Commissione di Studi
Cyber Threat Intelligence
e Cyber Warfare

LE PROSPETTIVE DELLA CYBER INTELLIGENCE

Vol. 1

Anno 2022

SOCINT
Società Italiana di Intelligence

Quaderno Tematico

© 2022 Società Italiana di Intelligence (SOCINT)

Società Italiana di Intelligence
c/o Università della Calabria, Cubo 18-b, 7° piano
via Pietro Bucci
87036 Arcavacata di Rende (CS) - Italia
https://www.socint.org
ISBN 979-12-80111-32-6

Società Italiana di Intelligence
c/o Università della Calabria
Cubo 18/B, 7° Piano – 87036
Arcavacada di Rende (CS)
www.socint.org – info@socint.oorg

www.socint.org/commissioni-di-studio/
commissione.cyberwarfare@socint.org

https://creativecommons.org/licenses/by-nc- nd/4.0/deed.it

Le Prospettive della Cyber Intelligence©
Quaderno Tematico© – Anno 2022/Vol. N.1

Socint Press©
http://www.socint.org

Cover by Commissione Studi Cyber Threat Intelligence & C.W. – Free Design
Licenza Creative Commons

INDICE

INTRODUZIONE

"La natura delle minacce cyber e le informazioni derivanti dalle attività d'Intelligence interessano tutti gli attori istituzionali e non".

di **Mattia Siciliano**[1]

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 Cyber Intelligence e Cyber Warfare.

I risultati del progetto di ricerca e studio sono di seguito 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 illustrato più avanti.

La ricerca, si divide in due macro parti: la prima si focalizza soprattutto sugli aspetti giuridici e di scenario geopolitico 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, tale da incidere sulla capacità delle stesse istituzioni di definire nuovi meccanismi per fronteggiare i nuovi rischi (non necessariamente riferibili solo alla sfera economica) bensì anche agli aspetti d'innovazione tecnologica.

Molte, infatti, sono le variabili in gioco – tra loro interdipendenti – interne ed esterne al campo d'azione. Il fenomeno cyber, infatti, non è facilmente prevedibile sia per gli 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 pubbliche di regolamentazione, ed infine per i comportamenti di imprese ed individui.

[1] Presidente Commissione di Studi Cyber Threat Intelligence e Cyber Warfare.

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 ed intelligence, nell'ottica di prevenire gli effetti rischiosi sulla protezione degli asset essenziali, e di salvaguardare la capacità d'innovazione degli operatori;

- suggerire le possibili soluzioni\azioni 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 nell'ambito del contesto cybersecurity e cyber intelligence,

Il lavoro complessivo che ne è scaturito può essere visto come un approfondimento della proposta[2] già inoltrata alla neonata Agenzia di Cybersicurezza Nazionale (ACN) che ha di recente visto l'apporto di contributi anche da altre Associazioni e Istituzioni italiane.

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

01 UNA RIFLESSIONE PRELIMINARE SUL PROCESSO DI ISTITUZIONALIZZAZIONE DELLA CYBER INTELLIGENCE (CYBINT)

di ACHILLE PIERRE PALIOTTA

Aspetti concettuali e definitori propedeutici a un 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)

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

[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>.

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 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

[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, <https://bit.ly/3HsevVS>.

[5] Kurt Baker, *What is Cyber Threat Intelligence?*, 18 February 2021, < https://bit.ly/3sC8mmd>.

[6] Gartner, 2013, <https://www.gartner.com/en/documents/2487216/definition-threat-intelligence>.

[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/cyberintelligence. html>.

a identificare, penetrare o neutralizzare le azioni 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, con quello di "dati" e di "informazioni che con quello di cyber (spazio)[13] il quale, anch'esso, viene spesso 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 que-

[10] *Ivi*.

[11] Carnegie Mellon University, Software Engineering Institute, <https://bit.ly/359hfL5>.

[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.

[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://bit.ly/3JZn7VR>.

sto 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 abbondantemente 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 colpire le attività e le risorse degli avversari. È per questa ragione che il suo utilizzo è più sporadico e viene poco sottolineata 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

[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*).

[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.

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 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 sottocampi 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 centralità 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

[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.

