#01

ICT Security MAGAZINE

CYBER INTELLIGENCE

INTRODUZIONE DI

MATTIA SICILIANO

Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare

2022

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINIT.ORG

ICT Security MAGAZINE

QUADERNI DI CYBER INTELLIGENCE

La presente collana, frutto della collaborazione tra ICT Security Magazine e la Società Italiana di Intelligence (SOCINT), inaugura una serie di contenuti volti ad arricchire ed approfondire il dibattito scientifico sulla Cyber Intelligence.

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT è un'associazione scientifica senza fini di lucro, il cui obiettivo è quello di promuovere la cultura e lo studio dell'intelligence in Italia.

Indice

Introduzione a cura di Mattia Siciliano, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

INTRODUZIONE

La Commissione *Cyber Threat Intelligence* e *Cyber Warfare* (di seguito "Commissione"), parte integrante della SOCINT (Società Italiana di Intelligence), ha avviato un progetto di ricerca e studio volto a comprendere il fenomeno C*yber Intelligence* e *Cyber Warfare*.

I risultati del progetto sono rappresentati in un quaderno tematico che si apre con questo primo volume di inquadramento del fenomeno e prosegue con approfondimenti su aspetti più specifici, come di seguito illustrato.

La ricerca si divide in due macro-parti: la prima si focalizza soprattutto sugli aspetti giuridici e geopolitici, mentre la seconda parte fa riferimento all'applicazione di tecnologia cyber utile al sistema Paese, con l'obiettivo di comprenderne le dinamiche, le sfide, i rischi e le opportunità. La natura delle minacce cyber e le informazioni derivanti dalle attività d'intelligence interessano tutti gli attori istituzionali e non, tanto da incidere sulla capacità delle stesse istituzioni di definire nuovi meccanismi per fronteggiare inediti rischi: non necessariamente riferibili

solo alla sfera economica, bensì anche agli aspetti di innovazione tecnologica.

Molte, infatti, sono le variabili in gioco – tra loro interdipendenti – interne ed esterne al campo d'azione. Il fenomeno cyber non è facilmente prevedibile sia per i continui sviluppi della tecnologia, sia per le strategie messe in campo dai diversi attori esistenti nel mercato, sia per la capacità competitiva degli operatori pubblici e privati, sia per le politiche di regolamentazione e sia, infine, per i comportamenti di imprese e individui.

Ciò detto, pur con i limiti concettuali sopra esposti, gli obiettivi generali della ricerca possono essere così declinati:

- evidenziare le principali tematiche aperte in ambito cyber e intelligence, nell'ottica di prevenire gli effetti rischiosi sulla protezione degli asset essenziali e di salvaguardare la capacità d'innovazione degli operatori;
- suggerire possibili azioni/soluzioni, tecnologiche e non, ove ritenute utili.

Per la realizzazione del progetto di ricerca, la Commissione ha scelto di chiedere ad ogni membro della stessa di analizzare nel dettaglio un tema specifico nel contesto della *cyber security* e della *cyber intelligence*.

Il lavoro complessivo che ne è scaturito può essere visto come un approfondimento della proposta[1] già inoltrata alla neonata Agenzia di Cybersicurezza Nazionale (ACN) che ha di recente visto l'apporto di significativi contributi anche da altre Associazioni e Istituzioni italiane.

Mattia Siciliano, Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare

[1] https://news.socint.org/agenzia-cybersicurezza-nazionale/

BIOGRAFIA

Mattia Siciliano

L'ing. Siciliano ha oltre 15 anni di esperienza in Cyber Security e Cyber Intelligence. Attualmente è Business Director per una società internazionale con sede negli Emirati Arabi Uniti. In precedenza, partner e co-fondatore di DeepCyber, una società boutique focalizzata sulla Cyber Threat Intelligence e manager in diverse società di consulenza come EY e KPMG. Docente all'Università degli Studi di Napoli Federico II. Consulente per Ministero della Difesa (Innova Difesa), agenzie di intelligence e forze dell'ordine. Presidente della Commissione di Studio in Cyber Threat Intelligence e CyberWarfare della Società Italiana di Intelligence.

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**

Una riflessione preliminare sul processo di istituzionalizzazione della Cyber Intelligence

«There is nothing more necessary than good intelligence to frustrate a designing Enemy: and nothing that requires greater pains to obtain»

George Washington a Robert Hunter Morris, 1 January 1756[1]

«Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool and therefore strange, spooky"

New York magazine, 23 December 1996

ASPETTI CONCETTUALI E DEFINITORI PROPEDEUTICI A UN PROCESSO DI ISTITUZIONALIZZAZIONE DELLA CYBER INTELLIGENCE

L'attuale campo disciplinare della *Cyber Security* (CS)[2] è connotato da un'inflazione di termini definitori di cui *Cyber Threat Intelligence* (CTI), *Cyber Intelligence* (CI) e *Cyber Counter Intelligence* (CCI) ne rappresentano esempi preclari. Tutti e tre, difatti, sono costrutti concettuali chiaramente collegati gli uni agli altri in quanto vi sono sì differenze sostanziali tra gli stessi ma vi sono altrettanti aspetti comuni, sia nei metodi di collazione delle informazioni che nel loro più generale modus operandi. Vi è da dire, inoltre, che le stesse definizione di CTI, CI e CCI che si ritrovano comunemente in documenti ufficiali, articoli scientifici, materiale divulgativo e pubblicitario non sono per nulla univoche e, dunque, con significativi gradi di variabilità interna. Una breve esposi-

zione, di carattere definitorio, può senz'altro esemplificare tale aspetto.

Si può iniziare da quello relativo alla CTI in cui è centrale il concetto di minaccia la quale è «*any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability*»[3] .

Una definizione di CTI[4], utilizzata da un fornitore di servizi, è la seguente: «*Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security*

[1] https://founders.archives.gov/documents/Washington/02-02-02-0255

[2] A solo titolo esemplificativo, il "Dictionary of Military and Associated Terms" così definisce il termine CS facendo uso di un'accezione un po' datata, quella di cyberspace security. Cyberspace security: «Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation» (DoD, 2021:55), Department of Defense (DoD), Dictionary of Military and Associated Terms, November, 2021.
Un'altra definizione è la seguente, più estesa e onnicomprensiva. «Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure», National Initiative for Cybersecurity Careers and Studies (NICCS), <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[3] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, 2006.

[4] CTI «is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Examples of cyber threat information include indicators (system artifacts or observables associated with an attack), TTPs, security alerts, threat intelligence reports, and recommended security tool configurations», National Institute of Standards and Technology (NIST) SP 800-150, Guide to Cyber Threat Information Sharing, October, 2016.

decisions and change their behavior from reactive to proactive in the fight against threat actors».[5]
In questo caso, l'accento è posto sull'acquisizione di dati mentre in una definizione utilizzata da una società di consulenza viene evidenziato l'aspetto della conoscenza basata sulle evidenze empiriche, dunque, con modalità non troppo dissimili dalla precedente.

«*Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard*».[6]
In una terza definizione, essa è maggiormente incentrata sulle motivazioni, intenzioni e metodi messi in atto dagli attori malevoli.
«*Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise*».[7]

Se si passa a prendere in esame il costrutto di CCI si nota la stessa variabilità[8]. Essa viene definita come «*all efforts made by one intelligence organization to prevent adversaries, enemy intelligence organizations or criminal organizations from gathering and collecting sensitive digital information or intelligence about them via computers, networks and associated equipment*»[9].
In essa sono contemplate, in buona sostanza, tutte le misure atte a identificare, penetrare o neutralizzare le azio-

[5] Kurt Baker, What is Cyber Threat Intelligence?, 18 February 2021

[6] Gartner, Definition: Threat Intelligence, 16 May 2013

[7] Jon Friedman & Mark Bouchard, Definitive Guid to Cyber Threat Intelligence. Using Knowledge about Adversaries to Win the War against Targeted Attacks, Annapolis (MD), CyberEdge Press, 2015, p. 6.

[8] Per una panoramica generale del concetto, cfr. Petrus Duvenage & Sebastian "Basie" von Solms, Cyber Counterintelligence. Back to the Future, "Journal of Information Warfare", v. 13, n. 4, 2014.

[9] Cyber Intelligence and Investigations, https://www.aslitsecurity.com/cyber-intelligence.html

ni dell'avversario e il focus è non solo sull'intrusione, ma anche sull'intento dell'attore malevolo e sulle modalità operative da questi utilizzate. Essa si connota, dunque, come un sottocampo della CI, di cui ne rappresenta una postura prettamente offensiva.

Il concetto di CI può essere inteso in termini più generali rispetto a quelli di CCI e CTI in quanto ci si riferisce agli «*efforts made by intelligence organizations to prevent adversaries or enemy intelligence organizations from gathering and collecting sensitive information or intelligence about them*»[10].
In un'altra definizione l'accento è posto sulle modalità di raccolta delle informazioni, ovvero «*the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision-making*»[11].
Come si è potuto vedere da questa breve esposizione, ridotta solo per ragioni di spazio, vi sono concetti quali CI, CCI e CTI che si sovrappongono in parte tra di loro ma anche con una forte variabilità nell'utilizzo dello stesso termine.

Vi è, infine, da aggiungere che lo stesso concetto CI è interessato da tali ambiguità semantiche sia dal lato del concetto di "intelligence"[12] il quale viene spesso utilizzato, in maniera intercambiabile, sia con quello di "dati" e di "informazioni sia con quello di cyber (spazio)[13] il quale, anch'esso, viene spesso

[10] Ivi

[11] Carnegie Mellon University, Software Engineering Institute, https://resources.sei.cmu.edu/library

[12] Intelligence: «1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities», Department of Defense (DoD), Dictionary of Military and Associated Terms, November, 2021, p. 107

[13] «Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations targeting the physical and informational dimensions of the IE also have an impact in the human cognitive dimension», Department of Defense (DoD), Strategy for Operations in the Information Environment, June 2016, p. 3.

inteso come un sottocampo di quello di *"Information Environment"* (IE)[14].

Tornando alla disamina dei tre costrutti concettuali della CI, CTI e CCI, nell'interpretazione degli stessi può essere utile far riferimento a quello che viene chiamato il ciclo dell'intelligence[15] mediante il quale i dati grezzi vengono identificati, raccolti e poi sviluppati in informazione rifinita, messa a disposizione del processo decisionale. In questo senso, si può operare una suddivisione analitica tra intelligenza tattica, operazionale e strategica[16] . Facendo uso di questo *framework* operativo si può mettere in evidenza che la CTI sembra essere caratterizzata soprattutto da un livello tattico ed operazionale così come, a livello di scala, essa agisce tipicamente su un livello prettamente organizzativo, mentre la CI è caratterizzata da un livello strategico, in quanto è più legata a un focus olistico e, in qualità di attori, riguarda i vertici aziendali e i decisori politici a livello nazionale. La CTI mira, difatti, al rilevamento di possibili indicatori di minaccia al livello dell'analista operativo e, considerato il flusso continuo di dati, il suo utilizzo necessita di essere abbondan-

[14] «The IE is a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. With its function as a conduit for influence on decision-making and command and control, the IE is a key component of the commander's operational environment. Characterized by ubiquitous on-demand media and interpersonal hyper-connectivity, today's IE enables collaboration and information sharing on an unprecedented scale», *ivi.*

[15] Sono stati proposti molteplici cicli dell'intelligence ma questa non è la sede adatta per approfondire tali aspetti. Qui basti presentarne uno composto da 5 fasi: 1) Planning and Direction; 2) Collection; 3) Processing and Exploitation; 4) Analysis and Production; 5) Dissemination and Integration, https://countuponsecurity.com/2015/08/15/the-5-steps-of-the-intelligence-cycle/

[16] L'intelligenza tattica «provides analysis, maps, and data to support an operation or disaster response effort, and fulfilling short term, case-specific needs», Luisa Dall'Acqua & Irene Maria Gironacci, Transdisciplinary Perspectives on Risk Management and Cyber Intelligence, Hershey (PA), IGI, 2021.
Quella operazionale «provides an investigative team with hypotheses and inferences concerning specific elements of illegal operations of any sort. These will include criminal networks, individuals or group involved in unlawful activities, as well as methods, capabilities, vulnerabilities, limitations and intentions» *(ivi)*.
In ultimo, l'intelligenza strategica «takes a "big picture" view of competitor/criminal/terrorist activity. It focuses on the long-term aims of law enforcement agencies, and, in a criminal context, on crime environment, threats to public safety and order, counter programs, avenues for change to policies, programs, and legislation» *(ivi)*.

temente filtrato prima di essere utilizzato, come informazione strategica, dai responsabili delle decisioni strategiche.

La CCI, invece, è la stessa CI, intesa in maniera speculare, ovvero impiegata con una postura prettamente offensiva tesa a colpire le attività e le risorse degli avversari. È per questa ragione che il suo utilizzo è più sporadico e viene poco enfatizzata nei documenti ufficiali, negli articoli scientifici e nel materiale divulgativo in quanto tipicamente di competenza delle autorità militari e statuali, ovvero non nell'effettiva disponibilità delle imprese.

Del resto, tale interpretazione viene sottolineata anche in letteratura. «*The focus on CTI is more due to a catch-phrase in marketing services than real understanding of the concepts. CTI as is provided cannot be considered true intelligence as it is a stream of data; it is not in context and it is limited in how actionable it is. Whilst network security devices and cyber security analysts can use CTI as an aid in detecting possible threats, the real intelligence is the analysis and interpretation of any indicators that have found matches in the network. Therefore, CTI on its own is of limited use; it needs to correlated with internal data (processing) to provide possible threat detections, which can then be analysed and interpreted to form an improved view of the threat environment*»[17].

Come si può evincere da questo lungo estratto la CTI si riferisce ai dati che vengono raccolti, elaborati e analizzati per comprendere le motivazioni, gli obiettivi e i comportamenti di attacco di un attore malevole. L'intelligence relativa alle minacce cibernetiche consente, difatti, di prendere decisioni di sicurezza basate sui dati le quali sono più rapide, più informate così come, più in generale, di cambiare il comportamento di difesa cibernetica da uno meramente reattivo a uno più proattivo. Si tratta di una tipica conoscenza basata sulle evidenze apportate dai dati, vale a

[17]-Brett van Niekerk, Trishana Ramluckan & Petrus Duvenage, An Analysis of Selected Cyber Intelligence Texts, 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal, July, 2019, p. 555.

dire *data-driven*, relativa alle minacce esistenti o emergenti o sui rischi per gli *asset*, sia essi aziendali oppure statuali.

Di tutt'altra natura, invece, l'essenza precipua della CI la quale si situa a un livello superiore e può racchiudere, dunque, al suo interno, come sotto-campi specifici sia la CCI che la CTI. In questo senso, la CI riesce a ricomprendere al suo interno gli aspetti tattici e operazionali davvero importanti al fine di includere sia l'ambiente tecnologico e operativo delle minacce sia per identificare ciò che è legato al fattore umano ed è basato, dunque, su una serie di fattori organizzativi interni. Nello stesso tempo, la CI riesce ad esplicare tutta la sua funzione precipua al livello laddove vengono prese le decisioni strategiche, nell'interesse della nazione o dell'azienda.
Il passaggio da una conoscenza tipicamente tecnica e operativa a quella di più alto livello rappresenta un passaggio obbligato compiuto da tutte le discipline che, nel corso del loro sviluppo, hanno consolidato e sistematizzato vieppiù il loro *background* di conoscenze teoriche tanto da divenire un campo disciplinare ampiamente legittimato a livello internazionale, con un crescente peso all'interno dei boards aziendali e nei livelli apicali delle entità statuali, con propri percorsi di studi universitari, conferenze e riviste scientifiche dedicate[18].
Il che vuol dire, sostanzialmente, l'aver contribuito a creare una diffusa comunità di esperti i quali si riconoscono in una serie di principi scientifici, codici deontologici e di tecniche operative.

È chiaro, dunque, che per un ulteriore consolidamento di un processo di istituzionalizzazione della tematica della CS appare rilevante accentuare, ancor di più, rispetto a quanto fatto finora gli aspetti legati alla CI. L'intelligence a tutto tondo da svolgere anche nel dominio cyber non può che basarsi sulla centra-

[18] In questo percorso, la nascita di una rivista scientifica è, infine, un chiaro indizio di un processo di istituzionalizzazione del campo disciplinare. Storicamente, difatti «new scholarly journals appeared when new subjects of study achieved disciplinary or subdisciplinary status. Today, they are also created when new audiences and communities of scholarly practice appear», Susan Maret, The Charm of Secrecy. Secrecy and Society as Secrecy Studies, "Secrecy and Society", November, 2016, p. 1.

lità di tale componente ed essa abbisogna di essere maggiormente innervata dalle competenze di altre discipline, siano esse appartenenti alle scienze "dure" ma anche a quelle latamente umanistiche. Tale percorso, del resto, è lo stesso compiuto, già in precedenza, dalla disciplina madre, ovvero quella degli studi dedicati all'Intelligence[19]. Detto in altri termini, in un campo quale quello della CI dove sembrano predominare gli aspetti tecnico informatici e che da questi traggono la loro stessa esistenza materiale (reti, hardware, software, ecc..) potrebbe essere, invece, nondimeno utile fuoriuscire in direzione di un percorso nettamente multidisciplinare piuttosto che solo disciplinare, peraltro del tutto complementari. Anche solo da un punto di vista della pratica professionale quotidiana le competenze apportare da altre discipline possono essere, in moltissimi casi, di estremo interesse per la CI, in quanto la metodologia per affrontare i problemi conoscitivi e i processi decisionali sono sostanzialmente gli stessi. L'intelligence è, allo stesso tempo, un prodotto e un processo di raccolta, elaborazione, analisi e utilizzo delle informazioni per soddisfare un obiettivo ben preciso.

In una conferenza del 2012 veniva messo in evidenza proprio questo aspetto comune a più discipline. *«Professionals in other fields… also face many similar challenges to those that exist in intelligence analysis, including: difficulties acquiring information from a wide variety of sources, vetting and evaluating the information that is acquired, deriving understanding and meaning from that information, impact of deadlines, editing, and other production processes on accuracy of analysis and assessment, problems in dissemination and*

[19] Ad esempio, il processo di accademizzazione seguita da quest'ultima può essere definita come «the academic research, conceptualization, and teaching about the field of intelligence. Its goal is to study the world of intelligence's essence, activities, and influence on the national security of the state and its decision-making processes. The process of the academization of intelligence presupposes its interdisciplinary character and its inherent connection to cognate fields of knowledge, such as political science, international relations, history, psychology, and so forth», Kobi Michael & Aaron Kornbluth, The Academization of Intelligence. A Comparative Overview of Intelligence Studies in the West, "Cyber, Intelligence and Security", v. 3, n. 1, May, 2019, p. 118.

distribution to consumers or customers, managing relationship between producer and consumer (role, responsibility, independence & objectivity), developing professional infrastructure (recruit, select, train, & develop personnel; code of ethics), and overcoming impact of changing technology and alternative information distribution systems. How do practitioners in various non-intelligence fields overcome these kinds of challenges? How are their challenges similar to or different from those that exist in the intelligence arena? What can be learned from the comparison?»[20]

In definitiva, molte delle sfide che la CI affronta non sono uniche come si può credere a un primo e superficiale sguardo e questo anche perché una certa insularità e tecnofilia del campo disciplinare può ostacolare la messa in comune di metodologie e pratiche da parte di altre discipline.

CONCLUSIONI

A livello di costrutti concettuali il campo disciplinare della CI è attraversato da tensioni definitorie promosse da parte di tutte le entità e gli attori che ne fanno parte. Tale frammentazione è, tuttavia, indizio sia di una crescita impetuosa che di un carente consolidamento a livello disciplinare. A questo riguardo, ulteriori indagini dovrebbero essere svolte in una prossima fase, anche mediante ricerche qualitative di analisi testuale, al fine di acquisire maggiori informazioni in merito a tale aspetto.

Dalla breve disamina qui condotta sono emerse delle differenze tra il concetto di CI e quello di CTI mentre quello di CCI appare speculare a quello di CI. Tra tutti e tre i termini la CI viene considerata maggiormente adatta a sottolineare il carattere olistico, strategico e di alto livello di tale disciplina emergente mentre quello di CTI sembra far riferimento soprattutto a un livello organizzativo,

[20] Stephen Marrin, Intelligence Studies, Intelligence Analysis, and Multidisciplinary Learning, 2017, p. 1, https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179893.pdf

localizzato su scala locale nonché tattico ed operazionale.

Un altro aspetto che emerge dalla breve ricognizione sul campo, svolta con modalità di fonti aperte, è che la prevalenza delle definizioni attualmente in uso deriva soprattutto dal campo delle agenzie governative e del settore commerciale dei fornitori di tecnologia e servizi della CS e già ciò appare essere un indizio di un parziale o carente processo di istituzionalizzazione di tale tematica. In buona sostanza, nel suo sviluppo continuano a prevalere aspetti istituzionali ed economici piuttosto che esigenze correlate allo sviluppo di un campo scientifico univoco e ben determinato.

Si ritiene inoltre che, riguardo all'ulteriore consolidamento disciplinare della CI, potrebbe giovare non solo una maggiore acribia di tipo concettuale quanto piuttosto un orientamento teorico maggiormente comprensivo dell'apporto di altre discipline scientifiche, in una tipica ottica multidisciplinare. Il passaggio da un insieme di tecniche e metodologie, di attività e di pratiche professionali, in direzione di una disciplina scientifica orientata da una conoscenza istituzionalizzata necessita, difatti, a parere dello scrivente, di una serie di ulteriori passaggi i quali devono per forza ricomprendere sia una chiarificazione concettuale che una maggiore definizione dei suoi confini disciplinari.

Vale qui sottolineare, *en passant*, che la multidisciplinarità riguarda lo studio di una tematica non in una sola disciplina ma in più discipline contemporaneamente ma essa rimane sempre al servizio, prettamente in funzione ancillare, della disciplina centrale, che in questo caso sarebbe la CI.

Un ulteriore aspetto è quello, infine, dell'orientamento al valore sotteso a questa tematica così come alla socializzazione diffusa delle basilari tecniche e metodologie corrispondenti, ad esempio in termini di cyber igiene divulgata presso tutto il corpo sociale[21], che la società nel suo complesso considera degna di rappresentare l'interesse collettivo. Quest'ultimo aspetto sembra, oggigiorno, essere in via di consolidamento sia per l'incremento degli at-

tacchi ransomware i quali hanno accresciuto tantissimo il valore sociale e collettivo della sicurezza cibernetica sia per il crescente processo di digitalizzazione del Paese, anche a seguito delle ingenti risorse messe a disposizione del pino Nazionale di Ripresa e Resilienza (PNRR) il quale non potrà che accentuare maggiormente tale orientamento al valore.

In conclusione, la consapevolezza finale che deriva da questa breve esposizione è che per una piena comprensione della valenza strategica della CI essa non possa essere declinata solo dal punto di vista tecnico e tecnologico.

Il campo della CI è, di fatto, socialmente e culturalmente costruito in quanto lo spazio cibernetico è uno spazio costantemente ri-descritto e ri-negoziato e il cui potere può essere appannaggio anche da parte di piccole entità organizzative quali gli attivisti, le *gang* cybercriminali di media entità oppure potenti entità di emanazione statuale. Intesa in questo senso, il fondamento multidisciplinare della CI ha come precipuo *focus* di interesse il tessuto costitutivo di molteplici discipline in vista del consolidamento della CI. Ciò implica che quest'ultima debba sempre più mettere in conto una relativa espansione del campo di analisi al fine di includere nuove teorie e nuove metodologie; ciò significa tendere verso una più complessiva integrazione del più ampio contesto socioeconomico entro cui essa si situa ed è storicamente situata.

Achille Pierre Paliotta, *Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL).*

[21] Achille Pierre Paliotta, Cybersicurezza, dall'Agenzia nazionale l'impulso per un vero cambiamento, "Agenda digitale", 1 ottobre, 2021, https://www.agendadigitale.eu/sicurezza/cybersicurezza-i-tempi-sono-maturi-dallagenzia-nazionale-limpulso-per-un-vero-cambiamento/

BIOGRAFIA

Achille Pierre Paliotta

Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL). Laurea in Sociologia all'Università di Roma "La Sapienza", Master in Data Science (DS) all'Università di Roma "Tor Vergata" nel 2015 e Master in Cybersecurity (SIIS) all'Università di Roma "La Sapienza" nel 2021. Svolge studi e ricerche sull'innovazione tecnologica, sulla cyber intelligence, sulla cybersicurezza, sulle professioni, sull'incrocio tra domanda ed offerta di lavoro, sulla formazione continua, sull'invecchiamento attivo, sulla contrattazione collettiva e, in generale, su tematiche di sociologia economica.

La Strategia dell'Unione europea sulla cibersicurezza a fronte delle recenti minacce ibride: l'istituzione di un'Unità congiunta sul ciberspazio finalizzata alla realizzazione del ciber-scudo europeo

L'intensità, la sofisticazione e la pervasività degli attacchi informatici1 specie ibridi, compiuti a danno di entità critiche (pubbliche e private) nel panorama internazionale ha spinto l'Unione europea a dotarsi di una politica e di una strategia della cibersicurezza[1].

L'azione dell'UE risponde all'esigenza avvertita nel contesto internazionale di garantire un ciberspazio globale, stabile e sicuro[2] in quanto ritenuto indispensabile per favorire una trasformazione digitale sicura dell'economia[3] e per affrontare le nuove sfide poste dai servizi e prodotti digitali, quali i Cloud, il 5G e l'intelligenza artificiale[4].

A fronte delle profonde vulnerabilità tecnologiche di sistemi e reti dell'informazione e della comunicazione, il legislatore europeo ha previsto un quadro

[1] V. State of the Union: Commission Proposes a Path to the Digital Decade to Deliver the EU's Digital Transformation by 2030, in www.digital-strategy.ec.europa.eu

[2] V. Commissione europea, Alto Rappresentante dell'Unione per gli affari esteri e la politica della sicurezza, Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, 7 febbraio 2021, Join(2013) 1 final, p. 2.

[3] V. A. BENDIEK, E. PANDER MAAT, The EU's Cybersecurity Policy: Building a Resilient Regulatory Framework, in G. SIBONI, L. EZIONI (eds.), Cybersecurity and Legal-Regulatory Aspects, Tel Aviv, 2021, p. 23.

[4] Cfr. Consiglio UE, Relazione del 16 dicembre 2020 sull'impatto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G, SWD(2020) 357 final.

di azioni coerenti relative agli aspetti normativi, operativi, diplomatici e di difesa della cibersicurezza. Esso è rivolto a garantire il funzionamento del Mercato unico[5] e la protezione della sovranità digitale[6] anche alla luce dei crescenti investimenti degli Stati – membri e terzi - nelle *cyber capabilities* offensive, realizzati non solo per scopi militari.

La finalità perseguita dall'Unione è la strutturazione di una risposta rapida, efficiente ed efficace alle azioni offensive da attuare sulla base di un coordinamento politico, tecnico e operativo e attraverso strumenti innovativi, tra i quali spicca la proposta di istituire un'Unità congiunta sul ciberspazio.

Infatti, nelle **Conclusioni** dell'8 ottobre 2021 su "Esplorare il potenziale dell'iniziativa concernente un'Unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala"[7], il Consiglio UE partendo dalla condivisione del quadro giuridico proposto dall'ONU sul **comportamento responsabile** degli Stati nel ciberspazio, ha iniziato a elaborare una propria linea di *cyber defense*.

In proposito, si rammenta che, attualmente, il quadro normativo internazionale si incardina sul progetto di un Codice internazionale di condotta per la sicurezza delle informazioni[8] e sulle nor-

[5] V. Commissione europea, Alto Rappresentante dell'Unione per gli affari esteri e la politica della sicurezza, Comunicazione congiunta al Parlamento europeo, cit., p. 2.

[6] V. Sulla nozione di sovranità riferita al ciberspazio, G.P. CORN, R. TAYLOR, Sovereignty in the Age of Cyber, in American Society of International Law, 2017, p. 207; M.N. SCHMITT, L. VIHUL, Tallin Manual 2.0, The International Law Applicable to Cyber Operations, Cambridge, 2017, p. 12 ss., Rule 4, secondo cui «[c]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law» sul presupposto che «States enjoy sovereignty over cyber infrastructure, persons, and cyber activities located on their territory. This includes both public and private cyber infrastructure». V. anche J. POHLE, Digital Sovereignty, in Internet Policy Review, 2020

[7] V. conclusioni del Consiglio dell'8 ottobre 2021, Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala, Doc. 12534/21, par. 8.

[8] La proposta del Codice è stata redatta da Cina, Russia, Tagikistan e Uzbekistan e sottoposto all'Assemblea generale che lo ha pubblicato nella risoluzione del 13 gennaio 2015, UN Doc.AG/RES/69/723.

me di *cyber international law* contenute nei rapporti redatti dai gruppi di lavoro[9] che, parallelamente, in seno all'ONU si occupano di individuare «il comportamento responsabile degli Stati nel cyber spazio nel contesto della sicurezza internazionale»[10].
Nello specifico, nei rapporti indicati sono richiamati i principî di diritto internazionale generale relativi al rispetto della sovranità territoriale o dell'indipendenza politica degli Stati[11], al divieto della minaccia o dell'uso della forza, alla non ingerenza negli affari interni di uno Stato, all'obbligo di soluzione pacifica delle controversie e all'obbligo degli Stati di impedire che sul loro territorio si svolgano attività illecite, per citare i principali[32].

Sulla base di tali principî, gli Stati possono coordinare una risposta cinetica qualora l'attacco cibernetico subito assuma proporzioni ed effetti tali da minacciare la pace e la sicurezza internazionale. In tal caso è pacifico l'esercizio del diritto naturale alla legittima difesa individuale e collettiva (ex art. 51 della Carta ONU) e l'operatività del sistema di sicurezza collettiva della Carta dell'ONU (ex art. 39 ss. Carta ONU).

