersonando; alle volte possono essere sfruttati dati rubati in precedenza per aggiungere credibilità alla pantomima, doxing e data lake di informazioni rubate possono contribuire grandemente al successo di una truffa. Si dice **spear-phishing** quando il bersaglio di messaggi ingannevoli è scelto in modo specifico per via della sua posizione all'interno di un'organizzazione; spesso e volentieri indica l'inizio di un piano di attacco complesso a più fasi (vedi APT sotto).

Come ci si protegge dai malware?

Quando gli avvisi e sistemi di certificazione (il sistema dell'infrastruttura di chiave pubblica di cui sopra) non bastano per proteggere gli utenti in rete, entrano in gioco gli strumenti informatici di cui ogni computer è fornito: antivirus e firewall. L'**antivirus** è un programma di sorveglianza che monitora lo stato di un dispositivo, controllando per applicazioni e file sospetti. Il programma scansiona periodicamente il pc in cerca di minacce con il fine di isolarle o possibilmente rimuoverle. I programmi antivirus eseguono procedura molto complesse per complesse come controllare le linee di codice alla ricerca di "dna" sospetti, grazie agli estesi database delle aziende di sicurezza che vengono aggiornati periodicamente e che contengono lo storico di tutti i malware mai prodotti finora. Le funzioni di protezione possono anche basarsi su complesse regole logiche per riconoscere i comportamenti sospetti e dunque poter individuare minacce che ancora non sono state scoperte ed inseriti nei registri. I sistemi di antivirus più avanzati possono simulare una "stanza virtuale" in cui inserire il file o programma sospetto, per poi cercare di innescare il comportamento malevolo potenzialmente nascosto e farlo uscire allo scoperto in ambiente protetto, dove è incapace di fare danni. I sistemi di antivirus oltre che sul computer dell'utente, possono essere presenti a livello di rete informatica e di server esterno, come per esempio i sistemi anti intrusione pensati per individuare le infiltrazioni esterne. Il **firewall** è l'altro componente fondamentale per la sicurezza informatica, siccome filtra tutti i dati in entrata ed uscita dal computer e dalla rete, è la barriera di protezione che si frappone tra l'utente e ciò che proviene dalla rete. Gli antivirus e i firewall sono prodotti da aziende specializzate nella sicurezza informatica, sono disponibili sia in modo gratuito che a pagamento e sono costantemente aggiornati per rispondere alle ultime minacce. Esistono soluzioni più radicali al problema delle intrusioni esterne, come per esempio scollegarsi tout court dalla rete

globale. “Air gap” o “Air gapping” significa isolare l’intranet (rete di computer “interna”, sistema chiuso di computer collegati tra loro, spesso dentro gli uffici della stessa azienda) di un’organizzazione dall’accesso ad internet. L’idea è quella di creare un “cuscinetto d’aria” tra il sistema informatico e il web; se non esistono porte di accesso non esistono possibilità di effrazione. Come si vedrà più avanti (vedi Stuxnet e Wikileaks), è difficile isolarsi completamente: i programmi avranno comunque bisogno di scaricare gli aggiornamenti prima o poi e gli utenti spesso e volentieri necessitano di spostare file tramite supporti di memoria esterni che possono fungere da vettore per il contagio, dunque si possono sollevare dubbi legittimi sull’effettiva possibilità di “sigillare ermeticamente” ogni porta di accesso al mondo esterno. Anche antivirus e firewall non sono infallibili; produrre un software è molto complesso, periodicamente si scoprono falle nella programmazione, errori o dimenticanze involontarie da parte dei professionisti di settore; quando una vulnerabilità viene scoperta per la prima volta per via di un attacco informatico si chiama in gergo “**zero day**” (ovvero che l’attacco avviene al giorno numero “0” di consapevolezza della criticità, quando non ci si è ancora resi conto di avere una falla; Singer and Friedman 2014, 299). Le informazioni riguardo alle zero day sono estremamente di valore per gli hacker, tant’è che possono essere vendute o scambiate proprio come un bene prezioso. Il termine esiste ed è comunemente usato quando si parla di cyber sicurezza perché, gli esperti lo ripetono quasi come uno slogan, è impossibile essere completamente a prova di attacco: la domanda non è “se” verrai attaccato, ma “quando”. Toni fatalistici a parte, una verità di base del campo della sicurezza informatica è che non esiste una soluzione semplice, diretta ed univoca a tutte le minacce informatiche. Ciò è particolarmente vero per quando riguarda il fattore umano: per parafrasare gli autori di “Cryptography Engineering Design Principles and Practical Applications”, è inutile installare una porta blindata in una tenda, che nel contesto originale fa riferimento all’inutilità di sviluppare raffinatissimi algoritmi di cifratura se poi è l’utente stesso a rappresentare una vulnerabilità per il sistema di sicurezza. La formazione del personale e l’educazione all’uso del computer e di internet sono fondamentali per prevenire molti dei problemi di sicurezza informatica; ciò significa imparare a riconoscere siti poco affidabili, truffe e tentativi di phishing online, ma anche disimparare cattive abitudini come l’utilizzo di password deboli (la classica password “password”), l’uso di supporti di memoria esterni non controllati, i download rischiosi, il non aggiornare i programmi e i sistemi operativi. Per esempio uno dei modi migliori per mitigare grandemente gli effetti di un attacco ransomware è quello di effettuare back up automatici dei dati, ovvero implementare un sistema di salvataggio periodico delle informazioni su hard disk esterni, in modo da poter recuperare la maggior

parte dei dati che sono stati bloccati dal malware senza dover pagare il riscatto (Ransomware Task Force 2021).

Cyber sicurezza, non solo un problema del singolo

Finora sono state presentate le minacce più comuni in termini di problemi e scomodità che qualsiasi utente del web si è bene o male trovato a fronteggiare almeno una volta nella sua vita (digitale). La lente di analisi concentrata sull'esperienza del singolo però non aiuta a comprendere l'intera portata del tema della cyber sicurezza. L'acquisizione dei dati di una carta di credito, il blocco del proprio computer o il furto di foto personali possono legittimamente rappresentare un grave problema per una singola persona, ma il tema della cyber sicurezza cresce di rilevanza solo quando si prendono in considerazione la relazione tra le possibilità di azione offerte dalle nuove tecnologie digitali e l'impatto più generale sulla società, l'economia e la politica.

Il lato economico: ransomware e spionaggio industriale

La cyber sicurezza lungi dall'essere di nicchia, è invece un settore essenziale per il mondo economico moderno; avere un'azienda significa doversi preoccupare della sicurezza ed integrità dei propri sistemi informatici, ignorare il problema significa esporsi a grossi rischi, a perdita di competitività e nei casi più gravi al fallimento. Al 2014 il 97 percento delle compagnie Fortune 500 risulta avere subito un attacco informatico verso le proprie reti, il restante 3 percento invece probabilmente o non vuole ammettere di avere falle nei suoi sistemi o non sa di essere stato attaccato (Singer and Friedman 2014, 2). I danni economici derivanti possono essere difficili da quantificare: molti attacchi possono non essere rilevati per mesi o addirittura non essere mai scoperti, inoltre né le vittime né chi li attacca ha particolare desiderio di divulgare le informazioni nel dettaglio. Ciononostante esistono delle stime che possono aiutare a comprendere la scala del problema: il Centro per gli Studi Strategici e Internazionali (CSIS), in partnership con McAfee, ha stilato un report sull'impatto che gli attacchi informatici hanno sull'economia globale, arrivando ad individuare perdite economiche pari a 600 miliardi di dollari ogni anno, ovvero l'1% del PIL globale. Nel 2014 le stime erano di 445 miliardi di dollari (Lewis, 2018). I ransomware rappresentano una delle minacce più dirette e diffuso ai business commerciali, nel 2020 il totale dei soldi versati dalle vittime di ransomware è salito del 311%, raggiungendo circa i 350 milioni di dollari di valore (Ransomware Task Force 2021). Il costo non si

ferma solo all'ammontare versato per il riscatto ma deve includere anche i costi indiretti come il tempo speso per ripristinare i servizi, la mancata operatività dell'azienda e la perdita di reputazione. Sta inoltre emergendo la tendenza da parte dei cyber criminali ad effettuare un doppio ricatto ai danni delle vittime; prima si chiedono i soldi per riavere i dati, poi si minaccia l'azienda di pubblicare le informazioni se non si erogano ulteriori versamenti in denaro (Senatore et al. 2019). I motivi per cui le aziende si ritrovano sempre più esposte alle cyber minacce sono diversi: aumento della digitalizzazione delle imprese, incremento di sofisticazione delle tecniche di attacco, mancanza di consapevolezza da parte delle aziende dei rischi connessi al digitale. In aggiunta, è stato notato come si sia sviluppato un mercato illegale di strumenti di attacco hacker, dove per esempio i ransomware vengono venduti come pacchetti pronti all'uso in cambio di una tariffa o una porzione del futuro ricavato (Ransomware Task Force 2021) (Singer and Friedman 2014, 88-91). In questo moto anche chi non possiede elevate competenze tecniche può effettuare lucrose intrusioni ai danni di imprese ed organizzazioni. Nel 2020 due terzi degli attacchi del genere, analizzati dall'azienda di cyber sicurezza Group-IB sono stati portati avanti seguendo il modello "ransomware come servizio" (modello "Ransomware as a Service", RaaS). La questione dunque della cyber sicurezza dovrebbe quindi acquisire, anche solo in forza dei suoi numeri, una posizione di primaria importanza. In realtà ci sono motivi molto specifici per preoccuparsi della sicurezza informatica aziendale: non comprenderne le dinamiche significa esporsi a nuovi e precedentemente sconosciuti modi di fare spionaggio industriale. Gli attacchi di cyber spionaggio industriale non risparmiano alcun settore, per alcuni di essi come quello manifatturiero essi rappresentano il 94% di tutti gli attacchi informatici (Salvatore et al. 2019). Ad essere i target più attraenti sono chiaramente le aziende di R&S, ma anche le compagnie di punta dei settori di eccellenza di un Paese: negli ultimi anni gli attacchi si sono concentrati sul settore finanziario nel Regno Unito, sul settore del lusso in Italia e sulle compagnie di difesa svedesi. La Germania risulta essere il Paese europeo più bersagliato, con il 17% delle sue imprese che riportano furti di informazioni sensibili tra il 2015 e il 2017. Nel 2016 invece la Spagna ha assistito ad una crescita del cyber spionaggio a fini economici nei campi della difesa, IT, chimica e sanità (Salvatore et al. 2019). In tutti questi casi spesso in aggiunta ai già citati ricatti economici e ai danni all'operatività aziendale, si deve anche considerare la perdita di preziosi segreti commerciali, che possono causare a volte uno svantaggio a favore delle aziende rivali durate le trattative commerciali o nei casi più gravi una progressiva diminuzione della competitività nel mercato.

Di seguito sono presentati alcuni tra i più noti incidenti di esfiltrazione di dati con fini economici che mostrino nella pratica come vengano utilizzati mezzi digitali per compiere vere e proprie operazioni di attacco informatico.

Il caso Thyssenkrupp

L'8 Dicembre 2016 il conglomerato industriale tedesco Thyssenkrupp rivelò al pubblico che a seguito di un'intrusione informatica nei loro sistemi furono rubati diversi segreti commerciali di natura tecnica. L'obiettivo dell'attacco erano i design dell'impianto manifatturiero e di produzione dell'acciaio, gli hacker una volta introdottisi nelle reti aziendali furono in grado di spostarsi di sistema in sistema fino all'individuazione dei server di ricerca e sviluppo. L'attacco fu scoperto 45 giorni dopo l'effettiva incursione, grazie ad un team dedicato alla sicurezza informatica che era stato istituito nel 2012, e ai tecnici CERT. Si presume che gli autori del furto siano parte di un gruppo criminale del Sud-Est asiatico, ma l'identità non è mai stata confermata (Senatore 2019).

Dragonfly

Nell'estate 2014 fu lanciato un attacco su larga scala verso aziende del settore energetico in Europa e Nord America. Secondo la compagnia di sicurezza informatica Symatec, gli attacchi compromisero organizzazioni di rilevanza strategica (impianti di produzione di energia) con chiari obiettivi di sorveglianza e mappatura delle infrastrutture, presumibilmente per poi eseguire future invasioni di sistema. La serie di incidenti fu chiamata con il nome dell'organizzazione criminale responsabile per questa ed altre operazioni simili. Il gruppo Dragonfly, conosciuto anche come Electric Bear, è attivo fin dal 2010 e finora ha preso di mira numerosi settori industriali, come quello manifatturiero, farmaceutico, edile, informatico, dell'educazione e dei macchinari industriali. Pre-2013 sono stati anche bersagliati i settori dell'aviazione e della difesa militare di diversi Paesi e più recentemente (2014-2015) operatori di reti energetiche, grandi aziende produttrici di energia elettrica, operatori di oleodotti e produttori di apparecchiature per sistemi di controllo industriale; questi ultimi in particolare sono le aziende che producono i software di gestione degli impianti industriali e delle infrastrutture di servizi come luce, gas, acqua e così via, chiamati **sistemi SCADA** ("supervisory control and data acquisition" system). Essi sono fondamentali perché regolano l'utilizzo e il funzionamento di complessi impianti e macchinari, che come tutto il resto oggigiorno sono gestiti tramite computer.

Il modus operandi del gruppo Dragonfly è illuminante per quanto riguarda le procedure tipiche di effrazione virtuale ai fini di spionaggio industriale. Il gruppo per prima cosa procedette con diverse operazioni di spear-phishing tramite account Gmail rubati e mail con allegati PDF virulenti indirizzate ai dirigenti o dipendenti senior in possesso di credenziali di alto livello di accesso al sistema. Allo stesso tempo utilizzarono un attacco watering hole, infestando siti web di interesse nel campo dell'energia, reindirizzando gli utenti ad altri siti (di loro creazione o precedentemente compromessi) dove essi finivano per scaricare involontariamente dei Trojan per l'accesso remoto (RAT). Il passo più ambizioso del gruppo di hacker fu quello di infiltrarsi nei sistemi informatici aziendali dei produttori di sistemi SCADA per compromettere dei pacchetti software legittimi. Nell'operazione del 2014 furono compromessi tre fornitori di software, inserendo malware nei programmi messi a disposizione per il download sui loro stessi siti. Una volta che un dipendente avviava il programma di gestione dell'impianto (SCADA), i malware si innescavano dispiegando moduli dedicati alle più disparate funzioni di furto e spionaggio: mappatura dei computer infestati (ID utente, sistema operativo, account utenti, Paese, browser predefinito, processi in esecuzione, mail, lista di file e cartelle etc.), furto di password con sistema integrato di decifratura delle password protette, ricerca di software SCADA nelle reti aziendali. I dati copiati venivano poi spediti attraverso un'estesa rete di siti internet hackerati (sono stati individuati 219 domini unici), gli stessi che venivano utilizzati per ospitare i malware, le informazioni delle vittime o i server di comando per gestire i sistemi infettati. Le investigazioni da parte dell'azienda di sicurezza informatica Kaspersky individuarono la maggior parte dei server negli Stati Uniti ed in Germania, ma analizzando l'orario delle attività principali risultò che gli hacker erano più attivi tra le 8 del mattino e le 5 del pomeriggio nella zona orario UTC+3, dunque Est Europa. Sfortunatamente (ma non è un caso, vedi sotto "il problema dell'attribuzione") non sono mai stati fermati i responsabili. (Wangen 2015)

Shamoon

Nel 2012 la compagnia saudita Saudi Aramco fu il bersaglio di un attacco su larga scala tramite un malware di diversi moduli che infetto 30.000 computer aziendali, danneggiando gravemente le loro reti informatiche. La funzione principale di Shamoon consisteva nel cancellare documenti e pezzi di codice necessari per l'avvio del sistema operativo; un vero e proprio tentativo di sabotaggio industriale. Non sono state trovate tracce delle fasi iniziali di infezione, però si è scoperto che una volta all'interno il malware si è propagato attraverso la rete aziendale. Il virus aveva una componente di cancellazione e una di report ad un server esterno, ciononostante non si hanno notizie certe di

furto di dati. Il malware per prima cosa stilava una lista di tutti i file da cancellare, principalmente i contenuti delle cartelle “Documenti” e “Desktop”, per poi inviare l’informazione ad un server di comando e procedere alla cancellazione dei dati. (Wangen 2015)

Scorrendo i resoconti dei casi più celebri di attacco informatico, ciò che risalta dalle ricostruzioni senza ombra di dubbio è l’elevata sofisticazione delle incursioni informatiche. I responsabili possiedono capacità organizzativa, risorse economiche e conoscenze tecniche notevoli, non si tratta di un “script kiddie”, cioè di un ragazzino con un computer e qualche conoscenza di base di hackeraggio, o di un truffatore solitario a cui è stato fornito un software illegale. Dietro a questo genere di operazioni si celano vere e proprie organizzazioni criminali.

Le APT (Advanced Persistent Threats)

Le organizzazioni responsabili di vere e proprie campagne di cyberspionaggio ed esfiltrazione dei dati vengono chiamate “**APT**” (Advanced Persistent Threats) o Minacce Avanzate e Persistenti. Le APT si distinguono dagli altri cyber criminali in virtù del notevole livello di pianificazione che contrassegna i loro interventi. Esse hanno obiettivi specifici di alto livello, aziende grandi o personaggi in vista della politica. Nelle APT gli individui lavorano come una squadra con una combinazione di organizzazione, ingegno, competenza tecnica e pazienza. Ogni membro ha un ruolo specifico da svolgere nelle diverse fasi del piano: ricognizione, intrusione e sorveglianza. La prima fase di solito consiste nel raccogliere più informazioni possibili sulle persone che lavorano all’interno dell’organizzazione bersaglio: Google è il principale strumento per scoprire informazioni personali come CV, amici, parenti, abitudini e gusti. Vengono anche effettuate le prime intercettazioni telematiche e la ricerca delle vulnerabilità dei sistemi; la fase di ricognizione può anche durare mesi. Le squadre di APT non cercano solo informazioni tecniche, ma mirano anche a comprendere il contesto in cui opera il bersaglio a 360°. In un caso una APT stava prendendo di mira una delle maggiori aziende di tecnologia con sede nel Minnesota; i membri della squadra sfruttarono la loro conoscenza delle abitudini della compagnia unitamente alle condizioni del meteo per lanciare l’offensiva: in prossimità di una tempesta di neve inviarono delle mail contraffatte riguardo il cambio di politica interna a proposito dell’imminente innevata. La comunicazione, oltre ad essere specifica e credibile, trattava di qualcosa di cui tutto il personale si doveva preoccupare: ciò permise all’attacco di phishing di andare a buon fine e di iniziare l’infiltrazione. In un altro caso gli hacker riuscirono a stilare delle mail particolarmente verosimili arrivando persino ad imitare i tipici saluti in fondo al messaggio che i dipendenti dell’azienda si scambiavano tra loro. Una volta all’interno del sistema la squadra di

intrusione va alla ricerca di specifici file da rubare, un'altra differenza dai più comuni cyber crimini che invece rubano i dati bene o male a casaccio; gli intrusi spesso non hanno neanche bisogno di aprire i documenti da sottrarre, segno che nella fase di ricognizione si è riuscito a mappare i contenuti dei computer e server fin nei minimi dettagli (si pensi al caso Dragonfly). Quando i dati vengono spediti "a casa", è solo allora che molti attacchi vengono scoperti a causa del traffico anomalo di dati verso l'esterno, ma ormai è troppo tardi. I dati a questo punto possono rimbalzare su server in diversi Paesi, rendendo difficile capire la provenienza dell'attacco. I problemi non si fermano qui, perché alle volte a seguito dell'esfiltrazione dei dati può intervenire un'altra squadra con il compito di mantenere la presenza e la sorveglianza all'interno dei server aziendali infetti; l'APT potrebbe avere interesse nel ripetere le incursioni o nel monitorare le operazioni di indagine sull'incidente. Un altro elemento degno di nota è che spesso le APT non bersagliano l'azienda principale, ma preferiscono infettare i sistemi di fornitori fidati o collaboratori esterni, che ovviamente possiedano i privilegi di accesso al sistema. In genere è molto più facile minare i sistemi di sicurezza di PMI collaboratrici piuttosto che attaccare direttamente un colosso industriale dai fondi e dal know-how di sicurezza presumibilmente più elevato. Per comprendere come le APT siano un fenomeno a sé stante, basti pensare che in genere esse effettuano simulazioni di attacco e finte incursioni per poter assicurare il "controllo qualità" dei propri servizi, esattamente come qualsiasi altro business. (Singer and Friedman 2014, 60) Le APT sollevano delle fondamentali domande riguardo alla provenienza delle ingenti risorse finanziarie, infrastrutturali e umane che permettono l'esistenza e l'efficacia di tali gruppi; come si vedrà più avanti la linea di demarcazione tra attività a scopo di lucro indipendenti e affiliazioni politiche sotterranee piuttosto sottile e confusa in certi casi. Tanto più che le APT non rappresentano un problema solamente per le industrie, anzi solitamente è difficile trovare gruppi organizzati di hacker che non prendano di mira uffici governativi e aziende tecnologiche collegate al settore militare; gli stessi attacchi alle aziende produttrici di energia rappresentano una potenziale minaccia per la sicurezza nazionale di un Paese. È utile delineare il panorama degli attori che popolano il **cyberspazio**, siccome il filo rosso che accomuna una buona parte di essi è la motivazione ideologica e politica. La questione di cosa si può fare con i mezzi digitali sconfina dunque la cybersicurezza come scienza informatica di nicchia e obbliga una riflessione su fenomeni più complessi come lotta politica e, come verrà presentato successivamente, politica internazionale.