[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

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 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 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.

---

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.

[20] Stephen Marrin, *Intelligence Studies, Intelligence Analysis, and Multidisciplinary Learning*, 2017, p. 1, <https://bit.ly/3po9EPk>.

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, 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 corrispon-

denti, 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 attacchi 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 piano 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.

[21] Achille Pierre Paliotta, *Cybersicurezza, dall'Agenzia nazionale l'impulso per un vero cambiamento*, "Agenda digitale", 1 ottobre, 2021, <https://bit.ly/3tjSyDp>.

02 LA STRATEGIA DELL'UNIONE EUROPEA SULLA CYBERSICUREZZA A FRONTE DELLE RECENTI MINACCE IBRIDE

di ANNITA SCIACOVELLI

L'intensità, la sofisticazione e la pervasività degli attacchi informatici 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'istituzione di un'unità congiunta sul ciberspazio finalizzata alla realizzazione del cyber-scudo europeo"

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 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

[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.

[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.

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 norme 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].

---

[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.

[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 cyber difesa 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).

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

[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.

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

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 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].

[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.

[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.

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

---

[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.eucybernet.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.

[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.

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.*

[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.

03 ANALISI GEOPOLITICA A SUPPORTO DELLA CYBER THREAT INTELLIGENCE

di ANDREA LEONI

"Un approccio multidisciplinare per la previsione dell'attività di Threat Actors"

Il cyberspazio oggi è a tutti gli effetti una dimensione reale, con effetti reali 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 blackout 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 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,

[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".
[4] Colin Flint, "Introduction to Geopolitics".

anche la NATO infatti parlando di risposta comune ai cyber attacchi 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.

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 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.

---

[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".

[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, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

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).

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 società 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

[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/

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 e 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 cyber attacco 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 d'informazione per la sicurezza della Repubblica per creare *alert* più mirati da diffondere alle pubbliche amministrazioni e al settore produttivo privato italiano.

04 ANALISI DEL RISCHIO CIBERNETICO

di ANDREA GIORDANI

> *"Nel settore economico italiano si rende urgente un'azione di difesa, attraverso un ruolo di stimolo alla sensibilità sulle tematiche della cyber guerra, da parte dell'Agenzia per la Cibersicurezza"*

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 d'intelligence. La competizione tra le diverse entità statuali si è allargata evolvendo 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 d'informazioni sensibili e proprietà intellettuale in possesso d'imprese e centri di ricerca scientifica e tecnologica;
- ✓ L'elevato tasso di profitto per gli attori statuali o para-statali che praticano operazioni d'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 atta 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 d'intelligence al fine di contrastare azioni ostili da parte attori statuali e para statali nei confronti del nostro paese.

Il World Economic Forum ha pubblicato il "Global Risk Landscape 2021" da quale si evince che gli attacchi cibernetici comportano 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, azzerando il possibile rendimento nel tempo di investimenti già 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 fasti-

dioso accessorio dell'attività d'impresa. L'Agenzia 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, già in passato ha emanato la direttiva NIS e si prepara a emanare 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 di ogni singolo attore.

Il rischio cibernetico non impatta solo la singola impresa ma ha anche un'importante componente sistemica, cioè il rischio che un attacco (o altri eventi avversi) ad 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 d'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 a esse. Si passa dalla "logica dell'adempimento" alla "logica della respon-

sabilità", laddove il singolo operatore, attraverso l'Analisi del Rischio, deve essere in grado d'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 e 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 e 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.

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. 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;
- ✓ Elevato livello di automazione;
- ✓ 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.

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.

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 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:

quantitative in quanto direttamente e oggettivamente misurabili:

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

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 e asset in fun zione 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 è 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 d'investimenti e di consapevolezza in questo campo rendono le PMI estremamente esposte ad attività ostili d'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 cyber guerra da parte dell'Agenzia per la Cibersicurezza Nazionale. Dal canto loro gli apparati d'intelligence devono essere coinvolti per l'esecuzione di attività di contrasto alle ingerenze estere anche attraverso l'uso di tecniche Humint e Osint, che costituiscono un imprescindibile mezzo di difesa dell'interesse economico nazionale.