Analogamente, la NATO riconosce che al verificarsi di tale ipotesi sia consentito il ricorso alla capacità difensiva collettiva anche ibrida, cioè inclusiva dell'impiego di armi cibernetiche e cinetiche ex art. 5 del suo Statuto[12].

[9] L'individuazione del diritto internazionale applicabile alle attività nel ciberspazio è condotta sia dal UN Openended Working Group on Development in the Field of Information and Telecommunications in the Context of International Security (OEWG), creato dall'Assemblea generale nel 2018 e costituito da venticinque esperti internazionali, sia dal UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security (UNGEE) creato dall'Assemblea generale nel 2004, al quale partecipano gli Stati membri dell'ONU interessati. A ciò si aggiunga l'attività del Open-ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study of the Problem of Cybercrime, istituito nel 2019.

[10] Per il Segretario generale dell'ONU si tratta di attività "complementari"; v. l'ultimo rapporto del UNGEE contenuto nella lettera del 14 luglio, UN Doc. A/76/135, p. 4.

[11] V. l'art. 2 del Codice citato.

[12] V. l'art. 5 dello Statuto della NATO del 4 aprile 1949, www.nato.int. Cfr. M.N. SCHMITT, Tallinn Manual on the International Law Applicable to the Cyber Warfare, Cambridge, 2017, II ed., p. 24 ss.; E.D. BORGHARD, S.W. LONERGAN, Cyber Operations as Imperfect Tools of Escalation, in Strategic Studies Quarterly, 2019, p. 122 ss.

Dal canto suo, l'Unione europea già dal 2001 ha elaborato una politica di sicurezza delle reti e dell'informazione[13], che è uno degli obiettivi realizzati sia con l'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[14], sia con la prima Strategia sulla cibersicurezza nel 2013[15]. Le priorità strategiche ivi individuate - tutt'oggi attuali - riguardano lo sviluppo di capacità industriali e tecnologiche; la creazione di una politica internazionale coerente sul ciberspazio e lo sviluppo di una politica e di una capacità di resilienza e di ciberdifesa incardinata nella Politica di sicurezza e di difesa comune dell'Unione.

Successivamente, nel 2016 l'Unione ha proceduto all'adozione della direttiva sulla sicurezza delle reti e dei sistemi informativi[16] (direttiva NIS) al fine di garantire un elevato livello comune di cibersicurezza nell'UE. Tale direttiva rappresenta il punto di partenza nella gestione del rischio perché introduce requisiti di sicurezza obbligatori per i principali operatori economici che forniscono servizi essenziali e per i fornitori di alcuni dei principali servizi digitali[17]. Sul punto, la cooperazione tra gli Stati membri in materia di cibersicurezza è garantita dal 'Gruppo di cooperazione NIS' e dalla 'Rete dei gruppi di intervento per la sicurezza informatica in caso di incidente' (CSIRT).

[13] Nel 2001 la Commissione ha adottato la comunicazione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" (COM(2001) 298 def.); nel 2006 ha adottato "Una strategia per una società.

[14] V. il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, cui sono seguiti altri regolamenti di revisione, di cui l'ultimo è il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

[15] V. la Comunicazione congiunta della Commissione europea e del Servizio europeo per l'azione esterna, Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN(2013) 1 final.

[16] V. la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[17] V. la comunicazione della Commissione, Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza, COM(2016) 410 final.

La Strategia dell'Unione europea sulla cibersicurezza a fronte delle recenti minacce ibride: l'istituzione di un'Unità congiunta sul ciberspazio finalizzata alla realizzazione del ciber-scudo europeo

Di recente, la crescente diffusione dei dispositivi connessi ai sistemi operativi, c.d. "internet degli oggetti" (IoT), ha spinto il legislatore europeo a proporre la direttiva "NIS2" (sostitutiva della NIS) volta a **favorire la resilienza in tutti i settori** esclusi dalla precedente versione[18].

Contestualmente, stante il mutato ecosistema della cibersicurezza, nel dicembre 2020 la Commissione europea e l'Alto rappresentante per gli affari esteri e la politica della sicurezza hanno presentato una nuova Strategia dell'UE per la cibersicurezza, inclusiva di strumenti normativi, strategici e di investimento per costruire un'Europa resiliente e digitale.

Obiettivi fondamentali della Strategia in parola sono il raggiungimento dell'autonomia strategica, intesa quale capacità di compiere scelte autonome nel settore mantenendo un'economia aperta, il potenziamento della *leadership* digitale e il rafforzamento delle capacità strategiche dell'UE.

Il Consiglio ha ulteriormente precisato i settori d'intervento dell'attuale **decennio digitale** tra i quali – oltre alla revisione della direttiva sulla resilienza dei soggetti critici[19] e del regolamento relativo alla resilienza operativa digitale[20] – particolare attenzione è dedicata alla creazione dell'Unità congiunta per il ciberspazio. A tal fine, nelle citate **Conclusioni** di ottobre 2021 è stato ricostruito il quadro normativo di riferimento richiamando i principî di sussidiarietà, proporzionalità, complementarità, non duplicazione e riservatezza nonché la natura esclusiva della competenza statale in materia di sicurezza nazionale (art. 4, par. 2, TUE). Ad ogni buon conto, è fatta salva la competenza degli organi dell'UE qualora si tratti di incidenti

[18] V. la proposta del 16 dicembre, COM(2020) 823 final.

[19] V. la proposta di direttiva sulla resilienza dei soggetti critici, COM(2020) 829 final.

[20] V. la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) N. 600/2014 e (UE) n. 909/2014, COM(2020) 595 final; proposta di direttiva che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE 2016/2341, COM(2020) 596 final.

e crisi di cibersicurezza su vasta scala che ledano il corretto funzionamento del Mercato unico e la sicurezza interna dell'UE. L'Unità in esame è stata ritenuta essenziale dalla Presidente della Commissione europea, Ursula von der Leyen, già nelle Linee guida per la Commissione europea 2019-2024[21], per dotare l'UE e gli Stati membri di una **risposta coordinata in situazioni di emergenza** dovute ad attacchi e incidenti di carattere transfrontaliero.

A tale Unità spetterà pertanto il compito di coinvolgere gli esperti delle comunità della cibersicurezza sulle decisioni di attribuzione di un attacco informatico e sulla gestione e mitigazione delle crisi informatiche dell'UE. Essa coordinerà anche i meccanismi di assistenza, su richiesta di uno o più Stati membri, integrando i meccanismi orizzontali e settoriali di risposta alle crisi dell'UE già esistenti. Il riferimento è all'allineamento di meccanismi e processi esistenti in ambito statale ed europeo, con particolare riguardo alle procedure di cooperazione e di condivisione delle informazioni esistenti a tutti i livelli necessari – tecnico, operativo, strategico/politico e diplomatico[22] – tra Stati membri[23] e tra istituzioni, organi e agenzie dell'UE[24].

Da un punto di vista operativo, l'Unità in parola e i centri operativi di sicurezza (SOC2) costutuiranno una **Rete** che, entro il 2023, rappresenterà il **ciberscudo** europeo. A tal fine, l'Unità sarà com-

[21] V. Ursula von der Leyen, Linee guida politiche per la prossima Commissione europea 2019-2024, 16 luglio 2019.

[22] V. la comunicazione congiunta al Parlamento europeo e al Consiglio, Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale, del 23.6.2021, JOIN(2021) 14 final.

[23] Si pensi al Gruppo di cooperazione NIS e alla rete di CSIRT, alla rete delle organizzazioni di collegamento per le crisi informatiche fra cui la Cyber Crisis Liaison Organisation Network (CyCLONe), alla Cooperazione strutturata permanente e volontaria (PESCO) che ha portato alla creazione di "gruppi di risposta rapida agli incidenti informatici"; alla Task force di azione congiunta contro la criminalità informatica (J-CAT) e alla Rrete giudiziaria europea per la criminalità informatica (EJCN).

[24] Il riferimento è alla cooperazione tra ENISA e CERT-UE, al memorandum d'intesa tra l'ENISA, l'Agenzia europea per la difesa (AED) e il Centro europeo di competenza per la cibersicurezza, istituito con il regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento, per citare i più significativi.

petente a individuare precocemente i segnali di attacchi informatici, grazie all'impiego di strumenti basati sull'intelligenza artificiale, in collaborazione con la rete CSIRTS, l'ENISA e il Cybercrime Centre (EC3) creato presso EUROPOL. Poiché l'Unità lavorerà a stretto contatto con l'ENISA, è il caso di specificare il diverso ruolo svolto dai due organi. Infatti, mentre gli obiettivi dell'ENISA riguardano l'assistenza alle istituzioni dell'Unione e agli Stati membri nel potenziare e condividere la capacità informatiche per prevenire, rilevare e rispondere a problemi e incidenti di sicurezza delle reti, stimolando una cooperazione tra attori del settore pubblico e privato, l'Unità si occuperà di cooperazione tecnica e operativa in caso di incidenti anche transfrontalieri, sul presupposto di una mappatura delle capacità disponibili a livello nazionale e dell'UE e dopo aver valutato le strategie nazionali sulla cibersicurezza, anche per evitare la duplicazione delle attività[25].
L'operatività dell'Unità è prevista a partire dal 30 giugno 2022 grazie alla creazione di una piattaforma virtuale fisica[26] e di un Comitato dell'UE per lo sviluppo delle capacità informatiche[27]. A tal proposito, il Gruppo di lavoro orizzontale sulle questioni nazionale e dell'UE, dopo aver valutato le strategie nazionali sulla cibersicurezza, anche per evitare la duplicazione delle attività, ha invitato l'Unione e gli Stati membri a impegnarsi nello sviluppo del quadro europeo sugli obiettivi e possibili ruoli e responsabilità dell'Unità[28].

In conclusione, la creazione dell'Unità risponde all'obiettivo primario dell'Unione di dotarsi di una **bussola strategica** per costruire un'Europa indipendente

[25]-V. Comunicazione congiunta della Commissione e dell'Alto rappresentante per gli affari esteri e la politica di sicurezza sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, del 16 dicembre 2020, JOIN (2020) 18 final.

[26]-V. la raccomandazione (UE) 2021/1086 della Commissione, del 23 giugno 2021.

[27]-V. EU CyberNet, The Bridge to Cybersecurity Expertise in the European Union, 28 ottobre 2021, www.eu-cybernet.eu.

[28]-V. Consiglio UE, Progetto di conclusioni sull'esplorazione del potenziale dell'iniziativa Joint Cyber Unit - complementare alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su larga scala, par. 23, 6 ottobre 2021.

da un punto di vista militare, economico e tecnologico e anche per realizzare le priorità di resilienza, sovranità e autonomia tecnologica. In tal senso, essa rappresenta un passo importante verso la creazione di un esercito dell'UE, sempre che la sua attività si basi su un approccio olistico, poiché la sicurezza informatica è un dominio interdisciplinare[29].

A tal fine, a nostro avviso, tra i compiti dell'Unità dovrebbe essere previsto il sostegno agli Stati membri nella creazione di una forza militare di cyber difesa proattiva e reattiva, sotto la direzione dell'Agenzia Europea della difesa[30]; il rafforzamento della capacità di *digital investigation*, sulla quale è già impegnata la Commissione europea[31]; la conduzione in collaborazione con l'EUROPOL di operazioni di contrasto agli attacchi di cyber-terrorismo e alle info-strutture per contrastare la *cognitive warfare* e altre minacce ibride.

A nostro avviso, per la realizzazione dei compiti indicati l'Unità dovrebbe potersi avvalere anche dell'ausilio di un proprio ***Hub* di *cyber intelligence***, posto che l'attuale Centro UE di analisi e di intelligence-INTCEN ha funzione meramente consultiva. Ciò consentirebbe un'autonomia di *detection* e valutazione delle minacce informatiche in coordinamento con le agenzie di informazione degli Stati membri, realizzando un'indispensabile sinergia con i 27 Stati membri in materia di difesa e di intelligence.

Annita Sciacovelli, *Prof. aggr. di Diritto internazionale e dell'Unione europea, Univ. degli studi di Bari Aldo Moro, Cybersecurity specialist*

[29] V. T. AMADOR, Enhancing Cyber Defense Preparation Through Interdisciplinary Collaboration, Training, and Incident Response, in Journal of The Colloquium for Information Systems Security Education, 2020, p. 5, cisse.info/journal/index.php/cisse/article/download/130/130.

[30] V. Parlamento europeo, Report on the State of EU Cyber Defense Capabilities, (2020/2256(INI)), 2021.

[31] Cfr. R.A. WESSEL, European Law and Cyberspace, in N. TSAGOURIAS, R. BUCHAN (eds.), International Law and Cyberspace, Cheltenham, 2021, p. 123 ss.

BIOGRAFIA

Annita Larissa Sciacovelli

Professore aggregato di Diritto internazionale presso l'Università degli Studi di Bari 'Aldo Moro', cybersecurity specialist e avvocato iscritto all'Ordine degli Avvocati di Bari. La Prof.ssa Sciacovelli è visiting Research Fellow presso l'IESE Business school di Barcelona (Spagna) e Researcher fellow in Cybersecurity presso l'Institute of National Security Studies, Jerusalem. È membro della Commissione Cyber Security and Warfare della Società Italiana di Intelligence, membro della Società Italiana di Diritto Internazionale e dell'UE e membro a pieno titolo dell'Istituto di Internazionale di Diritto Umanitario di Sanremo. La Prof.ssa Sciacovelli è membro del comitato scientifico della rivista Sicurezza e Intelligence, membro dell'Advisory Board dell'International Institute for Peace, Vienna, Austria, e insegna Diritto internazionale presso l'Università degli Studi Internazionali di Roma (UNINT).

FORUM ICT SECURITY 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **21ª Edizione del Forum ICT Security**

Analisi geopolitica a supporto della cyber threat intelligence. Un approccio multidisciplinare per la previsione dell'attività di Threat Actors

Il cyberspazio oggi è a tutti gli effetti una dimensione reale, con effetti concreti anche sul mondo fisico come insegna ad esempio il caso dell'attacco alla rete elettrica Ucraina del 2015[1]. Gli attaccanti, ottenendo prima credenziali amministrative tramite phishing, hanno lanciato un malware distruttivo su alcuni server di compagnie elettriche, causando un diffuso black out nella nazione.
Questo rende la **cybersicurezza uno dei temi principali del nostro tempo**, imperativa per tutelare gli interessi nazionali in un contesto in cui la cybersicurezza di uno stato non coincide più con quella dei suoi confini[2].

Per proteggersi dagli attacchi informatici, oltre a mezzi più storicamente conosciuti come protezioni perimetrali, protezioni per gli endpoint, messa a punto di processi adeguati ed altri, il trend degli anni recenti è anche l'utilizzo della *cyber threat intelligence.*

Una semplice definizione di *cyber threat intelligence* può essere il processo di acquisire, attraverso molteplici fonti, conoscenza su minacce ad un determinato ambiente[3]. Include la raccolta e l'analisi di informazioni al fine di profilare possibili minacce cyber dal punto di vista tecnico, di risorse, di motivazioni e di intenti. E proprio sulle motivazioni esiste

[1] https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)

[2] Iulian F. Popa "CYBER GEOPOLITICS AND SOVEREIGNTY. AN INTRODUCTORY OVERVIEW"

[3] SANS, "Threat Intelligence: What It Is, and How to Use It Efectively"

un punto di contatto con la geopolitica. La geopolitica non ricade facilmente all'interno di un'unica definizione. Semplificando, e in modo non esaustivo, si può definire come disciplina che identifica le sorgenti, le pratiche e le rappresentazioni che permettono il controllo di territori e l'estrazione di risorse[4].

La chiave di lettura della geopolitica sono quindi gli obiettivi degli Stati ed i mezzi che essi utilizzano per raggiungerli.

Parlando di mezzi, Internet è diventato una alternativa all'interazione fisica per vari motivi: è più economico e subito disponibile, è presente il problema dell'attribuzione delle azioni, ed eventuali ritorsioni restano attualmente al di sotto della soglia delle forze armate, anche la NATO infatti parlando di risposta comune ai cyberattacchi resta sul dominio virtuale[5].

Considerando invece gli obiettivi, è chiaro che nessun attacco avviene senza un contesto, ossia uno specifico momento, in uno specifico ambiente e con una specifica motivazione. È dunque possibile sfruttare la conoscenza di tali motivazioni per cercare di predire quali possibili minacce potrebbero attivarsi, e nello specifico per l'ambito cyber quali *state-sponsored actors* potrebbero compiere operazioni nel prossimo futuro per sostenere quegli obiettivi. Ad esempio, esaminando il Five Years Plan cinese 2016-2020[6] in cui, tra le misure presenti, aveva un ruolo importante "Made in China 2025"[7], che aveva come obiettivo il miglioramento dell'industria interna cinese e il riuscire ad occupare un ruolo più ampio nella *supply chain* globale, si sarebbe potuto ipotizzare che diverse aziende occidentali sarebbero potute essere vittima di attacchi volti alla sottrazione di *know-how* e proprietà intellettuale in ambito produttivo.

[4] Colin Flint, "Introduction to Geopolitics"

[5] https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

[6] THE 13TH FIVE-YEAR PLAN FOR ECONOMIC AND SOCIAL DEVELOPMENT OF THE PEOPLE'S REPUBLIC OF CHINA (2016–2020)

[7] U.S. Chamber of Commerce, "MADE IN CHINA 2025: GLOBAL AMBITIONS BUILT ON LOCAL PROTECTIONS"

Oppure guardando al più recente Five Years Plan 2021-2025[8], dove viene indicato come uno degli obiettivi l'aumento della capacità scientifica e tecnica del Paese, e unendolo col fatto che attualmente la Cina non è in grado di produrre in autonomia semiconduttori competitivi[9], si potrebbe supporre un'ondata di attacchi volti al furto di conoscenza in quei settori.

In questo caso la predicibilità si potrebbe pensare essere circoscritta solo ad un certo tipo di attori, gli *state-sponsored actors* ed eventualmente gli *hacktivist*, escludendo il cybercrime guidato dal solo profitto economico.

Ma eventi come l'arresto da parte del FSB russo dei membri del gruppo REvil, noto nel panorama del cybercrime per le grandi estorsioni tramite ransomware, può offrire informazioni interessanti se ben interpretato: potrebbe infatti essere un messaggio che la Russia invia ai gruppi del cybercrime attivi nel suo territorio, indicando che l'America non è un target strategico per gli scopi del governo, e questo potrebbe denotare un dirottamento di buona parte delle campagne verso Europa e Asia.

Questo livello di analisi può supportare due delle tre tipologie di intelligence ereditate dall'ambiente militare[10], nello specifico quella strategica e quella operativa.

La strategica, che consuma informazioni di più alto livello, ha lo scopo di consentire decisione informate da parte dei vertici di un'organizzazione, mentre l'operativa risponde a domande più tecniche come ad esempio il capire se la propria organizzazione offre superficie d'attacco per i vettori utilizzati solitamente dalla minaccia rilevata (TTP, Tactics, Techniques & Procedures).

[8] CSET, Georgetown University's Walsh School of Foreign Service, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035"

[9] https://gjia.georgetown.edu/2021/06/22/rethinking-chinas-strategy-of-technological-independence

[10] DOD Dictionary of Military and Associated Terms, https://www.jcs.mil/Portals/36/Documents/Doctrine.pdf

Continuando il secondo esempio esposto in precedenza, sul recente Five Year Plan cinese, un'analisi che tenga in considerazione elementi geopolitici potrebbe inserirsi nella threat intelligence strategica di un'organizzazione produttrice di semiconduttori fornendo elementi per considerarsi un potenziale target e magari decidere di aumentare il budget per la difesa o di intraprendere altre iniziative in quella direzione. Nella threat intelligence operativa, invece, potrebbe far individuare in APT31[11] un probabile attaccante, consentendo di andare preventivamente a verificare l'esposizione ai relativi TTP usati più recentemente dal threat actor. Il livello strategico dovrebbe già prendere in considerazione i trend geopolitici, le policy di altri Paesi ed elementi affini come politiche economiche o eventi diplomatici, ma raramente questo viene effettuato con un occhio al mondo cyber.

Un **approccio multidisciplinare che unisce geopolitica a *cyber threat intelligence*** potrebbe quindi aiutare a profilare più accuratamente le possibili minacce e a stabilire in un dato periodo quali potrebbero più probabilmente attivarsi. Questa informazione può poi essere utilizzata per concentrare maggiormente la propria azione sui TTP legati agli specifici attori individuati come più attivi nel prossimo futuro.

Un aspetto da sottolineare è che l'analisi geopolitica non va ad interessare solo entità pubbliche o aziende partecipate o di enormi dimensioni. Visto il trend sempre maggiore di attacchi rivolti alla *supply chain*, sotto gli occhi di tutti dopo quello avvenuto nei confronti di SolarWinds[12], è un livello di analisi di cui può beneficiare qualsiasi realtà. Il caso SolarWinds è di fatto il *case study* per eccellenza degli attacchi alla *supply chain*: un *threat actor* è riuscito ad avere accesso ai server dell'azienda, presumibilmente tramite phishing e password molto deboli, ed ha installato una backdoor all'interno di un aggiornamento di Orion, prodotto della so-

[11] https://malpedia.caad.fkie.fraunhofer.de/actor/apt31

[12] https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

cietà utilizzato da migliaia di clienti nel mondo, tra cui FireEye che per prima si è accorta dell'anomalia.

L'analisi geopolitica può quindi aiutare a prevedere potenziali operazioni cyber future, visto come spesso gli eventi geopolitici sono replicati nel cyberspazio. L'esempio dell'attacco all'Ucraina citato all'inizio di questo contributo, per indicarne uno tra molti, ha infatti avuto luogo durante le tensioni tra Russia e Ucraina legate a Crimea e Donbass. Conoscere il panorama geopolitico ed avere consapevolezza di quello attuale può aiutare dunque a individuare trends e patterns, che possono trasformarsi in indicatori di minacce future. E non si limita soltanto a questo, in quanto può essere utile anche durante l'analisi di un cyberattacco attuale: conoscere lo stato geopolitico attuale può supportare nel capire le motivazioni dietro un attacco e nel tentare di attribuirlo a certi threat actors.

Un'analisi del tipo proposto richiede competenze e risorse che non tutte le aziende possono mettere in campo. Molte non possiedono le risorse per definire propri processi di cyber threat intelligence, tantomeno per dotarsi di servizi di analisi geopolitica. Sarebbe auspicabile che un servizio di questo tipo possa venire fornito dalla nuova Agenzia Nazionale per la Cybersicurezza, che potrebbe utilizzare analisi di scenari geopolitici provenienti dal Sistema di informazione per la sicurezza della Repubblica per creare alert più mirati da diffondere alle pubbliche amministrazioni e al settore produttivo privato italiano.

Andrea Leoni, *Cyber Security Manager, Segretario Commissione Studi Cyber Threat Intelligence & Cyber Warfare di SOCINT*

BIOGRAFIA

Andrea Leoni

Andrea Leoni è cyber security manager presso una società multinazionale nel settore del credit and business information, è specializzato in governance e ambito GRC, con esperienza pluriennale di security advisory verso realtà nazionali ed internazionali. Già ricercatore di intelligence presso il Laboratorio di Intelligence dell'Università della Calabria, presso cui ha conseguito un Master di II livello in Intelligence, si è occupato anche di politica e geopolitica e del loro rapporto col dominio cyber. Attualmente, presso la Società Italiana di Intelligence, è Segretario della Commissione Studi Cyber Threat Intelligence & Cyber Warfare.

Analisi del Rischio Cibernetico

Il presente contributo ha lo scopo di proporre un'analisi di alto livello sul concetto di "analisi del rischio cibernetico" in relazione all'evoluzione degli scopi e delle metodologie di intelligence. La competizione tra le diverse entità statuali si è allargata partendo dal tradizionale ambito delle potenzialità dell'apparato militare di ciascun attore.

Oltre il potenziale militare è sempre più prevalente quello economico, cioè la capacità delle imprese di ciascun paese di generare innovazione, di esportare, di aumentare la filiera del valore aggiunto portando, se possibile, a fare dipendere altri paesi da sé.

L'aumento esponenziale del fenomeno dello spionaggio industriale, con un elevato utilizzo degli strumenti cibernetici, può essere ricondotto principalmente a:

- La sempre maggior presenza di informazioni sensibili e proprietà intellettuale in possesso di imprese e centri di ricerca scientifica e tecnologica.
- L'elevato tasso di profitto per gli attori statuali o para-statuali che praticano operazioni di intelligence in modalità cibernetica allo scopo di sottrarre segreti industriali, idee innovative e/o *know-how* tecnologico.
- La difficoltà per le intelligence dei paesi target nel contrastare azioni cibernetiche ostili.

I settori tecnologici che costituiscono i target più appetibili sono i seguenti:

- Tecnologie dell'informazione e della comunicazione;
- Tecnologie militari, e in particolare sistemi marittimi e tecnologie aerospaziali e aeronautiche;
- Tecnologie energetiche a bassa emissione di anidride carbonica;
- Nuovi materiali e tecnologie manifatturiere avanzate, tra cui le nanotecnologie;
- Tecnologie biomediche e farmaceutiche; Tecnologie avanzate di produzione agricola, tra cui quelle basate sull' ingegneria genetica.

Nel nostro paese è cresciuta la sensibilità delle istituzioni sul tema e si è arrivati alla recente costituzione dell'Agenzia per la Cibersicurezza Nazionale incaricata di prendere ogni iniziativa attua a garantire una maggiore sicurezza e resilienza del mondo IT italiano. Per le citate implicazioni sulla sicurezza nazionale italiana tali azioni devono procedere di concerto con l'operare degli apparati di intelligence al fine di contrastare azioni ostili da parte attori statuali e para statuali ne confronti del nostro paese.

Il World Economic Forum ha pubblicato il "Global Risk Landscape 2021" da quale si evince che gli attacchi cibernetici comportino un rischio (probabilità x impatto) più elevato rispetto agli attacchi terroristici, alle crisi alimentari, alla disoccupazione e a tutta una serie di altri rischi che riempiono in ogni istante i notiziari radiotelevisivi e i social.

Le motivazioni sono:

- il funzionamento delle moderne economie è sempre di più basato sulle tecnologie digitali;
- l'interdipendenza delle Infrastrutture critiche aumenta costantemente;
- aumento del rischio che un danno prodotto in un nodo del sistema si ripercuota sui nodi circostanti con effetti a catena potenzialmente catastrofici.

In questo contesto gli obiettivi delle attività di intelligence sono molteplici: difesa dell'interesse nazionale, contrasto alla competizione economica condotta in maniera surrettizia, tutela delle libertà individuali ed in ultima analisi del sistema democratico.

L'intelligence economica sta assumendo un ruolo sempre più rilevante al fine di evitare danni consistenti alla competitività dello stato e delle singole aziende. In particolare lo spionaggio industriale mira alla sottrazione di capitale intellettuale delle singole aziende privandole del loro *asset* di maggiore importanza e mettendone a rischio la stessa sopravvivenza. Un attacco spionistico, condotto da un'azienda concorrente o da un apparato d'intelligence straniero, sottrae *know-how* all'azienda colpita, azzerandone il possibile rendi-

mento nel tempo di investimenti eseguiti.

La particolare configurazione del sistema industriale italiano, con una forte prevalenza di PMI, rende indispensabile l'avvio di una politica di sensibilizzazione sui temi della sicurezza cibernetica e della protezione del patrimonio informativo, rivolta alle figure apicali delle PMI stesse. La sicurezza cibernetica non può essere vista come un costoso e fastidioso accessorio dell'attività d'impresa.

L'Agenza per la Cibersicurezza Nazionale deve porsi come attore primario di questa attività di diffusione e mantenimento della sensibilità ai temi della sicurezza cibernetica da parte delle PMI, attori imprescindibili del sistema economico nazionale.

L'Unione Europea considera la sicurezza cibernetica come obiettivo prioritario dell'attività di tutela del patrimonio informativo da parte degli stati membri e, a tale proposito, ha emanato la direttiva NIS e si prepara ad emanarne una seconda versione allo scopo di una migliore gestione del rischio cibernetico. La logica che pare intravedersi nella direttiva NIS è *"secure us to secure me"*; ne consegue che il presupposto fondamentale per il conseguimento di una maggiore sicurezza sistemica è, quindi, l'adozione di *best practices* da parte dei singoli attori.

Il rischio cibernetico non impatta solo la singola impresa ma ha anche una importante componente sistemica che è «il rischio che un attacco (o altri eventi avversi) in un singolo componente di un ecosistema infrastrutturale critico, causi ritardi significativi, diniego, guasto, interruzione o perdita, tali da influire sui servizi non solo nella componente originaria, ma anche nelle componenti dell'ecosistema logicamente e / o geograficamente correlate.

La magnitudo dell'impatto deriva da:

- aumento costante della superficie digitale;
- crescita della velocità della trasformazione digitale;
- semplicità ed economicità della realizzazione degli attacchi;

- aumento della complessità delle minacce.

Affrontare il rischio sistemico vuol dire lavorare su tre livelli: quello interno e dell'ecosistema dei principali *stakeholder* dell'azienda; quello degli upstream provider e quello degli eventi esterni imprevisti. Quest'ultimo livello comporta una rinnovata importanza delle attività di intelligence in quanto gli organismi preposti sono attori imprescindibili per l'individuazione di azioni ostili che impattano sul "rischio sistemico" dei singoli soggetti economici.