Il lato politico: hacktivismo e geopolitica

Il termine "**Hacktivism"** (italianizzato Hacktivismo) sta a identificare l'attivismo politico portato avanti tramite attacchi informatici. I nuovi mezzi digitali diventano un tramite per le proteste dei comuni cittadini (più spesso di giovani studenti) che si coordinano online: allora gli attacchi DDoS, eseguiti tramite computer messi a disposizione volontariamente da altri utenti, diventano un mezzo per oscurare il sito di un'azienda che ha commesso nefandezze, o in altri casi si eseguono operazioni collettive di doxing per smascherare chi viene additato come criminale. Il nome che la stampa tradizionale ha cementato nella mente del pubblico quando si parla di hacktivism è "Anonymous". Definire chi sono i membri della comunità hacker Anonymous è piuttosto difficile, non tanto in termini d' identità dei partecipanti ma in quanto motivazioni e valori che li contraddistinguano. Anonymous è teoricamente fondato sui valori della libertà di parola, dell'anonimato e della rete come un insieme di pari, ma nella realtà risulta essere più un mostro a moltissime teste con istanze persino contrastanti tra loro, alle volte. Il collettivo è giunto alle luci della ribalta tra il 2007 e il 2011, quando attraverso attacchi informatici coordinati in rete riuscì a fare scalpore mediatico. Per esempio nel 2007 finirono sui notiziari canadesi per aver contribuito all'arresto di un pederasta di 53 anni tramite una lunga operazione di doxing e di intercettazione delle comunicazioni dell'uomo; un vero e proprio caso di vigilantismo su internet. Nel 2008 invece si resero famosi per aver sottratto e rilasciato un video intervista da parte di Scientology a Tom Cruise; quando il gruppo religioso minacciò di intraprendere azioni legali nei loro confronti, il collettivo lo vide come un tentativo di censura della libertà d'informazione. Come conseguenza fu avviato il "progetto Chanology", ovvero una serie di sistematici attacchi DDoS ai siti della setta per mandarli offline. Nello stesso anno riuscirono a intrufolarsi nell'account di Yahoo mail di Sarah Palin e nell'anno successivo parteciparono alle protese in Iran contro l'elezione del presidente Mahmoud Ahmadinejad, organizzandosi assieme al gruppo hacker The Pirate Bay e diversi hacker iraniani per favorire il libero scambio d'informazioni tra i cittadini della nazione e il mondo esterno. Dal 2010 in poi i bersagli divennero entità e persone sempre più in vista, facendo crescere la notorietà del gruppo. Nel 2011, a seguito delle rivoluzioni in Tunisia, in Egitto e durante la guerra civile in Libia i siti governativi dei rispettivi Paesi furono messi offline dal collettivo. (Singer and Friedman 2014, 80). La lista di operazioni riconducibile ad Anonymous è molto lunga e il gruppo sembra essere tuttora in attività. Ciò che più importa è notare come siano le motivazioni politiche ed ideologiche a fare da sfondo agli

attacchi informatici organizzati e che Anonymous non è di certo l'unico gruppo di vigilanti/attivisti presente in rete.

Il caso Wikileaks

Nel 2006 fu lanciato un sito internet dal nome Wikileaks dall'ormai famigerato Julian Assange, giornalista, programmatore ma soprattutto attivista australiano per la libertà di informazione. Durante le operazioni militari in Iraq e Afghanistan tra il 2004 e il 2009 l'esercito e il governo americano registrarono mezzo milione di eventi legati alla guerra, compreso di scambi di mail tra diplomatici e funzionari governativi, rapporti militari, persino registrazioni video dal campo di battaglia. Nel 2010 Chelsea Manning (ex Bradley Manning) allora facente parte dell'intelligence militare dispiegata su Baghdad, in accordo con Assange fece trapelare un video del 2007 dove due elicotteri Apache statunitensi abbattono a colpi di mitragliatrice 18 civili disarmati; il caso scoppiò sui maggiori giornali mondiali. Poco dopo vennero rilasciate anche un gran numero di documenti privati, tra cui i report sulle vittime di guerra (con numeri ben maggiori di quelli riportati alla stampa) e i documenti diplomatici sopra citati. Wikileaks divenne il centro di un incidente diplomatico internazionale a danno degli Stati Uniti, raccogliendo sui propri server una quantità incredibile di dati rubati dai sistemi governativi e trasmettendo periodicamente informazioni alla stampa. Vennero resi pubblici segreti imbarazzanti per i diplomatici americani, come per esempio le loro opinioni riguardo le controparti estere, operazioni di spionaggio delle conversazioni del Segretario Generale delle Nazioni Unite nel periodo prima dell'inizio della guerra in Iraq, ma anche casi di corruzione o inadempienza da parte di altri governi nazionali. Ad un certo punto, forse a causa di pressioni esterne o litigi interni, Wikileaks pubblicò il restante dei dati (finora pubblicati poco alla volta) senza nessun tipo d'intervento di selezione o redazione; in mezzo a una marea di conversazioni noiose tra funzionari burocratici emersero anche informazioni pericolose, come l'identità di dissidenti politici o agenti sotto copertura, che misero a rischio la vita di diverse persone. Le vicende giudiziarie che ne seguirono furono lunghe e complesse, ma emerse chiaramente il peso dei mezzi digitali nel rendere possibile una vicenda del genere. Per prima cosa il sistema di autorizzazioni e sicurezza del pentagono, nonostante il sistema di credenziali, crittografia e sorveglianza dei dati, celava una falla notevole: le misure di air-gapping vietavano la connessione ad internet e l'uso di chiavette USB, ma non impedivano l'utilizzo di supporti CD sovrascrivibili. In questa maniera il soldato scelto Chelsea fu in grado di portare con sé i propri CD musicali ed usarli per copiare i dati nel corso di 8-9 mesi di lavoro indisturbato. Secondariamente, nei mesi e negli anni successivi all'esfiltrazione dei dati, Julian

Assange poté sfruttare server fuori dalla giurisdizione americana per rendere pubbliche le informazioni senza che il governo potesse intervenire, oltra a contare sulla proliferazione spontanea dei file sul web. Quando la svista di sicurezza riguarda un'azienda, quello che può succedere è un furto di segreti commerciali e una perdita di fatturato futuro, quando ad essere rilasciate sono pagine e pagine di file governativi segreti, le conseguenze sono molto più gravi e profonde. (Singer and Friedman 2014, 51-55)

Gli Hacker Patriottici

Quando si fa riferimento alla sottile linea che separa taluni gruppi di cyber criminali e organizzazioni mosse da fini politico-ideologici, l'esempio in mente è quello degli hacker patriottici. Un esempio: in Estonia nel 2007 numerosi siti governativi, commerciali, giornalistici e via dicendo, vennero bloccati da imponenti attacchi DDoS assieme ad altri atti di vandalismo digitale. Non ci volle molto prima che accuse d'istigazione e supporto alla campagna di hacking venissero mosse nei confronti della Russia; negando ogni tipo di accusa, il governo russo si dichiarò estraneo ai fatti. In effetti, il gruppo di giovani tra i diciassette e i venticinque anni riuniti sotto il movimento chiamato "Nashi" (Nostro) non faceva ufficialmente parte del governo, sebbene fosse ideologicamente schierato a suo favore. Il collegamento con il governo era sottile, ambiguo ma senz'altro presente. I giovani russi infatti, oltre ad effettuare attacchi informatici verso chi veniva visto come un "nemico della patria", organizzavano campi estivi pro-governo e partecipavano con raid violenti alle proteste in piazza degli avversari politici. Nei giorni precedenti all'assalto informatico furono postati su diversi forum russi manuali e kit per eseguire DDoS e si sospetta che i fondi utilizzati per sostenere i costi degli attacchi provenissero dallo Stato; all'epoca inoltre il leader del movimento giovanile ricopriva il ruolo di assistente di Sergei Markov, un membro parlamentare del partito di governo. L'anno successivo, durante lo scontro tra Russia e Georgia nella regione del Caucaso del sud, non solo si ripeté la storia, ma questa volta gli attacchi DDoS coincisero con l'assalto da parte delle truppe militari; secondo uno studio successivo, l'intelligence Russa fornì una lista di siti governativi da bersagliare durante l'operazione (Singer and Friedman 2014, 111-112). Fenomeni di questo tipo non succedono solamente in Russia, gli hacker patriottici esistono in ogni parte del mondo dove le infrastrutture tecnologiche sono abbastanza sviluppate. Infatti permettano ai governi di avere abbastanza copertura da poter negare ogni collegamento dimostrabile. In aggiunta determinare la provenienza di un assalto virtuale può risultare estremamente difficile, come si può confermare che il terminale usato non sia parte di una botnet usata per confondere le acque e sia stato usato solamente per far

rimbalzare i dati in un tentativo di depistaggio? Come si verifica l'identità dell'utente che ha utilizzato il terminale? Nel caso di Conficker 2008 (vedi sopra) si è dovuto ricorrere ad una particolare linea di codice che escludeva come bersagli chi utilizzasse una tastiera ucraina, o nel caso del worm Mahdi (Wangen 2015) alcune backdoor furono scritte in Delphi, ma il problema rimane, come si può essere certi che non si tratti di un abile depistaggio? Senza una collaborazione di confine tra i Paesi non è possibile condurre indagini sul luogo. Nel cyberspazio il problema dell'attribuzione diventa un terreno di delicato equilibrio di diplomazia internazionale; accuse troppo repentine o depistaggi intenzionali possono esacerbare le relazioni tra Paesi e dall'altro lato i governi hanno accesso a forza di sabotaggio e spionaggio che possono colpire alla velocità della luce (o meglio, di internet) a grandissima distanza, incuranti dei confini nazionali e i cui legami con lo Stato possono essere facilmente negati. Il problema della cyber sicurezza diventa anche un problema di politica e diplomazia internazionale.

Il caso Stuxnet

Nel 2010 un particolare tipo di worm si stava diffondendo nei sistemi di controllo industriali; migliaia di computer nel mondo risultavano infettati da un malware specificatamente disegnato per prendere di mira i sistemi di gestione automatizzata degli impianti industriale, i già citati sistemi SCADA. Tracce del malware si potevano trovano in posti come India e Stati Uniti, ma la maggior parte delle infiltrazioni erano concentrate in Iran, suggerendo che o il Paese possedessse difese informatiche particolarmente scarse o che forse il programma fosse sfuggito di mano a qualche hacker locale. Ralph Langner, consulente tedesco con più di trent'anni di esperienza nel campo della protezione di grandi impianti industriali, assieme al suo team fu uno dei primi ad analizzare il codice di **Stuxnet**, come verrà poi conosciuto in futuro, e a trovare immediatamente delle peculiarità notevoli. Per prima cosa, il pacchetto malware conteneva quattro nuove "zero day", ovvero quattro strategie di infiltrazione che sfruttassero vulnerabilità ancora sconosciute agli utenti e ai creatori di software. L'utilizzo di quattro falle segrete non aveva avuto precedenti fino a quel momento, le "zero day" sono considerate informazioni preziosissime dagli hacker e sul mercato nero avrebbero avuto un valore notevole; usarne quattro in una volta significava voler avere l'assoluta certezza di riuscire a penetrare la rete bersaglio. Secondariamente Stuxnet era programmato per funzionare su tutti i sistemi operativi Windows, dalla versione del 2010 a quella del 1995, in più possedeva un ulteriore asso nella manica per oltrepassare le difese del sistema operativo, uno particolarmente complesso da ottenere. Per poter aver accesso al kernel del computer, ovvero al pannello di controllo del

sistema operativo, Il programma necessitava di installare delle componenti apposite provenienti dall'esterno, in questo caso gli autori scelsero di utilizzare dei "driver delle periferiche", dei pacchetti software pensati per far comunicare parti di hardware con il software. Windows utilizza delle firme digitali (vedi CA e certificati digitali) assegnate ai produttori fidati (aziende tecnologiche private) per contrassegnare i propri programmi (e quindi driver) come sicuri per il download e l'installazione. Scaricare driver senza contrassegno attiverebbe immediatamente l'antivirus del sistema. Dunque gli hacker in questione possedevano ben due firme digitali di altrettante aziende private di Taiwan collaboratrici di Windows. Le chiavi digitali usate per firmare i programmi sono estremamente difficili da falsificare o da rubare, una volta ottenuto poi hanno anch'esse un valore potenziale sul mercato illegale altissimo. Il team di sviluppo del malware doveva possedere incredibili risorse economiche e umane per mettere in campo un ariete di sfondamento del genere. Ma le peculiarità del codice non si fermavano qui. Il worm, per quanto si fosse diffuso in modo assai virulento, non era pensato per agire su obiettivi di massa, bensì era programmato per cercare un tipo specifico di gestionale industriale e di disattivarsi in caso non rilevasse tale software. Il malware possedeva inoltre una bomba logica pronta a cancellarlo completamente entro il 2012. Il programma bersaglio di Stuxnet consisteva in un software di gestione delle centrifughe nucleari prodotto da Siemens, nello specifico il software WinCC/PCS 7 SCADA per la gestione di un set di centrifughe di dimensione e numero ben definiti, ovvero più esattamente l'esatta configurazione delle centrifughe dell'impianto Natanz situato in Iran, reo di essere additato come sospetto impianto di sviluppo illegale di armi nucleari. Stuxnet, che in seguito si scoprì essere arrivato dentro la centrale tramite i laptop e le chiavette usb degli scienziati, non aveva il compito di sabotare i macchinari in modo palese, ma di intervenire subdolamente sull'integrità dei sistemi. Il malware aveva il compito di eseguire diversi tipi di funzioni: una di queste causava micro aggiustamenti nella pressione interna, un'altra manipolava la velocità dei rotori delle centrifughe, alternando rallentamenti e accelerazioni irregolari, in aggiunta ad intervalli casuali spingeva la velocità dei macchinari ben oltre il limite di sicurezza. L'impianto non solo non riusciva a produrre l'uranio arricchito, ma spesso e volentieri causava guasti irreparabili alle turbine, che dovevano poi essere sostituite. Le vibrazioni causate dal comportamento bizzarro dei rotori infatti provocavano ingenti danni agli stessi, fino a causare la perdita di controllo dei macchinari e conseguenti esplosioni. Successivamente Lagner definì l'effetto di Stuxnet come paragonabile "all'uso di espolsivi", un tentativo di minare l'integrità strutturale dell'impianto nucleare in piena regola. Come emerse in seguito, l'attacco andò; per più di un anno gli scienziati della centrale continuarono a sostituire le centrifughe danneggiate, fare controlli ai macchinari e ai sistemi informatici: tutto risultava in perfette condizioni, fino a che ovviamente il malware non

rientrava in funzione. I ricercatori Iraniani alla fine gettarono la spugna, senza sospettare minimamente di essere stati vittima di un cyber attacco. Lagner senza saperlo aveva però svelato i dettagli di un'operazione segreta di sabotaggio militare: come emerse più tardi il malware Stuxnet fu il frutto degli sforzi congiunti dell'intelligence americana e israeliana per l'operazione "Olympic Games". (Singer and Friedman 2014, 114-118)

Stuxnet divenne presto un caso di studio per teorici militari ed esperti di cyber sicurezza. Il worm rappresentò un nuovo modo di utilizzare i mezzi informatici come arma. Il termine "**guerra cibernetica**" ("Cyberwar" o "cyberwarfare" in inglese) viene utilizzato spesso per descrivere fenomeni molto diversi tra loro, si pensi al caso di Nashi e degli attacchi informatici verso l'Estonia più simili ad atti di vandalismo e il malware Stuxnet progettato per sabotare un impianto nucleare. Ciononostante ci sono due criteri che definiscono cosa siano vere e proprie azioni di guerra: 1) dietro alle azioni intraprese ci deve essere un chiaro motivo politico 2) tali azioni devono risultare nel danneggiamento fisico di persone o cose (Singer and Friedman 2014, 121). Stuxnet può essere considerato a pieno titolo un nuovo tipo di armamento militare e come tale rappresenta un precedente unico nel suo genere. Ovviamente ben prima dell'emergere di Stuxnet si possono trovare tracce della consapevolezza del ruolo delle nuove tecnologie nelle operazioni di carattere militare. Nella sua ricerca Warner (2012) riporta come dai documenti ufficiali governativi statunitensi emerga già chiaramente il problema dell'integrazione dei computer negli arsenali militari e come tale problema fosse al centro dei discorsi dei "think tank" dell'esercito già dagli anni '80 e '90 quando si menziona il timore che altre nazioni possano tentare di infiltrarsi e compromettere il funzionamento dei sistemi informatici militari. I ricercatori militari, dopo la guerra del Vietnam degli anni '70 cominciarono a notare la tendenza in aumento da parte delle forze militari di utilizzare armamenti tele-guidati, sensori remoti da campo e in generale i sistemi informatici per la gestione dei vari aspetti logisitico-amministrativi e operativi dell'esercito. Ciò si traduceva in un invariabile aumento dei rischi legati alle vulnerabilità delle tecnologie informatiche. Il nuovo modo di fare guerra cibernetica, scrisse Thomas P. Rona nel 1976, richiedeva un flusso di informazioni digitali sempre più interconnesse al fine di far funzionare le armi più avanzate e dunque ad un inevitabile aumento delle fragilità strutturali; man mano che i sistemi diventavano più complessi, essi diventano anche più fragili. Una seconda lezione tratta dalla storia militare americana legata all'importanza del flusso di informazioni digitali, può essere individuata nella campagna militare "Desert Storm" svoltasi in Iraq. Nel 1991 Kuwait fu liberata dalle forze di Saddam con una schiacciante vittoria delle forze di coalizione; uno dei fattori critici nel determinare il vantaggio delle forze americane fu l'accesso ad immagini satellitari in tempo reale del campo di battaglia. Il flusso di dati e comunicazioni da parte

dell'intelligence fu fondamentale al completamento della campagna, il tutto reso possibile dai collegamenti satellitari, dalle tecnologie informatiche e di rete avanzate. Il punto è che ancora oggi le forze militari fanno grande affidamento su comunicazioni accurate e puntuali trasmesse tramite sistemi di controllo e comando. Tali sistemi sono composti da personale, equipaggiamento, strutture e soprattutto reti di computer; un attacco alle reti informatiche di comando militare equivarrebbe alla decapitazione della catena di comando e ad una vulnerabilità potenzialmente fatale per le forze sul campo. Inoltre c'è da aggiungere che i sistemi di puntamento delle armi automatizzate e i sistemi di navigazione dei veicoli dipendono grandemente da connessioni protette; dovessero poter essere interrotte o anzi controllate da forze nemiche, i risultati sarebbero disastrosi. Se poi si pensa al caso Stuxnet, una volta individuati gli impianti critici per l'approvvigionamento dell'esercito (come raffinerie o aziende produttrici di armamenti), si potrebbe procedere con una campagna di sabotaggio che comprometterebbe la sostenibilità a lungo termine degli sforzi militari.

In riassunto, quello della cyber sicurezza è un campo che finisce per intrecciarsi con temi di ordine e ampiezza superiore, come la politica, geo-politica e la teoria militare. Quando le tecnologie informatiche vengono militarizzate per colpire bersagli militari, economici o civili con evidenti fini politici, si può parlare di guerra cibernetica o di **cyber terrorismo**, a seconda dello schieramento a cui si appartiene. Il caso Stuxnet mostra chiaramente come i malware possono trasformarsi in armi di sabotaggio estremamente efficaci, occorre infatti sottolineare che i sistemi SCADA non sono solo utilizzati per le centrali nucleari, ma anche per la maggior parte delle industrie pesanti, energetiche e per la gestione degli impianti di gas, acqua e luce di paesi e città. Il caso Wikileaks può invece essere considerato un proverbiale esempio di fuga di notizie a causa di vulnerabilità dell'infrastruttura di sicurezza informatica: air gapping, crittografia, sistemi di autenticazione non garantiscono sicurezza totale; più le informazioni sono sensibili più va riflettuto sulle conseguenze di un'eventuale fuoriuscita. Anche quando non si tratta di operazioni di intelligence, gli attori più o meno politicamente indipendenti del web possono rappresentare un problema di sicurezza nazionale: i ransomware colpiscono ogni anno ospedali, scuola, uffici governativi (RTF 2021) riducendone l'operatività e causando ingenti danni economici agli Stati. Allo stesso modo le operazioni di spionaggio industriale vanno considerate come tentativi di minare le industrie critiche per la competitività internazionale di un Paese, è difficile non individuare una motivazione politica secondaria dietro a gruppi ben organizzati e finanziati, che occasionalmente si scoprono avere contatti con governi nazionali esteri. Dunque il campo della cyber sicurezza richiede un approccio di ampio respiro, con influenza multidisciplinari e letture a differenti livelli di analisi per poter comprendere tutte le sfumature di un campo apparentemente solo tecnico; in realtà le tematiche e i

fenomeni che si incrociano ed intrecciano attorno al concetto di cyber sicurezza vanno a toccare sfide e problemi caratteristici dell'epoca odierna, che tutti i Paesi sviluppati in giro per il mondo si stanno trovando ad affrontare.

Capitolo 2

La Cina e la Cybersicurezza

Tra i Paesi che più spesso vengono citati nella letteratura, negli articoli e nelle cronache di settore, sicuramente uno di quelli che affiora con stabilità e sempre maggiore frequenza da ormai molti anni è la Cina. Con il processo di riforma iniziato negli anni ’70 e ’80 sotto Deng Xiaoping, la Cina ha compiuto i primi passi di trasformazione radicale del proprio Paese, ormai è largamente riconosciuto come l’impeto di cambiamento iniziato in quel periodo ha propulso la Cina verso un futuro di grande crescita economica, urbanizzazione e sviluppo. Internet in Cina arriva negli anni ’90 grazie alla costruzione e al progressivo ampliamento delle infrastrutture di telecomunicazione, da subito il governo ne intravede le grandi possibilità e mette lo sviluppo tecnologico al centro degli sforzi di ammodernamento del Paese. Ad oggi la Cina con il suo miliardo (o quasi) di utenti internet rimane ineguagliata dal punto di vista dei numeri, seguita dagli utenti indiani e molto in coda quelli europei e statunitensi. La digital economy o il cosiddetto e-commerce nel Paese ha raggiunto un livello di maturità notevole, molto superiore a quello italiano per esempio; le tecnologie digitali rappresentano un forte motore di crescita tutt’ora, a quaranta anni di distanza. Non è inoltre un mistero che la Cina stia da tempo muovendo passi molto lunghi e ambiziosi nel cyber spazio, lasciando spesso le proprie orme su diversi fatti di cronaca che riguardano casi di spionaggio internazionale, infiltrazioni clandestine e altre operazioni nel reame digitale. Il rapporto conflittuale con gli Stati Uniti d’America ha dato vita ad un profluvio di letteratura e di articoli allarmistici che denunciano le scorribande cinesi su internet. Ma qual è effettivamente la situazione della cyber sicurezza in Cina? Cosa c’è di vero nelle accuse di spionaggio mosse dalla maggior parte dei media mainstream occidentali? La seconda parte del presente elaborato tenta di disegnare una mappa delle tematiche generali riguardanti la sicurezza informatica e dei principali attori nel reame digitale in Cina.