05

CYBER-ENABLED INFORMATION WARFARE

di FRANCESCO ARRUZZOLI

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.

“Tra le nuove dimensioni di combattimento delle guerre ibride il cyberspazio è sicuramente il più utilizzato, grazie alla sua predisposizione a sviluppare asimmetrie hi-tech”

Nessuna guerra è eguale a 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 e 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, e 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 d’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 e 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 interna-

zionale, 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 distruggere 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 d'influenzare la conoscenza dell'avversario per determinarne il comportamento alterando la sua percezione. Una campagna IW/C-IW non deve limitarsi a 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 d'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, a 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.

In realtà il simbolo rappresentato in Figura A non è quello della svastica nazista (Fig. C) ma quello della svastica induista (Fig. B), 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.

Fig. A

Fig.B

Fig. C

In un ipotetico attacco C-IW, l'immagine in Figura 3 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.

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 nostre 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'intelligence (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", profes-

sionisti 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 maniera "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 socioculturale 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". È un'arma che consente a chi la usa con successo di esercitare la manipolazione o l'eterodirezione.

La disinformazione è un argomento centrale del pensiero politico e strategico occidentale e orientale sin dall'antichità, basti pensare ai 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 e 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 rapidamente 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 d'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 inten-

zioni 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 d'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 a 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 e 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 d'informazione, in modo che siano percepite come utenti legittimi (umani) e 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.

di FRANCESCO SCHIFILLITI

"Identificare un gruppo come responsabile di un attacco informatico è sempre stata un'attività molto impegnativa per gli analisti dell'intelligence. Nel corso di questo lavoro, si vogliono affrontare brevemente gli aspetti di complessità connaturali alla fase di attribuzione e, soprattutto, i collegamenti che stanno diventando sempre più frequenti tra lo Stato Nazione e il gruppo eCrime".

Connessioni tra gruppi cyber criminali e gruppi *statali*

Synopsis

Identifying a group as responsible for a cyber-attack has always been a very challenging activity for intelligence analysts. In the course of this work, we want to briefly deal with the aspects of complexity connatural with the attribution phase and, above all, the connections that are becoming more and more frequent between the Nation State and the eCrime group.

Main Categorization of Threat Actors

Before starting the discussion of the main topic of this article, it is essential to introduce the main categories of Threat Actors (or Adversaries) associated with cyber-attacks. The categorization used is the one also used in the MISP Galaxy[1]:

Nation States: entities who work for the government or military of a nation state or who work at their direction. These actors typically have access to significant support, resources, training, and tools and are capable of designing and executing very sophisticated and effective *Intrusion Sets* and *Campaigns*.

Chief Goal: espionage, theft, or any other activity that furthers the interests of a particular nation groups.

Typical Targets: businesses and government-run organizations.

[1]Galaxies in MISP are a method used to express a large object called cluster that can be attached to MISP events or attributes. *https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json*

Individuals: an individual that tends to break into networks for the thrill or the challenge of doing so. Hackers may use advanced skills or simple attack scripts they have downloaded. As individual there are also non-hostile insider who unintentionally exposes the organization to harm. In this context, “insider” includes any person with extended internal trust, such as regular employees, contractors, consultants, and temporary workers.

Chief Goal: work from within an organization to get around its cybersecurity framework.

Typical Targets: not limited to any specific type of organization.

eCrime: an enterprise organized (or Individual) to conduct significant, large-scale criminal activity for profit. eCrime (or Organized Crime) are generally large, well-resourced groups that operate to create profit from all types of crime. Intellectual property theft, extortion via ransomware, and physical destruction are common examples.

Chief Goal: financial gain.

Typical Targets: cash and/or data-rich organizations and businesses.

Hacktivists: highly motivated, potentially destructive supporter of a social or political cause that attempts to disrupt an organization's business model or damage their image. This category includes actors sometimes referred to as anarchists, cyber vandals, extremists, and hacktivists.

Chief Goal: exposing secrets and disrupting services/organizations that are perceived as evil.

Typical Targets: not limited to any specific type of organization or business.