Lo strumento più idoneo per una mitigazione del rischio efficace (non esiste in nessuna organizzazione un contesto con rischio uguale a zero) è l'adozione di adeguate metodologie di Analisi del Rischio, di tipo quantitativo o qualitativo, al fine di considerare tutte le possibili vulnerabilità di diversa natura valutando la probabilità di accadimento di eventi negativi legati ad esse. Si passa dalla "logica dell'adempimento" alla "logica della responsabilità", laddove il singolo operatore, attraverso l'Analisi del Rischio deve essere in grado di identificare le minacce incombenti sulla protezione del proprio patrimonio informativo con l'individuazione delle vulnerabilità presenti e, attraverso un processo di Gestione del Rischio, la definizione di adeguate contromisure.

Le metodologie di Analisi del Rischio più conosciute ed utilizzate sono:

- ISO:IEC 27005: unico standard internazionale de iure.
- NIST SP800-30: standard federale adottato dagli Stati Uniti.
- Magerit: standard nazionale spagnolo adottato da ENISA (European Network and Information Security Agency).
- Octave: sviluppata dalla Carnegie-Mellon University per soddisfare le esigenze del Department of Defence degli Stati Uniti.

Normalmente lo standard ISO:IEC 27005 è quello ritenuto più utilizzato e ritenuto più idoneo, specialmente in ambito IT.

Il crescente aumento della *cyberwarfare* nella competizione globale tra stati ed aziende rende necessario l'utilizzo di

metodologie e strumenti allo scopo di conseguire un adeguato livello di protezione degli *asset* aziendali o statuali. A tal fine sarebbe auspicabile l'adozione di metodologie di Analisi del Rischio tra gli strumenti in uso da parte della Agenzia per la Cibersicurezza Nazionale.

In generale ogni soggetto si caratterizza per la presenza di rischi collegati al proprio business aziendale ed è costretto a definire una soglia minima di esposizione al rischio (cd. "Rischio accettabile"). La definizione di questa soglia è un processo molto complesso e critico che può essere governato unicamente attraverso modalità di "Gestione del Rischio" metodiche e formali.

In particolare la Gestione del Rischio si caratterizza nell'applicazione sistematica di:

- Politiche di gestione
- Procedure
- Azioni

Volte all'esecuzione delle seguenti fasi inerenti al rischio:

- Identificazione
- Analisi
- Valutazione
- Mitigazione controllo eventuale

La Gestione del Rischio è, quindi, un processo volto ad assicurare che gli impatti dovuti a minacce incombenti su vulnerabilità di sistemi e processi IT siano contenuti a livelli accettabili a fronte di costi sostenibili da parte dell'organizzazione del soggetto. Per raggiungere tale obiettivo è necessario un adeguato bilanciamento tra l'esposizione al rischio ed i costi di mitigazione attraverso l'implementazione di adeguate contromisure e controlli.

L'adozione di una metodologia formale per la gestione del rischio è preferibile in quanto ha le seguenti caratteristiche:

- Oggettività
- Ripetibilità
- Verificabilità anche da attori esterni
- Automatizzabili
- Applicabilità ad organizzazioni anche complesse
- Fornitura di risultati confrontabili anche nel tempo

- Misurabilità dell'efficacia con possibilità di azioni correttive

Un adeguato programma di Gestione del Rischio deve quindi prevedere i seguenti passi:

- Analisi del contesto e dichiarazione dell'ambito
- Identificazione e valorizzazione degli asset
- Classificazione degli *asset*
- Individuazione delle minacce e delle vulnerabilità
- Determinazione dei rischi
- Valutazione degli impatti
- Trattamento dei rischi
- Sensibilizzazione alle tematiche di sicurezza degli utenti
- Effettuazione di attività di monitoraggio e revisione costanti
- Comunicazione dei risultati

È opportuna una classificazione delle terminologie adottate nel processo di esecuzione della Gestione del Rischio:

Asset: qualsiasi bene materiale o immateriale, persone comprese, che costituiscono un valore per l'organizzazione dell'operatore.

Vulnerabilità: caratteristica intrinseca di qualsiasi processo o sistema IT che può provocare, anche per azione indotta, eventi indesiderati che possono comportare danni all'organizzazione.

Minaccia: evento potenziale che se attuato porta a conseguenze indesiderate o perdite all'organizzazione dell'operatore.

Agente di Minaccia: entità in grado di attuare, deliberatamente o meno, una minaccia.

Rischio: probabilità del verificarsi di una minaccia attraverso lo sfruttamento di una vulnerabilità.

Impatto: conseguenza indesiderata che si abbatte sull'organizzazione dell'operatore in seguito al verificarsi di un rischio.

La valutazione del rischio è un processo che comporta analisi di tipo quantitativo così come qualitativo. La determinazione dell'impatto, ad esempio,

comporta una quantificazione delle grandezze di entrambe le tipologie:

1) Quantitative in quanto direttamente ed oggettivamente misurabili:

- perdite di fatturato e/o di utili di bilancio;
- incremento dei costi di produzione;
- costi sostenuti per la risoluzione di anomalie.

2) Qualitative non oggettivamente misurabili:

- perdita di credibilità con ricadute sull'immagine dell'organizzazione;
- danni indiretti ad interessi dell'organizzazione
- violazioni della riservatezza delle informazioni.

La stessa frequenza o probabilità di accadimento può aversi nelle tipologie suddette, quantitativa, ad esempio nel caso di stima del verificarsi di un *black-out* elettrico, oppure qualitativa come la stima della probabilità di essere oggetto di attacco informatico.

Più in generale un approccio quantitativo presenta:

Punti di forza:

- Rischi ai quali si riesce a dare priorità secondo l'impatto economico ed *asset* in funzione del loro valore economico.
- Aiuto alla gestione del rischio con una puntuale definizione del ritorno dell'investimento sostenuto per la mitigazione del rischio stesso.
- Facilità di comprensione da parte dei vertici aziendali dei risultati ottenuti dalle attività poste in essere per la mitigazione del rischio.

Punti di debolezza:

- I valori degli impatti assegnati ai rischi sono frutto di valutazioni soggettive da parte delle strutture organizzative interessate.
- Necessità di dover impiegare molto tempo e costi elevati al fine di raggiungere un obiettivo misurabile.
- Non misurabilità di tutti i valori necessari

Altresì l'approccio qualitativo presenta:
Punti di forza:

- Migliore comprensione dell'importanza relativa dei rischi al fine di un'adeguata assegnazione delle priorità.
- Maggiore facilità di condivisione degli obiettivi tra le diverse strutture aziendali.
- Non occorre una quantificazione delle minacce.
- Non è necessaria una determinazione economica del valore economico degli *asset*.

Punti di debolezza:

- Insufficiente granularità dei rischi più significativi.
- Difficoltà nel giustificare investimenti economici volti alla mitigazione del rischio in assenza di un'analisi costi/benefici quantitativa.
- Risultati che vengono influenzati dalle qualità professionali del gruppo di lavoro preposto all'analisi del rischio.

Una soluzione per una più efficace azione di analisi del rischio consiste nell'adozione di un approccio intermedio o semi qualitativo con l'individuazione di classi di valori definite da intervalli di una certa ampiezza con l'associazione alla classe più congrua di ciascun valore di occorrenza e impatto.

Tali attività di gestione del rischio sono già in essere nelle realtà di maggiori dimensioni del nostro paese; tuttavia e innegabile la necessità di un maggiore implementazione delle stesse. Un alto fattore di rischio è dato dalla situazione delle PMI italiane in questo campo; scarsità di investimenti e di consapevolezza in questo campo rendono le PMI estremamente esposte ad attività ostili di intelligence straniere volte all'acquisizione di delicate informazioni industriali ed economiche.

La notevole importanza delle PMI nel settore economico italiano rende urgente un'azione di difesa delle stesse attraverso un ruolo di stimolo alla sensibilità sulle tematiche della cyberguerra da parte dell'Agenzia per la Cibersicurezza Nazionale. Dal canto loro gli apparati di intelligence devono essere coinvolti per l'esecuzione di attività di

contrasto alle ingerenze estere anche attraverso l'uso di tecniche Humint ed Osint, che costituiscono un imprescindibile mèzzo di difesa dell'interesse economico nazionale.

Andrea Giordani, *Esperto Senior di sicurezza dei sistemi informativi*

BIOGRAFIA

Andrea Giordani

Andrea Giordani è un esperto senior di sicurezza dei sistemi informativi. Ha conseguito rilevanti certificazioni internazionali nella materia ed ha una notevole esperienza di sviluppo sicuro dei sistemi IT nonché in molteplici attività di governance della sicurezza IT. Già lead auditor presso aziende per la verifica della certificazione ISO_27001 e 27002, ha svolto attività di audit e di verifica dell'analisi del rischio presso rinomati clienti internazionali per determinare lo stato di sicurezza dei loro sistemi informativi deputati alle operazioni finanziare svolte con carta di credito. Ha conseguito un Master di II livello in Intelligence e Sicurezza. Attualmente è membro della commissione Cyber Threat Intelligence e Warfare presso la Società Italiana di Intelligence.

Cyber-enabled information warfare. Manipolazioni delle informazioni ed armi cognitive

LA GUERRA "IBRIDA" DI QUINTA GENERAZIONE

La guerra è principalmente un fenomeno politico/sociale e non tecnologico/materiale. La natura della guerra, consiste nell'uso della violenza organizzata da parte di Stati ma anche di altri attori geopolitici, non sostituisce la politica con i suoi canali diplomatici, economici e culturali, ma aggiunge l'utilizzo di mezzi militari.

Nessuna guerra è eguale ad un'altra, la sua natura rimane identica ma le sue caratteristiche, negli ultimi decenni, sono mutate profondamente e si sono aperte nuove dimensioni di combattimento. Infatti oggi i conflitti non hanno origine solo fra gli Stati forti, ma soprattutto fra quelli deboli ed al loro interno. Le guerre, o conflitti armati, come ora si chiamano, sviluppano sempre di più caratteristiche di conflitti asimmetrici definiti anche "ibridi", mix di guerra regolare, ad alta intensità operativa e tecnologica, ed irregolare, dove forze belligeranti con potenziale bellico "tradizionale" inferiore utilizzano strategie in grado di compensare le proprie carenze quantitative e qualitative.

Con il termine "asimmetrico" ci si riferisce ai conflitti irregolari, mentre con il termine "ibrido" si sottolinea il fatto che occorre preparare le forze a fronteggiare un'intera gamma di possibili minacce eterogenee.

Ed è così ad es., che oggi i gruppi terroristici pur essendo inferiori in termini di potenza militare tradizionale, possono permettersi di intraprendere campagne di guerra nei confronti di super potenze.

Tra le nuove dimensioni di combattimento delle guerre ibride, oltre allo spazio extra-atmosferico, ancora appannaggio delle super potenze e di qualche nuovo attore geopolitico che potrebbe

in futuro essere presente (si pensi ad es. alla SpaceX di Elon Musk) , il cyberspazio è sicuramente il più utilizzato, grazie alla sua predisposizione a sviluppare "asimmetrie hi-tech", permette di attaccare le vulnerabilità del potenziale avversario in maniera estremamente efficiente e multidimensionale: virtuale, fisico e soprattutto cognitivo.

I costi d'accesso "all'infoguerra" nel cyber spazio sono relativamente bassi, non richiedono grandi eserciti, contraddicendo la teoria secondo cui il successo di un movimento dipende direttamente dalla quantità di risorse che riesce a mobilitare. Piccoli movimenti e gruppi particolarmente motivati possono così intraprendere un'infoguerra anche solo per acquisire visibilità, l'assenza di un fronte, l'incertezza delle fonti inoltre spaventano e fanno slittare il conflitto verso la guerriglia, terreno in cui la paura dell'imprevedibile,

la mancanza di limiti dello scenario di combattimento aggiungono elementi di guerra psicologica.

In conflitti ormai multispettro, la strategia deve tener conto del possibile impiego di tutti i possibili effetti derivati dalle combinazioni di risorse utilizzabili nelle guerre ibride, il concetto strategico della NATO "*comprehensive approach*" va proprio in questa direzione.

La combinazione di queste capacità può generare ulteriori risorse militari da utilizzare verso il nemico, ad es. il solo "raccontare", attraverso i media, social network, la propria capacità di arsenale cinetico può evitare che potenziali conflitti diventino reali, i loro effetti sono virtuali.

Le armi possono servire non solo quando impiegate, ma anche quando non lo sono, anzi si rivelano più utili, perché i costi ed i rischi sono inferiori ed hanno solo effetti potenziali. L'equilibrio, anche solo presunto tra le forze, previene lo scoppio di conflitti o come più semplicemente dicevano i romani *"si vis pacem para bellum"*.

GENESI DELLA CYBER-ENABLED INFORMATION WARFARE (C-IW)

La guerra nel cyberspazio basata sull'informazione è diventata una minaccia esistenziale a sé stante, il suo uso crescente mina i pilastri stessi (logica, verità e realtà) delle moderne democrazie.

Il controllo e la manipolazione delle informazioni per scopi strategici e operativi, Information Warfare (IW), non è una novità.

Ma la crescita esponenziale dell'Information Technology (IT) degli ultimi decenni, la sua pervasività nei vari strati del tessuto sociale ed economico degli stati a livello internazionale, ha avuto un effetto moltiplicatore sull'IW, che sempre più spesso si rivela uno strumento fondamentale per il raggiungimento di obiettivi politici e militari.

L'IW non è un'attività limitata al tempo di guerra, è costantemente in corso a prescindere dallo stato di relazioni con l'avversario. L'obiettivo è trafugare, interdire, manipolare, distorcere e di-

struggere le informazioni tramite tutti i canali di comunicazione e metodi disponibili.

L'Information Warfare è il punto di partenza di ogni guerra ibrida in cui si fa ampio utilizzo dei mass media e delle reti informatiche globali.

Come conseguenza della significativa sovrapposizione dell'IW con il cyberspazio, gli analisti hanno adottato il termine "Cyber-enabled Information Warfare" (C-IW).
Da un punto di vista ambientale poi, il domino cibernetico si distingue significativamente dagli altri ambiti di conflitto, non solo perché rappresenta una realtà artificiale e ibrida, ma soprattutto perché la geografia del cyberspace è molto più mutevole rispetto ad altri ambienti. Infatti a differenza delle montagne e degli oceani, nel cyberspace possono essere attivate e disattivate con un semplice click scenari, interi mondi ed ecosistemi virtuali. Questa caratteristica "geografica" dello spazio cibernetico ha reso necessario un nuovo approccio in relazione all'evoluzione degli scenari bellici.

L' C-IW E LA GUERRA DI QUINTA GENERAZIONE

In termini generali possiamo definire l'C-IW l'elemento chiave della guerra di quinta generazione, dove il campo di battaglia è il cyberspazio e l'architettura dell'informazione globale, sia nella sua forma immateriale attraverso il dominio cibernetico e virtuale, sia nelle sue infrastrutture tecnologiche fisiche interconnesse.

Nella guerra di quinta generazione il raggiungimento dell'obiettivo avviene quindi attraverso la persuasione e l'influenza dei popoli e dei governi piuttosto che con la violenza. Avere il controllo delle informazioni, dominarle, permette di mantenere una superiore comprensione del campo di battaglia, identificare i punti deboli del nemico, su cui concentrare gli attacchi nel modo più produttivo, e nascondere contestualmente i propri punti critici.

Obiettivo finale di un attacco IW/C-IW è quello di influenzare la conoscenza dell'avversario per determinarne il comportamento alterando la sua per-

cezione. Una campagna IW/C-IW non deve limitarsi ad influenzare una singola decisione, ma deve essere strutturata per creare una persistenza temporale a vantaggio di una errata posizione resiliente.

La persistenza implica il controllo degli obiettivi. La multidimensionalità di un attacco IW/C-IW ha come obiettivo quello di alterare il processo intellettuale del nemico, avendo preventivato a priori la possibile propagazione degli effetti a qualsiasi livello. Gli attacchi possono avere bersagli ed effetti immediati, creando diversi effetti funzionali a cascata, in grado di propagarsi anche da punti diversi rispetto al punto di attacco iniziale.

IL POTERE DELLE INFORMAZIONI

Un aspetto fondamentale è non sottovalutare il potere dell'informazione. L'essere umano crea modelli mentali e formula idee in base alla sua percezione della realtà, acquisendo, elaborando e producendo informazioni.
Allo stesso modo, attraverso le interazioni nell'ambiente virtuale (ad es. i social network), i processi mentali si comportano e si sviluppano. In quello stesso ambiente artificiale, le persone o meglio gli utenti, interagiscono, condividono idee e principi senza avere un reale senso di fiducia per la qualità delle informazioni scambiate.
La tecnologia ci impone di elaborare flussi continui di informazioni spesso progettati per influenzare il modo in cui pensiamo, creano distrazione.

La distrazione consiste nell'orientare e distrarre l'attenzione del pubblico verso argomenti irrilevanti, sovraccaricandoli di informazioni in modo da tenere occupato il loro interesse. Ad es. si dà eccessiva importanza, ad eventi mondani, sportivi, etc. e questo fa sì che la gente perda di vista i problemi reali e importanti come il lavoro o la salute. Attraverso questi strumenti diventa relativamente facile diffondere informazioni false su Internet mentre la percezione e la capacità di discernimento degli utenti viene costantemente plasmata.

Il flusso costante, "in real time" delle informazioni (verificate e non) tende ad

annullare la capacità di analisi critica dell'utente, a vantaggio del giudizio collettivo. Nel cyber spazio, le informazioni non verificate ma ritenute veritiere dagli utenti, influenzano la percezione e la comprensione generale degli eventi. La condivisione di queste informazioni amplifica la diffusione senza permettere un confronto nel breve termine.

La disinformazione è applicata anche agli utenti più riflessivi, quelli che preferiscono analisi approfondite con fonti apparentemente accurate e credibili, ma i riferimenti di solito, rimandano ad altri siti di disinformazione. Le "forme" della disinformazione e delle fake news sono progettate per manipolare i pensieri ed i sentimenti di ogni specifica tipologia di destinatari, ad es. i giovani utenti vengono colpiti con messaggi visivamente più strutturati e più fruibili per loro, come video, immagini, meme e caricature.

Il potere dei simboli, delle immagini, ad es., e la loro manipolazione può modificare il pensiero o lo stato d'animo degli utenti, facendo leva su meccanismi culturali con cui il cervello elabora l'informazione stessa. Se ad esempio, ad un utente di cultura occidentale, viene mostrato il simbolo nella figura A, il suo primo pensiero andrà inconsciamente al concetto di nazismo.

Fig. A

In realtà il simbolo rappresentato in figura A è quello della svastica induista, e nella cultura orientale rappresenta un segno di buon auspicio, è un segno mistico che sul corpo di una persona, luogo o cosa, sta ad indicare buona sorte e fortuna.

Svastica Induista

Svastica Nazista

In un ipotetico attacco C-IW, l'immagine in figura B potrebbe essere condivisa su tutti i social network, magari con un commento in cui si sostiene che l'ideologia nazista è stata ispirata dalla religione buddista e fomentare così odi e paure nei confronti dei suoi credenti. Se a questo fosse poi scatenata un'ondata massiva di condivisioni, commenti ed interazioni sui social, l'analisi sull'affidabilità della fonte e dell'informazione verrebbe meno.

Fig. B

Questo è soltanto un banale esempio di come le convinzioni degli utenti sulla rete potrebbero diventare certezze in base ad un pregiudizio. L'informazione viene sempre manipolata studiando la sfera culturale e politica dei bersagli.

Nell'esempio precedente un altro elemento importante da notare è che l'informazione a secondo del modo in cui viene formulata e/o veicolata può manipolare il pensiero critico, la comprensione e le decisioni del ricevente, in quanto se adeguatamente "confezionata" può far leva e sfruttare anche aspetti della coscienza umana più interiori, tra quelli più utilizzati nell'ambito C-IW ci sono i bias cognitivi.

I bias sono limiti cognitivi, errori nella percezione delle informazioni che interferiscono con il pensiero, l'analisi ed il ragionamento di ogni essere umano. Nessun uomo ne è esente, perché insiti nella cultura, nel comportamento e nella diversità etnico-sociale dell'uomo. Possono interferire con il pensiero, instillando la convinzione di prendere la decisione corretta o di compiere l'azione giusta, e questo vale per qualsiasi attività lavorativa, ludica, religiosa, etc.., impedendo di percepire la realtà come

essa è e non come si pensa o si vuole che sia.

La C-IW sviluppa algoritmi sempre più sofisticati e sempre di più aiutati dall'intelligenza artificiale per manipolare la realtà delle informazioni a vantaggio dell'attaccante. Questa strategia non è nuova e soprattutto è utilizzata da anni ad es. sui social network dove la nostra interazione è manipolata da algoritmi che registrano e immagazzinano le nostri azioni e informazioni, per poterle riutilizzare a scopi specifici. Ad es. le notizie presenti sulla homepage di facebook, le immagini su Instragram o i video che ci propone Tik Tok sono diversi per ogni utente perché costruiti in base ai nostri interessi personali.

Ogni volta che facciamo un commento, condividiamo un post o mettiamo un "mi piace", i nostri dati vengono registrati e immagazzinati. In questo modo i social studiano i nostri gusti, convinzioni, ideologie e ci propongono altri contenuti simili, convogliando l'attenzione esclusivamente su alcuni prodotti e pubblicità di marketing allettanti e mirate sui nostri gusti. L'obiettivo è catturare l'attenzione, filtrando le informazioni in un'unica direzione.

In pratica gli utenti interagendo con i post, danno maggior valore e credibilità a quelli che confermano le proprie convinzioni e, ignorano quelli che li contraddicono.

Le campagne di C-IW utilizzano tecniche simili per influenzare il pensiero politico e decisionale degli stati e manipolare il pensiero delle masse a vantaggio dell'attaccante. Gli aggrediti spesso non sanno di dover combattere, a differenza degli aggressori che attraverso campagne anonime ed invisibili, acquisiscono informazioni pregiate e comportamentali sull'avversario di cui avvalersi per neutralizzarli.

IL CICLO DELL'INTELLIGENCE NEL C-IW

In questo momento storico dove l'informazione domina più che mai gli scenari decisionali globali, anche le fasi che compongono il processo di analisi delle informazioni detto ciclo dell'intelligen-

ce (o ciclo delle informazioni), quando applicato all'ambito C-IW, subisce significative variazioni nella sua modalità applicativa. Brevemente identifichiamo sei fasi che compongono il ciclo dell'intelligence:

- **Identificazione del fabbisogno informativo (*requirements*).**
  Vengono delineate le aree di interesse per le quali è necessario un contributo d'intelligence.
- **Raccolta delle informazioni (*collection*).** Questa fase comprende:
  - L'attività di raccolta delle informazioni connessa al fabbisogno informativo.
  - La quantità corretta di informazioni da assumere, nella corretta proporzione tra intelligence proveniente da fonti umane rispetto alle fonti tecnologiche.
- **Trattamento delle informazioni (*processing and exploitation*).**
  Tutte le informazioni raccolte, specialmente se ottenute attraverso fonti tecnologiche, devono essere trattate per assumere una valenza significativa nelle successive fasi del processo d'intelligence.
- **Analisi, valutazione e produzione (*analysis and production*).**
  Il momento dell'analisi e della valutazione che trasforma l'informazione in un prodotto finito, il passaggio chiave nel processo d'intelligence, dove generalmente si sviluppa un'analisi tattica, più circoscritta, utile per esigenze di breve termine e un'analisi strategica a lungo termine e più ampia e qualificante nell'individuare ed ipotizzare scenari e possibili eventi.
- **Disseminazione (*dissemination*) e utilizzazione (*consumption*).**
  È il momento nel quale il prodotto d'intelligence, opportunatamente lavorato e trasformato, viene utilizzato, raggiungendo il suo scopo. Inoltre l'informazione elaborata continua ad esplicare un ruolo importante all'interno del processo come patrimonio informativo.
- **Feedback.**
  La fase finale di feedback, o ritorno informativo, permette di effettuare una valutazione sull'efficacia del processo e della metodologia di analisi svolta.

Nel contesto C-IW, le fasi del processo di analisi delle informazioni, devono adattarsi alle regole dell'informazione nel mondo di internet. Nuove capacità di raccolta, verifica e velocità di analisi delle informazioni sono alcuni dei principali aspetti che devono essere presi in considerazione.

La fase più sensibile nella ricerca di informazioni su internet riguarda la valutazione delle fonti, difatti, il valore delle informazioni reperite attraverso internet è estremamente variabile. L'enorme flusso di contenuti presente in rete cresce in maniera esponenziale (*Big Data*) ma le informazioni veicolate hanno spesso un ciclo di vita molto breve, in quanto possono apparire, modificare il significato dei loro contenuti e scomparire dalla rete in tempi estremamente rapidi.

I Big Data rappresentano uno strumento di grande utilità per l'intelligence ed in particolare per la *cyber intelligence*, ma per poterli utilizzare al meglio è necessario dotarsi di nuovi strumenti e risorse umane in grado di trattarle, come ad es. i *"data scientist"*, professionisti del data mining, in grado cioè di individuare informazioni di varia natura (non risapute a priori) tramite l'estrapolazione mirata da grandi banche dati, singole, multiple o dati non strutturati. La priorità delle analisi, oggi risiedere nella faticosa e complessa selezione delle informazioni piuttosto che nella ricerca delle stesse, disponibili in quantità fino a poco tempo fa impensabile. Tutte le informazioni raccolte, specialmente quelle ricavate da strumenti automatici, quasi mai sono pronte per essere utilizzate, infatti necessitano di essere trattate per assumere valenza e significato nelle successive fasi del processo d'intelligence, manifestando così la sproporzione tra informazioni raccolte ed informazioni realmente utili. Il pericolo maggiore per un analista consiste nel condurre analisi su informazioni parziali, non oggettive e provenienti da una errata valutazione delle fonti. L'accuratezza, credibilità ed autorevolezza delle fonti divengono così un aspetto più che mai fondamentale nell'analisi delle informazioni in rete. Un altro aspetto che riguarda l'analisi delle informazioni in un ambito C-IW è che la raccolta delle stesse non viene effettuata in manie-

ra "asettica", senza cioè interagire con la controparte, ma sempre più spesso, per ottenere una raccolta informativa efficace, è richiesta una notevole esposizione e sollecitazione dell'avversario.

Si pensi ad es. all'OSINT, che per definizione non prevede alcun contatto diretto col nemico, ebbene esso stesso può soffrire di un'attività ostile e occulta dell'avversario, quando questi diffonde artatamente informazioni inutili o false. Questo spesso modifica il contesto in cui le fasi di analisi vengono svolte, il che introduce un nuovo aspetto, e cioè che le varie fasi di analisi vengono sempre più frequentemente avviate come *task* paralleli in continuo aggiornamento tra loro.

Gli analisti si trovano così a lavorare non su dati e specifici contenuti ma su processi dinamici, globali, non deterministici con un elevato grado di complessità. In scenari e contesti così ampi analizzare e comprendere i processi vuol dire non solo poterli modificare ma anche controllare l'essenza stessa, il "DNA", delle informazioni e delle azioni subliminali o manifeste sottostanti, veicolate tramite essi, punto questo fondamentale, essenziale da dominare, se si vogliono svolgere campagne di C-IW efficaci.

La risultanza delle informazioni utilizzate, in particolare in ambito I-CW, ha una ulteriore doppia valenza:

- I modelli di ricerca utilizzati in fase di analisi consentono non solo di interpretare le informazioni raccolte ma soprattutto di essere utilizzati come base per successive nuove ricerche e fungono da acceleratori di nuove campagne I-CW.
- Eventuali risultati ottenuti da azioni intraprese dall'analisi delle informazioni possono essere riutilizzati per successive campagne I-CW ottenendo risultati molto più stabili e duraturi sul lungo periodo. Ad es. campagne di C-IW che mirano a controllare il voto politico in uno stato, spesso svolgono attività di analisi dei processi e delle informazioni dell'intero contesto socio culturale elettivo operando nel tempo, modificando e/o inserendo specifiche informazioni mirate piuttosto

che intervenire direttamente su una specifica tematica e/o votazione. Cambiare l'opinione delle masse in generale su determinati temi, piuttosto che su uno specifico evento, da maggiori vantaggi in termini di efficacia nel tempo, infatti una volta modificata l'opinione pubblica, questa impiegherà più tempo a "disintossicarsi", ed eventuali nuove campagne IW/C-IW potranno sfruttare quanto già fatto e richiederanno un minor sforzo per raggiungere nuovi e più efficaci risultati.

ARMI COGNITIVE

Uno degli aspetti che la C-IW mette in luce in questo scenario di conflitti ibridi, è la natura umana che non viene più considerata come parte di un'entità cosmologica che evolve autonomamente attraverso la conoscenza e l'esperienza, ma come un dispositivo aggiornabile sulla base delle nuove scoperte scientifiche. Questa concezione tra l'altro, in ambito filosofico e sociale, è sostenuta da due correnti di pensiero: il trans-umanesimo, che si propone di rivoluzionare, potenziare e far evolvere l'essere umano attraverso la scienza e la tecnologia, e il post-umanesimo, che interpreta l'uomo come un essere ibrido, cioè umano e non umano, trasformabile fisicamente e mentalmente in qualcosa di nuovo sulla base del periodo storico in cui vive. La tecnologia da strumento a nostra disposizione, sta diventando sempre di più l'ambiente che ci circonda e al quale siamo diventati subordinati.

Una Tecnologia con cui interagiamo con specifici criteri: funzionalità, efficienza e convenienza, subordinando concetti come: cultura, individuo, dignità, libertà, verità, etica, politica, religione, storia, etc., nonché le esigenze ed i bisogni dell'uomo alle necessità del sistema globale. Un campo di battaglia nel quale stiamo subendo involontariamente una immersione sempre più completa, una realtà artificiale e ibrida.

Questo scenario ha permesso di sviluppare nuove tipologie di armi: le armi cognitive, che sfruttando la manipolazione dell'informazione e la tecnologia per trasferirla, nell'ambito di conflitti ibridi

possono rivelarsi la strategia vincente nei conflitti.