Il quadro generale del settore presenta un complesso intreccio di parti interessate con obiettivi e punti di vista differenti. Il settore industriale ed economico privato ha da tempo individuato nelle tecnologie digitali un potente mezzo per la crescita della produttività, dell’efficienza e del fatturato, i nuovi modelli di business sono incentrati sull’economia digitale, dal commercio online, all’intrattenimento, ai servizi di microcredito/debito tramite app del cellulare, a tutta l’elettronica di consumo. Per le aziende il web è uno spazio che permette l’esistenza di modi per fare business

completamente sconosciuti anche solo vent'anni fa. Il processo di digitalizzazione dell'economia non è dissimile da quello avvenuto in altri Paesi sviluppati, è un fenomeno globale che non poteva che investire anche la Cina. Per alcuni aspetti essa ha visto una maggiore penetrazione del digitale rispetto all'occidente. Per esempio, la Cina ha un tasso di diffusione degli smartphone ben superiore a quello italiano e i cinesi sono stati molto più veloci ad adottare i metodi di pagamento quasi completamente digitali (tramite appunto smartphone). Il motivo per cui i tassi di diffusione sono superiori è da ricercare negli ingenti investimenti fatti dal governo centrale per ampliare le infrastrutture internet e ampliare la copertura di rete sul proprio territorio. È risaputo, per esempio, che la Cina detiene il primato per quanto riguarda la tecnologia di connessione senza fili, non è un caso che le tecnologie 5G di cui si è spesso discusso negli ultimi anni provenissero proprio dal gigante asiatico. I privati cittadini, altra parte spesso trascurata nelle narrazioni occidentali, posseggono anch'essi una voce nel dibattito riguardo le nuove tecnologie e si battono, come le controparti europee ed americane, per una sempre maggiore sicurezza degli spazi virtuali. Recentemente la Cina ha emanato delle normative per la tutela della privacy equiparabile (e secondo alcuni osservatori, addirittura superiore) al GDPR europeo, proprio perché i cittadini cinesi stanno diventando sempre più coscienti dei problemi che le tecnologie digitali possono portare all'interno della società. Oltre al settore privato però, anche il governo possiede delle proprie mire e necessità che contribuiscono a formare il particolare scenario cinese riguardo la sicurezza informatica. Se da un lato i cittadini cinesi richiedono più privacy e tutele, dall'altro è altrettanto importante per la dirigenza mantenere il controllo sulla sorveglianza interna da parte delle agenzie di intelligence e la capacità di intervenire per censurare i contenuti web che minacciano "la stabilità interna" del Paese. Il web da che mondo e mondo (occidentale ed orientale) è un veicolo potenzialmente virale di nuove idee, ma soprattutto esso è nato in America e porta invariabilmente con sé, per via della sua stessa costituzione, un'evidente marcatura valoriale di stampo occidentale; il web per forza di cose si pone agli antipodi rispetto all'approccio cinese nei confronti della circolazione di idee: senza controllo sulle idee e i dibattiti in rete, si mette a repentaglio la stabilità sociale e dunque la Cina tutta. Andando ad esaminare la situazione specifica della sicurezza informatica, appare un evidente squilibrio tra l'attenzione dedicata ai problemi di carattere ideologico (la propaganda estera, i dissidenti, il consenso) e i problemi di carattere tecnico/economico; infatti molto del sottobosco criminale che lucra sui modelli di business a base di malware e truffe informatiche prospera più facilmente che in altri Paesi, proprio grazie ad un vuoto normativo riguardo la proprietà intellettuale e il cyber spazio in generale. Spesso i criminali rischiano di meno a rubare sul web proprio per l'enfasi della dirigenza sulle questioni ideologiche e la disattenzione ai problemi più pratici della vita digitale di aziende e

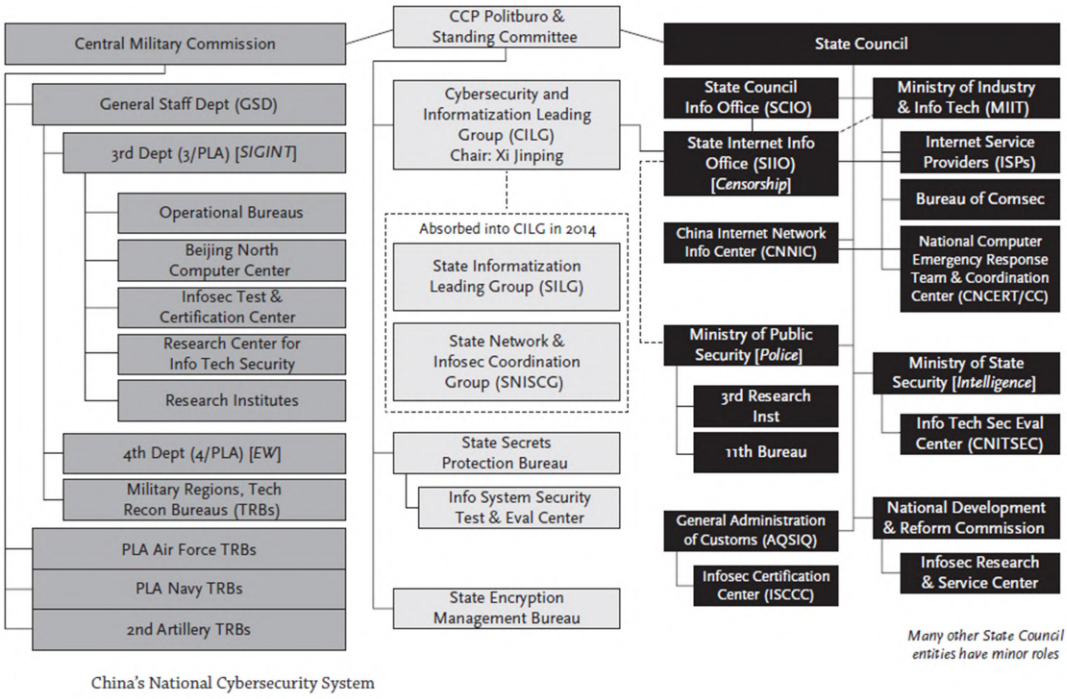
privati cittadini. C'è da sottolineare che l'ambiguità normativa riguardo alla proprietà intellettuale e agli standard di sicurezza aziendali viene anche sfruttata da parte delle autorità commerciali per "mettere i bastoni tra le ruote" delle aziende straniere che mettono a rischio la competitività locale; le aree grigie della normativa (su diverse aree, sicurezza informatica inclusa) permette una forma di protezionismo occulto ed altamente arbitrario. Un altro giocatore molto importante presente sulla scacchiera degli interessi nazionali riguardo alla sicurezza delle tecnologie informatiche è l'esercito, la cui agenda degli ultimi anni ruota attorno alla "sicurezza nazionale" riguardo le reti informatiche. Sotto l'egida della protezione della Cina e dei suoi interessi legittimi, i dipartimenti militari informatici portano avanti operazioni di monitoraggio e cyber spionaggio, nonostante si fatichi a trovare tracce scritte e documentate di ciò che fanno talune unità e divisioni specializzate dei sopracitati dipartimenti. Le parti in gioco che hanno un interesse nell'influenzare il discorso di policy riguardo alla sicurezza informatica sono molteplici, ciò unitamente al complesso sistema di frammentazione decisionale tipicamente cinese rende il processo di sviluppo di una riposta coordinata, chiara e concisa, particolarmente arduo.

I policy maker della cybersicurezza cinese

Per comprendere meglio la topografia del fenomeno, occorre delineare i principali responsabili istituzionali. Da una parte si può collocare l'esercito, più precisamente la Commissione Militare Centrale (中央军事委员会) a capo del Dipartimento di Stato Maggiore dell'Esercito Popolare di Liberazione (中国人民解放军总参谋部) e delle forze aereonautiche e di artiglieri, che a loro volta comprendono alcune unità specializzate nella guerra informatica e nella sicurezza delle reti nazionali (più nel dettaglio più avanti). Dalla parte opposta si può collocare il Consiglio di Stato della Repubblica Popolare Cinese (中华人民共和国国务院), a cui fanno capo numerosi ministeri, dipartimenti ed uffici che si occupano di internet in un modo o nell'altro, come per esempio il Ministero dell' Industria e delle Tecnologie Informatiche (MIIT), Ufficio Informazioni del Consiglio di Stato (SIIO, a capo delle operazioni di censura), gli ISP cinesi, il Ministero della Sicurezza di Stato (a capo dei servizi di intelligence nazionale) e molti altri ancora. *Ça va sans dire*, le sovrapposizioni di competenze e la coincidenza dei differenti ruoli sono moltissime, tanto più che al centro dell'organizzazione istituzionale presentata risiede il Partito Comunista Cinese, più precisamente il Comitato permanente dell'ufficio politico del Partito Comunista Cinese (中国共产党中央政治局常务委员会) che sorveglia e indirizza gli sforzi collettivi. La figura 7 presenta una schematizzazione della struttura soggiacente alla gestione delle politiche di cyber sicurezza. Ad oggi lo sviluppo delle policy

di sicurezza informatica ricade tra le responsabilità primarie del "Cybersecurity and Informatization Leading Group (CILG)" con a capo Xi Jinping e altri collaboratori stretti del presidente. I "Leading Small Groups" sono sempre stati corpi informali

Figura 7 (Lindsay et al. 2015, 9)



China's National Cybersecurity System

creati dal politburo cinese, con il ruolo essenziale di ricerca, analisi e consiglio in merito a temi specifici su cui emanare ed implementare policy nazionali (Miller 2008). Il fatto che a capo del CILG ci sia il presidente stesso, indica quanto centrale venga percepita la problematica della sicurezza delle reti e del cyber spazio nazionale. Inoltre, dal 2014 è stata formata l'"Amministrazione del Cyberspazio Cinese (CAC)" (国家互联网信息办公室), ovvero l'organo regolatorio centrale responsabile per le legiferazione, la supervisione e la censura di Internet; esso andrebbe dunque ad aggiungersi all'organigramma presentato sotto il lato del Consiglio di Stato e comprende il già citato SIIO e l' Ufficio della Commissione centrale per gli affari del cyberspazio. Ed è proprio l'Amministrazione del Cyberspazio Cinese che si occupa di gestire uno dei più ambiziosi progetti di controllo di Internet ad oggi esistente: il Great Firewall cinese.

Il Great Firewall cinese

Il Great Firewall consiste in un sistema di sorveglianza del traffico dati che copre l'intera rete nazionale cinese. Il termine fu coniato dal periodico Wired che in un articolo del 1997 paragonava il sistema di filtraggio dati alla grande muraglia cinese ("The Great Wall") (Griffith 2019, 42); in realtà esso fa parte di una serie di progetti di riforma partiti negli anni '90 e che comprendevano cambiamenti nel settore economico, finanziario ed informatico. Con l'avvento di internet nel 1994, il governo cinese si rese ben presto conto della necessità di porre sotto controllo la circolazione di idee, e due anni più tardi avviò il "Golden Shield Project" o il cosiddetto "Progetto nazionale di sicurezza pubblica delle reti" (Chandel 2019); il Great Firewall dunque è una sotto componente del Golden Shield Project e si riferisce in particolare al complesso insieme di infrastrutture, personale e protocolli informatici utilizzati per bloccare l'accesso da parte degli utenti cinesi verso i siti considerati pericolosi, spesso provenienti da server esteri. Il progetto fu iniziato nel 1996 e dopo diverse fasi di sviluppo fu effettivamente implementato a partire dal 2008. Il sistema in partenza era pensato per bloccare i domini e gli indirizzi IP dei server contenenti siti "da lista nera", ma ben presto le sue capacità furono sviluppate ben oltre; curiosamente alle prime fasi di sviluppo contribuirono alcune aziende occidentali, tra cui l'americana CISCO, un'autorità nel settore informatico. La CISCO infatti contribuì a sviluppare il sistema di monitoraggio automatico delle parole chiave e frasi sensibili che ancora oggi viene utilizzato per individuare il traffico sospetto dentro e fuori il cyber spazio cinese. Assieme al continuo sviluppo e potenziamento delle funzionalità del sistema, gli organi regolatori cinesi si sono occupati di emanare dei regolamenti ferrei (nel 1996, 1998, 2000, 2005, 2017 e 2018) con il fine di diminuire l'anonimato online e di mettere al bando le tecnologie in grado di aggirare il controllo digitale delle informazioni (Chandel 2019). Il Great Firewall è correntemente gestito dall'Amministrazione Centrale del cyberspazio Cinese, ed è una componente fondamentale per la censura interna operata dallo Stato, anche se non l'unica, in quanto si occupa principalmente di impedire l'accesso ai contenuti esterni alla Cina, mentre la sorveglianza del traffico interno cinese ricade sempre sotto il Golden Shield Project, ma viene per lo più fatta ricadere sulla capacità delle aziende e degli ISP di auto-sorvegliarsi e censurarsi, prima ancora di dover utilizzare controlli a tappeto centralizzati.

Il principale meccanismo di funzionamento del Great Firewall è quello dell'"avvelenamento del DNS"; come già spiegato, il DNS si occupa di collegare il nome di un sito web con l'indirizzo IP numerico appropriato, operazione fondamentale per individuare dove la pagina desiderata viene conservata e

per trasmetterla al computer dell'utente. Il firewall cinese si occupa di frapporsi tra i server DNS e l'utente, per fornire informazioni scorrette a quest'ultimo, il sito risulta così irraggiungibile o non presente. Il firewall inoltre controlla che negli URL dei siti non ci siano parole chiave sensibili, conserva una lista di indirizzi IP banditi e all'occorrenza scandaglia i contenuti delle pagine visitate alla ricerca di termini "fuorilegge". Per finire, esso è il motivo per cui alcune tra le più famose applicazioni di aziende occidentali non funzionano in Cina: Facebook, Instagram, Twitter, Google, Telegram, Whatsapp sono tutti bloccati dal firewall perché non forniscono i dati dei propri utenti al governo. La censura effettuata in questa maniera non solo è automatica e capillare (I protocolli automatici che dettano il funzionamento del Great Firewall sono conservati sui nodi di rete principali delle nazione), ma è pensata per nascondersi agli occhi degli utenti meno esperti, camuffandosi da errore di collegamento. Il Great Firewall non è infallibile, infatti uno dei metodi più utilizzati per aggirare il blocco delle informazioni consiste nell'utilizzo delle VPN (Virtual Private Network) cioè applicazioni che sfruttano la crittografia end-to-end, i server proxy (server in altre parti del mondo che fanno rimbalzare i dati mascherandone la provenienza) e l'oscuramento dell'indirizzo IP per creare "tunnel" sicuri di comunicazione. È dunque questo il motivo per cui dal '96 il governo cinese ha emanato numerose leggi per rendere illegali le VPN e le aziende che offrono tali servizi; occorre notare che le VPN sono regolarmente utilizzate anche a livello aziendale, in quanto esse forniscono un livello di protezione aggiuntivo dei dati, è per questo motivo che in ogni caso è stato necessario istituire una lista di aziende fornitrici di VPN autorizzate a commercializzare tale prodotto; il bando delle VPN in Cina non è quindi non è né totale, né completamente efficace: esistono numerose VPN gratuite ed illegale che vengono utilizzate dagli utenti in Cina. Ciononostante risulta sempre più difficile aggirare i controlli del grande filtro cinese, soprattutto se si considera che il Great Firewall è in grado, anche senza poter leggere i dati trasmessi, di riconoscere alcune tipologie di connessioni criptate tipiche delle VPN e di sopprimere il collegamento in toto.

Il Great Firewall in sé non rappresenta solamente uno dei progetti più ambiziosi di controllo del cyber spazio che ad oggi si possono osservare, ma è molto utile per capire con quale tipo di priorità e accezione viene concepito internet in Cina. Il governo si preoccupa e si è sempre più preoccupato di individuare con grande chiarezza i pericoli di carattere ideologico insiti nelle nuove tecnologie digitali e al nuovo spazio virtuale che si è andato creando. I discorsi sulla cyber sicurezza dunque possiedono una dimensione squisitamente politica, dal protezionismo economico alla lotta contro l'evasione della sorveglianza dei dati, temi che sicuramente sono presenti anche nelle discorso pubblico occidentale, ma con la stessa intensità o con gli stessi fenomeni come in Cina. È molto interessante, dal punto di vista della sicurezza informatica, come il Great Firewall non faccia nulla per aumentare la

sicurezza delle reti nazionali contro tentativi di intrusione, diffusione di malware o truffe informatiche, ma che invece ruoti solamente attorno ai pericoli politico-ideologici. Il livello di sicurezza dello spazio virtuale cinese, infatti, risulta alquanto debole e mancante, tanto che permette lo sviluppo di floridi ecosistemi criminali.

L'economia sommersa su internet

Il crescente sviluppo di internet e della sua integrazione nella vita di tutti i giorni ha portato, in Cina così come altrove, opportunità e minacce inedite. Il particolare ambiente di alfabetizzazione digitale ancora troppo scarsa soprattutto in termini di sicurezza, unitamente al vuoto normativo sugli standard di sicurezza diffusi e sul furto della proprietà virtuale, creano le condizioni per un ecosistema illegale sotterraneo particolarmente florido. In Cina si stima che il danno complessivo all'economia locale, solo nel 2011, ammontava a più di 5,36 miliardi di RMB (USD 852 milioni), con un numero di partecipanti al mercato illegale online di circa 90.000 utenti (Lindsay et al. 2015, 88). Dietro a crimini online come furto di profili, furto di credenziali bancarie o dati delle carte di credito, truffe, vendita di strumenti per hacking (malware et simili), si celano vere e proprie comunità organizzate e modelli di business abbastanza definiti.

Le quattro value chain dell'economia sommersa

Il mercato sotterraneo sul web è formato dallo scambio di merci virtuali e servizi tra comuni cittadini, con la caratteristica distintiva di sfruttare metodi illegali di hacking e furto dati per ricavare profitto. La compravendita di beni e servizi (illegali) avviene sul web praticamente alla luce del sole, le due piattaforme più utilizzate da domanda e offerta per incontrarsi risultano infatti essere il social network QQ di Tencent e il forum Baidu Post Bar; i due luoghi di ritrovo virtuale sono utilizzati da un'ampia gamma di utenti e la stragrande maggioranza dei contenuti sono perfettamente legale. Esiste però una minoranza di utenti che utilizza tali piattaforme per scopi illegittimi. Gli utenti di questo tipo postano richieste od offerte utilizzando un gergo criminale conosciuto solo da chi fa parte dell'ambiente criminale (e occasionalmente conosciuto dai ricercatori interessati alle dinamiche del sottobosco criminale su internet). La struttura generale dell'economia underground cinese su internet è organizzata attorno a quattro value chain specializzate, ognuna con funzioni economiche ben precise ma altamente dipendenti una dall'altra.

I quattro tipi di business criminali online si possono dividere in 1) furto di beni (furto di soldi da account bancario carte di credito), 2) furto di risorse virtuali di rete (furto di valute o

equipaggiamenti virtuali da account videoludici online, per venderli in cambio di soldi veri), 3) dirottamento di risorse e servizi di rete (utilizzare a proprio vantaggio risorse internet compromesse, come server e computer in botnet), 4) vendita di tecniche, strumenti o formazione hacker (offerta di strumenti per poter effettuare operazione di hacking). Le quattro value chain sono interdipendenti: la base economica è costituita dagli strumenti di hacking (n°4), siccome sono necessari per effettuare le operazioni illegali su cui si basano le altri catene di valore. Il principale movente dietro al mercato senza ombra di dubbio è l'ampio profitto che si riesce a ricavare dai diversi cyber crimini, in alcuni casi il vuoto normativo riduce persino i rischi in cui si può incorrere facendo questo tipo di cose.

Furto di beni online

Il mercato del furto di beni online è il più florido tra quelli presentati, nonché quello più rischioso per gli esecutori dei cyber attacchi. L'obiettivo di tali attacchi sono gli account bancari, di pagamento online, di investimento finanziario, più precisamente sono le credenziali di accesso a rappresentare il target effettivo. Le operazioni sotto questa categoria sono divise in due fasi, una di penetrazione del sistema di autenticazione e del cambio delle password, un'altra di riciclaggio di denaro per ricavare profitto. I metodi più utilizzati sono i Trojan, phishing, frode telefonica e clonazione della carta di credito. In questa metà della value chain i protagonisti sono gli "scrittori di Trojan" (木马作者), ovvero i produttori dei malware, e i "maestri del materiale" (料主), ovvero chi effettivamente sottrae le informazioni necessarie e prende il controllo dell'account con i soldi. La seconda fase, quella di lavaggio del denaro sporco, consta di diversi tipi di partecipanti; gli "adetti alla pulizia del materiale" (洗料人) possono vendere le informazioni sul mercato nero oppure ingaggiare dei "maestri d'auto" (车主) o "autisti" (车手) incaricati di impersonare la vittima di furto tramite documenti falsi per trasferire o prelevare i soldi dall'account, spesso richiedendo una nuova carta di credito.

Furto di risorse virtuali

Il furto di risorse virtuali va a colpire principalmente il settore del gaming online. Molti tipi di giochi online sono progettati in modo da possedere un particolare sistema di economia interna; i giocatori investendo tempo nel gioco possono guadagnare punti o valuta virtuale che permette loro di comprare risorse di valore interno al gioco stesso: equipaggiamenti, decorazioni, personaggi aggiuntivi etc etc. Questo tipo di risorse virtuali possiedono un effettivo valore anche al di fuori del gioco stesso, siccome i giocatori possono decidere di investire soldi reali per acquistare valuta virtuale (del gioco) a sua volta utilizzata per comprare le risorse di cui sopra. Per la comunità di videogiocatori le risorse di questo genere e le valute dei giochi possono arrivare ad acquisire uno

status di bene di valore vero e proprio. Le operazioni di furto di asset virtuali si suddividono in tre fasi: nella prima i criminali rubano le credenziali di accesso ai videogiochi; le valute e le risorse acquistate da un giocatore sono collegati al suo account. Nella seconda fase, chiamata fase di "lavaggio del pacchetto" (洗信) le credenziali dell'account vengono modificate escludendo il proprietario originale dall'accesso, oppure inviano i beni virtuali ad altri account. Nell'ultima fase si vengono le risorse rubate oppure direttamente l'accesso all'account compromesso in cambio di soldi reali. Per questo tipo di business risulta molto favorevole l'ambiente normativo cinese, siccome cose come account e asset virtuali non sono riconosciuti come beni veri e propri, dunque il rischio che corrono gli hacker in questo campo sono decisamente minori rispetto ad altri genere di crimini online, motivo per cui tale modello di business risulta particolarmente popolare in Cina.