Of the types of attackers that have been described above, the major ones are Nation States and eCrime groups. While the description and purpose of the eCrime groups are univocal, the Nation State groups can be characterized on basis of the responsibility of the States in the cyber-attacks carried out by these groups.

The spectrum of state responsibility is a tool to help analysts with imperfect knowledge assign responsibility for a particular attack (or campaign of attacks), with more precision and transparency. This spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack. The spectrum starts from a very passive responsibility up to very active responsibility:

- State-prohibited: the national government will help stop the third-party attack, which may originate from its territory or merely be transiting through its networks. Nations cannot

ensure the proper behavior of the tens or hundreds of millions of computers in their borders at all times.

- State-prohibited-but-inadequate: the national government is cooperative and would stop the third-party attack, but is unable to do so. The country might lack the proper laws, procedures, technical tools, or political will to use them. Though the nation could itself be a victim, it bears some passive responsibility for the attack, both for being unable to stop it and for having insecure systems in the first place.

In the following four categories, in contrast to the previous two, the nation is actively ignoring or abetting attacks:

- State-ignored: the national government knows about the third-party attacks but, as a matter of policy, is unwilling to take any official action. A government may even agree with the goals and results of the attackers and tip them off to avoid being detected.
- State-encouraged: third parties control and conduct the attack, but the national government encourages them to continue as a matter of policy. This encouragement could include editorials in state-run press or leadership publicly agreeing with the goals of the attacks; members of government cyber offensive or intelligence organizations may be encouraged to undertake supportive recreational hacking while off duty. The nation is unlikely to be cooperative in any investigation and is likely to tip off the attackers.
- State-shaped: third parties control and conduct the attack, but the state provides some support, such as informal coordination between like-minded individuals in the government and the attacking group. To further their policy while retaining plausible deniability, the government may encourage members of their cyber forces to undertake “recreational hacking” while off duty.
- State-coordinated: the national government coordinates the third-party attackers—usually out of public view—by “suggesting” targets, timing, or other operational details. The government may also provide technical or tactical assistance. Similar to state-shaped attacks, the government may encourage its cyber forces to engage in recreational hacking during off hours.

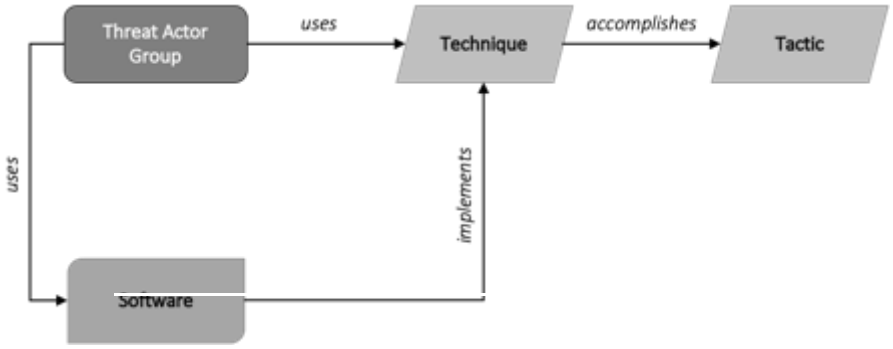
In the final four categories, the state, far from ignoring or encouraging attacks, has a much more direct hand in them, either ordering attacks or conducting them itself.

- State-ordered: the national government, as a matter of policy, directs third-party proxies to conduct the attack on its behalf. This is as “state-sponsored” as an attack can be, without direct attack from government cyber forces. Any attackers that are under state control could be considered to be de facto agents of the state.

- State-rogue-conducted: elements of cyber forces of the national government conduct the attack. In this case, however, they carry out attacks without the knowledge, or approval, of the national leadership, which may act to stop the attacks should they learn of them. A state could likely be held responsible by international courts for such rogue attacks.
- State-executed: the national government, as a matter of policy, directly controls and conducts the attack using its own cyber forces.
- State-integrated: the national government integrates third-party attackers and government cyber forces, with common command and control. Orders and coordination may be formal or informal, but the government is in control of selecting targets, timing, and tempo. The attackers are de facto agents of the state.