Alla base di queste armi c'è la manipolazione delle informazioni. Una delle tecniche da sempre utilizzate è la diffusione di notizie false e la "*buzzword*" che più identifica questa strategia nel secolo che stiamo vivendo è: fake news, la fake news è diventata la parola d'ordine collettiva per identificare qualsiasi forma di disfunzione informativa nella nostra società.

Le fake news sono informazioni false (disinformazione) o fuorvianti per indurre il bersaglio a prendere decisioni (o ad adottare atteggiamenti o idee) contrarie ai suoi interessi e che favoriscono gli interessi del "disinformatore". E' un'arma che consente a chi la usa con successo di esercitare la manipolazione o l'eterodirezione.

La disinformazione é un argomento centrale del pensiero politico e strategico occidentale e orientale sin dall'antichità, basti pensare a trattati di strategia militare come "l'arte della guerra" di Sun Tzu, secondo cui tutte le guerre si basano sull'inganno. Grazie poi alla tecnologia dei "nuovi media" (Google, YouTube, Twitter, Facebook, etc.) le azioni disinformative attraverso notizie deliberatamente falsificate sono sempre più efficaci, consentendone la diffusione massiccia, incontrollata e pressoché istantanea.

Le fake news sfruttano una debolezza cognitiva sempre più evidente nella nostra società moderna dominata da internet, la tendenza ad accedere e diffondere informazioni senza valutarle criticamente, la refrattarietà all'approfondimento, la sindrome da deficit di attenzione (*Attention Span Deficit Disorder*) sono tra le principali cause dell'analfabetismo funzionale, l'incapacità di avere la comprensione ed un giudizio critico su quello che si legge. Tuttavia la definizione di fake news rappresenta solo la parte più nota ed evidente delle capacità di manipolazione delle informazioni, tant'è che in ambito di C-IW / IW si parla più specificatamente di *"information disorder"*.

Anche se l'uso dell'etichetta "*information disorder*", si sta sempre più rapida-

mente sostituendo alla locuzione fake news per via dell'utilizzo delle stesse strategie e metodologie anche da parte di attori non governativi e militari, l'*information disorder* definisce una serie di dinamiche legate all'inquinamento delle informazioni più articolate e complesse, sviluppandosi su tre diverse dimensioni:

- ***DISINFORMATION***, in cui il contenuto che viene diffuso è intenzionalmente falso e progettato ad hoc per creare conseguenze dannose;

- ***MISINFORMATION***, in cui la condivisione di "parti" di contenuti falsi viene veicolata attraverso utenti inconsapevoli, che diventano vettori presso le proprie reti, convinti di immettere nel loro canale comunicativo contenuti utili;

- ***MALINFORMATION***, in cui informazioni vere vengono condivise con l'intenzione di creare conseguenze dannose, attraverso l'uso di frame deformati che vengono strumentalizzati all'interno di contesti geopolitici e di conflitto.

Queste tre dimensioni rappresentano le tipologie di contenuti che possono essere strumentalizzati e veicolati attraverso la rete in una campagna IW/C-IW in base alle intenzioni dell'attaccante, pensati per ingannare e generare conseguenze manipolando la sfera delle informazioni. I driver utilizzati tipicamente sulla rete per veicolare campagne C-IW sono di natura tecnologica e driver (dinamiche) di natura sociale.

L' approccio utilizzato non è selettivo, tecnologico o sociale ma integrato, infatti gli elementi tecnologici e quelli sociali si influenzano a vicenda senza soluzione di continuità, rendendo le strategie di information disorder, endemiche nella sfera dei conflitti basati sulle informazioni digitalizzate. Nelle campagne C-IW il driver tecnologico non è solo un vettore privilegiato ma un acceleratore in grado di generare effetti di attrazione e polarizzazione.

Internet è una rete ad invarianza di scala che segue la legge di potenza (*power law*). Questo vuol dire che indipendentemente dal numero di nodi che compongono ogni insieme della rete

(invarianza), il meccanismo di distribuzione delle risorse (*link*) sarà sempre guidato dalla *power law*, ovvero dalla coesistenza tra nodi più ricchi (*hub*) e nodi meno ricchi (nodi comuni).

All'interno di questi insiemi, i nuovi utenti scelgono di connettersi ai nodi già presenti mediante un meccanismo noto come "attaccamento preferenziale", cioè tenderanno a preferire l'interazione con i nodi più popolari, gli *hub* appunto, siano essi persone (attori, politici, *influencer*, etc.), contenuti (post, meme, video, etc.) o servizi digitali (social network, motori di ricerca, etc.).

Più un elemento è popolare, più connessioni possiede, più sarà "scelto" dagli altri nodi, aumentando così la sua popolarità e diventando sempre più appetibile per le scelte di nuovi utenti, in un processo noto come l'effetto San Matteo, un meccanismo iniquo per cui i ricchi diventano sempre più ricchi.

Ed è a questo punto che si sviluppano nuove interazioni tra il driver tecnologico ed il driver delle dinamiche sociali, disegnando un ambiente digitale in cui più una informazione viene diffusa, più saranno elevate le sue probabilità di ricevere maggiori attenzioni e di essere a sua volta propagata. Grazie a questo meccanismo l'informazione manipolata e inizialmente "inoculata", verrà, durante la fase di propagazione, continuamente rimaneggiata (spesso modificata ripetutamente anche da altri utenti), sia in termine di "*trust*" degli utenti sia in termini di contenuto della stessa, cioè si arricchirà di ulteriori informazioni (ad es. commenti, condivisioni con altri post, etc.) questo processo renderà l'informazione sempre più difficile da analizzare e valutare, non solo in termini di credibilità ma anche in termini di affidabilità e verifica della fonte.

Altri strumenti utilizzati in ambito C-IW sono stati introdotti proprio per manipolare ulteriormente le dinamiche sociali, ad es. per aumentare la visibilità di un *hub* creato per diffondere notizie manipolate "credibili" sono stati sviluppati dei generatori di "*fake follower*", finti utenti per ingannare altri utenti, rappresentando così gli hub generatori di fake, più popolari di quanto in realtà lo siano.

Ad es. i *social bot* rispondono proprio a questa esigenza, sono programmi per computer che imitano gli esseri umani e i loro comportamenti nei social network, con l'obiettivo di manipolarne i comportamenti.
La caratteristica di questa tecnologia e che imita gli utenti umani fingendo anche interazioni tra finti utenti ed eludendo così gli algoritmi di controllo dei social network. E anche se negli ultimi tempi gli algoritmi di controllo sono sempre più sofisticati, per poterli ingannare ulteriormente è stata affiancata ai social bot la figura "dell'untore digitale", cioè umani che si comportano bot, rendendo così il riconoscimento e contrasto molto più difficile.

Il fine rimane dunque la possibilità di aumentare la credibilità delle fonti di informazione, in modo che siano percepite come utenti legittimi (umani) ed interessati a diffondere informazioni utili.

L'evolversi delle tecnologie inoltre sta manipolando anche la natura stessa delle informazioni. I fotomontaggi, i ritocchi alle immagini, comunemente chiamate "immagini photoshoppate", sono un esempio di informazione manipolata a cui siamo ormai abituati anche come utilizzatori, infatti esistono oggi centinaia di applicazioni di uso comune sugli smartphone che permettono di modificare le proprie foto con una qualità di contraffazione sempre più fedele alla realtà.

Negli ultimi anni però si sta aprendo un nuovo capitolo nel panorama dei contenuti costruiti in laboratorio, soprattutto grazie all'aiuto dell'intelligenza artificiale.

Ne è un esempio la tecnologia Deep Fake, questa tecnologia è in grado di riprodurre la voce e generare volti umani identici a persone reali ma completamente creati dal computer, realtà "sintetiche" che riproducono azioni, discussioni o intere scene (anche in tempo reale) ritraendo ed impersonando persone totalmente estranee alle ricostruzioni.

I video elaborati tramite questa tecnologia vengono processati più volte da algoritmi gestiti dall'A.I. che ottiene alla

fine dei filmati, tecnicamente, sempre più indistinguibili da quelli reali.
Le strategie e le tecnologie della C-IW sono sempre di più utilizzate anche in altri ambiti, dove gli attacchi sono sempre rivolti all'utente e non al computer ma dove l'obiettivo è esfiltrare informazioni o inoculare malware per attività di *cyber crime*, come nel caso del social engineering un insieme di tecniche utilizzate dai cybercriminali per attirare gli ignari utenti ad inviare loro i propri dati riservati, infettare i loro computer tramite malware o aprire collegamenti a siti malevoli.

Francesco Arruzzoli, *Resp. R&D e Centro Studi Cyber Defense Cerbeyra*

BIOGRAFIA

Francesco Arruzzoli

Con oltre 30 anni di esperienza nell'ambito della sicurezza delle informazioni Francesco Arruzzoli è Sr. Cyber Security Threat Intelligence Analyst presso la Winitalia di cui è cofondatore. Responsabile del Centro Studi Cyber Defense Cerbeyra presso il polo di cyber security del Gruppo Vianova, coordina le attività di R&D, analisi delle cyber minacce e progettazione di nuove soluzioni per la cyber security di aziende ed enti governativi. Progettista di sistemi esperti, software developer, network e system engineer, è stato tra i primi ethical hacker italiani certificati. Autore di libri ed articoli sue riviste del settore, in passato ha lavorato per multinazionali, aziende della sanità italiana, enti governativi e militari. In qualità di esperto di Cyber Intelligence e contromisure digitali ha svolto inoltre attività di docenza presso alcune università italiane.

Relazioni tra State Nation ed eCrime Actor

SINOSSI

Per gli analisti d'intelligence, l'identificazione degli avversari responsabili di un attacco informatico è sempre stata un'attività molto impegnativa. In questo articolo si vogliono sinteticamente affrontare gli aspetti di complessità connaturati alla fase di *attribution* e, soprattutto, i punti di connessioni sempre più frequenti tra i gruppi *Nation State* e quelli *eCrime.*

PRINCIPALE CATEGORIZZAZIONE DEGLI AVVERSARI (THREAT ACTOR)

Al fine di rendere più chiara la trattazione dell'argomento di questo articolo, è fondamentale introdurre le principali categorie utilizzate. Per categorizzare i Threat Actor responsabili degli attacchi informatici. La categorizzazione utilizzata è quella impiegata anche nel *MISP Galaxy*[1]:

NATION STATES: entità che lavorano per il governo o i militari di uno Stato o che operano sotto la loro direzione. Questi attori hanno in genere accesso a supporto, risorse, formazione e strumenti significativi e sono in grado di progettare ed eseguire campagne molto sofisticati ed efficaci.

- Obiettivo principale: spionaggio, furto o qualsiasi altra attività che favorisca gli interessi di un particolare gruppo nazionale
- Obiettivi tipici: Aziende ed organizzazioni governative

[10]-DOD Galaxies in MISP sono un metodo utilizzato per esprimere un oggetto di grandi dimensioni chiamato cluster che può essere collegato a eventi o attributi MISP. https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json

eCRIME: un'organizzazione (anche individuale) in grado di condurre un'attività criminale significativa e su larga scala a scopo di lucro. L'eCrime (o Criminalità Organizzata) è generalmente costituito da gruppi di grandi dimensioni e dotati di buone risorse che operano per trarre profitto da tutti i tipi di crimini informatici. Il furto di proprietà intellettuale, l'estorsione tramite ransomware e la distruzione fisica sono esempi comuni.

- Obiettivo principale: Guadagno economico
- Obiettivi tipici: Organizzazioni e aziende ricche di denaro e/o di dati

HACKTIVIST: sostenitori, altamente motivati e potenzialmente distruttivi, di cause sociali (ad esempio, commercio, lavoro, ambiente, ecc.) o di ambiti politici che tenta di annientare il modello di business di un'organizzazione o di danneggiarne l'immagine. Questa categoria comprende attori talvolta definiti anarchici, vandali informatici ed estremisti.

- Obiettivo principale: svelare segreti e distruggere servizi/organizzazioni percepiti come malvagi
- Obiettivi tipici: Non limitati a un tipo specifico di organizzazione o azienda

INDIVIDUALS: un individuo che tende a penetrare nelle reti per il brivido del rischio o come gesto di sfida. Gli hacker possono avere competenze avanzate o utilizzare semplici script di attacco scaricati da sorgenti pubbliche. Tra gli individuals ci sono anche insider non ostili che espongono involontariamente l'organizzazione a un danno. In questo contesto, il termine "*insider*" comprende qualsiasi persona, interna all'organizzazione, che goda di una fiducia estesa, come dipendenti regolari, appaltatori, consulenti e lavoratori temporanei.

- Obiettivo principale: Lavorare dall'interno di un'organizzazione per aggirare la sua struttura di *cyber security*
- Obiettivi tipici: : Non limitati a nessun tipo specifico di organizzazione

Tra gli avversari appena elencati, quelli di maggiore interesse sono i gruppi *Nation States* e *eCrime*. Mentre gli obiettivi dei gruppi eCrime sono sempre di natura utilitaristica, i gruppi Nation States possono essere contraddistinti anche sulla base del coinvolgimento degli Stati negli attacchi.

Lo spettro delle responsabilità di uno Stato è uno strumento che può aiutare gli analisti, con conoscenze limitate, ad assegnare la paternità di un particolare attacco (o di campagne di attacchi) con maggiore precisione e trasparenza. Lo spettro attribuisce dieci categorie, ciascuna contrassegnata da un diverso grado di responsabilità, a seconda che una nazione ignori, favorisca o conduca l'attacco. Lo spettro parte da una responsabilità molto passiva di uno Stato fino ad una notevolmente attiva:

- ***State-prohibited*:** il governo nazionale contribuirà a fermare l'attacco di terzi che può provenire dalle sue regioni o semplicemente transitare attraverso le sue reti perché non può garantire il costante comportamento corretto delle decine o centinaia di milioni di computer presenti all'interno dei loro confini.
- ***State-prohibited-but-inadequate***: il governo nazionale collabora e fermerebbe l'attacco di terzi se fosse in grado di farlo. Il Paese potrebbe non avere le leggi, le procedure, gli strumenti tecnici o la volontà politica di utilizzare tali mezzi di contrasto. Anche nel caso in cui fosse quella stessa nazione la potenziale vittima, ad essa può comunque essere attribuita una responsabilità passiva per l'attacco determinata sia dall'incapacità di fermarlo che, soprattutto, dal non avere predisposto dei sistemi sicuri.

Nelle quattro categorie seguenti, a differenza delle due sopra elencate, le nazioni ignorano o favoriscono attivamente gli attacchi:

- ***State-ignored*:** il governo nazionale è a conoscenza degli attacchi di terzi ma, per questioni politiche, non è disposto a intraprendere alcuna azione ufficiale. Un governo può persino essere d'accordo con gli obiettivi ed interessato ai risultati degli aggressori e perciò coprire le loro attività.

- ***State-encouraged***: terze parti controllano e conducono l'attacco, ma il governo nazionale li sostiene per questioni politiche. Tale incoraggiamento potrebbe avvenire a mezzo stampa o attraverso dichiarazioni pubbliche offerte dai dirigenti politici in cui si mostrano d'accordo con gli obiettivi degli attacchi; i membri delle organizzazioni governative di *cyber offensive* o di intelligence potrebbero essere incoraggiati a intraprendere un'attività di supporto che può essere definito "hacking ricreativo" (*recreational hacking*).
- ***State-shaped***: terze parti controllano e conducono l'attacco, ma lo Stato fornisce un certo supporto, ad esempio un coordinamento informale tra persone che la pensano allo stesso modo all'interno del governo e del gruppo attaccante. Per promuovere la propria politica e mantenere una plausibile negabilità il governo può incoraggiare i membri delle proprie forze informatiche a intraprendere un'attività di "hacking ricreativo".
- ***State-coordinated:*** il governo coordina gli attaccanti terzi, di solito al di fuori dell'opinione pubblica, "suggerendo" obiettivi, tempistiche o altri dettagli operativi. Il governo può anche fornire assistenza tecnica o tattica. Analogamente agli attacchi sopra descritti, il governo può incoraggiare le proprie forze informatiche a impegnarsi in attività di "hacking ricreativo" durante le ore non lavorative.

Nelle ultime quattro categorie, lo Stato partecipa agli attacchi in maniera diretta, commissionandoli o conducendoli esso stesso:

- ***State-ordered***: il governo ordina a dei proxy terzi di condurre l'attacco per suo conto. Questo è ciò che si definisce "sponsorizzato dallo Stato", e si posiziona appena prima di un attacco effettuato direttamente da parte delle forze informatiche governative. Gli aggressori, possono essere considerati, di fatto, agenti dello Stato.
- ***State-rogue-conducted:*** elementi delle forze informatiche governative conducono l'attacco. In questo caso, gli attacchi possono essere perpetuati con l'approvazione o all'insaputa della *leadership* nazionale, che

potrebbe intervenire per fermare gli attacchi qualora ne venisse a conoscenza. In entrambi i casi, lo Stato potrebbe essere ritenuto responsabile dai tribunali internazionali.

- ***State-executed*:** il governo nazionale controlla e conduce direttamente l'attacco utilizzando le proprie forze informatiche.
- ***State-integrated*:** il governo nazionale affianca attaccanti terzi alle forze informatiche governative, comandate e controllate da un'unica entità. Gli ordini e il coordinamento possono essere formali o informali, in entrambi i casi, è il governo a selezionare e schedulare gli obiettivi. Gli aggressori sono, a tutti gli effetti, agenti dello Stato.

DEFINIZIONE DI ATTRIBUTION

Alla base delle attività di classificazione degli avversari viene svolta l'attività di attribuzione che ha come obiettivo quello di identificare gli attori responsabili di un attacco informatico. Quotidianamente, i *threat actor* prendono di mira settori come l'energia, la finanza e l'industria manifatturiera e quindi fornire un'intelligence specifica per ciascun

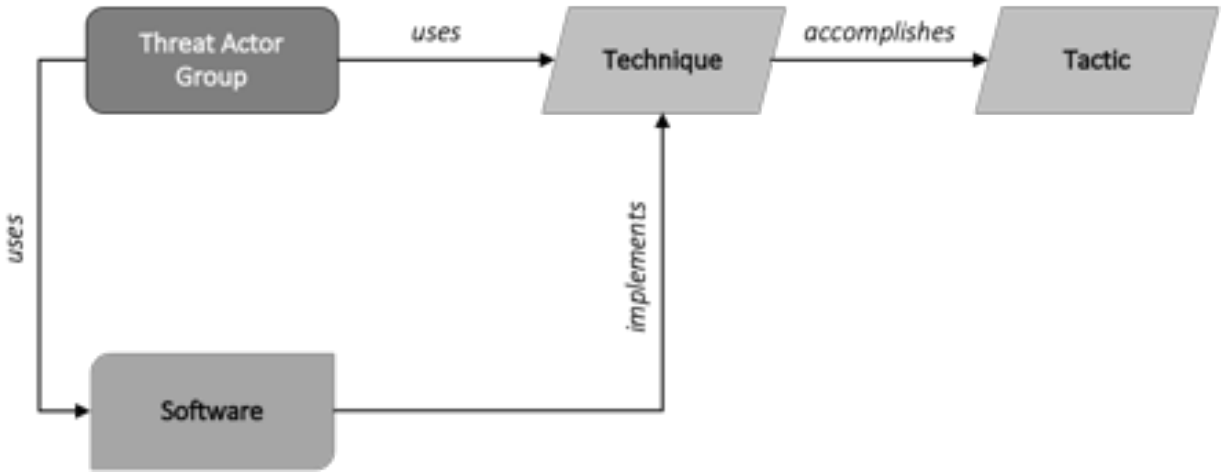


Fig. 1 – Relazioni tra gli elementi principali nel modello MITRE ATT&CK

settore industriale è fondamentale al fine di proteggere le organizzazioni dalle minacce sconosciute. La Fig. 1 mostra il rapporto tra i principali elementi utili ad indentificare un attore malintenzionato.

Un prerequisito importante è la conoscenza degli strumenti e delle tecniche di attacco più comuni in modo da identificarle quando sono impiegate all'interno di un'infrastruttura colpita.
Risulta fondamentale capire quanto siano affidabili le conclusioni basate sull'indagine di determinati artefatti rilevati, poiché questi potrebbero essere falsificati con l'intento di depistare la reale attribuzione al fine di celare il reale attaccante. Questi aspetti si verificano frequentemente nelle infrastrutture ICT complesse in quanto la complessità dei sistemi odierni non solo rende difficile il compito degli investigatori di reperire dati rilevanti per le indagini, ma -di converso- complica il lavoro degli attaccanti nel realizzare campagne f*alse flag*.

Un requisito dell'attribuzione informatica è quello di identificare le tattiche, le tecniche e le procedure (TTP) applicate dagli attaccanti. A tal fine si procede con l'identificazione della fonte di determinati attacchi per poi arrivare all'individuazione dell'attore della minaccia. Entrambi gli argomenti, l'investigazione degli attacchi informatici (cioè sapere cosa è successo) e l'attribuzione dell'attaccante, hanno lo scopo di servire come punto di partenza per le attività di *law enforcement* e della sicurezza nazionale (come nel caso di guerra informatica o il terrorismo).
Su questo argomento, esiste un'ampia letteratura che segue approcci diversi, anche se spesso si tratta di un mix di analisi tecnica degli attacchi e di *profiling* degli attori delle minacce che, a volte, genera confusione. I ricercatori evidenziano che non sono utili solo i sample di malware e le loro proprietà specifiche (come le configurazioni del compilatore utilizzato, il linguaggio di programmazione, la presenza di schemi ricorrenti e simili), ma anche le informazioni disponibili al di fuori dell'infrastruttura attaccata, compresi i dati sui server di Command & Control (C2). Ulteriori elementi presi in considerazione sono gli indirizzi IP che sono stati utilizzati, i nomi di dominio e le relative informazioni di registrazione come -ad esempio- quelle

legate all'acquisto di quel determinato dominio. Tutto ciò fa sì che si arrivi ad una categorizzazione dei dati che distingua tra persone fisiche, personaggi virtuali, campagne di attacco, infrastrutture e strumenti.

È importante tenere presente che l'attribuzione di un attacco a un gruppo specifico è solitamente difficile e raramente può essere confermata. In tale processo, gli indicatori possono essere il riutilizzo di malware (o di parti di esso), ma non c'è la garanzia che altri gruppi abbiano avuto accesso al codice sorgente, magari attraverso la condivisione o l'acquisto sul mercato nero. Anche la lingua e l'encoding possono svolgere un ruolo importante nell'individuare il Paese o la regione di provenienza di un'APT, contribuendo così all'attribuzione.

Inizia ad imporsi sempre di più l'approccio in cui l'attribuzione rappresenta l'identificazione o la classificazione di un incidente a una determinata entità, dove quest'ultima è un identificatore flessibile che va dall'attribuzione *"how-centric"*, che collega le analisi di gruppi, comportamenti o TTP simili, all'attribuzione *"who-focused"* molto specifica, che fa riferimento ad una persona o ad un'organizzazione in particolare, facendo così emergere molteplici possibilità.
La fase di attribuzione è inoltre indispensabile perché può aiutare a determinare le azioni preventive, individuare i probabili obiettivi e consentire l'azione penale. Se una azienda sa di essere stata presa di mira da un attaccante conosciuto, può essere in grado di conoscere i metodi di attacco arrivando così a strutturare una difesa più efficace e mirata. Alcuni attori delle minacce possono essere associati a malware, indirizzi IP, domini, vettori di attacco specifici; il loro operato potrebbe ambire al sabotaggio, ad esempio, attraverso attacchi DDOS, o al furto di segreti aziendali, dati finanziari, ecc.
Conoscere i vettori di attacco tipici di specifiche APT è di aiuto nel mettere in relazione le tecniche utilizzate in uno o più attacchi, perpetuati verso la stessa vittima, arrivando così ad identificare l'attaccante. Un'azienda che subisce una perdita finanziaria a causa di un attacco informatico potrebbe voler intraprendere un'azione legale per recu-

perare parte dei costi, il che rappresenta una motivazione per scoprire chi si cela esattamente dietro un attacco.

PROBLEMI DI ATTRIBUZIONE

I problemi di attribuzione costituiscono un labirinto che continua a preoccupare tutti coloro che sono coinvolti nella difesa informatica e nella sicurezza in generale. Determinare cosa è avvenuto, a chi e da chi è stato commesso è un processo che manca di ripetibilità e spesso di una soluzione chiara. Tuttavia, l'importanza dell'attribuzione lo rende un lavoro indispensabile su cui è utile concentrare le risorse, poiché senza la possibilità di attribuire un attacco informatico a un individuo, a un gruppo o a uno Stato, non è possibile intraprendere un'azione di contrasto a livello politico o legale.
Ciò rappresenta un'enorme limitazione nelle relazioni internazionali dove l'attività informatica continua a crescere, influenzando la diplomazia e i conflitti e quella che alcuni potrebbero considerare un'indagine tecnica si rivela un problema geopolitico di primaria importanza.

Naturalmente, oltre alle numerose complessità intrinseche nell'attività di attribuzione, gli analisti di intelligence devono affrontare le tattiche di *deception*, definite *false flag* messe in atto dagli aggressori al fine di evitare l'associazione con gli attacchi informatici.

Le *false flag* fanno parte, da lunga data, della strategia militare della *deception* e risale alle schermaglie navali in cui la bandiera di una nave veniva nascosta o modificata perché sembrasse un'altra. Lo scenario è il seguente: Il Paese X utilizza tattiche ed equipaggiamenti solitamente impiegati dal Paese Y per attaccare o provocare il Paese Z, in modo che il Paese Y si prenda la colpa e l'attenzione del Paese Z venga distolta dal Paese X, il che permette al Paese X di avere libertà di manovra per adoperarsi in altri ambiti. Impegnarsi in un combattimento indossando un'uniforme diversa da quella del proprio Paese è vietato dalla Convenzione dell'Aia, ma il concetto di *false flag* è stato anche esteso allo scenario in cui il Paese X attacca o sottomette internamente i propri cittadini, agendo in veste di un altro Paese o di un gruppo con motivazioni politiche.

Nel campo informatico, le *false flag* si riferiscono alle tattiche impiegate dagli attaccanti per occultare, ingannare o fuorviare i tentativi di attribuzione, compresa la comprensione sull'origine dell'aggressore, della sua identità e dell'*exploitation*. In genere è molto difficile attribuire in modo definitivo gli attacchi informatici ai loro reali autori e l'impiego delle tattiche di depistaggio possono causare un'attribuzione errata, determinando così una risposta e/o un contrattacco in grado di portare a ritorsioni contro una parte sbagliata.

Un'altra modalità di utilizzo delle *false flag* è quella in cui un aggressore simula di essere un altro threat actor. Un'operazione di *false flag* può essere condotta semplicemente come azione di "marketing" malevolo inserendo immagini che rimandano ad un altro attaccante, oppure vengono inserire altre lingue nei *payload header* o malware.

Sebbene il trattamento approfondito delle tattiche di *false flag* utilizzate dagli avversari esuli dallo scopo di questo lavoro, di seguito vengono riportati alcuni esempi di casi noti:

- Dal 2012, gli hacker iraniani hanno utilizzato l'arabo anziché il farsi nei cyber attacchi alle banche statunitensi, mentre il gruppo Lazarus, sospettato di essere sponsorizzato dallo Stato nordcoreano, è spesso noto per i suoi tentativi di contraffazione linguistica.
- Nel 2016, la società di sicurezza CrowdStrike ha ricondotto alla GRU, agenzia di spionaggio russo, le operazioni false flag dirette contro gli Stati Uniti come l'hacking del Comitato Nazionale Democratico e successivamente della campagna presidenziale di Hillary Clinton. Il gruppo di hacker responsabile, chiamato Fancy Bear, si era camuffato da hacktivista rumeno chiamato Guccifer 2.0 e realizzato un sito di *whistle-blowing* (chiamato DCLeaks) che ha distribuito i documenti rubati.
- Secondo l'intelligence statunitense, le spie militari russe hanno violato diverse centinaia di computer utilizzati durante i giochi olimpici invernali del 2018, dalle autorità della Corea del Sud e lo hanno fatto cercando di far ricadere la colpa dell'intrusione alla Corea del Nord.

Distinguere i gruppi *Nation State* da quelli *No Nation State* (in particolare i gruppi eCrime) è estremamente complessa a causa di diversi fattori tra cui:

- Gli stessi gruppi possono agire in momenti diversi sia come *Nation State* e sia come *eCrime*
- I gruppi di *eCrime* possono collaborare o riutilizzare strumenti realizzati da *threat actor Nation State*
- I gruppi *Nation State* possono utilizzare strumenti o seguire motivazioni specifiche dei gruppi *eCrime*

A titolo puramente esemplificativo, si riportano di seguito alcuni esempi:

- **APT17** è un gruppo APT cinese responsabile di una serie di intrusioni nelle reti informatiche di diversi enti statunitensi e del Sud-Est asiatico, prendendo di mira settori legati alla difesa, studi legali, aziende informatiche, società minerarie e organizzazioni non governative. Nel luglio 2019, un gruppo di hacker che si fa chiamare *Intrusion Truth* ha affermato che tre membri dell'APT17 sono riconducibili dell'agenzia di intelligence cinese di Jinan (il Ministero della Sicurezza di Stato - MSS). Basandosi su quanto scoperto, Intrusion Truth ritiene che APT17 svolga operazioni di hacking commissionate dall'MSS. Questa storia diventa ancora più avvincente quando si scopre che APT17 prende contemporaneamente di mira anche i cittadini cinesi per scopi di lucro, Intrusion Truth fornisce dei documenti contenenti il listino prezzi di APT17 relativo alla messa in vendita di dati a gruppi di hacker in Cina.
- Secondo FireEye, il gruppo **APT41** ha spiato a scopo di lucro fornitori globali di tecnologia, telecomunicazioni e sanità per conto del governo cinese, prendendo di mira anche aziende di videogiochi e fondi di criptovaluta. Unico nel suo genere, APT41 ha sede in Cina ed impiega strumenti non pubblici impiegati in campagne di spionaggio. In particolare, l'APT41 ha preso di mira i distributori di videogiochi dell'Est e del Sud-Est asiatico e i loro popolari giochi online, compresi quelli con un considerevole mercato cinese, per manipolare le valute virtuali e rubarne il codice sorgente. FireEye, notando l'impiego dello stesso malware utilizzato sia nelle attività finanziarie e sia per le attività

sponsorizzate dallo Stato, valuta con "moderata fiducia" che gli hacker operino come un gruppo di appaltatori piuttosto che come dipendenti statali poiché, se così fosse, sarebbero soggetti a un maggiore controllo e avrebbero meno probabilità di operare in modo indipendente dall'MSS. Non rientrando nelle attività sponsorizzate dallo Stato, alcuni di questi terzisti pubblicizzano le loro competenze, i loro servizi e operano in mercati clandestini.