Dirottamento di risorse e servizi di rete

Il dirottamento di risorse di rete per fini illegali non è dissimile da quanto succede in molti altri Paesi. Gli standard di sicurezza non uniformi nel settore commerciale e civile privato permettono la compromissione delle reti e dei computer con il fine di sfruttare la larghezza di banda, lo spazio di archiviazione, la potenza di calcolo, le informazioni sensibili o gli indirizzi IP altrui; in breve la creazione di botnet di supporto ad altri atti criminosi. Questo tipo di value chain è il secondo supporto fondamentale alle attività illegali a scopo di lucro.

Vendita di tecniche, strumenti o formazione hacker

La formazione o gli strumenti per hacking rappresentano il cuore pulsante del sistema di economia sommersa cinese. La comunità hacker fornisce la propria expertise sotto forma di prodotti o servizi. I cosiddetti hacker scoprono vulnerabilità zero day e scrivono malware o altri strumenti di attacco per poi venderli a criminali distribuiti sulle altre value chain. Senza questi prodotti le barriere di accesso al mercato illegale sarebbero significativamente più alte. Alternativamente, gli hacker possono vendere i propri servizi, facendosi assumere temporaneamente per effettuare operazioni di attacco oppure facendosi pagare per della formazione specifica.

Alcuni aspetti del mercato sommerso sul web risultano particolarmente interessanti. Per prima cosa, il mercato risulta in espansione rapida ed allarmante, proprio per la mancanza di interventi atti ad arginare il problema sul lungo termine. Secondariamente lo spettro demografico è piuttosto omogeneo, i partecipanti sono generalmente tutti molto giovani, tant'è che si possono riconoscere chiari cicli di attività annuale, con una maggiore partecipazione degli utenti durante i mesi estivi (quando le scuole sono chiuse) e una minore attività durante i mesi invernali (specialmente durante il

Capodanno cinese e la Festa di Primavera). I partecipanti, inoltre, risultano provenire dalle aree costiere metropolitane, le più sviluppate sia in termini economici che tecnologici. La distribuzione degli utenti attivi in questo particolare settore di economia sommersa rispecchia la divisione geografica della crescita economica che negli ultimi trent'anni ha investito la Cina, con le città costiere notoriamente più ricche e sviluppate in grado di produrre giovani talenti con l'expertise necessaria per avvalersi delle nuove tecnologie per estorcere ingenti guadagni dalle attività illecite online. Il fenomeno degli hacker e della cultura hacker in Cina, in particolare la sua evoluzione nel corso degli anni, è legato a doppio filo con la traiettoria di sviluppo delle tecnologie digitali in Cina e più in generale con gli sforzi governativi per trasformare la Cina in una potenza globale. (Jianwei, Lion , Haixin, Roberts, via Lindsay et al. 2015, 87-114)

Chi sono gli hacker cinesi?

Il 1994 è nuovamente la data cardine per lo sviluppo degli eventi rilevanti alla storia della cultura hacker nel paese di mezzo. Secondo Henderson (Henderson 2007, 11) è tra il 1994 e 1996 che tra i pochi utenti privilegiati in grado di accedere ad internet stavano muovendo i primi passi quelli che poi sarebbero diventati i partecipanti ad alcune delle più famose comunità hacker cinesi. Il periodo di diffusione di una nuova tecnologia all'inizio è sempre caratterizzato da una fase di espansione ed esplorazione, si deve aspettare il 1997 infatti per trovare traccia della prima organizzazione hacker la cui presenza stabile ed in qualche modo strutturata da vita al gruppo chiamato Green Army (绿盟), anche conosciuto come Accademia Whampoa, in onore all'accademia originale fondata nel 1924 per l'addestramento degli ufficiali militari cinesi di Sun Yat-sen e del Partito Comunista Cinese (il tema del nazionalismo sarà centrale per la storia degli hacker cinesi, tuttora i legami tra Stato, esercito e società civile sono un argomento molto dibattuto tra gli osservatori occidentali della Cina riguardo al campo della cyber sicurezza); il gruppo era costituito da giovani studenti di Shanghai, Pechino e dello Shijiazhuan, zone molto ricche che per prime furono interessate dallo sviluppo di infrastrutture e dalla commercializzazione di internet. Un secondo momento fondante della cultura hacker cinese si può individuare nelle rivolte di Jakarta del 1998 quando in Indonesia scoppiarono disordini e proteste in diverse città contro la diffusa corruzione, la situazione economica disastrosa, la carenza di cibo e la disoccupazione. Ad attirare l'ira delle manifestazioni furono principalmente le comunità cinesi residenti in loco (Henderson 2007, 16) (Howlett 2016); a seguito di pesanti incidenti di saccheggio e vandalismo si registrarono moltissime vittime tra la popolazione di origine cinese. Quando le notizie giunsero in patria, l'opinione pubblica esplose per la violenza ingiustificata e si alzarono numerose

voci di protesta, sia per strada sia sul web. L'indignazione e la rabbia collettiva favorirono l'aggregazione spontanea di giovani studenti online, i quali cominciarono a lanciare numerosi attacchi DDoS verso pagine web indonesiane (tramite mail bombing, una tecnica molto basilare di intasamento delle linee di comunicazione) e nei mesi successivi proseguirono con la vandalizzazione di siti governativi e non; i messaggi che comparivano sulle pagine hackerate chiedevano giustizia per le vittime cinesi e denunciavano le violenze delle rivolte. Anche se con il tempo l'indignazione si sgonfiò, ciò che aveva unito gli utenti cinesi, il sentimento di patriottismo, di causa comune e di rivalsa, rimase; da lì a poco sarebbe nata la Red Hacker Alliance (中国红客联盟), una delle più estese e prolifiche comunità hacker cinesi. Se tradizionalmente si era importato il concetto di "**black hat hacker**" (黑客) e "**white hat hacker**" (白客) dall'America (Henderson 2007, 34) (Singer and Friedman 2014, 295), rispettivamente hacker dedito ad attività criminali e hacker impegnato nel miglioramento delle tecniche di difesa informatica, ora in Cina veniva coniato il nuovo termine "red hacker"(红客), ovvero hacker patriottico. Tra il 1998 e il 2004 si assistette alla nascita di altri movimenti spontanei simili: i China Eagle Union, gli NCPH, i Javaphile, gli Honkers sono tutti esempi di comunità online molto eterogenee, ma che condividevano alcune caratteristiche principali: membri giovani, valori comuni, linguaggio gergale semisegreto e approfondita expertise informatica (Henderson 2007, 62) (Howlett 2016). Un'altra caratteristica che accomuna tali movimenti è la prolifica quantità di materiale prodotto sul web, una costellazione di siti internet contenenti informazioni utili per gli aspiranti hacker: nozioni di sicurezza informatica (come penetrare le reti), istruzioni per la produzione e il download di malware (Henderson 2007, 51-57). Molte delle comunità storiche col passare del tempo si sono sciolte, sono state smantellate da crackdown governativi o si sono gradualmente trasformate in imprese commerciali per la sicurezza informatica; non è raro trovare storie di ex-hacker diventati consulenti per cyber sicurezza, probabilmente il mix di età anagrafica e vantaggio di essere dei pionieri delle tecnologie digitali ha permesso a molti dei giovani studenti di commercializzare le proprie competenze in un mercato più legittimo e legale.

Oggi cosa rimane della cultura hacker degli anni '90 e '00? Come già suggerito dall'analisi sull'economia sommersa online, in Cina si può trovare ancora oggi una comunità hacker molto vitale, eterogeneamente composta da criminali e truffatori, ma anche giovani appassionati di informatica, utenti occasionalmente interessati a contenuti illegali fino a professionisti della sicurezza informatica con differenti livelli di legittimità (Lindsay et al. 2015, 192). La tradizione di hacktivism della prima ora ha visto però un declino negli ultimi anni, con un calo drammatico dopo il biennio 2015-2016 (Leyden 2019) le cause del quale vanno ricercato in alcuni fattori economici, tecnologici e politici. Innanzitutto il livello di sofisticazione dei sistemi di sicurezza delle reti industriali, governative e private è

aumentato considerevolmente, le tecniche di attacco diffuse nel periodo di infanzia di internet non richiedevano gli sforzi coordinati, le differenti expertise e le lunghe tempistiche necessarie per le operazioni APT moderne; oggi la penetrazione delle reti di grandi obiettivi, come affrontato nella sezione delle APT nel capitolo 1, è frutto di team di professionisti specializzati in ruoli diversi con un piano di azione scandito su più fasi che possono richiedere mesi di lavoro. In breve, le operazioni nel cyber spazio richiedono maggiori fondi e maggiore professionalizzazione degli operatori, alzando dunque la barriera d'ingresso nel mercato degli attacchi informatici particolarmente lucrosi. Cionondimeno esistono nicchie di mercato illegale incentrate su crimini di più basso livello, come truffe, estorsioni e furto di beni online (come visto sopra); si tratta però per lo più di fenomeni meno risonanti a livello mediatico dei famosi casi di hacktivismo dei primi anni duemila. Un secondo motivo è che i "talenti hacker" oltre ad essere stati assorbiti dal tessuto commerciale privato come professionisti della sicurezza informata, sono stati inglobati in una certa misura dal settore militare, in un più grande processo di ammodernamento ed informatizzazione delle forze del PLA (People's Liberation Army o Esercito di Liberazione Popolare in italiano). In particolare vale la pena di far notare come nel 2015 sono state emanate una serie di leggi per la standardizzazione dell'educazione universitaria nella cyber sicurezza (simile a ciò che è stato fatto negli USA con la "US National Initiative for Cybersecurity Education") per migliorare la filiera di produzione di talenti nel settore. Nel 2017 invece sono iniziati i lavori di costruzione del Centro Nazionale per l'Innovazione e il Talento nel campo della Cyber Sicurezza (国家网络安全人才与创新基地) in Wuhan, lavori che continuano tuttora per realizzare un centro di ricerca in grado di formare 70.000 persone l'anno (Cary 2021, A). Si può dunque dire che il governo cinese, sotto l'egida degli investimenti nel settore della cyber sicurezza, abbia da una parte cercato di de-criminalizzare il pool di giovani talenti versati nella programmazione e nei sistemi di rete, dall'altra abbia cercato di coltivare del personale qualificato per colmare il gap di expertise tecnologica con gli altri Paesi. Infatti la Cina ad oggi se paragonata agli Stati Uniti presenta un deficit pari a 1.4 milioni in termini di personale qualificato in cyber sicurezza, disequilibrio che il governo centrale ha tutto l'interesse a ribilanciare anche per la propria competitività globale con le altre nazioni (Cary 2021, B). Sullo scacchiere internazionale le capacità di difesa e di offesa nel cyberspazio, lo sviluppo di nuove tecnologie e la potenza economica sono fattori critici per ottenere lo status di "superpotenza", obiettivo che la Cina ha deciso di perseguire da tempo ormai. Il cyber spazio oggi non è più quella frontiera tecnologica pregna di novità e "banditismo" che ha fissato nell'immaginario collettivo la figura fantascientifica dell'hacker solitario, bensì è diventato uno dei campi su cui si giocano i delicati equilibri di cooperazione e competizione tra le nazioni del mondo più sviluppato.

Il processo di informatizzazione e acquisizione tecnologica

Come osservazione generale, si può dire l'avvento dell'informatica e di Internet in Cina come altrove fu un potente motore di sviluppo ma anche di rivoluzione dell'industria, della società e del settore militare. La necessità di ammodernare il Paese con le tecnologie digitali fu subito individuata come fondamentale per procedere di pari passo con la crescita della potenza economica e successivamente politica cinese; le tecnologie digitali costituivano il fulcro di un futuro in cui la Cina sarebbe passata da Paese ferito ed arretrato a superpotenza mondiale. Nel 1986 viene rilasciato, internamente al Partito, un programma di ricerca e sviluppo portato a Deng Xiaoping da un gruppo di scienziati nucleari; quello che inizialmente doveva essere un piano di sviluppo militare si mutò velocemente in un più generale percorso di miglioramento tecnologico dell'intero Paese. Il Piano 863 (perché rilasciato nel Marzo del 1986) riguardava il finanziamento di numerose iniziative militari e civili di ricerca e sviluppo, ma come venne poi riportato dall'Intelligence americana, esso forniva supporto economico ed organizzativo a sforzi più o meno clandestini di acquisizione di tecnologia estera e informazioni economiche cruciali per l'ammodernamento delle forze armate cinesi. L'approccio viene descritto da Dave Szady, l'assistente direttore per il controspionaggio dell'FBI, come l'approccio "dai mille granelli di sabbia". Secondo quanto scritto da due ufficiali di intelligence cinesi nel 1991, accumulando un numero abbastanza elevato di informazioni non sensibili, frammentarie, circostanziali, in poche parole informazioni liberamente consultabili e reperibili da molte fonti differenti, si può ricostruire e ottenere conoscenza preziosa (Lindsay et al. 2015, 35). Le risorse più spesso utilizzate in questo periodo consistevano in scienziati cinesi di prima generazione emigrati all'estero (il caso più noto di spionaggio è quello di Wen-Ho-Lee, scienziato nucleare che nel '99 giocò una parte cruciale per il furto di segreti militari americani riguardo le testate nucleari miniaturizzate W-88; Purdy 2001), scienziati e studiosi non cinesi propensi alla libera circolazione di idee in ambito di ricerca scientifica, oppure accademici occidentali in visita in Cina, ma anche le conoscenze e connessioni personali formate dalle aziende di difesa cinesi negli anni. La maggior parte della raccolta di conoscenza tecnologica e scientifica avveniva al di sotto dei radar, attraverso metodi cauti ma efficaci di persuasione, favori personali e corruzione. Tre fattori principali hanno dato maggiore impeto alla campagna di acquisizione di know-how tecnologico ed economico cinese: il successo schiacciante delle operazioni militari americane del 1991 contro Saddam Hussein (operazione Desert Storm; cit. infra cap.1), lo sviluppo di internet e dei metodi di attacco informatico, la crescente forza economica e status globale cinese (Lindsay et al. 2015, 34). Le nuove tecnologie digitali potevano essere utilizzate con grande successo in combinazione con le forze militari per ottenere la

supremazia del campo di battaglia su avversari tecnologicamente meno avanzati; allo stesso tempo esse rappresentarono, per i servizi di intelligence, un salto di qualità in termini di portata ed efficienza degli sforzi di raccolta delle informazioni. Nel 2006 fu presentato il "Piano nazionale a medio e lungo termine per lo sviluppo della scienza e della tecnologia (2006-2020) " o "MLP". Al suo interno si poteva trovare la descrizione dei suoi intenti generali: migliorare l'innovazione originale tramite co-innovazione e re-innovazione basata sull'assimilazione di tecnologie importate; in pratica il MLP verrà visto da alcuni analisti più tardi come una mappa dei futuri sforzi di spionaggio industriale ed economico su scala mondiale da parte della Cina. Negli anni successivi al rilascio del piano si assistette ad un aumento dei casi di cyber spionaggio cinese, molti degli obiettivi inoltre coincidevano con i settori industriali esplicitamente identificati nel MLP come critici per lo sviluppo tecnologico (Lindsay 2015, 57).

In conclusione, si può notare che la Cina dagli anni '90 abbia individuato come cruciale la necessità di ammodernarsi e chiudere il gap che la separava dalle potenze industriali ed economiche dell'Occidente. I diversi piani di sviluppo includevano, volente o nolente, l'appropriazione di tecnologia estera dai Paesi più sviluppati per rafforzare i settori considerati cruciali per il futuro della Cina. Sebbene una buona parte di trasferimento di sapere tecnologico è avvenuto tramite acquisizioni commerciali perfettamente legali e collaborazioni di ricerca accademica alla luce del sole, è innegabile che si possa tracciare uno storico di operazioni di spionaggio economico quantomeno caldeggiate se non direttamente addirittura organizzate dalle autorità centrali. In questo contesto di acquisizione tecnologica l'arrivo di internet e delle tecnologie informatiche ha rappresentato un "salto di qualità" delle operazioni di raccolta informazioni. I dati di R&S conservati su server aziendali e universitari, i collegamenti alla rete globale e le capacità di analisi dei computer hanno reso gli attacchi informatici non solo particolarmente comodi da eseguire ma anche estremamente fruttuosi. Si può dire, con una certa cautela, che nella narrazione mediatica della Cina come grande "pirata" di know-how tecnologico/industriale, c'è del vero. Ciononostante gli autori Lindsay e Cheung (in Lindsay et al. 2015, 51-56) offrono un importante caveat per rispondere a chi cerca di fare dell'allarmismo riguardo al pericolo e alla gravità dello spionaggio cinese: raccolta di informazioni non equivale a capacità di innovazione. Per prima cosa, sostengono i due autori, molta della conoscenza che permette ad un'azienda di operare in maniera competitiva sul mercato non passa attraverso documenti scritti; tutta la conoscenza di come far girare gli ingranaggi interni di un business, il capitale umano rappresentato dai dipendenti, insomma tutta la conoscenza tacita di settore non passa sui server aziendali o di ricerca. Secondariamente, per sfruttare al meglio le grandi masse di dati rubati la filiera di digestione delle informazioni dev'essere coordinata e ben strutturata: data la

frammentarietà dell'effettiva governance dei territori della Cina, sembra improbabile ci sia un'elevata coordinazione e capacità sistematica di raffinazione delle informazioni sottratte, per lo meno su scala nazionale. Infine, sul lungo termine, l'innovazione necessita di risorse e capacità indigene, se la Cina continuasse a puntare solo su ciò che proviene dall'Occidente si condannerebbe ad un'eterna sudditanza scientifico-tecnologica nei confronti di quest'ultimo.

Cionondimeno, rimane innegabile che numerose operazioni di spionaggio sono state portate avanti dal gigante asiatico, ed una parte di esse è stata organizzata, finanziata ed eseguita dal governo stesso; oggi è possibile ricostruire con una ragionevole certezza chi si cela dietro le maggiori operazioni di spionaggio nel cyberspazio.

Cyber spionaggio ed esercito cinese

Il trend di evoluzione delle tipologie ed operazioni di spionaggio tramite internet indica una sempre maggiore professionalizzazione delle tecniche e tattiche dei gruppi coinvolte; inoltre parallelamente agli obiettivi industriali, si è registrata una maggiore attenzione verso target politici e governativi, il che aiuterebbe ad individuare una connessione tra le APT e il governo centrale cinese. Non ultimo, la Cina non è l'unico Paese ad aver cominciato a trasportare i conflitti politici e internazionali nel cyber spazio, l'America ne è un chiaro esempio. Ciononostante in diversi casi di risonanza internazionale sono stati tracciati collegamenti quantomeno sospetti con la RPC, in alcune istanze anche piuttosto evidenti: indirizzi IP, tracce di codice e parole chiave in lingua cinese, obiettivi di alto interesse per il PCC (es. Taiwan, Tibet, dissidenti cinesi). Gli attori protagonisti delle operazioni di spionaggio sono presumibilmente un insieme di dipartimenti militari in collaborazione con aziende private di cyber sicurezza, università più o meno direttamente affiliate con l'esercito ed occasionalmente hacker di alto livello. Il processo di informatizzazione generale descritto sopra, ha effettivamente portato alla creazione di dipartimenti specializzati in sicurezza, intercettazione e sfruttamento delle reti.

Perché i reparti militari cinesi sono sospettati di giocare un ruolo centrale nelle operazioni di cyber spionaggio? Innanzitutto perché la difesa delle reti nazionali è ormai diventata una priorità al pari della difesa degli spazi arei e marittimi di una nazione, in tutto il globo. Secondariamente, essere esperti di difesa delle reti significa necessariamente conoscere anche come esse si possono penetrare, disabilitare o manomettere. In terzo luogo, come già citato, alcuni casi di cyber spionaggio ruotano attorno a tematiche od obiettivi di particolare interesse per la Cina, ovvero per le autorità centrali, che si appoggiano all'esercito per realizzare gli obiettivi e gli interessi del Paese. Infine, nella

dottrina militare cinese, secondo gli esperti, le tecnologie digitali sono viste come “proiettile magico” utile a ridurre il divario di potenza tra le forze estere (i.e. America) e quelle cinesi. Secondo la teoria del “Unrestricted Warfare”, contenuta nel libro pubblicato nel 1998 infatti, i Colonnelli Liang Qiao e Wang Xiangsui identificano nell’eccessiva dipendenza delle forze armate dai sistemi di rete ICT (i.e. computer), il tallone d’Achille dell’esercito americano. Come citato nel capitolo 1, man mano che le catene di comando, le armi intelligenti e la logistica militare aumentavano la complessità dei propri sistemi, facendo sempre più affidamento sulla tecnologia digitale, aumentava di pari passo il potenziale distruttivo di un attacco disabilitante ai loro sistemi informatici. Le operazioni nel cyber spazio vengono dunque viste dai teorici militari cinesi come possibili “Assassin’s Mace”(杀手), ovvero strumenti per ottenere un vantaggio cruciale nello scontro con forze armate di potenza superiore, un modo dunque per riequilibrare un confronto asimmetrico in modo “semplice” (Lindsay et al. 2015, 139). Un esempio di ciò che si intende con questo concetto può essere chiarito dai fatti di cronaca del 2009: a seguito della cattura di un gruppo di ribelli in Iraq da parte dei soldati americani, questi ultimi scoprirono che sui laptop dei guerriglieri si trovavano ore e ore di filmati di sorveglianza effettuati dalle forze USA tramite droni senza pilota. I guerriglieri, tramite un software illegale utilizzato per piratare la TV satellitare da 25,99 dollari, erano riusciti ad intercettare i dati della sorveglianza aerea di droni dal valore di 45 milioni di dollari (Singer and Friedman 2014, 151). A fronte di un nemico soverchiante in termini di potenza militare, l’utilizzo scaltro delle tecnologie digitali ha permesso alla controparte meno tecnologica di avere una leva per ottenere un vantaggio cruciale. Le strategie di guerra informatica sono quindi entrate a far parte della dottrina militare cinese da molto tempo ormai.

Stoke in Lindsay (Lindsay et al. 2015, 163-177) ripercorre la struttura interna al PLA con il duplice scopo di individuare il potenziale per operazioni nel cyberspazio del PLA e per ricostruire l’organizzazione dei dipartimenti che potrebbero essere in grado di compiere incursioni informatiche nelle reti di altri Paesi. Non sempre esistono prove schiaccianti del coinvolgimento del PLA o di altre organizzazioni cinesi, va per tanto preso con cautela e buon senso il ragionamento presentato di seguito; quelle che vengono fornite sono ragionevoli ipotesi e collegamenti possibili con il fine di fornire un quadro informativo più completo e utile per un possibile approfondimento, e non di lanciare accuse o dipingere in maniera negativa sull’operato della Cina; ogni Paese sviluppato possiede simili dipartimenti ed è impegnato in attività di spionaggio sia online che offline.