Definition of Attribution

Attribution is used at the basis of the attacker classification activities. To be precise, attribution is the task of Identifying actors responsible for a cyber-attack. Everyday threat actors target sectors like energy, finance, manufacturing. Sector-specific threat intelligence is essential for protecting organizations from unknown threats. The follow figure shows the relations between the main elements needed to identify a threat actor:



An important prerequisite is to know about common attack tools and techniques and understand which traces they potentially leave in a victim's infrastructure. Starting from there, it is further important to understand what questions during the investigations of an incident can be answered by studying these artifacts. And eventually, it is key to understand how reliable the conclusions based on the investigation of certain artifacts are. In fact, some artifacts could be spoofed, certain traces faked to point at other parties than the real adversary. In a complex technical system this is realistic. However, the complexity of today's systems does it not only make hard for investigators to fetch the relevant data to achieve vital insights, but it also makes it hard for cunning attackers to consistently carry out false flags campaigns.

A prerequisite of cyber attribution is to discover the applied techniques, tools and procedures (TTPs). Based on that, the further goal is to identify the source of certain attacks that leads to the threat actor. Both topics, cyber-attack investigation (i.e., get to know what happened) and threat actor attribution (i.e., get to know who it did) aims to serve as a basis for actions in law enforcement and national security (such as cyber war or terrorism).

There is a wide range of literature on this topic with different approaches. It is often a mix of technical attack analysis and threat actor profiling, that sometimes leads to confusion. They highlight that not only malware samples and their specific properties (such as compiler settings, language settings, certain re-occurring patterns and the like) are useful, but also information available outside the actually attacked infrastructure, including data on the Command & Control infrastructure. The latter includes knowledge of what IP addresses have been used, what domain names and registration information of these domains. This boils down to payment information for the referenced domains. Eventually comes up with a categorization of data which distinguishes between physical persons, virtual personas, campaigns and infrastructure and tools.

The important thing to keep in mind is that attributing an attack to a specific group is usually difficult, and attribution can rarely be confirmed. Indicators may be reuse of malware or parts of malware, but there is no guarantee that some other group did not get access to the source code in some way, possibly through sharing or buying on the black market. Language and encoding may also play an important part in finding which country or region an APT comes from and may aid in attribution.

The approach to attribution that is beginning to be followed is to adopt a perspective where attribution represents the identification or classification of an incident to a given entity where entity is a flexible identifier ranging from “how-centric” attribution, linking observations to clusters of similar behaviors or TTPs, to very specific “who-focused” attribution, referencing a specific person or organization, multiple possibilities emerge.

Furthermore, the attribution phase is indispensable because it can aid in determining preventive actions, likely targets, and enable prosecution.

If a major corporation know they are being targeted by a known threat actor, they might be able to learn about this threat actor’s methods and better defend themselves against attacks. Some threat actors may be associated with specific malware, IP addresses, domains, attack vectors, their tactics could be sabotaging, i.e., through DDOS attacks, or theft of business secrets, financial data etc.

Knowing typical attack vectors for specific APTs may be helpful in trying to match the techniques used in one or more attacks against the same victim to one specific threat actor. A company that suffers financial loss due to a cyber-attack might want to take legal action to recover some of the cost, which is a motivation for finding out who exactly is behind an attack.

Problems in the Attribution

The problems with cyber attribution form a labyrinth that continues to trouble all those involved in cyber defense and wider security.

The challenges determining what has taken place, to whom and by whom is a process that lacks repeatability and often any clear solution. Nonetheless, the value of attribution makes it an indispensable exercise on which to concentrate resources. Without the ability to tie a cyber-attack to an individual, group or Nation State, there can be no political or legal enforcement of regulation or counteraction.

This represents a huge limitation on international relations where cyber activity continues to grow, influencing diplomacy and conflict. What some may consider a technical investigation has, therefore, shown itself to be a major geopolitical problem.

Of course, in addition to the many intrinsic complexities present in the activity of attribution, the intelligence analysts have to face the deception tactics that are implemented by the attackers in order to avoid being associated with their cyber-attacks. These deception tactics are generally referred to as false flags.