- Il **Gruppo Lazarus** è stato ritenuto responsabile di alcuni dei più noti attacchi informatici degli ultimi anni e alcuni ricercatori hanno ipotizzato che questo gruppo potrebbe essere sostenuto dal governo nordcoreano. Negli ultimi anni, il gruppo ha compiuto diversi furti a istituzioni finanziarie tradizionali e a *cryptocurrency exchanges* di tutto il mondo. Le prime attività del gruppo Lazarus risalgono al 2009, ma alcuni analisti suggeriscono che sia attivo già dal 2007. Lazarus è stato collegato ad alcuni dei cyber attacchi più noti della storia, tra cui quello del 2014 contro Sony Pictures Entertainment, il furto alla Bangladesh Bank del 2016 e alla diffusione del ransomware WannaCry del 2017. Alla fine del 2015, il gruppo ha iniziato ad abbandonare l'uso di malware finalizzati alla realizzazione di DDoS e di wiper e cominciando a sperimentare la compromissione di istituzioni finanziarie e ad effettuare furti attraverso lo SWIFT, ovvero l'invio e l'incasso di trasferimenti SWIFT fraudolenti. Questo è sintomatico di un cambiamento di motivazioni: perseguire per la prima volta un guadagno finanziario. Da allora, Lazarus ha continuato a prendere di mira le istituzioni finanziarie con l'obiettivo di compiere furti nel sistema SWIFT. Negli ultimi anni sono state bersagliate istituzioni finanziarie negli Stati Uniti, Messico, Brasile, Cile, Venezuela, Colombia, Uruguay, Regno Unito, Danimarca, Polonia, Turchia, Cina, Taiwan e Hong Kong. Lazarus Group indirizza la sua attività criminosa anche verso le borse di criptovalute: la società cinese 360 Security li ritieni responsabili del furto di fondi dalle borse di criptovalute Etbox, Biki e Dragonex. La maggior parte degli obiettivi originari di questa *gang* si è storicamen-

te concentrata sulla Corea del Sud e sugli Stati Uniti, con il passare del tempo, però, il gruppo ha mostrato un approccio più opportunistico, compromettendo organizzazioni in tutto il mondo. Questo spostamento di obiettivi è in linea con la tendenza di Lazarus a perseguire un guadagno finanziario e rende l'idea di quanto il gruppo sia altamente sofisticato ed adattivo. Alcuni analisti, a causa dell'uso di prodotti *crimeware* come il ransomware Hermes, sostengono che il gruppo Lazarus interagisce con i criminali informatici di lingua russa.

- Alla fine del 2016, gli hacker del GRU hanno iniziato a cambiare tattica. Nel dicembre dello stesso anno, gli analisti della società slovacca di cybersecurity ESET hanno notato che il gruppo **Telebots**, noto anche come Voodoo Bear o Sandworm, ingaggiava sia hacktivist che cybercriminali per i loro attacchi data-destructive contro le reti ucraine. In alcuni casi, si è scoperto che i computer cancellati mostravano il messaggio "NOI SIAMO LA FSOCIETY, UNITEVI A NOI", con un riferimento agli attivisti anarchici della serie televisiva Mr. Robot. Invece, in altri incidenti avvenuti nello stesso periodo, ESET ha scoperto che gli hacker richiedevano il riscatto in bitcoin del ransomware.

PUNTI IN COMUNE TRA GLI STATI NAZIONALI E GLI ATTORI DELL'ECRIME

Come ha affermato Mieke Eoyang (*Deputy Assistant Secretary of Defense for Cyber Policy*), *"the line between nation-state and criminal actors is increasingly blurry as nation-states turn to criminal proxies as a tool of state power, then turn a blind eye to the cybercrime perpetrated by the same malicious actors"*

Il punto di maggiore interesse non è più la distinzione tra le competenze e le caratteristiche tecniche degli strumenti utilizzati dai gruppi *Nation State* rispetto ai gruppi di *eCrime*, ma lo sfruttamento di quest'ultimi da parte dei gruppi *Nation State*. Un significativo e recente esempio dell'utilizzo dei gruppi di *eCrime* da parte dei gruppi *Nation State* è l'uso di ransomware come copertura per

operazioni di spionaggio da essi sponsorizzate.

Una chiara distinzione tra i diversi livelli di connessione che possono esistere tra Stati e criminali informatici è stata proposta da Recorded Future in un recente articolo. Sebbene l'esemplificazione dei diversi livelli di connessione sia stata applicata alla Russia e al suo ecosistema cybercriminale, riteniamo che la distinzione proposta possa essere estesa a qualsiasi Stato.

L'azienda di sicurezza, sulla base di attività e associazioni, ha identificato tre tipi di legami tra i servizi segreti russi e il sottosuolo criminale ruteno.
Basandosi sulla comprensione del contesto storico e considerando l'attuale panorama dei cybercriminali e del governo russo, Recorded Future ha classificato l'attività osservata in questo ecosistema in tre categorie principali:

- Le ***direct associations*** sono identificate da legami precisi tra istituzioni statali e hacker; un esempio è Dmitry Dokuchaev, un maggiore del Servizio di Sicurezza Federale Russo che è stato reclutato dopo aver lavorato come criminale informatico.
- Le ***indirect affiliations*** si verificano nei casi in cui non è possibile stabilire un legame diretto, ma esistono chiari segnali che indicano come il governo russo sfrutti le risorse o i cyber criminali a suo vantaggio; un esempio è il probabile utilizzo da parte del governo russo della botnet Game Over Zeus per lo spionaggio o gli attacchi DDoS da parte di "hacker patriottici" durante i conflitti militari.
- Il ***tacit agreement*** è definito come la sovrapposizione di attività criminali informatiche, compresa l'individuazione degli obiettivi e la tempistica, che favoriscono gli interessi o gli obiettivi strategici dello Stato russo; tali attività sono condotte senza legami diretti o indiretti con lo Stato, ma sono consentite dal Cremlino, che chiude un occhio quando avvengono.

Per **collegamenti diretti** si intende l'intersezione diretta tra la criminalità informatica e i servizi speciali russi, attraverso il reclutamento coercitivo o volontario, dove:

1. il ***willing recruitment*** (reclutamento

volontario) avviene quando individui interessati a sostenere gli interessi del governo russo cercano di propria iniziativa di impegnarsi in attività a sostegno dello Stato.

2. il ***coercive recruitment*** (reclutamento coercitivo) avviene quando il governo russo individua sui forum clandestini un programmatore esperto e di successo di malware, lo arresta per le sue attività e gli presenta due alternative: l'accusa e la prigione o la collaborazione e lo stipendio.

Un altro esempio di associazione diretta si verifica nei casi in cui i servizi segreti russi realizzano forum clandestini con il proposito di reclutare i cyber criminali, intensificando così gli sforzi per scopi specifici. Alcuni forum sembrano palesemente dei forum criminali consentendo così ai servizi di intelligence di individuare facilmente i talenti da reclutare.
Gli individui descritti qui sopra vengono impiegati in attività criminali informatiche, finanziariamente motivati attraverso il guadagno personale e hanno, quelli che riteniamo essere, legami diretti con lo Stato russo attraverso politici, contatti con il Cremlino o i servizi di intelligence russi.

Le **affiliazioni indirette** si riferiscono ai casi in cui lo Stato non impiega direttamente individui dell'ecosistema cyber criminale, ma utilizza invece le loro infrastrutture al fine di favorire gli interessi del governo russo. Inoltre, gli "hacker patriottici" possono condurre azioni che vanno a beneficio dello Stato, ma non sono direttamente collegati ad alcun governo o servizio di intelligence russo. A titolo di esempio, si possono considerare gli attacchi DDoS che hanno preso di mira il governo estone tra aprile e maggio 2007.

Le agenzie di intelligence russe hanno impiegato un malware, realizzato dai criminali informatici, per offuscare le loro attività e rendere più difficile l'attribuzione. Hanno utilizzato circuiti di riciclaggio di denaro e hosting inaccessibili per occultare il movimento di fondi e la sponsorizzazione di attività di ingerenza. Hanno anche utilizzato reti compromesse per scopi criminosi, come cercare dati sensibili e credenziali utili alle attività di spionaggio e prendere di mira sia l'opposizione interna che le organizzazioni e i governi occidentali.

Il **tacito accordo** si riferisce ai casi in cui l'esistenza o meno di connessioni tra le autorità russe e i criminali informatici diventa difficile da confermare. Si verifica quando i criminali informatici sono ampiamente conosciuti sia all'interno della Russia che all'estero e, a parte perseguire coloro che hanno preso di mira qualche realtà russe o che hanno oltrepassato una qualche linea politica, le autorità russe fanno ben poco per cercare di smantellare questo ecosistema criminoso.
La reazione silenziosa del Cremlino alle attività criminali informatiche provenienti dall'interno della Russia ha fatto sì che le organizzazioni criminali informatiche si trasformassero in vere e proprie imprese ben gestite.
La Russia rimarrà un rifugio sicuro per i cyber criminali fino a quando il Cremlino non deciderà di indagare e perseguire gli hacker che operano nel suo territorio.
Gli accordi taciti si verificano quando l'ecosistema cyber criminale russo conduce attività indipendenti da qualsiasi direttiva dello Stato. Questo tipo di attività, e le relative tempistiche, sono però allineate con gli obiettivi strategici del governo russo, pur non essendoci collegamenti diretti o indiretti. Il governo stabilisce un tacito accordo tra gli individui che conducono gli attacchi non perseguendoli finché questi prendono di mira il bersaglio "giusto" e non danneggiano gli interessi del Cremlino.
I collegamenti taciti si verificano anche quando un'attività sponsorizzata dallo Stato utilizza un ransomware per fornire una plausible negabilità o complicare l'attribuzione delle operazioni informatiche intraprese a vantaggio dello Stato. Non si tratta di collegamenti diretti, in quanto non è chiaro se gli individui che utilizzano questo malware siano o meno membri dell'ecosistema criminale informatico, ma il malware deriva da fonti criminali informatiche. Non si può neppure parlare di connessioni indirette perché non si tratta della messa a disposizione di una risorsa criminale a vantaggio dello Stato, ma si tratta di una tacita approvazione da parte dello Stato.

L'uso di malware da parte dei servizi segreti russi consente quasi certamente al governo di Mosca di mantenere una plausible *deniability* nelle intrusioni mirate, soprattutto quando vengono utiliz-

zate determinate varianti di malware. Oltre a modificare e utilizzare malware come Black Energy, Sandworm, la Russia è stata associata anche ad intrusioni dove venivano impiegate versioni modificate di ransomware utili a realizzare intrusioni dirompenti e distruttive.

Considerata la relazione di lunga data tra i servizi segreti russi e l'ecosistema criminale informatico del Paese, è quasi certo che queste connessioni persisteranno nel prossimo futuro e molto probabilmente continueranno a facilitare le operazioni dei servizi segreti sovietici. Finché i criminali informatici saranno protetti da procedimenti penali nazionali, essi potranno trarre profitto dalle loro azioni malevoli garantendo al governo russo una plausible *deniability*, non c'è alcuna speranza che queste attività si fermino, continuerà così la proliferazione di malware.

Francesco Schifilliti, *Consulente in Cyber Security & Threat Intelligence*

RIFERIMENTI

1. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks", Jason Healey, Atlantic Council (Available to https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.pdf)

2. "In Cyber, Differentiating Between State Actors, Criminals Is a Blur", C. Todd Lopez, U.S. Department of Defense (Available to https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur)

3. "Attributing Cyber Attacks", Thomas Rid and Ben Buchanan (Available to http://dx.doi.org/10.1080/01402390.2014.977382)

4. "Strife Series on Cyberwarfare and State Perspectives, Part II – Deception in Cyberspace: Nation States and False Flag operations", Amy Ertan, Strife (Available to https://www.strifeblog.org/2018/07/19/strife-series-on-cyberwarfare-and-state-perspectives-part-ii-deception-in-cyberspace-nation-states-and-false-flag-operations)

5. "How to Recognize and Mitigate State-Sponsored Attacks", Spiros Psarris, Reblaze (Available to https://www.reblaze.com/blog/recognize-mitigate-state-sponsored-attacks)

6. "Commodification of Cyber Capabilities: A Grand Cyber. Arms Bazaar", Analytic Exchange Program (Available to https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf)

7. "Under false flag: using technical artifacts for cyber attack attribution", Florian Skopik and Timea Pahi

8. "How states use non-state actors: A modus operandi for covert state subversion and malign networks", Magnus Normark, Hybrid CoE (Available to https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_15_Non-state-Actors.pdf)

9. "Blurred Lines Between State and Non-State Actors", Council on Foreign Relations (Available to https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors)

10. "Cyber Threat Intelligence for Banking & Financial Services. FOLLOW THE MONEY", Blueliv (Available to https://www.blueliv.com/resources/white-papers/financial_wp_21.pdf)

11. "A Brief History of Russian Hackers' Evolving False Flags", ANDY GREENBERG, WIRED

12. CTA-RU-2021-0909 "Dark Covenant: Connections Between the Russian State and Criminal Actors", Recorded Future

13. "Nation State Ransomware", Jon DiMaggio, Analyst1

14. "Ransomware as a Smokescreen for Nation-State Sponsored Espionage Operations", Ippolito Forni, EclecticIQ (Available to https://www.eclecticiq.com/resources/ransomware-as-a-smokescreen-for-nation-state-sponsored-espionage-operations?hsLang=en)

15. "Ransomware: Hope for the Best, Prepare for the Worst", EclecticIQ Threat Research Team (Available to https://blog.eclecticiq.com/21-september-2021-ransomware-hope-for-the-best-prepare-for-the-worst)

GLOSSARIO

Avversario (o *threat actor*) individui e gruppi che pongono minacce

Dimensione informativa è il contenuto informativo (generalmente indicato come informazione) disponibile nel cyberspace, compresi i contenuti leggibili da un elaboratore, i numeri, il testo, l'audio, le immagini e i video.

Cyberspace è l'ambiente globale, virtuale e basato sulle ICT, compreso Internet, che interconnette direttamente o indirettamente sistemi, reti e altre infrastrutture critiche per le esigenze della società.

Cyberactions sono un insieme di attività prevalentemente illegali condotte nel cyberspace, condotte da attori non statali, che causano danni o interruzioni, nel perseguimento di vari obiettivi politici, economici o personali.

Le **operazioni nel cyberspace (o *CyberOps*)** sono attività militari che impiegano le capacità del cyberspazio per raggiungere obiettivi strategici o effetti nel o attraverso il cyberspace.

Attacchi informatici sono un sottoinsieme delle operazioni nel cyberspace che impiegano l'uso ostile delle capacità dello stesso, da parte di Stati nazionali o di attori non statali che agiscono per loro conto, per causare danni, distruzione o vittime al fine di raggiungere obiettivi militari o politici.

Cyber threat si intende qualsiasi circostanza o evento con il potenziale di avere un impatto negativo sulle operazioni organizzative (comprese missione, funzioni, immagine, ecc.) sui beni dell'organizzazione, individui, altre organizzazioni o sulla Nazione attraverso l'accesso non autorizzato, la distruzione, la divulgazione o la modifica di informazioni e/o la negazione del servizio.

Cyberwar si verifica quando gli attacchi informatici raggiungono la soglia delle ostilità comunemente riconosciute come guerra dalla comunità internazionale e definite dal diritto internazionale.

Malware è un tipo di TTP che rappresenta un codice maligno. In genere si riferisce a un programma che viene inserito in un sistema, di solito in modo occulto. L'intento è quello di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o del sistema operativo (OS) della vittima o di infastidirla o disturbarla in altro modo.

Dimensione fisica comprende l'infrastruttura tecnica di base: hardware e software in rete attraverso la terra, il mare, l'aria e lo spazio che sfruttano l'EMS per consentire il flusso di informazioni tra produttori, consumatori, pubblico e sistemi.

Minaccia può essere definita come uno dei seguenti elementi:

- un'espressione dell'intenzione di nuocere, cioè di privare, indebolire, danneggiare o distruggere
- un'indicazione di danno imminente
- un agente considerato dannoso
- le azioni di un agente dannoso che comprendono tattiche, tecniche e procedure (TTP)

La **valutazione della minaccia** è il processo di valutazione formale del grado di minaccia a un sistema informativo o a un'impresa e di descrizione della natura della minaccia.

Gli **attacchi mirati** sono attacchi che prendono di mira organizzazioni specifiche o persone al loro interno. Una classe di attacchi mirati è la Computer Network Exploitation (CNE), in cui l'obiettivo è rubare (o esfiltrare) informazioni riservate dall'obiettivo. Si tratta di spionaggio nel cyberspace o, in termini di sicurezza informatica, di compromissione della riservatezza. L'altra classe di attacchi mirati è l'attacco alle reti informatiche (CNA), il cui obiettivo è interrompere o distruggere la capacità operativa dell'obiettivo. Si tratta di un vero e proprio sabotaggio nel cyberspace o, in termini di sicurezza informatica, di compromissione dell'integrità e della disponibilità.

Le **tattiche, le tecniche e le procedure (TTP)** descrivono il comportamento di un attore. Una tattica è la descrizione di più alto livello di questo comportamento, mentre le tecniche forniscono una

descrizione più dettagliata dell'azione nel contesto di una tattica e le procedure una descrizione ancora di più basso livello e dettagliata nel contesto di una tecnica.

Informazioni sulle minacce sono tutte le informazioni relative a una minaccia che potrebbero aiutare un'organizzazione a proteggersi da una minaccia o a rilevare le attività di un attore.

Strumenti sono software legittimi che possono essere utilizzati dai threat actor per eseguire attacchi. Conoscere come e quando chi attacca utilizza tali strumenti può essere importante per capire come vengono eseguite le campagne. A differenza del malware, questi strumenti o pacchetti software sono spesso presenti in un sistema e hanno scopi legittimi per i power user, gli amministratori di sistema, gli amministratori di rete o anche gli utenti normali. Gli strumenti di accesso remoto (ad esempio, RDP) e gli strumenti di scansione della rete (ad esempio, Nmap) sono esempi di strumenti che possono essere utilizzati da un attore della minaccia durante un attacco.

BIOGRAFIA

Francesco Schifilliti

Esperto in sicurezza delle informazioni, digital forensic e cyber threat intelligence per grandi aziende. È stato il Practice Manager di Forensic Technology & Discovery Services (FTDS) in Fraud Investigation & Dispute Services (EY). Ricercatore nel campo di Malware e Memory Analysis, Structured Analytic Procedures (SAT), OSINT, Intelligence Investigation Techniques, Incident Responding Techniques e Cyber Threat Intelligence. Laureato in Informatica presso l'Università degli studi di Catania e docente in corsi e master in digital forensics e malware forensics.

Il Social Engineering

«La guerra si fonda sull'inganno»

L'Arte della Guerra, Sun Tzu

Il *social engineering* – o ingegneria sociale – è una disciplina che sfrutta processi cognitivi di influenzamento, inganno e manipolazione per indurre una persona a compiere un'azione o a comunicare informazioni riservate.

La storia è Maestra di vita, e l'arte di ingannare l'avversario non si sviluppa certamente con la nascita dei computer e della sicurezza informatica: probabilmente la più antica prova di un attacco di ingegneria sociale si trova nella Bibbia, Genesi 27, dove Rebecca inganna suo marito Isacco facendogli benedire il secondogenito Giacobbe, rendendolo il suo successo re, invece di Esaù, che era il maggiore.

Ma i libri di storia sono pieni di episodi in cui si sono perpetrati inganni e tranelli, sicuramente l'esempio scolastico per eccellenza è quello del Cavallo di Troia, che i Greci usarono per espugnare la città di Troia (non per nulla con il termine "*Trojan Horse*" intendiamo un tipo di codice o software dannoso che sembra legittimo ma può prendere il controllo del tuo computer, progettato per danneggiare, interrompere, rubare o in generale infliggere altre azioni dannose ai tuoi dati o alla tua rete).

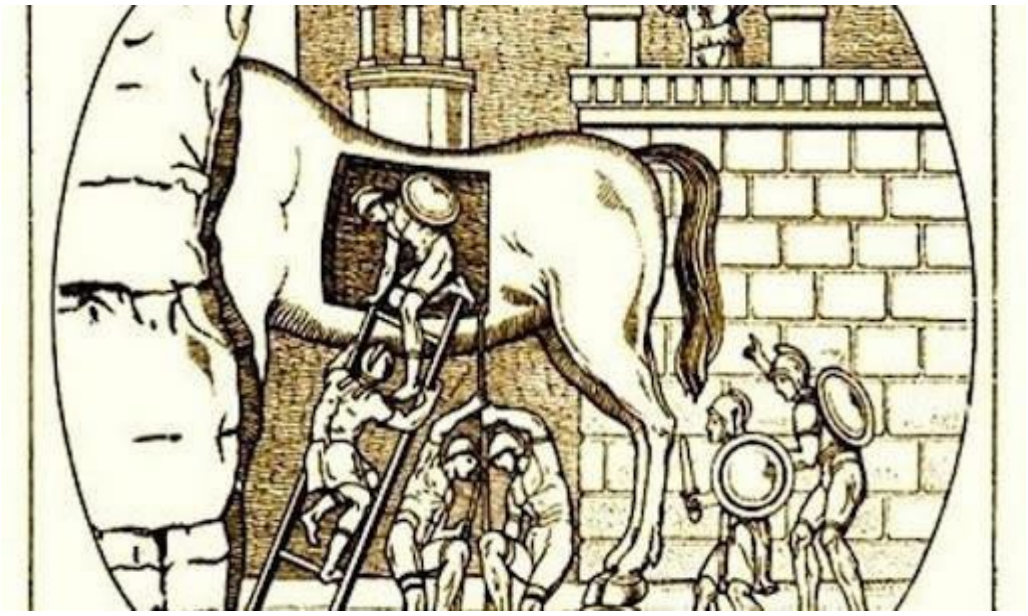
Le azioni criminali basate sull'ingegneria sociale, di cui abbiamo notizie fin dalla notte dei tempi, possono concretizzarsi con o senza l'ausilio di tecnologia.

Purtroppo è un dato di fatto che l'ingegneria sociale si è evoluta nel tempo da una tecnica di attacco che puntava esclusivamente sul carisma e l'abilità dell'attaccante verso una strategia ibrida, ancora più incisiva e subdola che sfrutta sia le abilità cognitive che quelle informatiche.

Questo è stato reso possibile negli ultimi anni grazie alla crescita della digitalizzazione della comunicazione con la diffusione dei social (fucina inesauribile di informazioni) e dei vari servizi di messaggistica. L'ingegnere sociale sfrutta, per l'appunto, la percezione distorta che l'utente medio ha di questi strumenti, ritenendoli puramente virtuali, privi di insidie e scollegati dal mondo reale.

I cybercriminali sanno che l'ingegneria sociale funziona meglio quando ci si concentra sulle emozioni delle persone. Approfittare delle emozioni umane è molto più facile che hackerare una rete o cercare delle vulnerabilità.

Il principio alla base dell'ingegneria sociale è quello di sfruttare il fattore umano, ovvero mettere le persone in situazioni in cui si sa già che faranno affidamento sulle forme più comuni di interazione sociale, come la tendenza a fidarsi delle persone e a rivelare informazioni private (magari pubblicando sui social network), il desiderio di un professionista nel dimostrare acume e superiorità nel suo campo, la tendenza della maggior parte delle persone ad essere più disponibili verso chi mostra interesse nei loro riguardi.

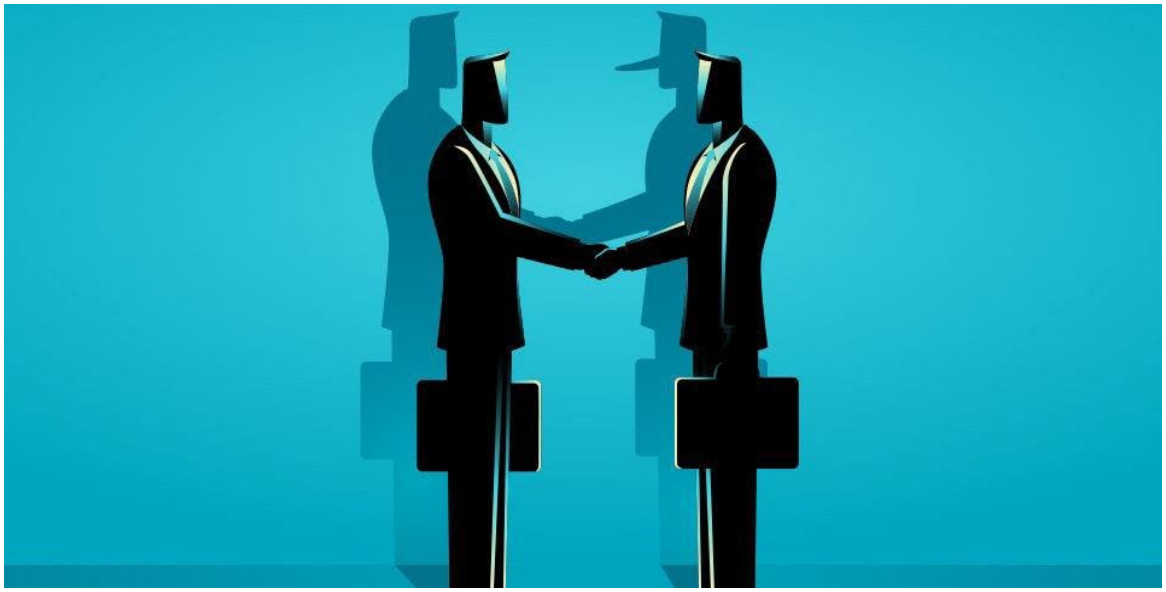


L'attacco fa, dunque, leva su tratti caratteristici dell'essere umano, come la disponibilità e la buona fede dell'attaccato, l'ignoranza e la disattenzione o, ancora, la paura, l'urgenza, la gratitudine.

"Si possono investire milioni di dollari per i propri software, per l'hardware delle proprie macchine e per dispositivi di sicurezza all'avanguardia, ma se c' è anche solo un unico dipendente della nostra azienda che può essere manipolato con un attacco di ingegneria sociale, tutti i soldi investiti saranno stati inutili" (dal libro l'Arte dell'Inganno di Kevin Mitnick).

In un contesto caratterizzato dall'incessante ricerca di nuovi e più sofisticati sistemi tecnologici di difesa informatica, tali da rendere le reti sempre più impenetrabili ed i software sempre più sofisticati, ciò che indebolisce il processo di security dagli attacchi di cognitive hacking è proprio l'uomo.

Le tattiche utilizzate per eseguire un buon attacco di ingegneria sociale si basano principalmente sull'elicitation (e "elicitazione") termine inglese che consiste nel porre domande preparate apposta, tramite un insieme di tecniche e metodi (utilizzati dai professionisti



dell'intelligence e della cyber intelligence) per raccogliere informazioni di nascosto.

In sostanza, un professionista dell'intelligence si impegna in una conversazione con l'obiettivo di raccogliere informazioni e, utilizzando metodi di elicitazione, carpisce le informazioni di cui ha bisogno senza che l'obiettivo si renda conto di essere sfruttato per ottenere informazioni, che possono essere successivamente utilizzate in una campagna di ingegneria sociale su larga scala.

L'elicitazione è un'attività poco rischiosa e difficile da individuare. Spesso e volentieri chi cade vittima rivelando informazioni importanti, neanche si rende conto di come sia potuta uscire l'informazione e, se anche una domanda ad un secondo ripensamento dovesse risultare sospetta, le vittime tendono a considerarla una domanda a cui avrebbero potuto rispondere oppure no, in cui nessuno si ricorda del contenuto delle informazioni che sono trapelate.

Basta fare al bersaglio individuato la domanda giusta al momento giusto e tutte le porte si apriranno.

"Se il vostro avversario ha un carattere iroso, dovete tentare di irritarlo, se è arrogante, provate a incoraggiare la sua arroganza... Colui che è in grado di muovere il proprio avversario lo fa creando una situazione che indurrà il nemico a compiere una certa mossa; questi alletta il nemico con qualcosa che l'altro pensa di poter far suo. Tiene in movimento il nemico facendogli pendere davanti un'esca e poi attaccandolo con truppe scelte."
(Sun Tzu, l'Arte della Guerra)

Ma se un qualsiasi cittadino, "custode" di informazioni riservate, rischia di mettere a repentaglio la propria sicurezza e di chi gli sta intorno, pensiamo cosa potrebbe verificarsi se la vittima è un soggetto che svolge un'attività di Pubblica Sicurezza.
In ambito di Sicurezza Nazionale, l'utilizzo di reti informatiche non classificate, come Facebook, Twitter, Instagram (solo per citarne i più conosciuti), espone le Forze Armate a rischi sempre più elevati di perdita di informazioni sensibili che, se inserite in un opportuno

ciclo di intelligence, possono arrecare un notevole danno alla sicurezza del contingente militare, delle operazioni in corso e più in generale della Difesa.
Si può a questo punto provare a definire il concetto di *cyber-intelligence* come l'insieme degli sforzi e delle attività svolte da o per conto di un'organizzazione, progettate e messe in atto per identificare, tracciare, misurare e/o monitorare, attraverso l'utilizzo di strumenti informatici, le minacce digitali, i dati e/o le operazioni di un avversario.