Organizzazione interna del PLA e le operazioni nel cyber spazio

L'infrastruttura di supporto alle operazioni informatiche si appoggia molto presumibilmente su tre dipartimenti: il "General Staff Department" (GSD), il "GSD Third Department" (3/PLA) e il "GSD Fourth Department" (4/PLA); esistono altri sospettati, ma i tre sopra elencati sono i candidati più papabili.

Il GSD è uno dei quattro dipartimenti che fanno capo alla Commissione Militare Centrale, massima autorità dell'esercito cinese. Il GSD è il cuore pulsante del PLA (People's Liberation Army), ne indirizza le decisioni in termini di policy, piani, programmi, inoltre si occupa di allocare le risorse di supporto alle missioni operative. Tra le responsabilità del GSD ricadono anche le operazioni di intelligence, l'addestramento e la mobilitazione delle truppe, la diplomazia militare e la sicurezza dei vertici di Partito e dello Stato. Il GSD comprende una burocrazia ampia e complessa composta da un ufficio generale e almeno dodici dipartimenti di secondo livello e uffici subordinati (Lindsay et al. 2015, 161-177).

Il 3/PLA, anche conosciuto come il "Technical Reconnaissance Department", tradizionalmente ha tra le sue competenze di base la SIGINT (intelligence dei segnali: informazioni ottenute tramite l'intercettazione di segnali radio, wifi, satellitari…), la computazione avanzata ad alte prestazioni e le attività di crittografia/de-crittografia, dunque anche della sicurezza delle reti nazionali cinesi; può essere paragonata alla "National Security Agency" (NSA) americana. Ad oggi il 3/PLA gestisce la più grande infrastruttura di raccolta di informazioni e di sicurezza informatica del mondo. Il compito principale del dipartimento è quello di impedire l'accesso da parte di Paesi stranieri alle preziose informazioni di sicurezza nazionale del Paese, si crede però che oltre alle funzioni ufficialmente riconosciute, il 3/PLA congiunga le funzioni di difesa e di attacco delle reti informatiche soprattutto per perseguire gli obiettivi e gli interessi del Partito, il termine di "technical reconnaissance" può essere visto in questo caso come un eufemismo per "guerra informatizzata", siccome ogni operazione di cyber attacco organizzato inizia sempre con una fase di ricognizione, come è già stato presentato nella sezione delle APT. Il 3/PLA è composto, a livello di organizzazione interna, da un quartier generale con sede a Pechino, dal "Beijing North Computing Centre", da tre istituti di ricerca e un polo ingegneristico, oltre che da dodici dipartimenti operativi.

Beijing North Computing Centre

Il “Beijing North Computing Centre” (BNCC) è composto da dieci divisioni operative. Ufficialmente un centro per lo sviluppo di sistemi di difesa delle reti nazionali, le funzioni del BNCC sono coperte da un velo di segretezza. Il centro si sospetta abbia giocato un ruolo centrale in alcuni case di attacco informatico come quello del 2000 nei confronti dei siti web del movimento Falun Gong (Minhui 2000). L’ipotesi, secondo le ricerche di Stokes (via Lindsay et al. 2015, 161-177) è che il centro svolga le funzioni di controllo e comando di sistemi infettati, si occupi di rotture del codice dei sistemi di sicurezza, sia un centro per lo sviluppo di malware avanzati e funga anche da deposito dati rubati. L’ipotesi sarebbe rinforzata anche dal fatto che i suoi ufficiali abbiano tutti una formazione in attacco e difesa informatica, intrusione e sorveglianza delle reti e raccolta di intelligence; gli ingegneri in posizioni di senior sono stati impiegati dallo “State Council Information Office” (il dipartimento responsabile per il controllo interno della censura e delle informazioni che circolano su internet, per chiarire) come consulenti. Il BNCC oltre ad aver sviluppato il più avanzato sistema di individuazione delle intrusioni e di valutazione delle vulnerabilità informatiche della Cina, si pensa abbia anche contribuito allo sviluppo dei primi “Remote Access Tools” (RATs), i malware trojan utilizzati in alcune delle operazioni attribuite al Paese asiatico (Shady RATs operation); si suppone inoltre che il centro sia utilizzato come piattaforma di supporto e collaborazione con le istituzioni accademiche e le aziende di sicurezza informatica nelle occasioni di collaborazione con l’esercito.

I centri di ricerca e il poli ingegneristico NISEC

Tra le sedi di ricerca e sviluppo interne alle forze militari cinesi del 3/PLA se ne possono individuare alcune che sono direttamente coinvolte con attività di supporto alle operazioni informatiche. Il 56esimo Istituto di Ricerca per esempio è diretto da un membro del gruppo di lavoro che si occupa di Software e Computing del programma 863 (spionaggio industriale, vedere sopra); il 57esimo Istituto di ricerca invece ha come aree di ricerca l’intercettazione delle comunicazioni e l’elaborazione dei segnali. Il 58esimo Istituto di ricerca effettua R&S su crittografia e cyber sicurezza, e ha stretti legami con il Primo Dipartimento del 3/PLA. Il “National Information Security Engineering Technology Center”(NISEC) è un polo ingegneristico nato nel 2001 a Shanghai, il cui direttore è anch’egli parte di un gruppo di lavoro impegnato nella Sicurezza Informatica del programma 863 (implicato tra le altre cose anche nell’implementazione del progetto “Golden Shield”, il firewall cinese nazionale e in due commissioni per la standardizzazione delle regole di Cyber sicurezza nel Paese, chiamate WG3 e WG7).

I dipartimenti operativi

Il Primo Dipartimento del 3/PLA, conosciuto anche come Unità 61786, ha come sede il complesso di comando sito nella parte Nord Ovest di Pechino. Il dipartimento è una delle autorità massime in fatto di operazioni informatica e sicurezza delle reti, sovrintende almeno dodici uffici differenti sparsi in tutta la Cina ed un centro di ricerca sulla sicurezza informatica. I compiti principali del dipartimento includono crittografia/decrittografia e altre operazioni di protezione e sicurezza. Il Primo Dipartimento è uno degli unici rappresentanti militari ufficiali inclusi nei gruppi di lavoro del programma 863.

Il Secondo Dipartimento, anche conosciuto come Unità 61398, è divenuto famosa nell'ambito (della sicurezza informatica) proprio grazie alle indagini dell'azienda di cybersicurezza Mandiant che nel 2013 ha un voluminoso report di 60 pagine sulle attività di spionaggio industriale e politico del gruppo APT-1, i cui IP hanno permesso di risalire agli uffici dell'unità 61398 del PLA, prima che fossero sgomberati in tutta velocità a seguito della pubblicazione sui giornali americani delle foto degli stabilimenti (Sanger et al. 2013). Le operazioni di raccolta di intelligence economica, politica e militare venivano condotte dagli uffici siti nel distretto Gaoqiao, nella parte Nord Est di Shanghai. La cellula militare ha avuto rapporti stretti con la Scuola di Ingegneria della Sicurezza Informatica della Jiaotong University di Shanghai, ovvero una delle università che tuttora ha la fama di produrre giovani talenti hacker per l'esercito. A tal proposito, non è raro trovare menzione dei legami che uniscono il sistema accademico con il PLA; secondo le ricerche di Sheldon e Mcreynolds (in Lindsay et al. 2015, 192) esistono diversi programmi atti a finanziare centri universitari e istituti di ricerca, in particolare hanno individuato almeno 46 università cinesi destinatarie di fondi per programmi di ricerca legati alla tecnologia per operazioni di guerra informatica. Secondo un report piuttosto recente (Dakota 2021; c), diverse università che attualmente stanno sviluppando programmi di ricerca sull'intelligenza artificiale finalizzata alla cyber sicurezza e, presumibilmente, alle applicazione di attacco informatico. Il sospetto è corroborato dal fatto che sei di queste università risultano avere legami con APT conosciute, come mostrato nella figura 8. In aggiunta, eventi come quello del "Tianfu Hacking Contest" mostrano come, in competizione con esperti internazionali di cyber sicurezza, i professionisti cinesi non hanno nulla da invidiare agli altri Paesi in termini di capacità di penetrazione delle reti e dei software (Tarabay 2021).

Il Terzo Dipartimento del PLA (unità 61785) svolge funzioni piuttosto standard di sorveglianza e difesa delle reti, è notevole il fatto che il dipartimento abbia condotto diversi studi sul cyberwarfare, incluso un'analisi approfondita sulle vulnerabilità dei sistemi operativi Android e dei sistemi di rete

locale di Windows. I membri del dipartimento si crede abbiano eseguito studi congiunti con il dipartimento di Scienze Informatiche e Ingegneria della Shanghai Jiaotong University.

La missione del Settimo Ufficio (Unità 61580), con sede nell'area di Shucun nel distretto di Haidian nord-ovest di Pechino, non è chiara. Gli ingegneri selezionati dell'ufficio sono specializzati nella difesa e nell'attacco della rete di computer e hanno condotto studi congiunti con la sezione Attacco e difesa della rete di computer della PLA Information Engineering Academy.

Figura 8 (Cimpanu 2021)

Institution's Name in English	Institution's Name in Mandarin	Affiliated APTs	Cybersecurity Courses Include AI/ML?	Individual Professors Researching AI/ML and Cybersecurity?	US Government BIS Entity List[14]
Hainan University	海南大学	APT40	Unknown	Yes	No
Southeast University	东南大学	Deep Panda	Yes	Yes	No
Shanghai Jiao Tong University	上海交通大学	APT1	Yes	Yes	No
Xidian University	西安电子科技大学	APT3	Yes	Yes	No
Zhejiang University	浙江大学	APT1	Yes	Yes	No
Harbin Institute of Technology	哈尔滨工业大学	APT1	Unknown	Yes	Yes

Oltre alle divisioni del 3/PLA che si crede possano essere state coinvolte in operazioni di APT di spionaggio, anche il 4/PLA potrebbe ricadere tra i sospetti; Il Quarto Dipartimento è responsabile

dello sviluppo di tecnologia radar e delle contromisure elettroniche (ECM). Le priorità sembrano includere il disturbo dei satelliti e sorveglianza radar anti-camuffamento.

In conclusione la Cina, come moltissimi altri Paesi negli ultimi anni, ha messo in cima alla lista delle proprie priorità lo sviluppo delle capacità di cyber difesa e offesa, tramite piani di policy nazionali come il programma 863 e il piano MLP 2006-2020, che però includevano tra le operazioni di acquisizione di know-how tecnologico anche vere e proprie campagne di spionaggio industriale informatico. Il particolare percorso storico di trasferimento di conoscenza economica, scientifica e tecnologica verso la Cina, unitamente ad alcuni casi di risonanza mediatica di attacchi informatici attribuiti al Paese (tabella 9), hanno contribuito a formare una fama (negativa) di nazione esportatrice di attacchi hacker. In realtà, la Cina risulta avere un livello di sicurezza informatica interna piuttosto insufficiente, per non parlare delle cifre che mostrano come faccia parte dei Paesi più sottoposti ad attacchi informatici (Lindsay et al. 2015, 3). Cionondimeno, la Cina possiede capacità di spionaggio e guerra informatica, individuate nei diversi componenti del PLA che possiedono strutture, expertise e interesse nell'effettuare operazioni di attacco in rete. L'ipotesi che le autorità militari cinesi abbiano la volontà di sfruttare i mezzi digitali in vista di scontri geopolitici, viene rafforzata dall'analisi della dottrina militare cinese, per cui le tecnologie digitali ben si applicherebbero ad un approccio di guerriglia e di scontro asimmetrico descritto al concetto di "Unrestricted Warfare" (Hagestad, 2012, 60) (Lindsay et al. 2015, 42). L'esercito sembra inoltre ad approvvigionarsi in termini di giovani talenti tramite diverse istituzioni accademiche i cui sforzi di ricerca riguardano la cyber sicurezza e le reti, università che occasionalmente sono state collegate a gruppi di APT conosciuti e a programmi di borse di studio e finanziamento provenienti dall'esercito stesso. Il PLA non collabora solo con le realtà universitarie, ma anche con aziende private di sicurezza informatica.

Tabella 9 (Lindsay et al. 2015, 58)

PUBLICLY REPORTED INTRUSIONS ATTRIBUTED TO CHINA				
Intrusion	Active	Report	Targets	Significance
Titan Rain	2003.09	2005.08	US defense orgs and national labs	First public indication of methodical state-sponsored
State Dep	2006.06	2006.07	US State Dept., US Embassy Beijing	Targeted Bureau of East Asian and Pacific Affairs; embassy lost connectivity for 2 weeks

US BIS	2006.07	2006.10	US Commerce Dept.	Bureau of Industry and Security that regulates US export license; attributed to PRC
US NWC	2006.11	2006.11	US Naval War College	PRC APT prompts NWC to shut down network
US Sec Def	2007.06	2007.09	Computers in the office of US sec. defense Gates	Cabinet-level CNE with confident attribution to PLA
Enfal	2006	2007.12	US NGOs, defense, govt	Linked to Byzantine Haydes
Ghost Net	2007.05	2009.03	Govts., firms in 103 countries; Dalai Lama	First detailed public report on APT methods; interaction with cybercrime ecosystem
F-35 JSF	2007.10	2009.04	BAE, Lockheed-Martin, Northrop-Grumman	APT compromised nonclassified data on F-35, monitored meetings and technical discussions
Aurora	2009.07	2010.01	Google and 34 other firms; dissident Gmail accounts	Prompted Google's exit from PRC and Sec. State Clinton's Internet freedom speech
Shadows in the Cloud	2009.01	2010.04	US, UK, India, SE Asian govts. and firms; UN	Exploits of cloud-hosted social media; classified information exfiltrated
Byzantine Haydes	2002	2010.12	US Defense, State, Energy; IMF, World Bank; international firms, NGOs	US code name for PLA intrusions; subsets Byzantine Candor/ Foothold/Anchor cover particular PLA APT actors
Night Dragon	2009.11	2011.02	Multinational firms in the oil/energy sector	Oil exploration, bidding, and control system data lost to technically unsophisticated attack

Shady RAT	2006.07	2011.08	71 govt., corporate, NGO orgs. in 14 countries (mainly US); ASEAN	Targets of interest to PRC including Intl. Olympic Committee and WADA prior to 2008 Beijing Olympics; probably APT1
Lurid	2011.06	2011.09	Russia, CIS, Tibetan targets	Related to previous Enfal Trojan campaigns
Luckycat	2011.06	2012.03	Defense and commercial firms, Tibetan activists	Linked to hacker working with students at Sichuan Univ. Information Security Institute
Ixeshe	2009.07	2012.05	East Asian govts., IT firms, German telecoms	Highly targeted, leveraging internal C2 servers, attribution unclear but suggests PRC
Elderwood, (Sneaky Panda)	2009.07	2012.09	Defense, manufacturing, human rights NGOs	Sophisticated Beijing-based APT group; used at least 8 zero-day exploits; multiple attack vectors; includes Aurora/Google hack
US News Media	2012.10	2013.01	NY Times, Washington Post, Wall Street Journal	Targeted journalists covering PRC leaders, politics, and business (e.g., Huawei and ZTE)
APT-1 (Comment Crew	2006	2013.02	141 English-speaking firms in 15 countries	Most detailed public attribution evidence to PRC to date, exposes Shanghai-based PLA GSD 3rd Dept., 2nd Bureau (Unit 61398)
Beebus, Mutte	2011.04	2013.02	Aerospace, defense, telecom in US, India	Focus on drone technology and South Asia politics; linked to APT-1

Telvent	2007	2013.05	Telvent/Schneider Electric	Prime evidence of Obama 2013 State of the Union claim of hackers in the power grid, likely PRC industrial espionage vice attack planning
Safe	2012.10	2013.05	Govt., NGOs, media, firms, academia	Author identified: professional engineer in PRC with access to ISP code repository
SCADA Honeypot	2012.12	2013.08	Decoy water control systems in 8 countries	APT1 lured into exploiting mock-up plant controls; demos interest in US SCADA
G-20	2013.05	2013.08	G-20 govt. and financial institutions	Traced to APT-12 (aka Calc Team) responsible for US news media intrusions
Hidden Lynx	2009	2013.09	100s of firms, focusing on financial services and defence industry	Highly skilled APT, concurrent campaigns, regular zero-day usage, sizable infrastructure, linked to Aurora, potentially "hackers for hire

Capitolo 3

Termine Cinese	Definizione Cinese	Definizione Italiana	Termine Italiano
高级持续性威胁 Gāojí chíxù xìng wēixié	**高级持续性威胁**，针对特定组织所作的针对性客制化的的网络持续性攻击，可能持续几天，几周，几个月，甚至更长的时间。（有道词典）	Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle infrastrutture IT del target. (CISRT 2019)	Advanced Persistent Threat (APT)
算法 Suànfǎ	**算法**是一系列解决问题的清晰指令。（有道词典）	Procedimento che consente la risoluzione di problemi di carattere logico e matematico, o pratico. (CISRT 2019)	Algoritmo
防毒软件 Fángdú ruǎnjiàn	**杀毒软件**，也称反**病毒软件**或**防毒软件**，是用于消除电脑病毒、特洛伊木马和恶意软件等计算机威胁的一类软件。（有道词典）	Software che riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli. (Treccani)	Antivirus
抗毒软件 Kàng dú ruǎnjiàn	（有道词典）		Antivirus
防毒软件 Fángdú ruǎnjiàn	（有道词典）		Antivirus
防毒软件 Fángdú ruǎnjiàn	（有道词典）		Antivirus
暴力破解攻击 Bàolì pòjiě gōngj	**暴力破解攻击**是一个自动化试验的过程，用于 web应用程序安全漏洞挖掘的研究 猜测用户名、密码、信用卡号或者密钥。（有道词典）	Metodo di risoluzione di un problema dato mediante l'impiego di un algoritmo che consiste nel verificare tutte le soluzioni teoricamente possibili fino a quando non si trovi quella effettivamente corretta. Nell'ambito informatico, questo metodo si utilizza soprattutto per individuare le password di accesso a un sistema. (CSIRT 2019)	Attacco Brute Force
搜索结果 Sōusuǒ jiéguǒ	**字典攻击**：首先使用用户提供的口令文件进行字典查找称为字典攻击.它对字典中的所有单词进行hash并与用户的口令hash进行比较。（有道词典）	Tecnica di brute force verso un cifrario o sistema di autenticazione, in cui l'attaccante impiega un "dizionario", ossia un insieme predefinito di stringhe aventi un'alta probabilità di successo. Solitamente i dizionari sono composti da un elenco di parole o stringhe di uso comune. Al fine di contrastare tale attacco, è consigliabile non utilizzare password ampiamente diffuse o già utilizzate altrove per chiavi crittografiche o credenziali di accesso. (CSIRT 2019 2019)	Attacco Dizionario

中间人攻击 Zhōngjiānrén gōngjí	**中间人攻击**：一种攻击形式，在这种攻击中，攻击者会秘密干预软件或计算机系统以拦截、捕获、更改或重播通信双方的信息。攻击者利用 MITM 攻击来捕获一方发送给另一方的信息。（ICANN）	Quando un utente malintenzionato reindirizza il traffico Web di una vittima (magari modificando le impostazioni DNS o modificando il file hosts sul computer della vittima) a un sito Web contraffatto. La vittima crede di essere collegata al sito web della propria banca e il flusso di traffico da e verso il sito della banca reale rimane invariato, quindi la vittima non vede nulla di sospetto. Tuttavia, il traffico viene reindirizzato attraverso il sito dell'attaccante, consentendo all'attaccante di raccogliere tutti i dati personali inseriti dalla vittima (login, password, PIN, ecc.). (Kaspersky)	Attacco man-in-the-middle
后门 Hòumén	**后门**是指一种绕过安全性控制而获取对程序或系统访问权的方法。	In un sistema informatico, un punto d'accesso secondario: conoscendolo, è possibile entrare nelle risorse di basso livello del computer. (Zanicchelli)	Backdoor
黑帽黑客 Hēi mào hēikè	**黑帽黑客**，也就是骇客（cracker），即闯入计算机系统或网络系统者。这种说法缘于美国早期西部片以白帽和黑帽区分正邪双方。（有道词典）	Black hat hacker, chi violi illegalmente sistemi informatici con o senza vantaggi personali. (Treccani)	Black Hat Hacker
逻辑炸弹 Luójí zhàdàn	**逻辑炸弹**，是写入计算机的指令程序，在符合特定条件时进行破坏或窃取信息。（有道词典）	Bomba logica loc. s.le f. Software scaricato dall'utente sul proprio computer in modo inconsapevole, che si può attivare a orologeria o in concomitanza con la presenza di altri file e che riesce a bloccare il sistema o a innescare operazioni dannose. (Treccani)	Bomba Logica
僵尸网络 Jiāngshī wǎngluò	**僵尸网络**：被一程序感染的计算机网络，该程序接收程序创建者指令，向互联网大量主机发送不请自来的邮件、攻击网络等（有道词典）	Botnet s. m. o f. Rete di computer collegati alla rete telematica che passano sotto il controllo di un'unica entità, diventando possibili oggetti di contagio da parte di virus informatici. (Treccani)	Botnet
浏览程序 Liúlǎn chéngxù	**浏览程序，浏览器**：用于在互联网上查阅信息。（有待词典）	Browser: in informatica, programma applicativo che permette di accedere in sequenza a informazioni d'interesse, disponibili nella memoria dell'elaboratore o di altri elaboratori a esso connessi. I b. (detti anche navigatori) hanno assunto grande rilevanza nella tecnologia della rete Internet, dove hanno lo scopo di garantire un'elevata possibilità di interazione fra le differenti piattaforme tecnologiche (Treccani)	Browser
浏览器 Liúlǎn qì	（有道词典）		Browser