False flags are a longstanding military deception strategy, originating back to naval skirmishes where the flag of a ship was concealed or modified to look like someone else. The scenario is as follows: Country X uses tactics and equipment usually employed by Country Y to attack or provoke Country Z, so Country Y gets the blame and Country Z's attention is diverted from Country X, which allows Country X freedom of maneuver to engage in other time or space. Engaging in combat dressed in a uniform other than your own country's is a no-no under the Hague Convention, but the concept of false flag has been expanded to the scenario where Country X internally attacks or subdues its own citizens, while acting as another country or group motivated by the notion that a political cause will gain support with such an action.

In the cyber field, false flags refer to tactics applied by cunning perpetrators in covert cyber-attacks to deceive or misguide attribution attempts including the attacker's origin, identity, movement, and exploitation. It is typically very hard to conclusively attribute cyber-

attacks to their perpetrators and misdirection tactics can cause misattribution (permitting response and counterattack, which can lead to retaliation against the wrong party).

Amongst other factors, the use of 'false flags', where an attacker pretends to be someone other than themselves, is a tactic to 'frame' other threat actors. A false flag operation could be as simple as malicious 'marketing', inserting imagery appearing to show another threat actor claiming responsibility. It could also be as simple as inserting other languages into payload headers or malware.

Though the deep treating of the false flag's tactics used by adversaries is out of scope in this work, in the following are reported few examples of known cases of false flag:

- From 2012, Iranian hackers used Arabic rather than Farsi when attacking US banks, while suspected North Korean state-sponsored Lazarus group is often known for attempting language imitation.
- And in 2016, security firm CrowdStrike identified the GRU as the spy agency behind US-targeted false flag operation, this time the hacking of the Democratic National Committee and later Hillary Clinton's presidential campaign. The Fancy Bear hackers responsible had hidden behind fronts like a Romanian hacktivist named Guccifer 2.0, and a whistleblowing site called DCLeaks that distributed the stolen documents
- Russian military spies hacked several hundred computers used by authorities at the 2018 Winter Olympic Games in South Korea, according to U.S. intelligence. They did so while trying to make it appear as though the intrusion was conducted by North Korea.

The distinction of groups into Nation State and Non Nation State (in particular, eCrime group) is made extremely complex due to several factors including:

- Same groups can act at different times both as Nation State and as eCrime
- eCrime groups that collaborate, or reuse tools made by nation-state actors
- Nation State groups that use tools or follow motives specific to eCrime groups
- Etc.

By way of example only, some examples are given below:

- APT17 is a China-based APT group that has reportedly been responsible for a number of network intrusions against U.S. and Southeast Asian government entities, defense industries, law firms, information technology companies, mining companies, and non-governmental organizations. In July 2019, a hacking group calling themselves Intrusion Truth claimed that three members of APT17 (also known as Deputy Dog and Axiom) are associated with the Jinan Bureau of China's intelligence agency (the Ministry of State Security - MSS). Based on their findings, Intrusion Truth believes that APT17 carries out

on-demand hacking operations for the MSS. What makes this story even more interesting was the discovery that APT17 has simultaneously targeted Chinese citizens for financial gain according to documents provided by Intrusion Truth on which APT17 has circulated a "Price List" of data it has been actively acquiring from Chinese targets to sell for profit among the hacking community in China.

- According to FireEye, Chinese state-sponsored threat group APT41 has spied on global technology, telecommunications, and healthcare providers for the Chinese government, while also targeting video game companies and cryptocurrency funds for profit. Uniquely among tracked China-based actors, APT41 deploys non-public tools that are typically aimed for espionage campaigns. In particular, APT41 has targeted East and Southeast Asian video game distributors as well as their popular online games, even those with sizable Chinese markets, to manipulate virtual currencies and steal source code. FireEye, based on the employment of the same malware used in financial and state-sponsored activity, assesses with 'moderate confidence' that it operates as a group of contractors rather than as state employees who would be subject to greater scrutiny and less likely to operate independently of the MSS. Outside of state-sponsored activities, some of these contractors conduct business in underground marketplaces, advertising their skills and services.