Data la peculiarità e la complessità delle attività che si celano dietro questo termine, le operazioni di *cyber-intelligence* spesso possono non essere sufficienti da sole a fornire al decisore una visione informativa completa. In questi casi, dunque, ad esse potranno essere affiancati altri metodi d'intelligence tradizionali come, prima fra tutti, la *Human intelligence* (HUMINT) o la *Signal intelligence* (SIGINT). Infatti, a differenza delle armi nucleari e delle altre armi di distruzione di massa, le c.d. *cyber-weapons* non richiedono particolari infrastrutture, né tantomeno materiali speciali e, spesso, neppure conoscenze tecniche particolarmente approfondite per essere predisposte. In quest'ottica, quindi, si dovrebbe fare esclusivo affidamento sulle poche, spesso labili, tracce elettroniche lasciate dall'avversario nelle fasi preliminari all'attacco informatico, ovvero quelle di *footprinting* o *fingerprinting*.

I tradizionali metodi di cyber-intelligence per la raccolta di informazioni riservate, pertanto, potrebbero mostrare il fianco quando l'obiettivo è quello di comprendere a pieno le capacità e/o le intenzioni reali del nemico, qualora non vengano comunque affiancati anche da attività similari nel "mondo fisico".
Un ulteriore elemento che si collega a quanto appena analizzato e che pertanto, seppure brevemente, deve essere tenuto in debita considerazione, è quello relativo alle tecniche d'ingegneria sociale, di cui finora abbiamo discusso.
Non si deve dimenticare, infatti, che la maggior parte dei malware o delle tecniche di phishing, ad esempio, utilizzano, seppur in maniera generalizzata e non mirata, delle tecniche di ingegneria sociale per far sì che l'utente del sistema informatico sia invogliato ad aprire

l'allegato infetto, ovvero ritenga valido e credibile il contenuto della mail ricevuta.

Appare evidente allora che, per fronteggiare una simile minaccia, che basa la sua forza sull'insicurezza degli strumenti tecnologici, sulla poca accortezza degli utenti e sulle tecniche di ingegneria sociale, un primo argine alla possibile fuoriuscita di informazioni classificate e sensibili viene proprio da policies di *cyber security* stringenti, accorte e, soprattutto, specificatamente tarate sulle esigenze operative del contingente che in un'ottica di sicurezza nazionale, va intesa come la capacità di resistere alle minacce intenzionali e non intenzionali attuate contro i sistemi informatici a rilevanza nazionale, nonché di rispondere e rimediare a dette azioni.

In una società che ormai poggia le fondamenta sul concetto stesso di informazione e sulla rilevanza che questo concetto ha all'interno dei meccanismi di funzionamento di tutti i sistemi cibernetici, su cui si basa il dialogo e l'infosharing tra i vari Stati su cui poggia il perno delle discussioni in atto a livello internazionale al fine di armonizzare il quadro normativo e gli standard di sicurezza, risulta particolarmente intuitivo comprendere come impossessarsi, proteggere e usare la maggior quantità possibile di esse sia lo sforzo più rilevante a supporto di un'efficace strategia di vittoria per molti dei conflitti che saranno combattuti in futuro. Se è vero, infatti, che: *"In linea di massima, a proposito della battaglia, l'attacco diretto mira al coinvolgimento; quello di sorpresa, alla vittoria"* (Sun Tzu, l'Arte della Guerra), allo stato attuale, proprio gli attacchi informatici possono essere ancora in grado di conseguire con facilità questo espediente.

"Se l'intelligence è indispensabile per comprendere la realtà, la cyber Intelligence lo è ancora di più per orientarsi nella realtà e nel suo doppio: le galassie in espansione del web" (Cyber intelligence, Mario Caligiuri).

Giuseppe Maio, *Security Advisor in ambito Governance, Risk and Compliance (GRC)*

BIOGRAFIA

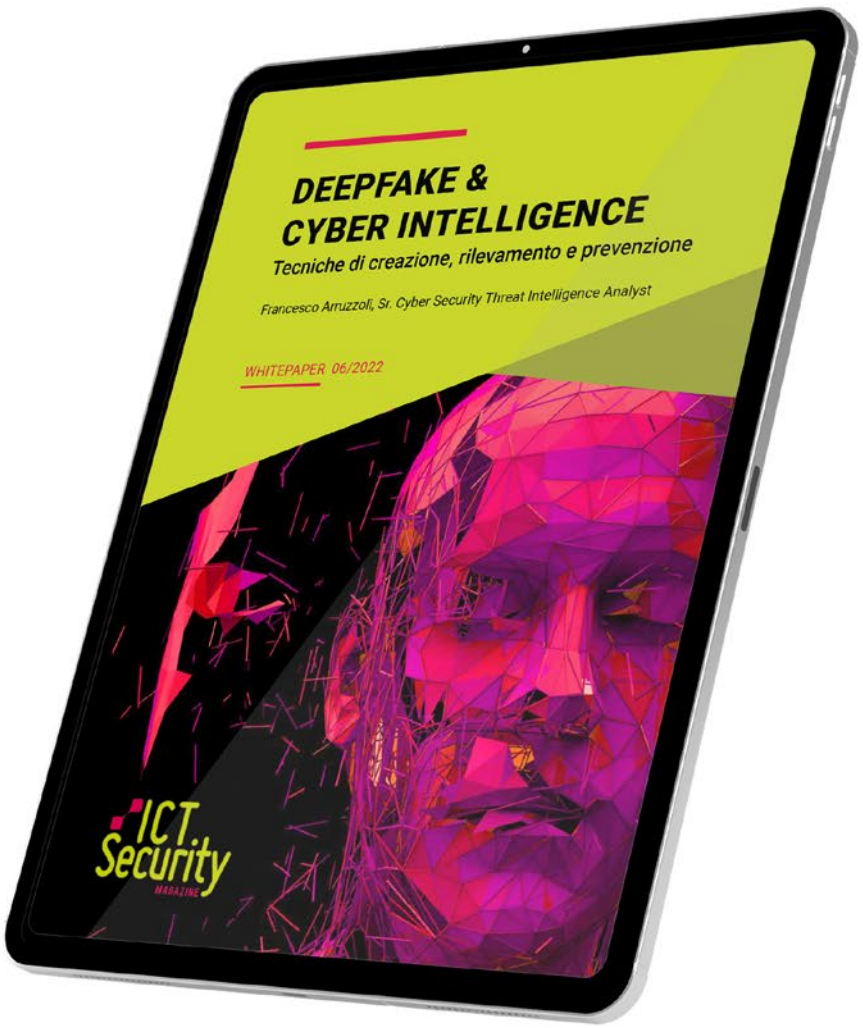
Giuseppe Maio

Giuseppe Maio è Security Advisor in ambito Governance, Risk and Compliance (GRC) per un importante società di Consulenza strategica. Dopo aver conseguito una laurea in Giurisprudenza presso l'Università Mediterranea di Reggio Calabria, ha frequentato un master di II Livello presso l'Università LUISS Guido Carli in "Cybersecurity: Politiche Pubbliche, Normative e Gestione". Attualmente è membro della Commissione Cyber Threat Intelligence & Warfare presso la Società Italiana di Intelligence.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com



Strategia di Patching per la sicurezza nazionale

La crescente esposizione dell'Italia agli attacchi informatici ha reso indispensabile l'individuazione di misure utili alla protezione di reti e sistemi dalle nuove minacce. La gestione delle patch di sicurezza del software è una pratica volta a prevenire lo sfruttamento delle vulnerabilità del software. Una disciplina legislativa sul patching e sui metodi basati sull'intelligence potrebbe essere un punto di partenza per garantire uno standard di sicurezza sufficiente ad allineare il quadro normativo e le dinamiche di sviluppo legate all'innovazione tecnologica.

La crescente esposizione dell'Italia agli attacchi informatici e alle minacce alla sicurezza ha reso indispensabile l'individuazione di misure normative utili alla protezione di reti e sistemi dalle nuove vulnerabilità e le diverse tipologie di attacchi. L'Italia ha recepito la direttiva Network and Information Security (NIS), n. 1148 dell'8 luglio 2016, nel D.lgs n. 65 [1] del 18 maggio 2018 che impone agli Stati membri dell'Unione Europea di adottare misure di sicurezza a[2] livello nazionale.

La direttiva NIS ha lasciato a ogni Stato membro la possibilità di individuare la strategia più adatta per conformarsi ai nuovi parametri individuati. Tuttavia, a differenza degli altri Stati membri, l'Italia si è limitata a recepire nel D.lgs 65/2018 quanto già stabilito dalla Direttiva NIS[3].

A seguito dell'adozione del D.lgs sopra citato, la normativa italiana in materia di sicurezza informatica è stata rafforzata con l'istituzione del "Perimetro nazio-

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148

[2] https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-06-09&atto.codiceRedazionale=18G00092&elenco30giorni=false

[3] D.lgs 65/2018 applies to two specific categories of subjects: Operators of Essential Services and Providers of Digital Services.

nale di sicurezza informatica", con il D.L. n. 105 del 21 settembre 2019, convertito nella Legge n. 133 del 18 novembre 2019, con successive modifiche e integrazioni.

In estrema sintesi, il D.L. 105/2019 evidenzia le modalità procedurali e i criteri per l'individuazione di tutti i soggetti da includere nel Perimetro (quali, ad esempio, pubbliche amministrazioni, enti pubblici e privati) e le misure di sicurezza che questi ultimi devono adottare per proteggere le proprie reti e i sistemi informativi.

Le finalità del Perimetro di Sicurezza Nazionale sono, in primo luogo, quelle di rafforzare lo standard di sicurezza delle reti, dei sistemi e dei servizi informatici dei soggetti all'interno del Perimetro, nonché di garantire la "continuità" di tutti quei servizi, ritenuti essenziali, la cui interruzione, anche parziale, potrebbe causare un danno alla sicurezza nazionale.

La maggior parte di questi elementi è stata affrontata, a livello normativo nazionale, nella cosiddetta "Strategia Nazionale di Cyber Security", delineata in precedenza nella Direttiva NIS e al D.lgs 65/2018 nel cosiddetto Quadro Strategico Nazionale per la Cyber Space Security adottato il 27.1.2014, ulteriormente sviluppato[4] dal Piano nazionale per la protezione cibernetica e la sicurezza informatica del 31.3.2017 (tuttora in vigore)[5].Considerando che le minacce informatiche sono notevolmente cambiate rispetto al 2018, la Commissione Europea ha presentato una proposta di revisione della Direttiva NIS (futura "NIS 2"). Sarà quindi necessario aggiornare l'attuale strategia di sicurezza con i prossimi nuovi dettami comunitari.

Dopo aver descritto l'attuale quadro normativo, sia nazionale che internazionale, è evidente che oggi manca una disciplina standard e omogenea della sicurezza delle informazioni, almeno a

[4]-https://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2014/02/quado-strategico-nazionale-cyber.pdf

[5]-https://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2017/05/piano-nazionale-cyber-2017.pdf

livello europeo. In attesa di ulteriori interventi legislativi, le *best practice* attualmente adottate dalle aziende pubbliche, private e dalle pubbliche amministrazioni rivestono un ruolo di primaria importanza. Il presente contributo si propone di esaminare uno dei principali profili di vulnerabilità, il *patching*, aspetto primario considerando i recenti eventi che hanno visto diverse violazioni di dati, soprattutto nel settore sanitario Italiano[6].

Una disciplina legislativa sul *patching* potrebbe costituire uno dei punti di partenza a garanzia di uno standard di sicurezza sufficiente a consentire un allineamento tra il quadro giuridico normativo e le dinamiche di sviluppo legate all'innovazione tecnologica. Le vulnerabilità del software rimangono infatti uno dei rischi critici per le imprese e le infrastrutture critiche.

L'applicazione di *patch*, che sono letteralmente "pezzi di codice sviluppati per risolvere i *bug* individuati all'interno del software", continua ad essere la strategia più efficace e ampiamente riconosciuta per proteggere i sistemi informatici e contro specifici attacchi. Tuttavia, nonostante il rapido rilascio di patch di sicurezza che risolvono le vulnerabilità del software, la maggior parte degli attacchi vengono comunque portati a buon fine grazie allo sfruttamento delle suddette vulnerabilità note anche se è già stata rilasciata la *patch*[7].

Nel corso del tempo, questa costante negligenza ha causato conseguenze devastanti a livello finanziario e[8] perdite di reputazione dovute alla violazione della riservatezza, dell'integrità dei dati aziendali e all'indisponibilità del software. Questo è dovuto principalmente ai complessi problemi inerenti all'applicazione delle *patch* di sicurezza negli ambienti organizzativi[9].

[6] https://www.sicurezzaterrorismosocieta.it/wpcontent/uploads/2021/11/SicTerSoc14-Ransomware-strikes-back-Il-racket-informatico-continua-a-colpire-le-infrastrutture

[7] https://www.sciencedirect.com/science/article/abs/pii/S0950584921002147

[8] https://www.hpe.com/us/en/insights/articles/rise-in-attacks-exposes-neglected-firmware-security-2111.html

[9] https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Il termine "*Patching*" indica l'applicazione di *patch* sulle criticità di sicurezza presenti nei software e nei sistemi implementati negli ambienti IT/OT di un'organizzazione. Vengono identificate le vulnerabilità esistenti nei sistemi e acquisite, testate, installate e controllate le patch di sicurezza del software. L'esecuzione di questi compiti comporta la gestione delle dipendenze tra più *stakeholders* e decisioni "socio-tecniche" che rendono l'amministrazione delle patch del software un problema complesso. Questo problema è aggravato dal bisogno di trovare un equilibrio tra la rapidità di applicazione di una *patch* di sicurezza e la necessità di farlo su una miriade di applicazioni aziendali e governative[10].

Nonostante la risaputa criticità legata alla gestione delle *patch* di sicurezza del software nell'industria, questa rimane ancora un'area emergente, di crescente interesse per la ricerca, che necessita di maggiore attenzione. Gli aspetti "socio-tecnici" (un processo organizzativo che riguarda la gestione delle competenze, delle risorse e l'interazione delle persone con le soluzioni tecniche, in cui le interazioni umane e le tecnologie sono strettamente legate) della gestione delle *patch* hanno goduto di un'attenzione relativamente limitata. Essa dipende in modo significativo dalla collaborazione efficace degli esseri umani con gli attuali sistemi automatici di rilevamento delle vulnerabilità. La comprensione degli "aspetti socio-tecnici" è essenziale per identificare i problemi predominanti e migliorare l'efficacia del processo di controllo delle *patch* di sicurezza del software[11].

La suddetta gestione della sicurezza del software è una pratica di garanzia progettata per prevenire in modo proattivo lo sfruttamento delle vulnerabilità all'interno del software (e talvolta dell'hardware) di un'organizzazione. In generale, un processo efficace di gestione delle *patch* di sicurezza del software è essen-

[10] https://www.rapid7.com/fundamentals/patch-management/

[11] https://www.crest-centre.net/socio-technical-factors-in-secure-software-engineering-methodologies-and-practices

ziale per mantenere la riservatezza, l'integrità e la disponibilità (CIA) dei sistemi informativi. Tale processo è uno sforzo di collaborazione tra più parti interessate: team IT, responsabili della sicurezza, ingegneri e amministratori di sistema, fornitori di software di terze parti, arrivando fino ai clienti e agli utenti finali.

Pertanto, la mancanza di collaborazione, coordinamento e comunicazione tra le varie parti interessate rappresenta uno dei principali ostacoli al mantenimento della sicurezza dei sistemi software. Inoltre, la necessità di bilanciare la conformità con organismi di *governance* eterogenei e il mantenimento della salvaguardia del software sono riconosciute come le sfide chiave della sicurezza del software.

Il rapido aumento del numero e della diversità delle aree di attacco ha portato ad un incremento del tasso di *patch*, sconvolgendo i processi esistenti. Inoltre, i limiti degli strumenti esistenti sono stati considerati un ostacolo significativo al raggiungimento degli obiettivi di gestione. Tra questi, la mancanza di una piattaforma standard per integrare gli strumenti eterogenei utilizzati per la gestione delle *patch*, la mancanza di accuratezza e la mancanza di scalabilità nella progettazione/architettura degli strumenti, che creano difficoltà nel patching di più sistemi che lavorano con sistemi operativi diversi.

A causa della maggiore complessità, della natura dinamica della gestione delle patch del software e dei limiti delle attuali tecnologie utilizzate per il *patching*, la necessità di competenze umane risulta inevitabile. Tuttavia, a causa del coinvolgimento umano nelle attività di esecuzione e nelle decisioni, i tempi di applicazione delle *patch* sono aumentati prestandosi così a numerosi attacchi. Il rischio di ritardi aumenta ulteriormente a causa della mancanza di risorse in termini di competenze e conoscenze, linee guida per i processi e supporto per l'automazione dei processi.

Un punto importante, evidenziato in letteratura riguardo alla mancanza di supporto per l'automazione dei processi, è che la maggior parte delle soluzioni esistenti si concentra solo sulla distribuzione delle *patch*, ma non fornisce soluzioni in grado di coprire l'intero processo.

Inoltre, esiste un divario significativo nelle competenze richieste per la gestione delle *patch* di sicurezza del software, soprattutto a causa della maggiore complessità delle stesse. Gli amministratori dei sistemi di IT sono costretti a passare ore monitorando le diverse fonti di informazioni a causa della mancanza di piattaforme centralizzate per il recupero e il filtraggio delle informazioni.

Le moderne fonti di informazione vanno dagli avvisi di sicurezza (78%)[12], notifiche ufficiali dei fornitori (71%), *mailing list* (53%), forum online (52%), notizie (39%), blog (38%) e social media (18%). Inoltre, a causa della velocità di rilascio delle patch, della mancanza di convalida automatica[13], filtraggio e classificazione delle informazioni in base alle esigenze organizzative, vi è un ritardo nel rilascio delle patch, che aumenta il rischio di attacchi *one-day*[14].

Uno dei fattori critici, relativo all'aumento dell'esposizione agli attacchi malevoli, è la mancanza di una soluzione di scansione completa, questa non riesce a comprendere il sistema in modo chiaro facendo sì che non vengano rilevate le vulnerabilità del software e causando una configurazione errata del sistema.

Gli approcci esistenti sono in genere univoci e creano difficoltà nel comprendere le diverse esigenze del contesto organizzativo richiedendo un notevole lavoro manuale, in particolare quando si applicano le *patch* in un ambiente virtuale. È sempre più necessario disporre di un insieme standard di metriche rigorose con informazioni quali le date di *exploit* delle *patch*, poiché gli scanner di vulnerabilità esistenti dipendono da informazioni pubbliche sulle vulnerabilità, comprese le date di divulgazione delle stesse. Inoltre, il divario di conoscenze tra il contesto tecnico e quello aziendale

[12] A. R. Gregersen, M. Rasmussen, B. N. Jørgensen, State of the art of dynamic software updating in java, in: International Conference on Software Technologies, Springer, 2013, pp. 99–113.

[13] https://arxiv.org/pdf/2012.00544.pdf

[14] M. Shahin, M. A. Babar, L. Zhu, Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices, IEEE Access 5 (2017) 3909–3943.

(ad esempio, la necessità di applicare le patch di sicurezza il prima possibile, dando priorità alla disponibilità del sistema) spesso porta a conflitti di priorità tra i diversi team[15].

Una delle sfide più significativa del patch testing moderno è una strategia di test automatizzata adeguata. La mancanza di test automatizzati può derivare da diverse ragioni, come la difficoltà di affrontare i problemi di dipendenza dalle *patch* e la notevole quantità di lavoro umano necessario per impostare un ambiente di test che simuli quello di "produzione".

Tuttavia, la maggior parte dei patch test attuali viene eseguita manualmente per evitare il rischio di guasti imprevisti al sistema causati da patch dannose o maligne. La scarsa qualità dei test sulle patch manuali aumenta l'esposizione alle vulnerabilità, poiché spesso ritarda la successiva distribuzione.

Un'altra sfida importante riguarda la gestione dei vincoli organizzativi sui tempi di inattività dei sistemi. La mancanza di un'adeguata strategia di distribuzione delle patch in fase di esecuzione e di politiche organizzative che evitino i tempi di inattività del sistema rappresenta un grave problema per la loro installazione tempestiva. Ciò è particolarmente deleterio nel contesto delle infrastrutture critiche come la sanità e la pubblica amministrazione, per le quali i tempi di inattività possono creare significative effetti collaterali negativi. La maggior parte delle soluzioni di gestione delle patch di sicurezza presenti nei software esistenti non dispone di una strategia efficiente di verifica, fornendo una panoramica limitata dello stato delle *patch* del sistema[16].

Inoltre, la maggior parte delle attuali soluzioni di controllo delle *patch* prevedono un lavoro manuale dei team di IT nell'ispezionare l'applicazione alla

[15] B. H. Ahmed, S. P. Lee, M. T. Su, A. Zakari, Dynamic software updating: a systematic mapping study, IET Software 14 (5) (2020) 468–481.

[16] A. R. Gregersen, M. Rasmussen, B. N. Jørgensen, State of the art of dynamic software updating in java, in: International Conference on Software Technologies, cit., pp. 99–113.

ricerca di segni di attacco e nel riparare i danni qualora venga individuata una minaccia. Si tratta di un'attività lunga e impegnativa che non garantisce l'individuazione di eventuali intrusioni e l'annullamento di tutte le modifiche apportate dall'aggressore. La necessità di effettuare questa verifica, non appena viene distribuita la patch, si aggiunge alla complessa, laboriosa e lunga verifica manuale, sottolineando la mancanza di una strategia di verifica automatizzata efficace.

Nel corso degli anni sono stati fatti diversi tentativi per integrare l'automazione nella gestione delle patch di sicurezza del software. Deve esistere un delicato equilibrio tra l'intervento umano e l'automazione della gestione delle patch di sicurezza. L'automazione consente ai professionisti di godere dei vantaggi di un minore sforzo manuale. Allo stesso tempo però, l'esperienza umana è necessaria per prendere il controllo del processo decisionale e delle attività che non possono essere completamente automatizzate a causa della complessità delle patch e dei limiti attuali della tecnologia. Poiché le patch possono modificare la semantica di un programma, è probabile che sia sempre necessario il giudizio umano per determinare se le modifiche semantiche sono rilevanti[17].

Le organizzazioni utilizzano molti prodotti software (ad esempio sistemi operativi o OS, applicazioni software, strumenti e piattaforme), aumentando le sfide dell'eterogeneità delle patch. È stato inoltre notato che la maggior parte delle soluzioni analizzate sono compatibili solo con il sistema operativo Linux, forse perché è *open-source*, più accessibile da configurare rispetto ad altri sistemi operativi e perché le *patch* applicate a molte distribuzioni Linux comportano modifiche minori rispetto alle patch di Windows. Di conseguenza, cresce l'esigenza di una piattaforma orchestrata che si concentri su questi strumenti eterogenei.

In conclusione, disporre di piattaforme di intelligenza artificiale automatizzate

[17]-https://www.manageengine.com/patch-management/automated-patch-deployment.html

e di una valutazione guidata dall'intelligence sulle minacce in base alle *patch* da distribuire, consentirebbe alle organizzazioni di aumentare le informazioni sulle minacce esterne attraverso indicatori che segnalano gli avversari e le aree di compromissione. L'uso di strumenti di intelligence su minacce specifiche, nella difesa di organizzazioni pubbliche e private, porterebbe a una valutazione più accurata delle priorità, modificando l'attuale piano di *patch* per dare precedenza ai sistemi che potrebbero essere attaccati in un determinato momento. Il risultato è una gestione delle *patch* guidata dall'intelligence che rafforza i processi di contrasto agli attacchi.

Purtroppo, la realtà è che la pubblica amministrazione italiana e parte del settore privato non hanno una visibilità al 100% dei propri *asset* e delle proprie vulnerabilità, per cui la mappatura dei dati sulle minacce esterne e degli indicatori interni, utile a perfezionare un piano di patch, potrebbe talvolta avere un valore parziale.

Tuttavia, la raccolta di informazioni dai *feed* delle minacce globali e da altre fonti di intelligence esterne ha un grande valore nel determinare se parti di un'organizzazione o di un governo stanno subendo un attacco specifico. Il framework MITRE ATT&CK è una di queste fonti.

L'inserimento dei dati MITRE ATT&CK in qualsiasi *repository* consente di partire da un punto di vista più elevato, con informazioni sugli avversari, sulle tattiche, tecniche e procedure associate. Si può adottare un approccio proattivo, partendo dal profilo di rischio di un'organizzazione, mappando tali rischi e associandoli a specifici avversari e alle loro tattiche, approfondendo le tecniche da essi utilizzate e successivamente indagando se potrebbero avere successo o se tali dati sono stati riscontrati all'interno dell'ambiente analizzato.

Cosimo Melella, *PhD candidate UniGe in security, risk and vulnerability, researcher at ITSTIME research center*

Cecilia Isola, *Avvocato specializzato in diritto commerciale e diritto delle nuove tecnologie*

BIOGRAFIA

Cosimo Melella

Cosimo Melella è ricercatore presso ITSTIME, cultore della materia in comunicazione e informazione per la sicurezza. Cosimo Melella ha conseguito un Master in Cybersecurity presso l'Università degli Studi di Milano. Ha frequentato corsi di specializzazione presso il NATO CCDCOE ed è certificato Cisco.

Cecilia Isola

Cecilia Isola è avvocato specializzato in diritto commerciale e diritto delle nuove tecnologie e PhD candidate presso il centro di Security, Risk and Vulnerability del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi dell'Università di Genova, curriculum Security&Law.

E-mail spoofing di Istituzioni e P.A.

INTRODUZIONE AL FENOMENO

Sono passati quasi 30 anni[1] dall'origine del termine phishing e dai primi attacchi documentati, tuttavia, la stretta correlazione tra la buona riuscita degli stessi attacchi ed il fattore umano, sommata a campagne sempre più mirate e "autorevoli" e ad una - non proprio estesa - conoscenza e adozione[2] globale dei meccanismi di prevenzione; fanno si che la prima posizione (per numero di vittime) dell'Internet Crime Report 2020[3] dell'FBI venga occupata da eventi criminosi di tipologia *Phishing*, al sesto posto quelli di tipo *spoofing* seguiti da *misrepresentation*, *business e-mail compromise* e, fuori dalla "top ten" di sole sei posizioni, la tipologia *Government Impersonation.*

Il fenomeno dell'*e-mail spoofing* e, più nello specifico, sender spoofing (impersonificazione di un indirizzo mittente di un dato nome di dominio) e *domain spoofing* (impersonificazione di un intero nome di dominio) sono spesso e da sempre, alla base delle campagne *phishing* e *spear phishing* in quanto consentono di condizionare negativamente il comportamento, le azioni e la scelte del destinatario, trasmettendo un falso senso di autorevolezza e attendibilità, sfruttando quindi proprio il "fattore umano" per la buona riuscita della campagna stessa.