缓存溢出 Huǎncún yìchū	**缓存溢出：** 攻击使得程序或者系统的操作存储机制（缓存）过载，在该状况下，程序或者系统会允许黑客做一些原本不可以做的事情。（有道词典）	Un errore in un programma informatico che si verifica quando si tenta di posizionare un blocco di dati in memoria che supera la quantità di spazio allocato per esso. L'overflow del buffer può essere sfruttato per eseguire un attacco denial of service (DoS) o eseguire codice arbitrario su un dispositivo. In quest'ultimo caso, viene eseguito uno script dannoso al posto di e con gli stessi diritti dell'applicazione il cui spazio è stato attaccato. (Kaspersky)	Buffer overflow
密钥 Mì yào	**密钥**是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥分为对称密钥与非对称密钥。（有道词典）	Chiave in crittografia, elemento utilizzato nella cifratura di un messaggio per la trasformazione di un testo in chiaro in testo cifrato. È l'informazione che determina le caratteristiche dell'algoritmo crittografico utilizzato nella cifratura; solo la conoscenza di tale informazione permette la decodifica del messaggio cifrato di crittografia. (Treccani)	Chiave (crittografia)
USB解密盘 jiěmì pán	**USB闪存盘**，简称**U盘**，根据谐音也叫**优盘**，几乎是人手一件的必备微型高容量移动储存工具。（有道词典）	Nel linguaggio dell'informatica, supporto di memoria rimovibile che può essere collegato a una porta USB (il suo nome deriva dalla somiglianza con alcuni dispositivi di protezione hardware presenti in alcuni programmi applicativi); è detto anche penna, pennetta, penna USB o pen-drive. (Treccani)	Chiavetta USB
U盘 Pán	（有道词典）		Chiavetta USB
优盘 Yōupán	（有道词典）		Chiavetta USB
二进制代码 Èrjìnzhì dàimǎ	所谓**二进位码**是指资料的型态只有0或1两种。（有道词典）	Còdice binàrio Codice basato su due soli simboli, usualmente 0 e 1. Un c.b. permette la trasmissione di dati e istruzioni mediante una sequenza di 0 e 1, che può essere realizzata con un circuito formato da un dispositivo capace di assumere due stati diversi di tensione (tipicamente acceso e spento). (Treccani)	Codice Binario
计算机网络战 Jìsuànjī wǎngluò zhàn	**计算机网络战**是现代战争中重要作战样式，网络战是信息战的重要组成部分，分布式、网络化的计算机系统是信息作战中实施攻击与防护首要作战目标。（有道词典）	Computer Network Warfare; una competizione tra due sistemi di comando operativi opposti, condotta all'interno del dominio delle reti informatiche per la supremazia delle informazioni, degradando o distruggendo le reti di un nemico e la sua capacità di condurre operazioni. (Tradotto dall'Inglese) (Lindsay et al. 2015, 140)	Computer Network Warfare

加密 Jiāmì	**加密**，是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。（有道词典）	Crittare (o criptare) v. tr. [der. del gr. κρυπτός «nascosto» con influsso del fr. cryptage «crittografia»]. – In informatica, e più genericam. in elettronica, attribuire un codice particolare a un messaggio sonoro o visivo, nel momento della trasmissione, in modo da renderlo inintelligibile a chiunque non sia in possesso di un decodificatore appropriato dotato dello stesso algoritmo usato dalla fonte di trasmissione: programma televisivo crittato, con immagini offuscate o distorte in modo da non essere chiaramente visibili (come invece sono i programmi cosiddetti «in chiaro»). (Treccani)	Crittare o Criptare
密码术 Mìmǎ shù	**密码术**是研究如何使用这蝗算法来保证系统和协议的安全。（有道词典）	Crittografia; Treccani (Bongiovanni 2004); "La crittografia (...) è la disciplina che si occupa di studiare le tecniche per trasformare un messaggio, detto 'testo in chiaro', in un altro messaggio, detto 'testo cifrato', che risulta incomprensibile a chiunque non conosca tutti i dettagli della tecnica usata per la trasformazione." (Treccani)	Crittografia
非对称加密 Fēi duìchèn jiāmì	**非对称式加密**就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为"公钥"和"私钥"，它们两个必需配对使用，否则不能打开加密文。 （有道词典）	I sistemi di crittografia utilizzati con risorse informatiche si suddividono in algoritmi a chiave privata (o simmetrica) e algoritmi a chiave pubblica (o asimmetrica). Negli algoritmi a chiave pubblica, ideati negli anni Settanta del secolo scorso, una parte della chiave può essere liberamente divulgata; in tal modo viene risolto il problema della distribuzione delle chiavi attraverso canali non sicuri come la rete Internet. (Treccani)	Crittografia asimmetrica
端到端加密 Duān dào duān jiāmì	**端到端加密** 是指一个完整的数据保护，其在网络的两个点之间流动 （有道词典）	Il trasferimento di un messaggio crittografato attraverso un sistema senza fasi intermedie di decrittografia e ricrittografia. (Tradotto dall'Inglese) (Oxford Reference)	Crittografia end-to-end
对称加密 Duìchèn jiāmì	**对称加密**是一种传统的密码体制，其加密和解密用的是 相同的密钥，即加密密钥和解密密钥是完全相同和等价的。（有道词典）	I sistemi di crittografia utilizzati con risorse informatiche si suddividono in algoritmi a chiave privata (o simmetrica) e algoritmi a chiave pubblica (o asimmetrica). Nei primi, la chiave da applicare all'algoritmo è la stessa per il mittente e per il destinatario, i quali devono quindi precedentemente accordarsi sulla chiave da utilizzare, che deve essere tenuta segreta. (Treccani)	Crittografia simmetrica
对称密码系统 Duìchèn mìmǎ xìtǒng	**对称密码体制**也称为秘密密钥密码体制、单密钥密码体制或常规密码体制。所谓对称，是指能够从解密密钥中推算出加密密钥，反过来也成立。 （有道词典）		Crittografia simmetrica

网络攻击 Wǎngluò gōngjí	**网络攻击**是低强度冲突，发动攻击的原因很少会上升到选择常规动能武器的地步。（有道词典）	Cyberattacco s. m. Attacco terroristico condotto con mezzi tecnologici, attraverso Internet. (Treccani)	Cyberattacco
网络犯罪 Wǎngluò fànzuì	**网络犯罪**：对电脑和网络的非法使用。（有道词典）	Cybercrime <sàibëkraim> s. ingl., usato in it. al masch. – Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo (rispettivamente, si parla di computer as a tool e computer as a target). (Treccani)	Cybercrimine
赛博战 Sài bó zhàn	**赛博战**是指以电磁波作为传导体，加入信息来达到破坏或摧毁对方武器系统，信息可以是木马、恶意软件、病毒，等等。（有道词典）	Cyberguerra s.f. – Guerra combattuta con l'impiego di mezzi tecnologici avanzati per l'attacco dei sistemi informatici nemici. Il concetto di c. racchiude diversi tipi di confronto, diverse strategie e diverse finalità.	Cyberguerra
计算机安全 Jìsuànjī ānquán	**计算机安全**指的是阻止攻击者通过未授权访问或未授权使用计算机和网络达到目的。安全包含开发和配置两方面的元素。（有道词典）	Cybersicurezza (cyber-sicurezza), s. f. Sistema di sicurezza che protegge la rete telematica di uno Stato da eventuali attacchi terroristici perpetrati per via informatica. (Treccani)	Cybersicurezza
网络空间 Wǎngluò kōngjiān	**网络空间**是一种崭新的电子信息技术环境，网络的易操作性、开放性、高速性以及普及性给知识产权特别是商业秘密的保护提出了严峻挑战 （有道词典）	Ciberspàzio (o, meno com., cyberspazio ‹saiberspàzio›) s. m. [comp. di ciber- (o cyber-) e spazio, sul modello dell'angloamer. cyberspace] (usato solo al sing.). – Lo spazio virtuale nel quale utenti (e programmi) connessi fra loro attraverso una rete telematica (v., per es., internet) possono muoversi e interagire per gli scopi più diversi, come, per es., la consultazione di archivî e banche dati o lo scambio di posta elettronica (v. pòsta1, n. 3 f): viaggiare nel ciberspazio. (Treccani)	Cyberspazio
电脑空间 Diànnǎo kōngjiān	**电脑空间**是随着计算机信息网络的兴起而出现的一种人类交流信息、知识、情感的生存环境。（有道词典）		Cyberspazio
赛博空间 Sài bó kōngjiān	**赛博空间**是哲学与计算机领域中一个共同的抽象概念,指在计算机以及计算机网络里的虚拟现实。（有道词典）	Usato per tradurre il termine "Cyberspazio" dalla letteratura fantascientifica o militare occidentale, ma non utilizzato negli scritti cinesi in ambito tecnico, scientifico o militare. (Lindsay et al. 2014, 197)	Cyberspazio
网络间谍 Wǎngluò jiàndié	计算机**网络间谍**入侵要具备一定的条件：计算机网络间谍必须以计算机网络为工具，窃取、篡改敌方或外国计算机网络上的信息。黑客并不等同于间谍，严格的说，所有的网络间谍都是黑客，而所有的黑客都是潜在的间谍。（有道词典）	Cyberspionaggio (cyber-spionaggio), s. m. Spionaggio esercitato mediante la rete telematica.	Cyberspionaggio

网络恐怖主义 Wǎngluò kǒngbù zhǔyì	**网络恐怖主义**; 非法使用电脑和网络以达到某种目的。（有道词典）	Cyberterrorismo s. m. – L'utilizzo di tecnologie informatiche al fine di sviluppare un'azione o una strategia terroristica. (Treccani)	Cyberterrorismo
信息丢失 Xìnxī diūshī	**信息泄露**，信息被暴露给不允许对它进行访问的人。（有道词典）	Data leakage <dèitë lìikiğ> locuz. sost. ingl., usata in it. al masch. – Esposizione accidentale o intenzionale di informazioni confidenziali, per es. dati personali come i numeri delle carte di credito, password, dati sensibili legalmente protetti come quelli sanitari e dati usati in ambito finanziario, commerciale e industriale, segreti o protetti da diritti di proprietà intellettuale. (Treccani)	Data leakage
数据库 Shùjùkù	**数据库**就是用来存放数据的地方。例如，将很多人的联系方式都写在一个本子上，那么这个本子就是一个数据库。（有道词典）	Data base ‹dèitë bèis› (o database) locuz. ingl. (propr. «base di dati»; pl. data bases ‹... bèisiʃ›), usata in ital. come s. m. (e comunem. pronunciata ‹dàta bèis›). – Archivio elettronico di dati correlati, registrati nella memoria di un computer e organizzati in modo da poter essere facilmente, rapidamente e selettivamente rintracciabili uno per uno, oppure per gruppi determinati, mediante appositi programmi di gestione e di ricerca (chiamati anch'essi data base, ma più propr. denominati data base management system, in sigla DBMS). (Treccani)	Database
数字数据 Shùzì shùjù	**数字数据**就是用取值为不连续数值的数据。（有道词典）	Dato In informatica, informazione elementare codificabile o codificata. (Treccani)	Dati (digitali)
解码 Jiěmǎ	**解密**：它是对数据进行加密的加密算法的逆运算。它能够将加密的数据恢复成原样，即为未加密时的状态。（有道词典）	Decrittare (o decriptare) v. tr. [comp. di de- e critto(gramma)]. – Interpretare una scrittura segreta o cifrata. (Treccani)	Decrittare o Decriptare
译码 Yìmǎ	（有道词典）		Decrittare o Decriptare
人肉搜索 Rénròu sōusuǒ	**人肉搜索，人肉搜索引擎，肉搜**: 未经允许在网上非法获得并发布他人个人信息，同 doxxing。（有道词典）	Doxing, da "to dox (someone/something)", rivelare informazioni su qualcuno su Internet, di solito per danneggiarlo. (Tradotto dall'Inglese) (Oxford Reference)	Doxing
人肉搜索引擎 Rénròu sōusuǒ yǐnqíng	（有道词典）		Doxing
肉索 Ròusuǒ	（有道词典）		Doxing
电子邮件 Diànzǐ yóujiàn	**电子邮件**是利用计算机网络传递的电子媒体信件，它是随着计算机网络出现的，依靠网络的通信手段实现普通邮件信息的.（有道词典）	E-mail ‹i mèil› locuz. ingl. [comp. di e-2 e mail «posta»], usata in ital. come s. f. – Nel linguaggio delle telecomunicazioni e dell'informatica, lo stesso che posta elettronica (v. posta1, n. 3 f); estens., il messaggio trasmesso con tale mezzo (Treccani)	E-mail

文件 Wénjiàn	**文件**是程序设计中一个重要的概念。所谓"文件"，一般指存储在外部介质上数据的集合。（有道词典）	File ‹*fàil* › s. ingl. [dal medio-fr. *fil* «filo1», incrociato con *file* «fila»] (pl. *files* ‹*fàil* ʃ›), usato in ital. al masch. – Termine, che significa genericam. filza di documenti, archivio, schedario, di uso frequente in informatica con il sign. ora di «documento», «archivio», ora di «flusso». (Treccani)	File
防火墙 Fánghuǒqiáng	**防火墙**: 新技术应该提供一个安全的防火墙以防御黑客。（有道词典）	Firewall <fàiëuool> (in it. fàireuol>) s. ingl., usato in it. al masch. – Dispositivo hardware o applicazione software che controlla la separazione tra una rete locale e la rete Internet, mediante il quale è possibile implementare un insieme di regole di sicurezza. (Treccani)	Firewall
补丁程序 Bǔdīng chéngxù	**补丁程序**是用来弥补漏洞的补救措施，保障操作系统安全的办法只有通过不断打辛卜丁才能实现。（有道词典）	In informatica, eliminazione di eventuali malfunzionamenti di un sistema (sia software, sia hardware) per renderlo solido e robusto. (Treccani)	Fix o Patch
灰帽黑客 Huī mào hēikè	**灰帽黑客**在多数情况下都具备白帽黑客的技术和意图，但是偶尔也使用这种知识来进行不太光明正大的行径。（有道词典）	In relazione agli scopi perseguiti, si distinguono tre differenti categorie di hacker: white hat hacker, il cui operato corrisponde a un rigoroso rispetto dell'etica h.; black hat hacker, chi violi illegalmente sistemi informatici con o senza vantaggi personali; grey hat hacker, l'h. cui non siano applicabili queste distinzioni o che passi facilmente dall'una all'altra categoria. (Treccani)	Grey Hat Hacker
电脑战争 Diànnǎo zhànzhēng	**电脑战争**: 使用计算机乱敌国活动，尤指故意袭击其通信系统。（有道词典）	Guerra cibernetica loc. s.le f. Guerra combattuta con l'impiego di mezzi tecnologici avanzati, che ha tra gli obiettivi l'attacco dei sistemi informatici nemici. (Treccani)	Guerra cibernetica
黑客 Hēikè	**黑客**是热心于计算机技术,水平高超的电脑专家,尤其是程序设计人员.他们要对计算机了如指掌对网络很精通才能算一个黑客高手。(有道词典)	Hacker In informatica, in particolare con riferimento alla rete Internet, esperto di programmazione e di reti telematiche che, perseguendo l'obiettivo di democratizzare l'accesso all'informazione e animato da princìpi etici, opera per aumentare i gradi di libertà di un sistema chiuso e insegnare ad altri come mantenerlo libero ed efficiente. s. Sebbene generalmente si tenda a confondere gli h. con i pirati informatici, o crackers, il cui scopo è danneggiare un sistema informatico, quest'ultimo termine, dal valore fortemente spregiativo, è stato invece coniato dagli h. stessi per definire chi non abbia rispetto delle proprie abilità informatiche. (Treccani)	Hacker
骇客 Hài kè	**骇客**：即机构以外的行为人，蓄意以非法手段，未经电脑主机所有人或系统管理者的允许，而迳自出入电脑系统并使用高超技术进行不法侵害.（有道词典）		Hacker

激进黑客 Jījìn hēikè	**激进黑客**：为达到社会或政治目的而从是计算机犯罪活动的黑金而活动分子。（有道词典）	Hacktivista agg. e s. m. e f. Che, chi effettua azioni di pirateria informatica con intenti di attivismo politico. (Treccani)	Hacktivista
硬磁盘 Yìngcípán	**硬磁盘**：硬盘中封装了一张或多张由硬质材料制成的圆盘，在圆盘的表面涂有一层磁性材料，通过磁化磁性材料来记录数据，具有很高的数据记。（有道）	Hard disk ‹hàad disk› locuz. ingl. [comp. di hard «duro, rigido», e disk «disco»] (pl. hard disks ‹... disks›), usata in ital. come s. m. – Nei calcolatori elettronici, disco di memoria realizzato su supporto magnetico rigido (di qui l'ital. disco rigido) e non asportabile (di qui l'altra denominazione di disco fisso). Ha grande capacità, fino a qualche centinaio di gigabyte. (Treccani)	Hard disk
蜜罐 Mì guàn	**蜜罐**技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。（ 江门市政务服务数据管理局： 网络信息安全术语）	Honeypot; "Inganno della rete fasulla", chiamato honey-potting in Occidente, si riferisce alla creazione di un sito Web falso per indurre il nemico ad accedervi in modo che il malware possa essere caricato. Viene utilizzato anche per invogliare gli attacchi nemici in modo che i metodi di attacco possano essere analizzati. (Tradotto dall'Inglese) (Lindsay et al. 2015, 145)	Honeypot
超连结 Chāo liánjié	**超连结**是一种连结的指令，被定义在网页中有底线的文本或高亮度的选项，当滑鼠点选时，便会开启另一个网页。（有道词典）	Collegamento, anche detto link (o hyperlink), in grado di rinviare a un contenuto informativo presente in un dominio fisicamente o virtualmente separato. Si viene così a creare un percorso non lineare fatto di un numero potenzialmente molto elevato di rimandi, legati o meno tra loro da affinità contenutistica. (Treccani)	Hyperlink o Link
网路位址 Wǎng lù wèi zhǐ	**网路位址**是网路上的每一台主机唯一的识 别码，让使用者可以正确的与网路上的任何一台电脑主 机连结。（有道词典）	Indirizzo IP <... ippì> locuz. sost. m. – Sequenza di numeri o di caratteri alfabetici che permette di individuare un elaboratore connesso in rete, indispensabile sia per ricevere sia per inviare dati. (Treccani)	Indirizzo IP
信息战 Xìnxī zhàn	**信息战**：敌对双方在信息领域的对抗活动。主要是通过争夺信息资源，掌握信息的生产、传递、处理等的主动权，破坏敌方的信息传输，为遏制或打赢战争创造有利条件。（有道词典）	Una forma di conflitto in cui l'obiettivo è catturare, degradare o distruggere i mezzi del nemico per raccogliere, analizzare e distribuire dati, in particolare dati riguardanti le forze armate nemiche. La guerra dell'informazione è normalmente condotta utilizzando computer e altri mezzi elettronici. (Tradotto dall'Inglese) (Oxford Reference)	Info War

信息 Xìnxī	**信息**是经过加工处理的、有一定含义的、并能对人类客观行为产生影响或对决策有价值的数据。（有道词典）	In informatica e nella teoria delle comunicazioni, unità d'i., la quantità d'informazione trasportata da un segnale che rappresenta la scelta fra due soli stati possibili ed equiprobabili e che costituisce un'unità binaria chiamata bit; la quantità d'informazione contenuta in un segnale è misurata dal logaritmo negativo (di base due) della probabilità del segnale. I. al secondo, unità di misura della potenza di calcolo di un computer, corrispondente all'elaborazione di una informazione (dato o istruzione di programma) al secondo. (Treccani)	Informazione
信息化 Xìnxī huà	**信息化**推广和应用电子计算机、通信、网络等信息技术和其他相关智能技术，促使工业社会向信息社会发展。（有道词典）	Informatiżżazióne s. f. [dal fr. informatisation, der. di informatiser «informatizzare»]. – L'introduzione dei sistemi informatici in uno o più settori di attività: i. dell'industria estrattiva; i. della ricerca scientifica; in senso più ampio, i. della società, la trasformazione che in essa avviene in seguito all'adozione sempre più diffusa dei mezzi informatici e dei calcolatori elettronici. (Treccani)	Informatizzazione
互联网 Hùliánwǎng	**互联网，因特网**：一种全球性的计算机网络，提供各种各样的信息和通知服务，由采用标准通信协议的网络相互连接而成。（有道词典）	Indica, nel mondo delle telecomunicazioni e dell'informatica, un vasto insieme di reti di computer interconnesse fra loro in modo che ciascun utente, con gli opportuni codici di accesso, possa collegarsi a tutta la rete e utilizzarne le risorse in qualsiasi località del mondo; il sistema rappresenta uno dei più potenti mezzi di raccolta e diffusione dell'informazione su scala globale (l'avvento, la rivoluzione di I.). (Treccani)	Internet
因特网 Yīntèwǎng	（有道词典）		Internet
互联网服务提供商 Hùliánwǎng fúwù tígōng shāng	**互联网服务提供商**是给个体用户和小型组织提供宽带链接和其他类型连接的公司，使他们能获得互联网上任何地方的服务。（有道词典）	ISP, Sigla di Internet service provider, operatore commerciale che, mediante l'uso di appositi computer con funzioni di server, fornisce ai suoi utenti la possibilità di accedere a Internet e di gestire un proprio sito e proprie caselle di posta elettronica. (Treccani)	Internet service provider (ISP)

按键监听程序 Ànjiàn jiāntīng chéngxù	**按键监听程序：**一种木马程序，可以在使用者不知情的情况下被记录下密码。（有道词典）	keylogger Programma o dispositivo che (una volta introdotto nel sistema) registra ogni movimento dell'utente e i tasti da questo premuti. È poi possibile accedere ai dati registrati non solo a livello locale (dal computer stesso), ma anche in remoto (i dati vengono trasmessi in automatico tramite internet). Nella maggior parte dei casi i k. sono progettati per rubare dati sensibili quali login e codici bancari (questo perché è molto difficile che un utente si accorga della presenza di un k. sul proprio computer); tuttavia esistono k. security oriented, come ad esempio quelli installati dalle aziende per controllare il lavoro e la produttività dei dipendenti. I k. possono essere hardware (dispositivi fisici inseriti nella tastiera o fra tastiera e case del computer) o software (programmi o driver di periferica). (Treccani)	Keylogger
序设计语言 Xù shèjì yǔyán	**序设计语言**是程序员与计算机或程序员与程序员之间沟通和交流的工具。（有道词典）	Linguàggio di programmazióne In informatica, insieme di parole e di regole, definite in modo formale, per consentire la programmazione di un elaboratore affinché esegua compiti predeterminati. (Treccani)	Linguaggio di programmazione
登录 Dēnglù	**登录**，意思是注册，进入系统。可作名词、动词使用。也指CISCO系统命令、Linux系统命令。（有道词典）	Login ‹lòġin› s. ingl. [comp. di (to) log «registrare sul giornale di bordo (di una nave)» e in «dentro»; propr. «iscriversi su un registro»], usato in ital. al masch. (e per lo più pronunciato ‹logìn›). – 1. Operazione con cui l'utente di una rete telematica si registra nel sito al quale accede per la prima volta. 2. estens. Codice identificativo per mezzo del quale avviene tale registrazione. (Treccani)	Login
恶意软件 Èyì ruǎnjiàn	**恶意软件**：专门为了破坏或干扰系统而特别开发的软件，诸如计算机病毒或者特洛依木马。（有道词典）	Malware Software che, una volta eseguito, danneggia il funzionamento e la sicurezza del sistema operativo; il termine deriva dalla contrazione di malicious e software e significa letteralmente "programma malvagio". Sempre più diffusi, i m. si trasmettono via internet; spesso tramite la posta elettronica, ma anche attraverso la semplice navigazione. Tra le categorie di m. più diffuse si ricordano virus, trojan horse, keylogger, worm e backdoor. Esistono poi i m. poliformici (che cambiano continuamente forma, pur mantenendo inalterata la funzionalità) e quelli metamorfici (che alterano completamente il loro codice), entrambi particolarmente difficili da individuare. (Treccani)	Malware
元数据 Yuán shùjù	**元数据**：是关于数据的数据或描述数据及其环境的数据，指用于描述要素、数据集或数据集系列的内容、覆盖范围、质量、管理方式、数据的所。（有道词典）	Metadati s. m. pl. L'insieme dei dati accessori che contribuiscono a descrivere in modo dettagliato e completo un oggetto o un soggetto; con particolare riferimento ai dati raccolti per via telematica sui comportamenti degli utenti della rete. (Treccani)	Metadata