Anche ENISA, sulla falsariga dell'FBI, già con le pubblicazioni Threat Landscape 2020[4] e 2021[5], pone l'accento verso gli "E-Mail Related Threats" dove le campagne BEC (*Business e-mail compro-*

[1] https://www.phishing.org/history-of-phishing

[2] https://dmarc.org/stats/farsight/dmarc/

[3] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

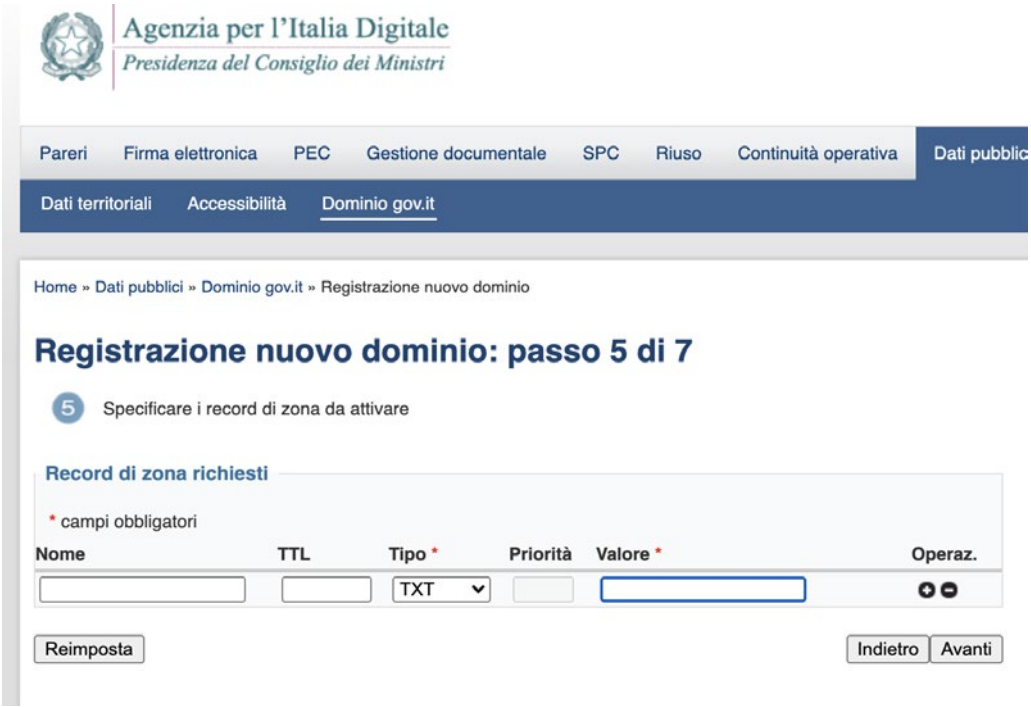
[4] https://www.enisa.europa.eu/publications/phishing

[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

mise) e *Phishing* la fanno da padrona, tanto da arrivare a suggerire azioni tecniche volte all'implementazione di specifici standard / protocolli: DMARC, SPF e DKIM. Al centro di questa analisi e proposta di strategia sono proprio gli standard DMARC e, parzialmente, Sender Policy Framework e la loro comprovata utilità nel contrasto, se adottati in un più strutturato processo di intelligence, e nella prevenzione (intesa come blocco) di attacchi a tipologia *Spoofing*, *Misrepresentation* e *Government Impersonation.*

ANALISI DEL CONTESTO NAZIONALE: DAL 2009 AD OGGI

La Direttiva n.8/2009 a firma dell'allora Ministro per la Pubblica amministrazione Renato Brunetta delineava le disposizioni in materia di riconoscibilità, aggiornamento, usabilità, accessibilità e registrazione al dominio ".gov.it" dei siti web delle P.A. assegnando al nome di dominio ".gov.it" l'obiettivo di « aggregare i siti web delle pubbliche amministrazioni che già erogano



servizi istituzionali con un adeguato ed omogeneo livello di qualità, sicurezza ed aggiornamento dei servizi » delegando all'ormai cessato CNIPA ora AgID, Agenzia per l'Italia digitale, la fornitura dell'assistenza tecnica necessaria per l'iscrizione al dominio .gov.it e la sua gestione operativa: AgID che risponde egregiamente al compito assegnatole implementando, ormai da anni, un portale per la registrazione e gestione dei nomi di dominio di terzo livello di .gov.it[6], portale che integra (già in fase di accreditamento della P.A. richiedente) la gestione dei record DNS - inclusi quelli di tipo TXT come DMARC e Sender Policy Framework oggetto della presente analisi - o la delega del dominio verso name server (e relativi pannelli di gestione DNS) terzi, esterni alla stessa AgID.

Nel panorama Istituzionale odierno, con il Piano Triennale per l'informatica nella Pubblica Amministrazione 2019-2021[7] e con la precedente determina AgID 36/2018[8] si è assistito al cosiddetto "riordino" del dominio di secondo livello gov.it, avviato, de facto, con lo scopo di aggiornare e riorganizzare i criteri di assegnazione e allocazione dei sottodomini secondo le politiche vigenti nell'Unione Europea; tale determina prevede nello specifico l'assegnazione del dominio di terzo livello di .gov.it « alle sole amministrazioni centrali dello Stato indicate all'elenco delle amministrazioni pubbliche individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196 e successive modificazioni e pubblicate annualmente in G.U. » e prevede inoltre:

- che le amministrazioni territoriali e scolastiche che attualmente lo utilizzano debbano abbandonarlo nei termini stabiliti dalla determina;
- che tutte le infrastrutture ICT utiliz-

[6] domini.agid.gov.it

[7] https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/09_strumenti-per-la-generazione-e-la-diffusione-di-servizi-digitali.html#la-riorganizzazione-del-dominio-gov-it

[8] https://www.agid.gov.it/sites/default/files/repository_files/36_-_dt_dg_n._36_-_12_feb_2018_-_riorganizzazione_dominio_gov_22.12.2017_003_1_4.pdf

zate per l'implementazione di tali siti siano conformi alle Misure minime di sicurezza ICT emanate da AgID[9] e le applicazioni siano immuni almeno per i Top 10 Risk di OWASP correnti (allora OWASP Top 10 : 2017).

In estrema sintesi è stata disposta, in tutta fretta, la sola migrazione dei domini di terzo livello appartenenti a istituzioni scolastiche dal dominio ".gov.it" verso il nuovo ".edu.it" (quest'ultimo assegnato al MIUR) mentre per gli enti territoriali interessati dalla determina AgID è stata disposta la migrazione verso il dominio ".it" indicante, dal 1987[10], l'estensione geografica ufficiale dell'Italia.

A fronte di una tale migrazione su larga scala, si è sprecata la possibilità di adottare una politica di conformità per adeguare le "identità web" delle P.A. rendendole conformi a standard *antiphishing* e *antispoofing* globalmente riconosciuti e adottati già prima del Dicembre 2019[11], meccanismi dei quali la stessa ENISA raccomanda l'implementazione nella sua pubblicazione Threat Landscape 2021[12].

Ciò che sembrerebbe infatti non essere stato preso in considerazione e tantomeno valutato da AgID nella sua determina del 2018 e nel successivo Piano triennale ICT 2019-2021 è, relativamente alle "misure minime di sicurezza ICT" (e per causa dell'obsolescenza delle stesse basate su profili di conformità del 2015), l'implementazione, per i sottodomini di ".gov.it" assegnati alle Amministrazioni centrali dello Stato (così come per tutti i domini di terzo livello ".edu.it" in uso alle Istituzioni scolastiche ed i ".it" in uso alle Istituzioni territoriali), di una strategia ed una rispettiva imple-

[9] Circolare AgID 18 Aprile 2017 n. 2/2017 ttps://cert-agid.gov.it/download/CircolareAgID_170418_n_2_2017_Mis_minime_sicurezza_ICT_PA-GU-103-050517-2.pdf

[10] https://it.wikipedia.org/wiki/Registro.it

[11] https://dmarc.org/2020/02/dmarc-policies-increase-300-over-2019/

[12] Enisa Threat Landscape 2021, Capitolo 6 "E-Mail Related Threats"

mentazione tecnica atta a prevenire, bloccando sul nascere e segnalando in autonomia, i tentativi di *domain spoofing* e *sender spoofing* volti alla diffusione di campagne di phishing per conto di identità (intese come nomi di dominio) appartenenti alle stesse Pubbliche Amministrazioni.

Tale strategia verterebbe, per larga parte, intorno all'abilitazione di due tanto elementari quanto funzionali protocolli:

- DMARC[13], Domain-based Message Authentication, Reporting & Conformance (rfc7489)
- SPF, Sender Policy Framework (rfc7208)

I due "protocolli", entrambi applicati a livello del nome di dominio interessato sottoforma di record TXT, collaborano per le finalità di autenticazione e validazione dell'indirizzo mittente (e del relativo nome di dominio in uso a quest'ultimo) delle email nel momento in cui queste raggiungono il mail exchanger del destinatario; in sintesi, il record SPF ha lo scopo di contenere una lista di indirizzi IP e FQDN di SMTP server autorizzati a spedire email per conto del nome di dominio dove esso è applicato, il record DMARC si occupa invece di imporre ai mail exchanger riceventi (dove sono definite le mailbox dei destinatari) l'azione da intraprendere qualora una o più mail da essi ricevute violassero le condizioni definite nel record SPF e provenissero quindi da un SMTP server il quale IP non risultasse autorizzato a spedire per conto del nome di dominio in uso al mittente, inoltre, DMARC include una funzionalità nativa di reporting che consente al dominio implementante di ricevere quotidianamente report dettagliati sulle violazioni (o tentativi) avvenute, quest'ultime spesso riconducibili a tentativi di *domain spoofing* e *sender spoofing*.

Il protocollo DMARC, pensato e progettato per un'adozione graduale al fine di consentire ai domini e sottodomini implementanti una transizione priva di

[13] https://dmarc.org/

disservizi e interruzioni, permette di specificare tre tipologie di policy da adottare in caso di violazione rilevata:

- ***none***: non viene chiesta al mail exchanger ricevente alcuna azione sulla mail in ingresso che ha fallito il controllo DMARC, consente però (se associato alla funzionalità di reporting) di ricevere *feedback* dettagliati sulle violazioni avvenute (controlli DMARC con esito negativo);
- ***quarantine***: viene chiesto al *mail exchanger* ricevente di trattare con diffidenza la mail in ingresso che ha fallito il controllo DMARC (classificazione come Spam / Spoofing);
- ***reject***: viene chiesto al mail exchanger ricevente di rifiutare la mail in ingresso che ha fallito il controllo DMARC.

Ne consegue che, la sola implementazione di DMARC in assenza di SPF o, nel caso opposto, lo specificare una lista di server autorizzati (SPF) in assenza di DMARC, rende nulli i benefici provenienti da entrambi in termini di prevenzione dello *spoofing* e *reporting* centralizzato delle violazioni.

SCENARIO DI RISCHIO

La mancata conformità agli standard DMARC e Sender Policy Framework, ossia l'assenza dei relativi record DNS di tipo TXT a livello dei nomi di dominio in uso a Pubbliche Amministrazioni, Enti Territoriali e Istituzioni Scolastiche, espone le stesse a scenari di rischio ulteriori che vertono su attacchi di tipo

```
v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:mailauth-reports@google.com	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

domain spoofing e *sender spoofing* volti all'impersonificazione di una o più identità (non per forza reali) appartenenti ad un dato nome di dominio quindi "*brand*", o per meglio dire, associabili all'identità della Pubblica Amministrazione vittima di questa tipologia di attacco.
Entrando nel dettaglio, poichè la pratica dell'impersonificazione e, più generalmente, gli attacchi *spoofing* hanno come fine "ultimo" (o come obiettivo iniziale) l'avvio e la diffusione di campagne *phishing* e *spear phishing* sfruttando per l'appunto la notorietà e l'autorevolezza di un determinato dominio (*domain spoofing*) o mittente (*sender spoofing*) è altamente probabile che bad actor, approfittando della ridotta - quasi nulla - complessità di attacco, possano sfruttare identità appartenenti a nomi di dominio non conformi a DMARC e Sender Policy Framework per la diffusione, incontrollata per via dell'assenza delle funzionalità di reporting proprie dello standard DMARC, di dette campagne.

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;_dmarc.salute.gov.it.          IN      TXT

;; AUTHORITY SECTION:
salute.gov.it.          300     IN      SOA     dns1-vf.aruba.it. hostmaster.salute.gov.it. 1 86400 7200 2592000 3600

;; Query time: 33 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Dec 31 23:32:03 CET 2021
;; MSG SIZE  rcvd: 110
```

```
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;_dmarc.interno.gov.it.         IN      TXT

;; AUTHORITY SECTION:
interno.gov.it.         300     IN      SOA     a1-59.akam.net. servizi.internet.ps.interno.it. 2021111018 172800 900 120
00

;; Query time: 74 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Dec 31 23:34:10 CET 2021
;; MSG SIZE  rcvd: 128
```

Nel peggior caso ipotizzabile bad actor o organizzazioni criminali potrebbero "istituire" una rete di server SMTP o sfruttare le migliaia di relay SMTP[14] aperti o compromessi e pertanto accessibili a chiunque per l'invio, massivo o mirato, di e-mail di *phishing* per conto di indirizzi mittente Istituzionali, in uso a Pubbliche Amministrazioni o ai Dipendenti di quest'ultime.

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;_dmarc.agid.gov.it.            IN      TXT

;; AUTHORITY SECTION:
agid.gov.it.           900     IN      SOA     wasat.agid.gov.it. administrator.agid.gov.it. 2021122321 10800 3600 25920