计算机网络 Jìsuànjī wǎngluò	**计算机网络**是指把散布在不同地舆位置的具有独建功用的计算机,通过各种通讯设备和线路物理地连接起来,根据网络协议相互通讯,以共享软件、硬件。 （有道词典）	Network ‹nètuëëk› s. ingl. [comp. di net «rete» e work «lavoro»; propr. «lavoro (o struttura) a rete»] (pl. networks ‹nètuëëks›), usato in ital. al masch. – Termine usato in varie discipline tecniche, spec. in elettrotecnica, elettronica e informatica, come sinon. di rete.	Network
口令 Kǒulìng	**口令，密码**是计算机安全工程中的重要基础，是计算机验证用户身份的主要机制。（有道词典）	Password ‹pàasuëëd› (o pass-word) s. ingl. [comp. di pass (v.) e word «parola»] (pl. passwords ‹pàasuëëdʃ› o pass-words), usato in ital. al femm. – In informatica, parola di riconoscimento, impiegata nei sistemi di elaborazione a scopo di sicurezza contro il loro uso improprio da parte di utenti non autorizzati; costituisce la chiave di protezione dei programmi inseriti nell'elaboratore, ed è formata da un gruppo ordinato e codificato di caratteri alfanumerici, assegnati ad ogni operatore abilitato, che devono essere digitati al terminale, su richiesta del sistema operativo, preventivamente alla connessione di questo con l'unità centrale di elaborazione. (Treccani)	Password
密码 Mìmǎ	（有道词典）		Password
网络钓鱼 Wǎngluò diàoyú	**网络钓鱼，网络欺诈**：以虚假的身份和形象随机骗取个人帐号和密码等。 （有道词典）	Phishing <*fìšiń* > s. ingl., usato in it. al masch. – Condotta illecita tesa a ottenere informazioni e dati personali degli utenti di Internet inviando e-mail con dati e link a siti web falsi, spesso clonati per renderli identici ai siti web originali. Le informazioni più ricercate attraverso questo meccanismo tecnico illegale sono numeri di conti correnti bancari e di carte di credito con relative password. Può anche prendere il nome di *spoofing* o *carding* . La traduzione di p. va intesa come «sottrarre con l'inganno». (Treccani)	Phishing
网络欺诈 Wǎngluò qīzhà	（有道词典）		Phishing
传输控制协议 / 互联网协议 Chuánshū kòngzhì xiéyì/ hùliánwǎng xiéyì	**传输控制协议/互联网协议**：大多数主要应用程序用于通过互联网进行通信的一组协议。TCP 和 IP 协同工作，为运行在连接到网络的主机系统上的应用程序之间提供可靠的数据传递。（ICANN）	TCP/IP. – Sigla di *Transmission control protocol/Internet protocol* . Coppia di protocolli di rete *host to host* , considerati altamente affidabili e pertanto usati, accoppiati, per comunicazioni tra gli host – le reti di computer a commutazione di pacchetto – e in sistemi interconnessi di tali reti. (Treccani)	Protocollo TCP/IP

TCP/IP 协议 xiéyì	（有道词典）		Protocollo TCP/IP
加密勒索软件 Jiāmì lèsuǒ ruǎnjiàn	**加密勒索软件**是一种恶意软件。黑客一般会想法设法将这类软件植入受害机构或者企业的系统中，将这类用户的数据资产包括文档、邮件、数据库、源。（有道词典）	Ransomware *s. m. inv.* Programma maligno che limita o impedisce l'accesso al dispositivo sul quale si installa a insaputa dell'utente, richiedendo un riscatto da pagare per ripristinare l'uso normale del dispositivo. (Treccani)	Ransomware (Malware)
红客 Hóng kè	**红客**是指维护国家利益，不利用网络技术入侵自己国家电脑，而是"维护正义，为自己国家争光的黑客"。红客是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神并热爱着计算机技术的都可称为红客。红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击。（有道词典）	Gli hacker hanno coniato la parola "Red Hacker", che significa che qualcuno è un hacker patriottico. A differenza delle controparti occidentali, la cui maggior parte è individualista o anarchica, gli hacker cinesi tendono a essere più coinvolti nella politica poiché la maggior parte sono giovani, appassionati e patriottici. Sono politicamente motivati, hanno bisogno di protestare contro le questioni estere. (Tradotto dall'Inglese) (Henderson 2007, 13-14)	Red Hacker o Honker
路由器 Lùyóuqì	**路由器**是连接两个或多个网络的硬件设备，在网络间起网关的作用，是读取每一个数据包中的地址然后决定如何传送的专用智能性的网络设备。（有道词典）	Router In telematica, dispositivo elettronico che, inserito in una rete di elaboratori, permette la loro interconnessione e connessione a Internet (v. fig.) e ha il compito di verificare il rispetto dei protocolli di comunicazione. Il r., una volta letto l'indirizzo dell'elaboratore destinatario, è in grado di far percorrere a ciascun pacchetto informativo il percorso migliore per giungere a destinazione. (Treccani)	Router
SCADA系统 xìtǒng	**SCADA系统，即数据采集与监视控制系统**：SCADA系统是以计算机为基础的DCS与电力自动化监控系统；它应用领域很广，可以应用于电力、冶金、石油、化工、燃气、铁路等领域的数据采集与监视控制以及过程控制等诸多领域。（项晓春, 刘广魁. SCADA系统及其应用[J]. 自动化技术与应用, 2000）	I sistemi di controllo industriale includono i sistemi di controllo di supervisione e acquisizione dei dati (Supervisory Control and Data Acquisition-SCADA), i sistemi di controllo distribuiti (Distributed Control Systems-DCS) e i controllori a logica programmabile (Programmable Logic Controller-PLC), impiegati usualmente negli impianti industriali. (CISR)	Sistema SCADA
即数据采集与监视控制系统 Jí shùjù cǎijí yǔ jiānshì kòngzhì xìtǒn	（有道词典）		Sistema SCADA

服务器 Fúwùqì	**服务器**是提供网络服务的物理载体，是一种计算机，只不过它是一种功能更为强大的计算机，特别是在网络应用服务方面。（有道词典）	Server ‹*së'ëvë*› s. ingl. [propr. «chi serve», der. di (*to*) *serve* «servire»] (pl. *servers* ‹*së'ëvës*›), usato in ital. al masch. – 1. non com. 2. In informatica (con riferimento a una rete di calcolatori), calcolatore che svolge funzioni di servizio per tutti i calcolatori collegati: in partic., *s. della rete* , il calcolatore che gestisce il traffico di informazioni sulla rete stessa; *file* ‹*fàil*› *s.* , calcolatore che gestisce l'accesso a un grande insieme di dati, organizzati in *file* ; *s. di posta elettronica* , server che gestisce lo smistamento dei messaggi; *s. ftp* , server programmato per il trasferimento di file con il protocollo FTP nella rete Internet. Con sign. analogo, programma, generalmente sempre attivo, che esegue determinate funzioni quando queste sono richieste da altri programmi. (Treccani)	Server
网络安全 Wǎngluò ānquán	**网络安全**是技术、程序和实践的主体，它们用来保护网络、计算机、程序和数据不受攻击、损坏或未授权访问的伤害。（有道词典）	Sicurézza informàtica Ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. Tali tentativi di violazione possono essere contrastati sia mediante programmi sia mediante specifici strumenti hardware. (Treccani)	Sicurezza Informatica
操作系统 操作系统 Cāozuò xìtǒng cāozuò xìtǒng	**操作系统 操作系统**(简称OS)是最基本、最重要的系统软件，已成为计算机系统必不可少的基本组成部分。（有道词典）	Sistema operativo, In informatica, Il software responsabile della gestione delle risorse di un calcolatore. Il nucleo di un sistema o. è costituito dal kernel (nocciolo), sempre presente in memoria principale, che permette la comunicazione tra soft-ware e hardware. Elementi fondamentali sono: il gestore del file system, che garantisce un utilizzo efficace ed efficiente della memoria di massa; uno scheduler (➔ scheduling) per la gestione dei processi in attesa di esecuzione; un gestore della memoria che sovraintende all'utilizzo della memoria principale (e della eventuale memoria virtuale) per garantire che su di essa siano presenti i dati necessari al processo in esecuzione; una interfaccia utente (tipicamente una shell o una GUI, graphical user interface) per permettere a un operatore di interagire con il calcolatore. (Treccani)	Sistema operativo

软件 Ruǎnjiàn	**软件**是指使计算机运行需要的程序、数据和有关的技术文档资料。软件是计算机的灵魂，是发挥计算机功能的关键。（有道词典）	Software ‹*sòftụeë*› s. ingl. [comp. di *soft* «molle, morbido» e *ware* «merce»], usato in ital. al masch. – Termine correntemente usato nella tecnica elettronica per indicare, in contrapp. a *hardware* (v.), tutti i componenti modificabili di un sistema o di un apparecchio e, più specificamente in informatica, l'insieme dei programmi che possono essere impiegati su un sistema di elaborazione dei dati: *s. di sistema*, quello relativo al sistema operativo dell'elaboratore; *s. di base*, l'insieme dei programmi e delle procedure di utilità generale, solitamente organizzato in librerie di sottoprogrammi, richiamabili dai programmi applicativi o dai programmi sviluppati dall'utente; *s. applicativo*, quello relativo ai programmi applicativi, sviluppati per una particolare funzione (scrittura, elaborazione di immagini, gestione di dati, ecc.). (Treccani)	Software
鱼叉式网络钓鱼 Yú chā shì wǎngluò diàoyú	**鱼叉式网络钓鱼**是面向特定组织的欺诈行为，目的是不通过授权访问机密数据。（有道词典）	Attacco informatico di tipo phishing condotto contro utenti specifici mediante l'invio di email formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o link malevoli. (CISR)	Spear phishing
欺骗 Qīpiàn	**欺骗**是一种主动式攻击，即网络上的某台机器伪装成另一台不同的机器。（有道词典）	Spoofing <spùufiń> s. ingl., usato in it. al masch. – Attività illecita su Internet che consiste nel furto di identità. Si esplicita attraverso la falsificazione di indirizzi di siti web e del contenuto di questi ultimi, sovente clonati, per indurre il navigatore a credere di essere nel sito web cercato mentre invece si trova in un sito copiato e falso, nel tentativo di carpirgli con l'inganno informazioni e dati personali, quali per es. numeri di conti correnti bancari o password. (Treccani)	Spoofing
间谍软件 Jiàndié ruǎnjiàn	**间谍软体**在很多方面都和特洛伊木马十分相似。这些程式未经您的同意而收集关于您和您的兴趣。如您的飙网习惯，您个人电脑上的其他软体等。（有道词典）	Spyware ‹*spàiueë* › s. ingl. [comp. di *spy* «spia» e (*soft*)*ware*] (pl. *spywares* ‹*spàiueëʃ*›), usato in ital. al masch. – Software che si installa nel computer di un utente di Internet, senza che questi se ne avveda, raccogliendo informazioni sulle varie operazioni che compie come utilizzatore della rete. (Treccani)	Spyware

SQL 注入攻击 zhùrù gōngjí	**SQL注入攻击**是黑客对数据库进行攻击的常用手段之一。(...)用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection，即SQL注入。(江门市政务服务数据管理局, 2020)	Tecnica mirata a colpire applicazioni web che si appoggiano su database accessibili con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in input e l'inserimento di codice malevolo all'interno delle interrogazioni (query). Tali attacchi consentono – in taluni casi – persino di accedere alle funzioni di amministrazione del sistema, oltre che di sottrarre o alterare i dati. (CSIRT 2019 2019)	SQL injection
PKI技术 jìshù	**PKI技术**是通过由CA认证中心发布证书的方式绑定了身份与公钥的。 同时PKI可以提供传输信息的机密性、完整性、身份鉴别和不可否认等的安全保障服务。（有道词典）	Da "Crittografia": l'autenticità delle chiavi pubbliche è garantita attraverso un sistema denominato Public Key Infrastructure (pki), in cui un'entità di certificazione (Certification Authority, ca) associa un soggetto alla propria chiave pubblica. (Treccani)	Struttura PKI
超级病毒工厂 Chāojí bìngdú gōngchǎng	**超级工厂病毒**是世上首个专门针对工业控制体系编写的破坏性病毒，它可假装成RealTek与JMicron两至公司的数码签名，入侵SimaticWinCCSCADA体系。 （有道词典）	Creato dalle agenzie di intelligence statunitensi e israeliane, un worm per computer specificatamente progettato per sabotare gli impianti di ricerca nucleare iraniani. (Tradotto dall'Inglese) (Singer Friedman 2014, 298)	Stuxnet
防火长城 Fánghuǒ chángchéng	**防火长城** **(功夫网/中国国家防火墙**[1]、**长城防火墙**或**万里防火墙**）是對中华人民共和国政府在其管辖互联网内部建立的多套网络审查系统（包括相关行政审查系统）的称呼。(Sensagent online dictionary)	Un sistema che impedisce l'accesso a siti Web ritenuti indesiderabili dal governo della Repubblica popolare cinese (Collins)	The Great Firewall
功夫网 Gōngfū wǎng	(Sensagent online dictionary)		The Great Firewall
中国国家防火墙 Zhōngguó guójiā fánghuǒqiáng	(Sensagent online dictionary)		The Great Firewall
长城防火墙 Chángchéng fánghuǒqiáng	(Sensagent online dictionary)		The Great Firewall
万里防火墙 Wànlǐ fánghuǒqiáng	(Sensagent online dictionary)		The Great Firewall
特洛伊木马病毒 Tèluòyī mùmǎ bìngdú	**特洛伊木马病毒**是一支程式，外表看起来像一支有用的程式，但是包含一些隐藏、可能会有安全危险的功能。（有道词典）	trojan horse ‹tróuğan hòos› locuz. ingl. (propr. «cavallo di Troia»), usata in ital. come s. m. – In informatica, virus, diffuso attraverso programmi apparentemente innocui o utili, destinato a compromettere il funzionamento del computer su cui viene installato. (Treccani)	Trojan (Malware)

误植域名 Wù zhí yùmíng	**误植域名**是网路蟑螂的一种形式，依靠网路使用者的打字错误所作的域名抢先注册。（有道词典）	typosquatting <taipëskyòtiñ> s. ingl., usato in it. al masch. – Tipologia di cybersquatting che consiste nella condotta di chi, senza averne diritto né autorizzazione, registra in mala fede come nome di dominio uno molto simile a quello di un personaggio famoso, un marchio o un altro segno distintivo, o qualsiasi altra denominazione non generica, allo scopo di trarre indebito profitto dalla rinomanza altrui. Il termine nasce dalla crasi tra typo «errore di battitura» e to squat «occupare abusivamente», per indicare il fatto che l'azione malevola si basa sul tentativo di intercettare il traffico causato da errori di digitazione fatti dagli utenti quando scrivono gli indirizzi in Internet. (Treccani)	Typosquatting
网址 Wǎngzhǐ	**网址**: 某一网站在互联网上的地址，用户通过点击就可访问、查询并获取该网站的信息资源。（有道词典）	URL: Sigla dell'ingl. Uniform resource locator, che in informatica indica l'indirizzo che identifica univocamente un sito web. Inizia sempre con la sequenza http:// e prosegue con una o più parole divise da punti (di solito la denominazione o il marchio dell'ente o persona proprietario del sito) e uno tra una serie di suffissi ammessi (it, com, org ecc.) che specificano la natura del sito. Il browser lo traduce automaticamente in una sequenza numerica che indica il server su cui è collocato il sito. (Treccani)	URL
计算机病毒 Jìsuànjī bìngdú	**计算机病毒**是指编制者在计算机顺序中拔出的毁坏计算机功用或许毁坏数据，影响计算机运用并且可以自我复制的一组计算机指令或许顺序代码。（有道词典）	vìrus informàtico locuz. sost. m. – Insieme di istruzioni destinato a danneggiare un sistema di calcolo (per es., attraverso la cancellazione di parte delle memorie). Il v. i. può essere introdotto direttamente o, più spesso, mascherato all'interno di programmi apparentemente innocui che, duplicati e trasmessi inconsapevolmente da un utente all'altro, lo diffondono su larga scala con modalità 'epidemiche', da cui il nome. I v. i. costituiscono una tipologia di malware, termine talvolta utilizzato impropriamente come sinonimo, e sono software che presentano caratteristiche simili a quelle dei virus biologici. Non possono essere eseguiti autonomamente senza un programma ospite; sono in grado di individuare possibili file da infettare e di replicarsi, contagiando questi ultimi. (Treccani)	Virus (computer)

弊端 Bìduān	**弊端**也叫**脆弱性**是谋划机系统在硬件、软件、和谈的具体兑现或系统安定计谋计划和筹划时存在的缺陷和不敷,从而使进攻者能够在未被合法授权的环境。（有道词典）	Le vulnerabilità possono essere sia organizzative che tecniche, spesso in combinazione tra loro. Le vulnerabilità organizzative e di processo sono riconducibili alla mancata o non corretta definizione o implementazione di misure di sicurezza volte alla tutela della riservatezza, integrità e disponibilità delle informazioni. Le vulnerabilità tecniche, invece, sono dovute a falle di sicurezza del software applicativo, del firmware, dell'hardware ovvero dei protocolli di comunicazione, dovuti principalmente a bug o non corrette configurazioni. Entrambi i tipi di vulnerabilità possono essere sfruttati da attaccanti per effettuare azioni malevole. (CSIRT 2019 2019)	Vulnerabilità
脆弱性 Cuìruò xìng	（有道词典）		Vulnerabilità
白帽黑客 Bái mào hēikè	**白帽黑客**：有能力破坏电脑或网络安全但不具恶意目的黑客，他们有清楚的道德规范并试图同企业合作改善被发现的安全弱点。（有道词典）	In relazione agli scopi perseguiti, si distinguono tre differenti categorie di hacker: white hat hacker, il cui operato corrisponde a un rigoroso rispetto dell'etica h.; black hat hacker, chi violi illegalmente sistemi informatici con o senza vantaggi personali; grey hat hacker, l'h. cui non siano applicabili queste distinzioni o che passi facilmente dall'una all'altra categoria. (Treccani)	White Hat Hacker
蠕虫 Rúchóng	**蠕虫**：能够把自身从一台计算机复制到另一台计算机的程序。与病毒不同，蠕虫不会感染文件或磁盘，而只是对自身进行复制。（有道词典）	worm ‹*ụòrm*› s. ingl. (propr. «verme»; pl. *worms* ‹*ụòrms*›), usato in ital. al masch. – Nel linguaggio informatico, virus che si diffonde tramite la rete e la posta elettronica. (Treccani)	Worms (malware)
即零日攻击 Jí líng rì gōngjí	**即零日攻击**：即在漏洞发现地同一天就发生了攻击事件。根据经验，一般黑客攻击漏洞在修复漏洞之前，有时是黑客先发现地漏洞。（有道词典）	In gergo informatico, si intendono con zero-day (o 0-day) vulnerabilità riferite a sistemi, apparati e applicazioni non ancora note al produttore della tecnologia. La gravità degli zero-day è costituita dall'assenza di aggiornamenti software a fini di mitigazione (cd. patching). Proprio tali caratteristiche rendono gli zero-day oggetto di compravendite illecite da parte di soggetti intenzionati a sfruttarli per finalità intrusive. (CSIRT 2019)	Zero day

Glossario ITA - CIN

Termine Italiano	Termine Cinese
Advanced Persistent Threat (APT)	高级持续性威胁 Gāojí chíxù xìng wēixié
Algoritmo	算法 Suànfǎ
Antivirus	防毒软件 Fángdú ruǎnjiàn
Antivirus	抗毒软件 Kàng dú ruǎnjiàn
Antivirus	防毒软件 Fángdú ruǎnjiàn
Antivirus	防毒软件 Fángdú ruǎnjiàn
Attacco Brute Force	暴力破解攻击 Bàolì pòjiě gōngj
Attacco Dizionario	搜索结果 Sōusuǒ jiéguǒ
Attacco man-in-the-middle	中间人攻击 Zhōngjiānrén gōngjí
Backdoor	后门 Hòumén
Black Hat Hacker	黑帽黑客 Hēi mào hēikè
Bomba Logica	逻辑炸弹 Luójí zhàdàn
Botnet	僵尸网络 Jiāngshī wǎngluò

Browser	浏览程序 Liúlǎn chéngxù
Browser	浏览器 Liúlǎn qì
Buffer overflow	缓存溢出 Huǎncún yìchū
Chiave (crittografia)	密钥 Mì yào
Chiavetta USB	USB 解密盘 jiěmì pán
Chiavetta USB	U 盘 Pán
Chiavetta USB	优盘 Yōupán
Codice Binario	二进制代码 Èrjìnzhì dàimǎ
Computer Network Warfare	计算机网络战 Jìsuànjī wǎngluò zhàn
Crittare o Criptare	加密 Jiāmì
Crittografia	密码术 Mìmǎ shù
Crittografia asimmetrica	非对称加密 Fēi duìchèn jiāmì
Crittografia end-to-end	端到端加密 Duān dào duān jiāmì
Crittografia simmetrica	对称加密 Duìchèn jiāmì
Crittografia simmetrica	对称密码系统 Duìchèn mìmǎ xìtǒng