;; Query time: 34 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Dec 31 23:35:46 CET 2021
;; MSG SIZE  rcvd: 103
```

Al verificarsi di un simile scenario, ai provider riceventi ossia ai *mail exchanger* dei destinatari della campagna malevola, siano essi basati su soluzioni *enterprise-grade* o "*community*", non riscontrando la presenza - verificata mediante query DNS verso il nome di dominio mittente - di record DMARC e/o SPF validi, non resterebbe altro che trattare la mail di phishing come lecita in una sorta di "modo di agire" estremamente garantista, fatto salvo il caso di ulteriori controlli operati dal mail exchanger ricevente che riescano a contrassegnare la mail come malevola basandosi, ad esempio, sulla reputazione dell'indirizzo IP del server mittente.

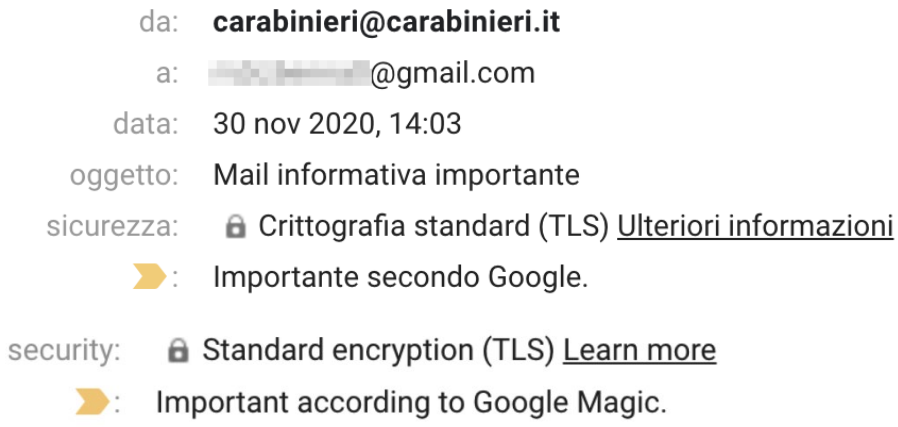
Un esempio lampante è dato dal comportamento di Google Mail, che alla ricezione di una mail con mittente (e dominio) *spoofed* da un nome di dominio per il quale non risultano "dichiarati" e validi i record SPF e/o DMARC delegherà la "decisione finale" (ovvero la classificazione come Posta in arrivo, Importante o Spam) all'algoritmo proprietario

[14] https://en.wikipedia.org/wiki/Open_mail_relay

"Google Magic" (citato espressamente nella sola versione US / UK di GMail) il quale si limita ad effettuare controlli per certi versi banali e non sempre funzionali a rilevare una campagna *phishing*, come:

- Numero di destinatari
- Presenza del destinatario in To o Cc
- Presenza tra i contatti / contatti frequenti del mittente e del dominio mittente
- Presenza di parole chiave "importanti"
- URL contenuti nella mail
- etc.

È quindi evidente come i *mail exchanger* riceventi e gli stessi provider siano "in difficoltà" nello stabilire l'autorevolezza e la provenienza lecita delle mail con indirizzo mittente appartenente ad un dato dominio per il quale non risultino dichiarati DMARC e/o Sender Policy Framework (questa analisi, finalizzata ad evidenziarne il solo rischio alla sicurezza non tiene conto degli ulteriori impatti alla *mail deliverability*[15] di un dominio in assenza di detti *record* che potrebbero tradursi in mancate ricezioni, bassa reputazione delle mail lecite, *blacklisting* e impatti al business nel caso di domini in uso ad aziende), ma sono ancora più evidenti i rischi ai quali le Pubbliche Amministrazioni sono attualmente esposte, specie quelle ad alto tasso di rapporti / comunicazioni da e verso il cittadino (basti pensare a comuni, enti locali, scuole, etc.) a



[15] Parametro in uso nel contesto dell'e-mail marketing

causa dell'assenza di una "strategia antispoofing" delle identità istituzionali - intese come nomi di dominio - che preveda, tra i suoi punti cardine, l'adozione e l'implementazione di misure efficaci come DMARC e Sender Policy Framework per i nomi di dominio Istituzionali (gov.it, edu.it, etc.) ed i relativi *third-level domain* appartenenti.

PROPOSTA DI SOLUZIONE

Le procedure di accreditamento e gestione DNS dei domini di terzo livello .gov.it, centralizzate in AgID, rappresentano ad oggi un terreno fertile ed un test case ideale per le azioni di enforcing e propagazione massiva dei record DMARC e Sender Policy Framework verso i nomi di dominio delle Pubbliche Amministrazioni aderenti al dominio gov.it, anche nell'ottica di una prima implementazione meno impattante che sfrutti la gradualità delle policy DMARC (ossia priva di policy DMARC decisionali[16], potenzialmente causa di disagi o interruzioni in assenza di un preliminare censimento dei mail server impiegati dalle singole P.A.) che abiliti la sola generazione e ricezione centralizzata dei *report* delle violazioni rilevate dai provider.

L'implementazione del solo "*stack*" DMARC - SPF, coordinata e condotta quindi da un organismo centrale o delegata ai responsabili tecnici delle rispettive Pubbliche Amministrazioni assegnatarie dei nomi di dominio .gov.it, .edu.it e ulteriori SLD, second level domain Istituzionali come sanita.it[17], apporterebbe certamente benefici tangibili - in termini di sicurezza percepita ed effettiva - estesi sia verso i Soggetti implementanti che verso i Dipendenti e Utenti a vario titolo (nel caso di pubbliche amministrazioni) di quest'ultime, comportando la riduzione, virtualmente prossima all'azzeramento (nel caso di policy DMARC decisionali non limitate al solo *reporting*) dei tentativi di *domain*

[16] Rispettivamente le policy quarantine e reject

[17] "Alias" di salute.gov.it

spoofing e *sender spoofing* e, più nel concreto, delle conseguenti campagne di *phishing* e *spear phishing* avviate da bad actor sfruttando la mancanza di conformità (appurabile da fonti pubbliche come i name server autoritativi) dei domini "istituzionali" gov.it, edu.it et similia a meccanismi di "autenticazione" e "validazione" come DMARC e Sender Policy Framework.

In un'ottica di prevenzione del *cyber crime* l'implementazione di una "strategia Nazionale anti-spoofing" per i nomi di dominio .gov.it e Istituzionali consentirebbe di beneficiare delle capacità di reporting native dello standard DMARC agli scopi di poter ricevere, indicizzare, analizzare e, preferibilmente, centralizzare verso un unico organo di controllo e "monitoraggio" della Cyber Security Nazionale come il CSIRT Italia, gli alert e le segnalazioni generate dai provider di Posta (presenti nello scenario globale) relative ad eventi di violazione del Sender Policy Framework e pertanto riconducibili a tentativi di *domain spoofing* e *sender spoofing* e delle conseguenti campagne phishing avviate per conto (inteso come "ai danni di" trattandosi di veri e propri tentativi di impersonificazione) dei domini appartenenti o assegnati a Istituzioni e Pubbliche Amministrazioni nazionali: ciò comporterebbe, per i soggetti adottanti ed i sopracitati organi centrali di controllo, l'apertura e la pronta disponibilità di un "nuovo" flusso informativo di *threat intelligence* per l'acquisizione di informazioni, autorevoli e dettagliate, inerenti i tentativi di campagne *phishing* avviati ai danni delle Pubbliche Amministrazioni e Istituzioni, dei loro Dipendenti o Utenti a vario titolo; informazioni fondamentali per le successive fasi di un potenziale processo di intelligence volto all'analisi, classificazione, disseminazione / divulgazione (tramite processi di *early warning*) e "risposta" - quest'ultima integrata nelle policy "decisionali" *quarantine* e *reject* dello standard DMARC.

Mirko Caruso, *Esperto in sicurezza delle informazioni e conformità delle infrastrutture critiche*

BIOGRAFIA

Mirko Caruso

Esperto in sicurezza delle informazioni e conformità delle infrastrutture critiche, membro e collaboratore della OWASP® Foundation. Ricercatore del progetto Domain-based Message Authentication, Reporting and Conformance e nei settori della sicurezza, prevenzione e contrasto della posta elettronica ai fenomeni di "Government impersonation" e pedopornografia. ISACA CISM e Cisco Certified Network Security Professional con esperienza diretta nei data center Tier IV di ISP italiani. Tre volte nella Hall of Fame del Gruppo TIM per la divulgazione responsabile di vulnerabilità critiche. Appassionato di OSINT, laureato in Studi Giuridici, con major in Informatica.

Tor, l'anonimato e la cifratura telescopica

Quando si sente parlare di Tor, o meglio, del Tor-browser, si pensa immediatamente a uno strumento legato alla malavita, all'illecito, al terrorismo. Eppure, il progetto è portato avanti da una organizzazione non-profit che ha sede a Seattle, stato di Washington, USA.

È una cosiddetta organizzazione 501(c)(3), che agisce cioè con il beneficio di essere esente da tasse federali e risulta essere una dei 29 tipi di organizzazioni non-profit che operano negli Stati Uniti. 501(c)(3).

Nel passato ha avuto molti sponsor illustri – come EFF[1] e Mozilla[2] – ma dobbiamo osservare che è finanziata dallo Stato americano e numerose altre organizzazioni non governative e non-profit, anche non americane, nonché da singoli individui; tutto ciò nonostante la NSA abbia dichiarato di non essere capace di determinare l'identità di tutti gli utenti di Tor tutte le volte[3]; tuttavia sembrerebbe che riesca a decifrarne le comunicazioni[4].

IL PROGETTO TOR

Il nome Tor viene spesso usato in modo impreciso. Tor sta per "The Onion Router" e si riferisce al software open-source che permette comunicazioni anonime usando una rete *"overlay"*[5], spesso chiamata ancora Tor, gratuita ed estesa su tutto il mondo, ed operata su base volontaria. L'intero prende il nome di progetto Tor portando dunque

[1] https://www.eff.org/

[2] https://www.mozilla.org/it/

[3] https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

[4] https://www.techtimes.com/articles/262645/20210709/tor-encryption-can-allegedly-be-accessed-by-the-nsa-says-security-expert.htm

[5] Viene così chiamata una rete definita da computer che operano su un'altra rete; nel caso di Tor: su Internet.

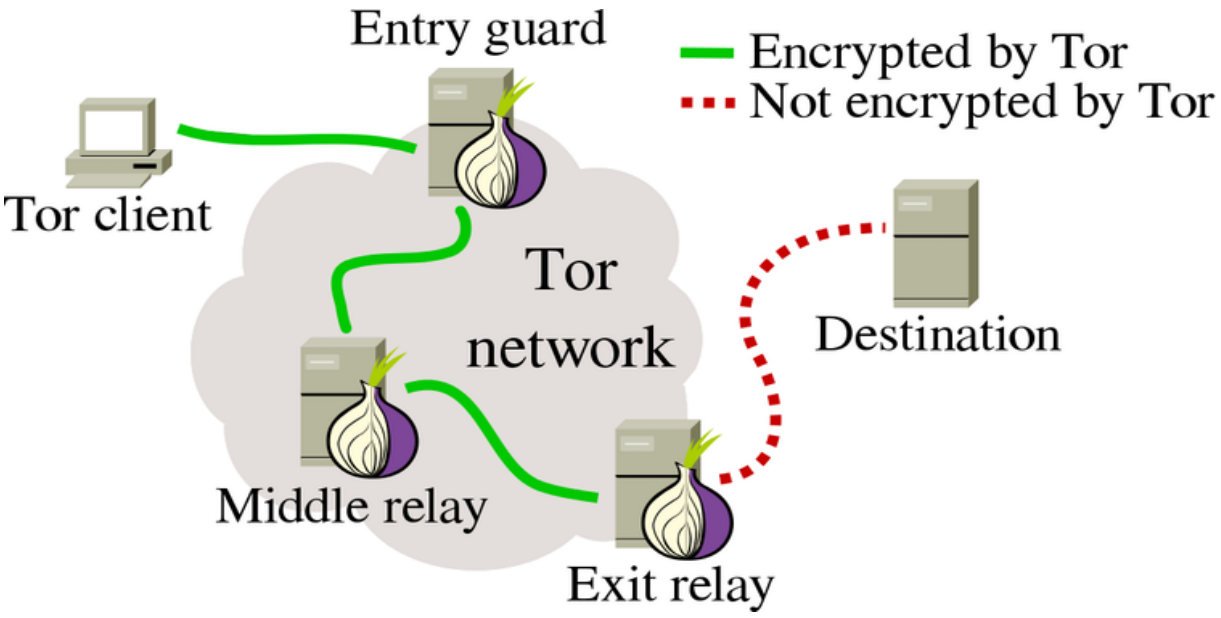


Figura 1. Schema logico di funzionamento della rete Tor

a creare confusione, essendo il termine usato in tre contesti differenti.

L'obiettivo del progetto è quello di costruire e gestire una rete *overlay*, consentendo agli utenti di connettersi a server, normalmente raggiungibili attraverso Internet, in pieno anonimato. Ciò viene ottenuto attraverso la cooperazione di diversi "*relay*", diffusi in tutto il mondo, che contribuiscono alla creazione e funzionamento della rete *overlay*. Una descrizione qualitativa è mostrata in Figura 1. L'utente che usa il Tor-browser si trova sul cosiddetto Tor client ed usa tre *relay* generati scegliendoli casualmente nell'insieme di tutti i *relay* (circa settemila).

I tre scelti, noti solamente al Tor-browser, prendono il nome di guardia, centro e punto di uscita (in figura, *entry guard*, *middle relay* ed *exit relay*).

Tutto ciò viene fatto per consentire al client di connettersi con la destinazione, transitando attraverso guardia, centro e punto di uscita (nell'ordine).

La sequenza di *relay* è ordinata dalla guardia al punto di uscita e contribuisce a definire il circuito (*relay circuit*), costituito appunto dal Tor client, la guardia, il centro, il punto di uscita e la destinazione.

L'unico soggetto che conosce completamente il circuito è il Tor client, mentre gli altri conoscono solo il punto precedente ed il successivo (se esiste): ciò per garantire l'anonimato. Infatti, nelle registrazioni presso la destinazione, dette file

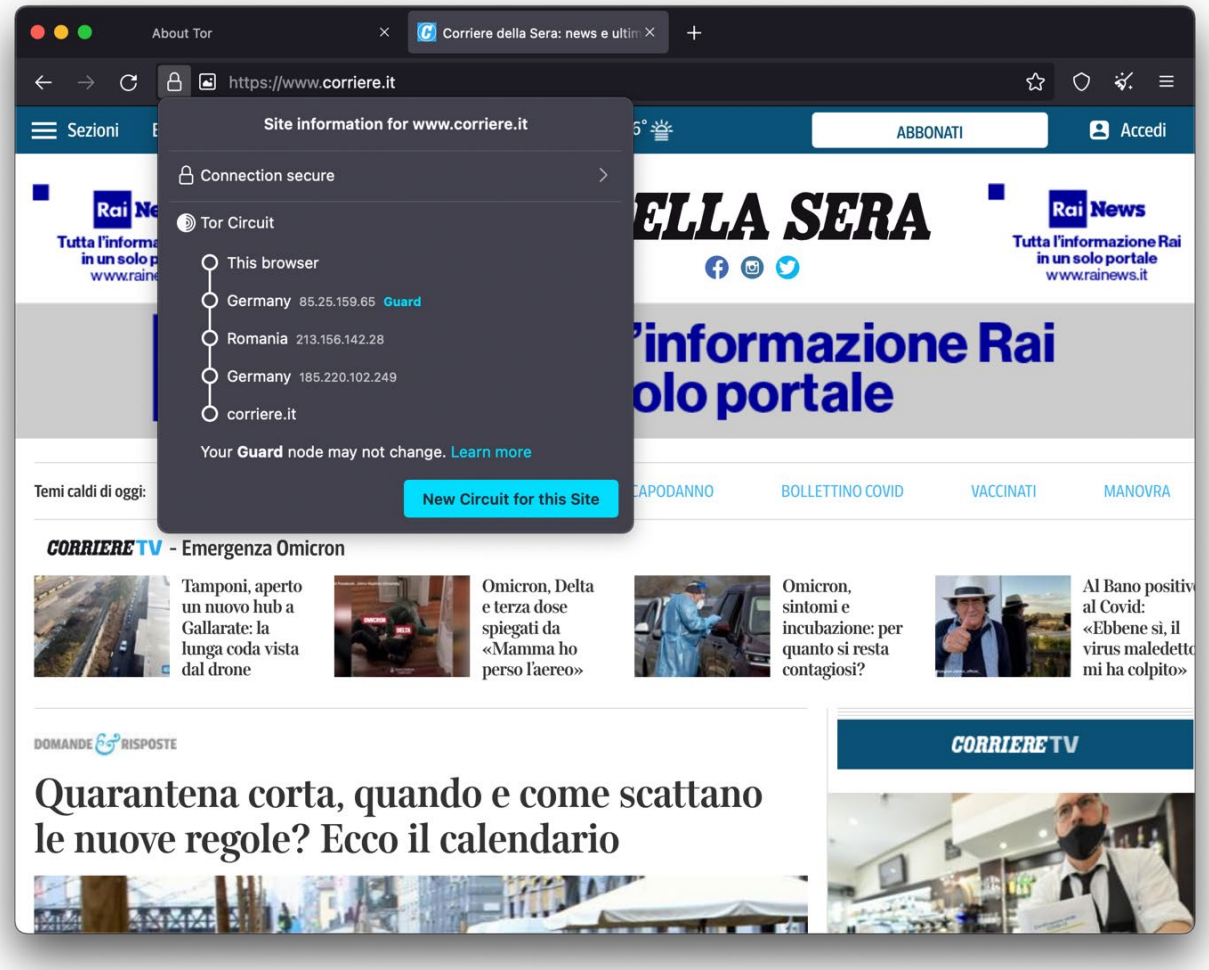


Figura 2. Esempio di circuito composto da un relay in Germania, uno in Romania e un altro ancora in Germania. La destinazione vedrà dunque una visita proveniente dalla Germania.

di *log*, apparirà solo una visita che sembra provenire dal punto di uscita.

Nel Tor-browser, che costituisce in pratica il Tor client, è disponibile la funzione "nuovo circuito per questo sito", nel caso l'utente, per qualche ragione, desideri un circuito differente (la guardia non può cambiare[6]). La funzione consente di generare istantaneamente un nuovo circuito per la stessa destinazione, avente la stessa guardia.

In Figura 2 si mostrano le informazioni di circuito relate al sito https://www.corriere.it/. Si nota il pulsante su sfondo blu che permette di generare un nuovo circuito.

Una volta richiesto e ottenuto un nuovo circuito, questo si rivelerà essere come mostrato in Figura 3; il nuovo punto di uscita si troverà dunque in Austria. Non molti sanno che si può agire sulla scelta del punto di uscita, configurando in maniera particolare il file torrc, che permette di esprimere alcune preferenze, come appunto una lista di paesi ai quali

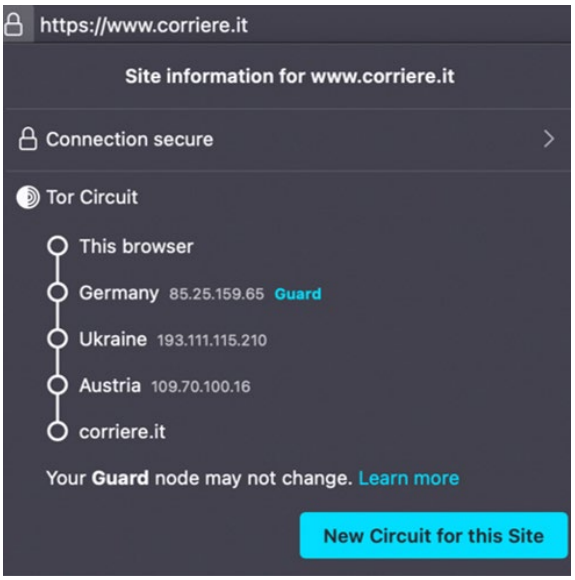


Figura 3. Nuovo circuito per il sito www.corriere.it.

debba appartenere il punto di uscita, ottenendo il risultato di visitare la destinazione come se ci si trovasse in uno dei paesi elencati.

Ancora dalla Figura 1 si può notare che le informazioni trasmesse/ricevute dal client mentre queste si trovano all'interno della rete Tor sono cifrate, mentre non è detto che lo siano le conversazioni fra il punto di uscita e la destinazione. Questo punto sarà meglio sviluppato nella prossima sezione.

[6] https://blog.torproject.org/improving-tors-anonymity-changing-guard-parameters/

LA CIFRATURA TELESCOPICA DI TOR

La parte di circuito dal *client* fino al punto di uscita è protetta da una cifratura, ad opera del software che realizza la rete Tor. Diverso è il discorso per l'ultimo tratto, fra il punto di uscita e la destinazione: se il collegamento (meglio: la URL) inizia con http questo sarà in chiaro, se invece inizia con https questo sarà cifrato, ma non per opera di Tor, ma grazie al protocollo TLS che la destinazione ha ritenuto di attivare[7].

Il circuito sarà dunque completamente cifrato, in alternativa alla cifratura offerta da Tor fino al punto di uscita, ma ciò dipende solo dalla destinazione.

Per meglio descrivere la cifratura operata da Tor, ricordiamo il modello generale della cifratura simmetrica. Si osservi la Figura 4, in cui si mostra un testo in chiaro (*plaintext*) che grazie a un algoritmo di cifratura simmetrico viene trasformato in testo cifrato (*ciphertext*). L'algoritmo di cifratura, oltre a prendere in *input* il *plaintext*, riceve anche una

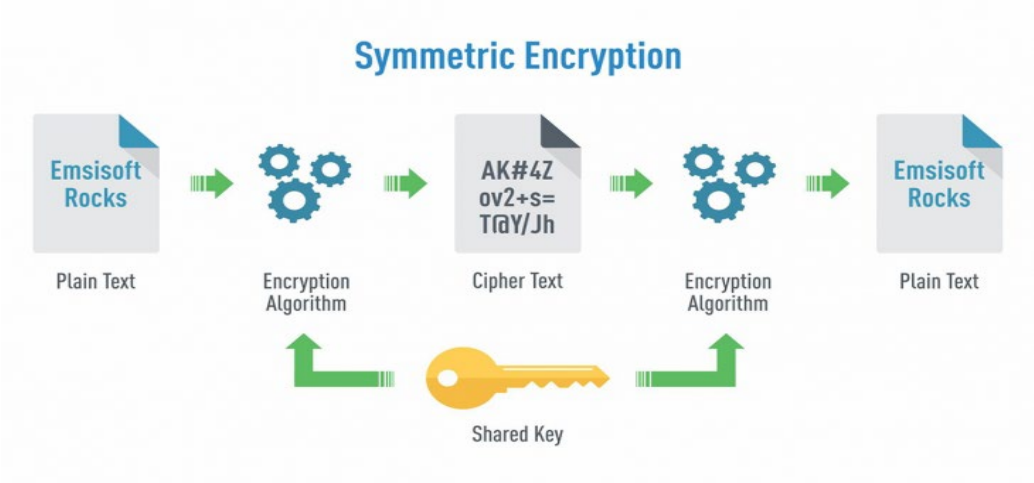


Figura 4. Modello di cifratura simmetrica

[7] In effetti, https = http + TLS. Ulteriori dettagli si possono trovare in https://en.wikipedia.org/wiki/HTTPS e https://en.wikipedia.org/wiki/Transport_Layer_Security

chiave, che possiamo pensare come sequenza casuale di qualche centinaio di bit (128 e 256 molto usati). Dalla parte opposta c'è un algoritmo di decifratura che prendendo in *input* il *ciphertext*, e la stessa chiave, restituisce in *output* il *plaintext*.

La cifratura si dice simmetrica perché si usa la stessa chiave per cifrare e decifrare; altrimenti si definirebbe asimmetrica.

Naturalmente la chiave deve essere mantenuta segreta, ma condivisa fra le due parti: la sicurezza ai fini della confidenzialità sta nella segretezza della chiave mentre algoritmo usato e altri parametri[8] possono essere pubblici.

Indichiamo il client con C, la guardia con Rin, il centro con Rc, il punto di uscita con Rout e la destinazione con D. All'inizio delle operazioni C concorda, rispettivamente, una chiave kin

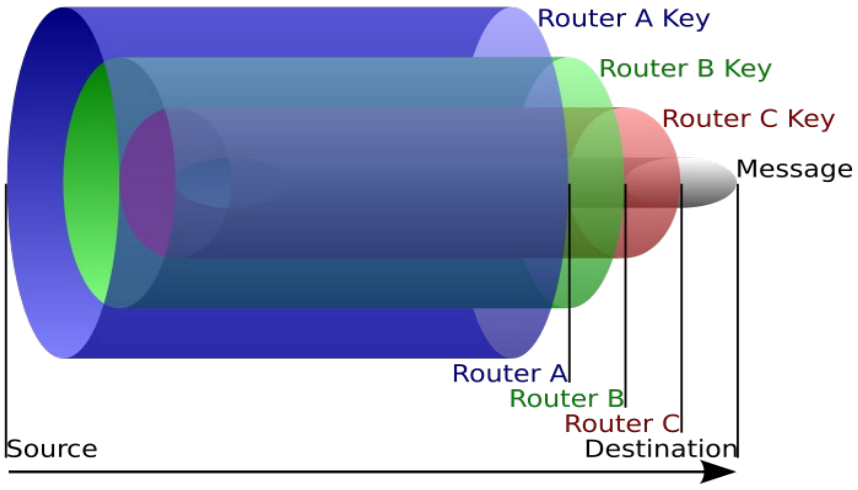


Figura 5. La cifratura telescopica di Tor, dove A, B e C stanno per Rin, Rc ed Rout. Figura tratta da https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Onion_diagram.svg/800px-Onion_diagram.svg.png.

[8] Spesso occorre generare un seme detto IV (initialization vector) per poter cifrare file di dimensione superiore a quella prevista dall'algoritmo (cifrario a blocchi, spesso di poche decine di byte per blocco). Si veda ad esempio https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation (tecnico).

con Rin, kc con Rc e kout con Rout[9].
Le informazioni trasmesse da C sono cifrate dapprima con kout, ottenendo un *ciphertext*, quindi cifrate di nuovo con kc, ottenendo un altro *ciphertext* e infine cifrate con kin, ottenendo un terzo *ciphertext*, che è quello che viene effettivamente trasmesso.

Si noti che se D prevedeva protocollo https, prima di cifrare con kout si sarebbe proceduto a cifrare i dati attraverso le primitive del protocollo standard TLS. Ignorando la questione se TLS sia presente o no, abbiamo tre livelli di cifratura annidati, operati dalla rete Tor e in particolare ricevuti dalla guardia.

All'arrivo del *ciphertext* presso la guardia questa, che conosce kin, l'ultima chiave usata per la cifratura multipla, può operare un livello di decifratura e inviare il *ciphertext* risultante al centro, che riceverà una sua volta un *ciphertext* recante cifratura a due livelli e che può decifrare con kc e inviare il *ciphertext* risultante al punto di uscita, che riceverà dunque un *ciphertext* con cifratura ad un solo livello e che potrà decifrare con kout.

Dunque, nel caso di https, dobbiamo aggiungere ai livelli appena usati un ulteriore livello di cifratura, dato da TLS. Il processo è illustrato in Figura 5, che mostra appunto il modello di cifratura telescopica usato da Tor.

Per il pubblico più tecnico aggiungiamo che le connessioni di rete che consentono l'invio lungo il circuito dei *ciphertext* descritti usano il protocollo TLS e quindi un ulteriore livello di cifratura la cui presenza non impatta sula cifratura telescopica e che è noto a tutti i sistemi operativi. Tor esegue cifratura basata su AES[10], famoso standard scelto dal NIST[11].

[9] In crittografia è possibile concordare chiavi con una controparte remota, in totale confidenzialità; ciò può essere fatto in svariati modi. Si veda ad esempio https://crypto.stackexchange.com/questions/10371/how-is-the-key-shared-in-symmetric-key-cryptography (tecnico).

[10] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (tecnico).

[11] https://en.wikipedia.org/wiki/Virtual_private_network

Concludendo, la cifratura descritta consente confidenzialità, inoltre vari accorgimenti aiutano i circuiti a funzionare (ogni *relay* può partecipare a vari circuiti) senza rivelare dettagli sull'intero circuito. Il miglior utilizzo del Tor-browser è quello con https. Un'ottima pagina che mostra come Tor funziona con/senza https è quella di EFF: https://www.eff.org/pages/tor-and-https. Alcuni usano Tor solo con una VPN[12], che mette in sicurezza il collegamento fra *client* e guardia.

L'IMPORTANZA DELL'ANONIMATO

Abbiamo in mente almeno tre scenari d'uso in cui l'anonimato proteggerebbe gli utenti di un browser. Nel primo pensiamo a tutti coloro che sono sottoposti a censura e non hanno libertà di espressione.

L'essere anonimi consente loro di accedere a reti sociali e più in generale ad Internet senza rivelare la propria identità. Infatti, ogni volta che facciamo l'azione di visitare una pagina web questa lascia delle tracce.
Nei file "di *log*" del *server web* ci saranno delle linee che descrivono data e ora dell'azione, tipo di azione, indirizzo IP di chi ha eseguito l'azione. Nel peggiore dei casi le pagine conterranno elementi invisibili destinati a tracciare e profilare l'utente (generalmente a scopo commerciale) che aiutano molto nell'identificazione dell'utente.
Il Tor-browser contrasta tali azioni, lasciando tracce falsate e l'IP del punto di uscita.
È vero che la lista dei Tor *relay* è pubblica[13], per cui il *server web* si accorgerà che la visita è stata fatta attraverso Tor, ma non ci saranno altri elementi che aiuteranno a identificare l'utente[14]. Per motivi che saranno discussi in segui-

[12] https://en.wikipedia.org/wiki/Virtual_private_network

[13] Queste informazioni, ed altre, sono ad esempio disponibili alla URL https://metrics.torproject.org/rs.html

[14] Il Tor-browser può essere configurato in vari livelli di sicurezza (tipicamente tre) e al più alto livello viene bloccato Javascript e vari altri elementi che è possibile usare nelle pagine web, contrastando efficacemente il tracciamento.

to, alcuni *server web*, riconoscendo un accesso proveniente da Tor, si rifiutano di erogare il servizio, negando la pagina all'utente.

Un secondo scenario è quello di un utente "normale," che effettua un comune uso del web: per prevenire il tracciamento e la profilazione, che lo condanneranno a subire certe pubblicità che risulterebbero più efficaci in base ai suoi interessi e ai comportamenti passati, si ricorre all'uso del Tor-browser, che, come detto, aiuta a contrastare la profilazione (incluso il *browser fingerprinting*[15]).

Il terzo è un tipo scenario della *business intelligence*, ove l'utente lavora in qualche organizzazione e magari effettua OSINT[16] sul web per determinare comportamenti e strategie dei concorrenti. Come detto, le azioni svolte dall'utente lasciano tracce, per cui l'organizzazione concorrente troverebbe nei *log* gli accessi effettuati e ne trarrebbe conseguenze, facendo la visita dell'utente inquinare lo scenario di indagine OSINT. Con l'uso del Tor-browser si riduce o si annulla tale rischio, ottenendo dunque uno strumento utile ai fini di intelligence.

Esistono ulteriori scenari, fra i quali l'uso del Tor-browser da parte di criminali e terroristi, che hanno evidentemente l'interesse a celare le proprie tracce. Questa è la ragione per cui molte organizzazioni non vogliono l'uso di Tor[17] e bloccano sia le visite provenienti da Tor sia gli accessi al sito web del progetto. Quindi esiste una percezione, giustificata dall'uso non etico di Tor, che spinge alcune organizzazioni a bloccare Tor. Un po' come bloccare la produzione di pistole perché potrebbero essere usate con intenti non etici.

[15] Si tratta di una pratica usata per riconoscere l'uso dello stesso browser. Nella pagina https://coveryourtracks.eff.org/ si può valutare quanto il browser in uso sia riconoscibile. Il Tor-browser contrasta questo fenomeno fornendo notizie false e/o rifiutandosi di fornire il risultato di certe analisi.

[16] https://en.wikipedia.org/wiki/Open-source_intelligence

[17] Curioso è il comportamento di Google, che con il suo servizio di email, gmail appunto, nel momento in cui un utente tenta di registrare una nuova casella di posta gmail, ed è collegato con Tor, non riceve divieto alcuno, ma ottiene un captcha praticamente irrisolvibile.

IL TOR-BROWSER

Ne abbiamo già parlato. Vale la pena precisare che si può scaricare dal sito del progetto[18], oltre che da numerose altre fonti, e che viene costruito, e aggiornato frequentemente, a parte da una versione "recente" di Mozilla Firefox (non l'ultima); talvolta ciò crea un problema sulla piattaforma in uso che "vede" erroneamente due istanze in esecuzione di Firefox. Si tratta in entrambi i casi di software open-source.

Il Tor-browser richiede, ai fini dell'anonimato, un uso accorto, che vede l'utente fare clic con cautela. In particolare, molti attacchi volti a de-anonimizzare l'utente, si sono basati sul fatto che, in corrispondenza a certi clic, il browser aziona automaticamente altri programmi, che magari si connettono a Internet autonomamente (senza usare Tor quindi) e finiscono con il rivelare il vero indirizzo IP dell'utente.

Questo avveniva specialmente nel passato, mentre oggi tali automatismi in genere non si verificano. È comunque buona pratica, all'installazione del Tor-browser, fare "un giro" attraverso le sue preferenze (command + ',' sul Mac, non abbiamo ora sottomano una macchina Windows); è una cosa che si fa una volta sola, ma che fornisce grande aiuto per il corretto funzionamento dello strumento e soprattutto senza sorprese.

Altra cosa che c'è da sapere è che il Tor-browser può essere scaricato senza installatore (si parla di "*bundle*")[19], poi messo su una penna USB. Può essere eseguito direttamente dalla penna, utile nel caso non si posseggano diritti di fare l'installazione.

Il Tor-browser può essere usato come un normalissimo browser, tutta via, a causa del fardello costituito dalla *overlay network* e la cifratura telescopica, risulta essere un po' lento. In presenza

[18] https://www.torproject.org/

[19] Si veda https://blog.torproject.org/ways-get-tor-browser-bundle/

di buona connessione la sua velocità è ancora accettabile, ma per *download*, torrent e *video streaming* è totalmente (se non proibitivamente) inefficiente.

È vero che possiamo usare il Tor-browser come un normale browser, ma le sue impostazioni di sicurezza faranno sì che alcune pagine non vengano mostrate correttamente. Questa è la ragione per cui qualunque utente Tor ha a disposizione anche un browser tradizionale.

HIDDEN SERVICE AND DARK NET

Si parla oggi molto della *dark net*, o *dark web*. Facciamo un po' d'ordine. Il web che tutti conoscono, indicizzabile da Google o da altro motore di ricerca, viene chiamato "web di superficie". Questo perché esiste un web molto più ampio chiamato "*deep web*" e costituito da tutte quelle pagine web che non possono essere raggiunte da un motore di ricerca (perché occorre una pas-

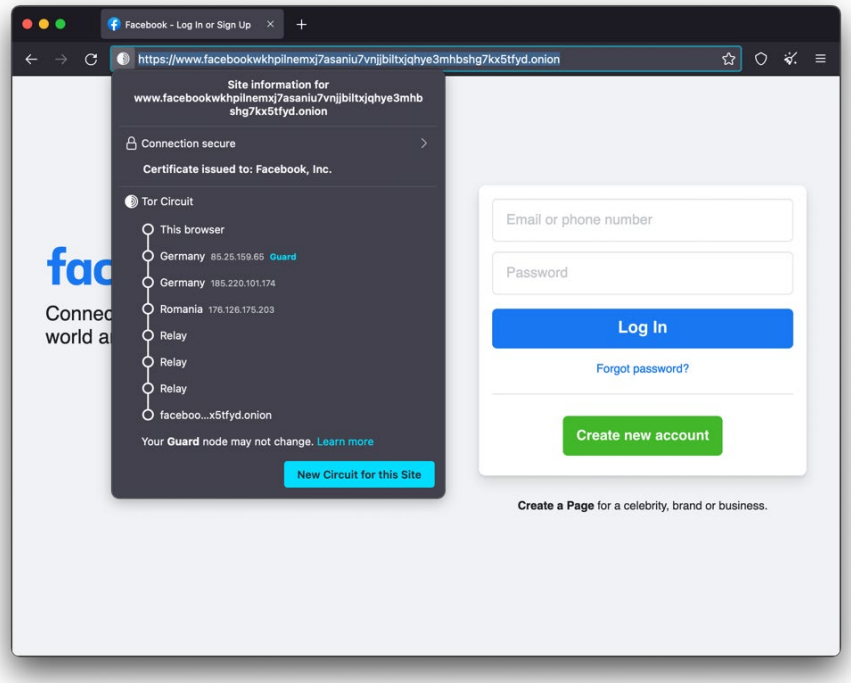


Figura 6. Sito web "hidden" di Facebook, per consentire l'accesso anonimo.

sword, o esiste un divieto, o qualunque altro motivo). Il *dark web* è una parte del deep web (in quanto non raggiungibile dai normali motori di ricerca). Ma in cosa consiste?

Abbiamo visto che l'utente del Tor-browser si trova a creare un circuito che passa attraverso tre *relay* per raggiungere la sua destinazione. Similmente, il proprietario di un sito web, può decidere di costruire un circuito per far raggiungere il proprio sito. In tal caso il sito risulta nascosto (non ne conosciamo l'IP), viene chiamato *hidden service*, e si fa riconoscere da un indirizzo incomprensibile per i normali browser, che termina con .onion, ma che viene perfettamente riconosciuto dal Tor-browser. In Figura 7 ne è mostrato un esempio.

Come si può vedere si ottiene un circuito più lungo sequenziando i due circuiti (meglio, i loro *relay*), ottenendo un circuito di lunghezza otto di cui non si conoscono i dettagli relativi al sito *hidden* che si visita. In tal modo si possono esportare servizi web in pieno anonimato: il servizio *hidden* è nascosto nella rete e l'insieme dei servizi *hidden* costituisce il *dark web*.

Muoversi nel *dark web* richiede la conoscenza dei relativi indirizzi, oltre che all'uso del Tor-browser. Questi indirizzi, per ragioni di sicurezza, variano molto nel tempo: così è frequente trovare l'indicazione di indirizzi nel *dark web* che non sono invece funzionanti. Non c'è nulla di cui stupirsi. A suo tempo, il proprietario del servizio ha probabilmente divulgato il nuovo indirizzo in qualche modo, anche pubblicandolo all'interno di qualche improbabile forum, magari sul web di superfice.

Ad ogni modo, esistono motori di ricerca specifici per il *dark web*, come ad esempio il Torch Search Engine[20] (v. Figura 7). L'utilizzo di un motore di ricerca per il *dark web* può facilmente convincere l'utente della soverchiante presenza di siti illegali nel *dark web*;

[20] Indirizzo, a dicembre 2021: http://torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion/

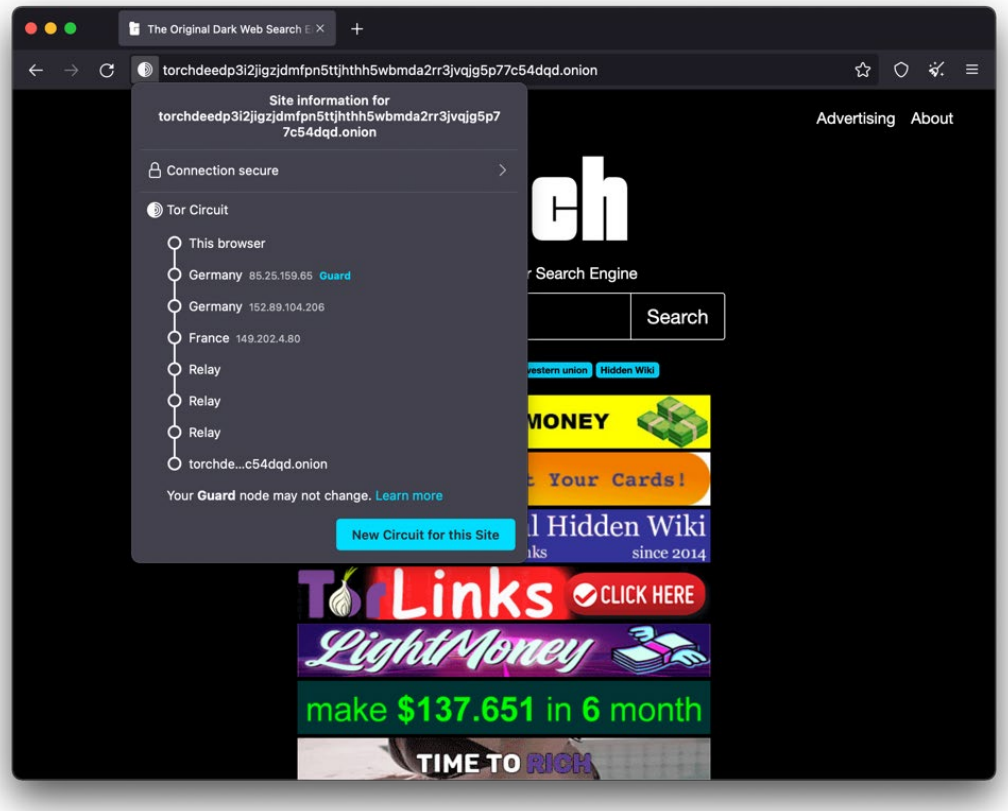


Figura 7. Esempio di motore di ricerca per rete Tor.

eppure, i siti *hidden* totalmente etici sono comunque tanti. Ecco una lista di altri motori di ricerca per il *dark web*: Ahmia, Onion Search Engine, Candle, The Uncensored Hidden Wiki, TorLinks, HayStack, TorDex; i rispettivi indirizzi (onion o tradizionali) sono stati aggiornati recentemente con il passaggio a una nuova versione di Tor, per cui occorre un po' di tempo e motivazione per ritrovarli.

CONCLUDENDO

Molte organizzazioni sono a favore dei diritti digitali e della privacy, a partire da EFF e Mozilla. Invero, ne esistono altre, oltre ad alcune che dicono di difendere la privacy (come Apple). Eppure, a guardare il loro comportamento, la cosa non sembra. Apple, ad esempio, negli smartphone realizza una configurabilità e un controllo delle connessioni

assai più debole di quanto fa su computer desktop e portatili. Per non parlare del fatto che lo smartphone contiene molti più dati di quello che pensiamo (quasi ogni nostro respiro) ed è pronto a cederli alle varie app se noi incautamente autorizziamo l'operazione, descritta in termini molto più aulici.
Un discorso collegato è la privacy della e-mail. È vero che viene trasmessa e ricevuta attraverso connessioni oggi cifrate, ma, considerando i vari intermediari (o agenti) che partecipano al processo di consegna della posta, loro, così come il server destinatario, hanno memorizzato il messaggio in chiaro, realizzando un sistema che non impiega cifratura *end-to-end*, ma potremmo dire, inventando il termine, *next-to-next*.
L'utilità di Tor è legata al numero di *relay*. Oggi sono circa settemila; sul sito del progetto è possibile visionare statistiche e serie storiche. Tanti più utenti decideranno di usare Tor, quanto più questo sarà maggiormente sicuro, e pronto ad accompagnare ogni utente in un viaggio anonimo, al contrario della modalità anonima dei browser che non consente di nascondere il proprio IP.
Esistono oggi molti servizi su Tor, come reti sociali, e-mail, chat, forum, blog, che funzionano all'insegna dell'anonimato totale. Inoltre, sono disponibili alcune distribuzioni linux[21] che eseguono qualunque connessione di rete usando Tor, proteggendo l'anonimato qualunque uso si faccia di ogni applicazione.
Tali distribuzioni risultano essere piuttosto apprezzate per lo svolgimento di attività forensi, test di sicurezza, intercettazioni di rete ed altro, proteggendo l'anonimato dell'utente.

Fabrizio D'Amore, *Docente presso l'Università degli Studi di Roma "La Sapienza", membro del Cyber Intelligence and Information Security Center*

[21] Come Tail, v. tails.boum.org/index.en.html. Tails è l'acronimo di The Amnesic Incognito Live System ed è resistente perciò ad ogni forma di intercettazione. A suo tempo era usato dal celebre Edward Snowden. Un'altra celebre distribuzione è Kali, v. www.kali.org, molto sicura ed usata per attività forensi, intercettazioni di rete anonime, penetration testing e ricerca sulla sicurezza

BIOGRAFIA

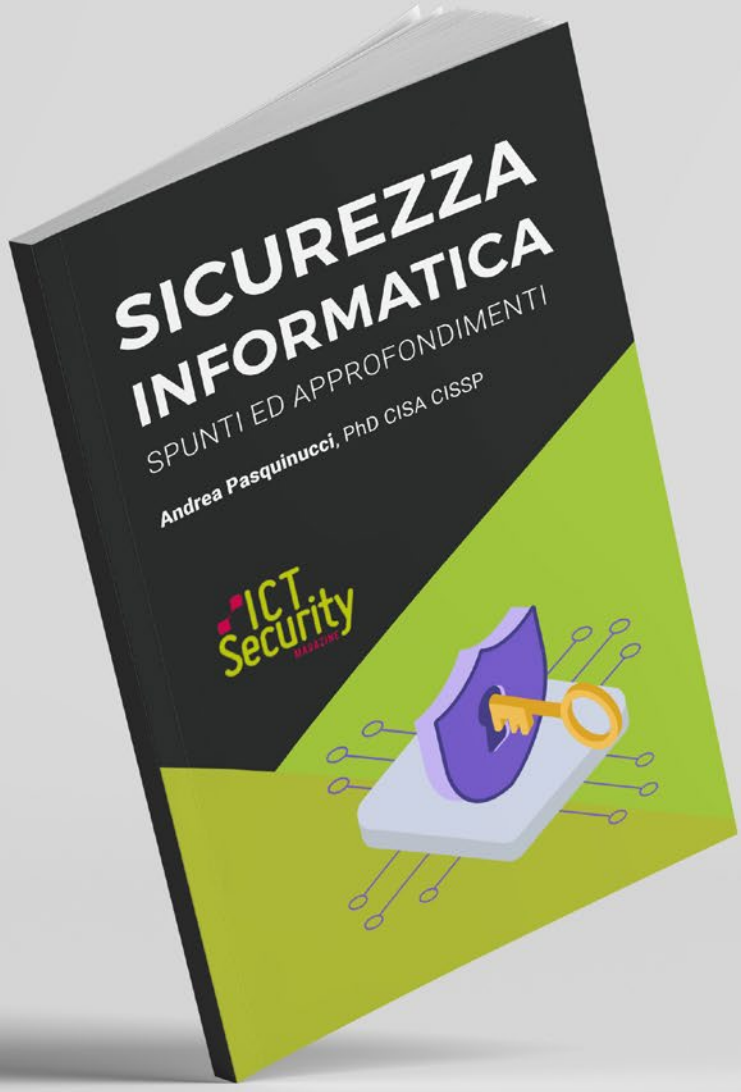
Fabrizio D'Amore

Romano, docente di Cybersecurity alla Sapienza Università di Roma. Ha trascorso periodi di studio e ricerca all'estero (Zurigo, Buenos Aires, Berkeley, UMIACS a College Park Maryland). Insegna inoltre corsi di crittografia, sicurezza delle informazioni, sicurezza applicativa e steganografia presso alcuni master ed altre iniziative di alta formazione. Direttore del master di 2° livello in Sicurezza delle informazioni e informazione strategica, in collaborazione con il DIS. Svolge attività di verificatore e di consulente tecnico di parte. Referente scientifico di contratti di ricerca applicata, studio e analisi fra università ed enti istituzionali e privati. Dal 2015 la sua attività di ricerca si concentra sul campo della steganografia/watermarking, sicurezza del software (antiplagio), cybersecurity del volo aero civile e delle infrastrutture, modelli di autenticazione, protezione dei dati & privacy e OSINT.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**