Cyberattacco	网络攻击 Wǎngluò gōngjí
Cybercrimine	网络犯罪 Wǎngluò fànzuì
Cyberguerra	赛博战 Sài bó zhàn
Cybersicurezza	计算机安全 Jìsuànjī ānquán
Cyberspazio	网络空间 Wǎngluò kōngjiān
Cyberspazio	电脑空间 Diànnǎo kōngjiān
Cyberspazio	赛博空间 Sài bó kōngjiān
Cyberspionaggio	网络间谍 Wǎngluò jiàndié
Cyberterrorismo	网络恐怖主义 Wǎngluò kǒngbù zhǔyì
Data leakage	信息丢失 Xìnxī diūshī
Database	数据库 Shùjùkù
Dati (digitali)	数字数据 Shùzì shùjù
Decrittare o Decriptare	解码 Jiěmǎ
Decrittare o Decriptare	译码 Yìmǎ
Doxing	人肉搜索 Rénròu sōusuǒ

Doxing	人肉搜索引擎 Rénròu sōusuǒ yǐnqíng
Doxing	肉索 Ròusuǒ
E-mail	电子邮件 Diànzǐ yóujiàn
File	文件 Wénjiàn
Firewall	防火墙 Fánghuǒqiáng
Fix o Patch	补丁程序 Bǔdīng chéngxù
Grey Hat Hacker	灰帽黑客 Huī mào hēikè
Guerra cibernetica	电脑战争 Diànnǎo zhànzhēng
Hacker	黑客 Hēikè
Hacker	骇客 Hài kè
Hacktivista	激进黑客 Jījìn hēikè
Hard disk	硬磁盘 Yìngcípán
Honeypot	蜜罐 Mì guàn
Hyperlink o Link	超连结 Chāo liánjié
Indirizzo IP	网路位址 Wǎng lù wèi zhǐ

Info War	信息战 Xìnxī zhàn
Informazione	信息 Xìnxī
Informatizzazione	信息化 Xìnxī huà
Internet	互联网 Hùliánwǎng
Internet	因特网 Yīntèwǎng
Internet service provider (ISP)	互联网服务提供商 Hùliánwǎng fúwù tígōng shāng
Keylogger	按键监听程序 Ànjiàn jiāntīng chéngxù
Linguaggio di programmazione	序设计语言 Xù shèjì yǔyán
Login	登录 Dēnglù
Malware	恶意软件 Èyì ruǎnjiàn
Metadata	元数据 Yuán shùjù
Network	计算机网络 Jìsuànjī wǎngluò
Password	口令 Kǒulìng
Password	密码 Mìmǎ
Phishing	网络钓鱼 Wǎngluò diàoyú

Phishing	网络欺诈 Wǎngluò qīzhà
Protocollo TCP/IP	传输控制协议 / 互联网协议 Chuánshū kòngzhì xiéyì/ hùliánwǎng xiéyì
Protocollo TCP/IP	TCP/IP 协议 xiéyì
Ransomware (Malware)	加密勒索软件 Jiāmì lèsuǒ ruǎnjiàn
Red Hacker o Honker	红客 Hóng kè
Router	路由器 Lùyóuqì
Sistema SCADA	SCADA 系统 xìtǒng
Sistema SCADA	即数据采集与监视控制系统 Jí shùjù cǎijí yǔ jiānshì kòngzhì xìtǒn
Server	服务器 Fúwùqì
Sicurezza Informatica	网络安全 Wǎngluò ānquán
Sistema operativo	操作系统 操作系统 Cāozuò xìtǒng cāozuò xìtǒng
Software	软件 Ruǎnjiàn
Spear phishing	鱼叉式网络钓鱼 Yú chā shì wǎngluò diàoyú
Spoofing	欺骗 Qīpiàn
Spyware	间谍软件 Jiàndié ruǎnjiàn

SQL injection	SQL 注入攻击 zhùrù gōngjí
Struttura PKI	PKI 技术 jìshù
Stuxnet	超级病毒工厂 Chāojí bìngdú gōngchǎng
The Great Firewall	防火长城 Fánghuǒ chángchéng
The Great Firewall	功夫网 Gōngfū wǎng
The Great Firewall	中国国家防火墙 Zhōngguó guójiā fánghuǒqiáng
The Great Firewall	长城防火墙 Chángchéng fánghuǒqiáng
The Great Firewall	万里防火墙 Wànlǐ fánghuǒqiáng
Trojan (Malware)	特洛伊木马病毒 Tèluòyī mùmǎ bìngdú
Typosquatting	误植域名 Wù zhí yùmíng
URL	网址 Wǎngzhǐ
Virus (computer)	计算机病毒 Jìsuànjī bìngdú
Vulnerabilità	弊端 Bìduān
Vulnerabilità	脆弱性 Cuìruò xìng
White Hat Hacker	白帽黑客 Bái mào hēikè

Worms (malware)	蠕虫 Rúchóng
Zero day	即零日攻击 Jí líng rì gōngjí

Glossario CIN - ITA

Termine Cinese	**Termine Italiano**
高级持续性威胁 Gāojí chíxù xìng wēixié	Advanced Persistent Threat (APT)
算法 Suànfǎ	Algoritmo
防毒软件 Fángdú ruǎnjiàn	Antivirus
抗毒软件 Kàng dú ruǎnjiàn	Antivirus
防毒软件 Fángdú ruǎnjiàn	Antivirus
防毒软件 Fángdú ruǎnjiàn	Antivirus
暴力破解攻击 Bàolì pòjiě gōngj	Attacco Brute Force
搜索结果 Sōusuǒ jiéguǒ	Attacco Dizionario
中间人攻击 Zhōngjiānrén gōngjí	Attacco man-in-the-middle
后门 Hòumén	Backdoor
黑帽黑客 Hēi mào hēikè	Black Hat Hacker
逻辑炸弹 Luójí zhàdàn	Bomba Logica
僵尸网络 Jiāngshī wǎngluò	Botnet

浏览程序 Liúlǎn chéngxù	Browser
浏览器 Liúlǎn qì	Browser
缓存溢出 Huǎncún yìchū	Buffer overflow
密钥 Mì yào	Chiave (crittografia)
USB 解密盘 jiěmì pán	Chiavetta USB
U 盘 Pán	Chiavetta USB
优盘 Yōupán	Chiavetta USB
二进制代码 Èrjìnzhì dàimǎ	Codice Binario
计算机网络战 Jìsuànjī wǎngluò zhàn	Computer Network Warfare
加密 Jiāmì	Crittare o Criptare
密码术 Mìmǎ shù	Crittografia
非对称加密 Fēi duìchèn jiāmì	Crittografia asimmetrica
端到端加密 Duān dào duān jiāmì	Crittografia end-to-end
对称加密 Duìchèn jiāmì	Crittografia simmetrica
对称密码系统 Duìchèn mìmǎ xìtǒng	Crittografia simmetrica

网络攻击 Wǎngluò gōngjí	Cyberattacco
网络犯罪 Wǎngluò fànzuì	Cybercrimine
赛博战 Sài bó zhàn	Cyberguerra
计算机安全 Jìsuànjī ānquán	Cybersicurezza
网络空间 Wǎngluò kōngjiān	Cyberspazio
电脑空间 Diànnǎo kōngjiān	Cyberspazio
赛博空间 Sài bó kōngjiān	Cyberspazio
网络间谍 Wǎngluò jiàndié	Cyberspionaggio
网络恐怖主义 Wǎngluò kǒngbù zhǔyì	Cyberterrorismo
信息丢失 Xìnxī diūshī	Data leakage
数据库 Shùjùkù	Database
数字数据 Shùzì shùjù	Dati (digitali)
解码 Jiěmǎ	Decrittare o Decriptare
译码 Yìmǎ	Decrittare o Decriptare
人肉搜索 Rénròu sōusuǒ	Doxing

人肉搜索引擎 Rénròu sōusuǒ yǐnqíng	Doxing
肉索 Ròusuǒ	Doxing
电子邮件 Diànzǐ yóujiàn	E-mail
文件 Wénjiàn	File
防火墙 Fánghuǒqiáng	Firewall
补丁程序 Bǔdīng chéngxù	Fix o Patch
灰帽黑客 Huī mào hēikè	Grey Hat Hacker
电脑战争 Diànnǎo zhànzhēng	Guerra cibernetica
黑客 Hēikè	Hacker
骇客 Hài kè	Hacker
激进黑客 Jījìn hēikè	Hacktivista
硬磁盘 Yìngcípán	Hard disk
蜜罐 Mì guàn	Honeypot
超连结 Chāo liánjié	Hyperlink o Link
网路位址 Wǎng lù wèi zhǐ	Indirizzo IP

信息战 Xìnxī zhàn	Info War
信息 Xìnxī	Informazione
信息化 Xìnxī huà	Informatizzazione
互联网 Hùliánwǎng	Internet
因特网 Yīntèwǎng	Internet
互联网服务提供商 Hùliánwǎng fúwù tígōng shāng	Internet service provider (ISP)
按键监听程序 Ànjiàn jiāntīng chéngxù	Keylogger
序设计语言 Xù shèjì yǔyán	Linguaggio di programmazione
登录 Dēnglù	Login
恶意软件 Èyì ruǎnjiàn	Malware
元数据 Yuán shùjù	Metadata
计算机网络 Jìsuànjī wǎngluò	Network
口令 Kǒulìng	Password
密码 Mìmǎ	Password
网络钓鱼 Wǎngluò diàoyú	Phishing

网络欺诈 Wǎngluò qīzhà	Phishing
传输控制协议 / 互联网协议 Chuánshū kòngzhì xiéyì/ hùliánwǎng xiéyì	Protocollo TCP/IP
TCP/IP 协议 xiéyì	Protocollo TCP/IP
加密勒索软件 Jiāmì lèsuǒ ruǎnjiàn	Ransomware (Malware)
红客 Hóng kè	Red Hacker o Honker
路由器 Lùyóuqì	Router
SCADA 系统 xìtǒng	Sistema SCADA
即数据采集与监视控制系统 Jí shùjù cǎijí yǔ jiānshì kòngzhì xìtǒn	Sistema SCADA
服务器 Fúwùqì	Server
网络安全 Wǎngluò ānquán	Sicurezza Informatica
操作系统 操作系统 Cāozuò xìtǒng cāozuò xìtǒng	Sistema operativo
软件 Ruǎnjiàn	Software
鱼叉式网络钓鱼 Yú chā shì wǎngluò diàoyú	Spear phishing
欺骗 Qīpiàn	Spoofing
间谍软件 Jiàndié ruǎnjiàn	Spyware

SQL 注入攻击 zhùrù gōngjí	SQL injection
PKI 技术 jìshù	Struttura PKI
超级病毒工厂 Chāojí bìngdú gōngchǎng	Stuxnet
防火长城 Fánghuǒ chángchéng	The Great Firewall
功夫网 Gōngfū wǎng	The Great Firewall
中国国家防火墙 Zhōngguó guójiā fánghuǒqiáng	The Great Firewall
长城防火墙 Chángchéng fánghuǒqiáng	The Great Firewall
万里防火墙 Wànlǐ fánghuǒqiáng	The Great Firewall
特洛伊木马病毒 Tèluòyī mùmǎ bìngdú	Trojan (Malware)
误植域名 Wù zhí yùmíng	Typosquatting
网址 Wǎngzhǐ	URL
计算机病毒 Jìsuànjī bìngdú	Virus (computer)
弊端 Bìduān	Vulnerabilità
脆弱性 Cuìruò xìng	Vulnerabilità
白帽黑客 Bái mào hēikè	White Hat Hacker

蠕虫 Rúchóng	Worms (malware)
即零日攻击 Jí líng rì gōngjí	Zero day

Bibliografia

Archivi Biblioteche. 2019. “I metadati: cosa sono?” Accesso 20 Ottobre 2021. https://www.archivibiblioteche.it/2019/04/07/che-cosa-sono-i-metadati/

Belcic, Ivan. 2020. “What Is a Computer Worm?” Accesso 11 Novembre 2021. https://www.avast.com/c-computer-worm

Bongiovanni, Giancarlo. 2004. “Crittografia; Enciclopedia del Novecento III Supplemento.” Accesso 19 Ottobre 2021. https://www.treccani.it/enciclopedia/crittografia_%28Enciclopedia-del-Novecento%29/

Brown, Justine. 2016. “Stolen digital certificates are hackers' latest weapon of choice.” Accesso 22 Ottobre 2021. https://www.ciodive.com/news/stolen-digital-certificates-are-hackers-latest-weapon-of-choice/415804/

Bursztein, Elie. 2017. “Understanding the prevalence of web traffic interception.” Accesso 27 Ottobre 2021. https://elie.net/blog/security/understanding-the-prevalence-of-web-traffic-interception/

Cary, Dakota. 2021. (A) “China’s next generation of hackers won’t be criminals. That’s a problem.” Accesso 17 Novembre 2021. https://techcrunch.com/2021/11/12/chinas-next-generation-of-hackers-wont-be-criminals-thats-a-problem

Cary, Dakota. 2021. (B) “China’s National Cybersecurity Center A Base for Military-Civil Fusion in the Cyber Domain.” Accesso 17 Novembre 2021. https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/

Chandel, Sonali, Jingji, Zang, Yunnan, Yu, Jingyao, Sun and Zhipeng, Zhang. 2019. "The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall." International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, pp. 111-119, doi: 10.1109/CyberC.2019.00027.

Cimpanu, Catalin. 2021. (A) “Chinese universities connected to known APTs are conducting AI/ML cybersecurity research.” Accesso 19 Dicembre 2021. https://therecord.media/chinese-universities-connected-to-known-apts-are-conducting-ai-ml-cybersecurity-research/

Cimpanu, Catalin. 2021. (B) “Malware group leaks millions of stolen authentication cookies.” Accesso 19 Dicembre 2021. https://therecord.media/malware-group-leaks-millions-of-stolen-authentication-cookies/

Coldewey, Devin. 2013. “ ‘Perfect privacy'? In Internet communication, that doesn't exist.” Accessed 15 Ottobre 2021. https://www.nbcnews.com/technolog/perfect-privacy-internet-communication-doesnt-exist-6c10962853

Craig, Scott. 2016. “Beware of older cyber attacks.” Accesso 3 Novembre 2021. https://securityintelligence.com/media/beware-of-older-cyber-attacks/

Crane, Casey. 2020. “What Is a Certificate Authority (CA) and What Do They Do?” Accessed 12 Ottobre 2021. https://www.thesslstore.com/blog/what-is-a-certificate-authority-ca-and-what-do-they-do/

Glaser, April. 2017. “The HBO Hackers Are Demanding $7.5 Million to Stop Leaking Game of Thrones.” Accesso 27 Novembre 2021. https://slate.com/technology/2017/08/hbo-hackers-want-7-5-million-to-stop-leaking-game-of-thrones.html

Griffith, James. 2019. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books

Hagestad, T. Willliam II. 2012. *21st Century Chinese Cyberwarfare*. UK: IT Governance Publishing

Henderson, Scott. 2007. *The Dark Visitor: inside the World of Chinese Hackers*. Scott Henderson

Howlett, William IV. 2016. “The Rise of China's Hacking Culture: Defining Chinese Hackers.” Tesi Mag., California State University https://scholarworks.lib.csusb.edu/etd/383

Johansen, A. Grace. 2020. “What is encryption and how does it protect your data?” Accesso 11 Novembre 2021. https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

Khalil, George. 2014. “Password Security-- Thirty-Five Years Later.” Accesso 11 Ottobre 2021. https://www.sans.org/white-papers/35592/

Kuksov, Igor. 2017. “Come dei metadati intangibili possono creare problemi reali.” Accesso 12 Novembre 2021. https://www.kaspersky.it/blog/office-documents-metadata/9924/

Lewis, James. 2018. “Economic Impact of Cybercrime – No slowing down.” Accesso 7 Ottobre 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Leyden, John. 2019. “Hacktivism returns to its roots as a cyber warfare tool.” Accesso 4 Dicembre 2021 https://portswigger.net/daily-swig/hacktivism-returns-to-its-roots-as-a-cyber-warfare-tool

Lindsay, R. Jon, Cheung, Tai Ming, Reveron, S. Derek. 2015. *China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain*. USA: Oxford University Press

Malenkovich, Serge. 2013. “Che cosa sono i rootkit?” Accesso 14 Novembre 2021. https://www.kaspersky.it/blog/che-cosa-sono-i-rootkit/645/

Marioni, Silvano. 2019. "Password e metodi di autenticazione: caratteristiche tecniche e nuove soluzioni.” Accesso 25 Ottobre 2021 https://www.cybersecurity360.it/soluzioni-aziendali/password-e-metodi-di-autenticazione-caratteristiche-tecniche-e-nuove-soluzioni/

Miller, L. Alice. 2008. “The CCP Central Committee’s Leading Small Groups.” *China Leadership Monitor*, No. 26; https://*doi*.org/10.1163/9789004302488_011.

Minghui. 2000. “Falun Gong Mailboxes Attacked.” Accesso 7 Dicembre 2021. http://en.minghui.org/html/articles/2000/4/28/8378.html#.UI6ApMXEZ_Q

Nohe, Patrick. 2019. “How strong is 256-bit Encryption?” Accesso 24 Ottobre 2021. https://www.thesslstore.com/blog/what-is-256-bit-encryption/

Perlman, Radia. 1999. “An overview of the PKI trust model” *IEEE Network: The Magazine of Global Internetworking* - Volume 13Issue 6 - November 1999 pp 38–43 - https://doi.org/10.1109/65.806987

Privacy365EU. 2019. “Definizioni e best practice : Data Encryption in-transit, at-rest, end-to-end.” Accesso 9 Ottobre 2021. https://www.privacy365.eu/definizioni-e-best-practice-data-encryption-in-transit-at-rest-end-to-end/

Purdy, Matthew. 2001. “The Making of a Suspect: The Case of Wen Ho Lee.” Accesso 4 Dicembre 2021. https://www.nytimes.com/2001/02/04/us/the-making-of-a-suspect-the-case-of-wen-ho-lee.html

Ransomware Task Force. 2021. “Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force” Accesso 17 Novembre 2021. https://securityandtechnology.org/ransomwaretaskforce/report/

Razzini, Andrea. 2019. “Attacchi Logic Bomb: cosa sono, come funzionano e come difendersi dai malware ad orologeria.” Accesso 19 Novembre 2021. https://www.cybersecurity360.it/nuove-minacce/attacchi-logic-bomb-cosa-sono-come-funzionano-e-come-difendersi-dai-malware-ad-orologeria/

Sanger, David. 2013. “Chinese Army Unit Is Seen as Tied to Hacking Against U.S..” Accesso 14 Dicembre 2021. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Schneier, Bruce, Ferguson, Niels, Khono, Tadayoshi. 2010. *Cryptography Engineering Design Principles and Practical Applications*. USA: Wiley Publishing

Sectigo. 2020. “Public Keys and Private Keys in Public Key Cryptography.” Accesso 13 Ottobre 2021. https://sectigo.com/resource-library/public-key-vs-private-key

Senatore, Giancarlo, Lorenzo, Fabio, Galasso, Giovanna. 2019. “Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber.” Accesso 17 Ottobre 2021. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwia6cTrh8P1AhX-_rsIHcuwDtIQFnoECAIQAQ&url=https%3A%2F%2Fwww.pwc.com%2Fit%2Fit%2Fpublications%2Fdocs%2Fstudy-on-the-scale-and-Impact.pdf&usg=AOvVaw3Ya2f5Fy6HJEkY28jLg5Ie

Singer, W. Peter, Friedman, Allan. 2014. *Cybersecurity and Cyberwar What Everyone Needs to Know*. USA: Oxford University Press

Tarabay, Jamie. 2021. “China Shows Its Hacking Prowess at $2 Million Contest.” Accesso 12 Dicembre 2021. https://www.bloomberg.com/news/newsletters/2021-10-29/china-shows-its-hacking-prowess-at-2-million-contest

Tiwari, Aditya. 2021. “What Is The Difference: Viruses, Worms, Ransomware, Trojans, Malware, Spyware, Rootkit.” Accesso 21 Ottobre 2021. https://fossbytes.com/difference-viruses-worms-ransomware-trojans-bots-malware-spyware-etc/

Vienazindyte, Ilma. 2020. “La crittografia end to end spiegata per bene.” Accesso 12 Novembre 2021. https://nordvpn.com/it/blog/crittografia-end-to-end/

Wangen, Gaute. 2015. “The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism.” *Information*, *6*, 183-211. https://doi.org/10.3390/info6020183

Warner, Micheal. 2012. “Cybersecurity: A Pre-history, Intelligence and National Security.” 27:5, 781-799, DOI: 10.1080/02684527.2012.708530

Wikipedia. n.d. “Conficker” Accesso 7 Novembre 2021. https://en.wikipedia.org/wiki/Conficker#Origin

Fonti Schede Terminografiche

Comitato interministeriale per la sicurezza della Repubblica (CISR). 2019. “Il glossario di sicurezza cibernetica” Accesso 7 Gennaio 2022. https://www.sicurezzanazionale.gov.it

Computer Security Incident Response Team (CSIRT). n.d. “Glossario”. Accesso 15 Gennaio 2022. https://csirt.gov.it/glossario

HarperCollins Publishers. n.d., Collins English Dictionary. Accesso 9 Gennaio 2022. https://www.collinsdictionary.com/

ICANN. n.d. “缩略语和专有名词” Accesso 10 Gennaio 2022. https://www.icann.org/zh/icann-acronyms-and-terms?nav-letter=a&page=1

Kaspersky. n.d. “Kaspersky IT Encyclopedia”. Accesso 10 Gennaio 2022. https://encyclopedia.kaspersky.com/glossary/

National Institute of Standards and Technology (NIST). n.d. “Glossario” Accesso 9 Gennaio 2022. https://csrc.nist.gov/glossary

Oxford University Press. n.d. Oxford Reference. Accesso 10 Gennaio 2022. https://www.oxfordreference.com

Sensagent. n.d. “Sensagent online dictionary”. Accesso 9 Gennaio 2022. http://dictionary.sensagent.com/

Treccani. n.d. Enciclopedia Treccani. Accesso 11 Gennaio 2022. https://www.treccani.it/

Zanichelli. 2014. “Glossario dei Termini Informatici” Accesso 8 Gennaio 2022. https://online.scuola.zanichelli.it/addomineinformatica/edizione-2011/glossario/

江门市政务服务数据管理局. n.d. “网络信息安全术语” Accesso 10 Gennaio 2022. http://www.jiangmen.gov.cn/bmpd/jmszwfwsjglj/ztzl/wlxxaq/syjs/

網易. n.d. 有道词典. https://www.youdao.com/

项,晓春, 刘, 广魁. 2000. "SCADA 系统及其应用." *自动化技术与应用* 19.6 (2000): 19-22.