- Lazarus Group has been linked to some of the most notorious cyberattacks in recent history, and some researchers have suggested that it may be backed by the North Korean government. In the past few years, the group has carried out several heists at traditional financial institutions and cryptocurrency exchanges around the world. Lazarus Group's activity dates back to 2009, with some analysts suggesting that the group has been active since as early as 2007. The group has been linked to some of the most notorious hacks in history, including the 2014 attack against Sony Pictures Entertainment, the 2016 Bangladesh Bank heist, and the 2017 WannaCry ransomware outbreak. In late 2015, Lazarus Group began to move away from the use of DDoS and wiper malware in their attacks and began to experiment with compromising financial institutions and carrying out SWIFT heists – that is to say, successfully initiating and cashing out fraudulent SWIFT transfers. This also represents a possible change in motivation - pursuing financial gain for the first time. Since that time, Lazarus has continued to target financial institutions with the goal of carrying out SWIFT heists. In recent years, targets included financial institutions in the US, Mexico, Brazil, Chile, Venezuela, Colombia, Uruguay, UK, Denmark, Poland, Turkey, China, Taiwan, and Hong Kong. Lazarus Group also targets cryptocurrency exchang-

es, with Chinese firm 360 Security linking the theft of funds from cryptocurrency exchanges Etbox, Biki, and Dragonex to Lazarus Group. Much of Lazarus Group's original targeting has historically focused on South Korea and the United States. With time, however, the group has displayed more opportunistic targeting, compromising entities from around the globe. This shift in targeting is in line with Lazarus Group's shift towards pursuing financial gain. Lazarus Group is considered highly sophisticated and adaptive. Some analysts have suggested that the threat group may interact with Russian-speaking cyber criminals due to their use of crimeware products such as Hermes ransomware.

- By the end of 2016, GRU hackers began to shift their tactics. In December of that year, analysts at the Slovakian cybersecurity firm ESET noted that the GRU hackers they called Telebots, also known as Voodoo Bear or Sandworm, used both hacktivist and cybercriminal fronts in their data-destructive attacks on Ukrainian networks. In some cases, they found that wiped computers displayed a message that said, "WE ARE FSOCIETY, JOIN US" in a reference to anarchic hacktivists from the television show Mr. Robot. But in other incidents around the same time, ESET found the hackers demanded a bitcoin ransomware payment.

Connections between Nation State and eCrime Threat Actors

As Mieke Eoyang (deputy assistant secretary of defense for cyber policy) said, "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".

The point of greatest interest is no longer the distinction between the skills and technical characteristics of the tools used by the Nation State groups compared to the eCrime groups, but the use of the latter by the Nation States. One of the recent and most significant examples of the use of eCrime groups by the Nation State ones is the use of Ransomware as a smokescreen for Nation-State Sponsored espionage operations.

A clear distinction between the different levels of connection that can exist between states and cyber criminals was proposed by Recorded Future in a recent article. Although the exemplification of the different levels of connection has been applied to Russia and its cyber-criminal ecosystem, we believe that the proposed distinction can be applied to any state.

Recorded Future identified three types of links between the Russian intelligence services and the Russian criminal underground based on historical activity and associations.

Based on an understanding of this historical context and considering the current cybercriminal and Russian government landscape, Recorded Future has classified the activity observed in this eco-system into three major categories:

- Direct associations are identified by precise links between state institutions and operators; an example of this is Dmitry Dokuchaev, a major in the Russian Federal Security Service who was recruited after working as a cybercriminal.
- Indirect affiliations occur in cases where a direct link cannot be established, but there are clear indications that the Russian government is leveraging resources or personnel for their benefit; an example of this is the Russian government's likely use of the Game Over Zeus botnet for espionage or DDoS attacks by "patriotic hackers" during military conflicts.
- Tacit agreement is defined as the overlaps in cybercriminal. activity, including targeting and timing, that benefit Russian state interests or strategic goals; such activity is conducted without direct or indirect links to the state but is allowed by the Kremlin, which looks the other way when such activity is conducted.

Direct Links refers to the direct intersect between cybercrime and the Russian special services, either through coercive or willing recruitment, where:

1. Willing recruitment occurs when individuals interested in supporting Russian government interests voluntarily seek to engage in efforts that support the state
2. Coercive recruitment occurs when the Russian government observes a skilled and successful malware coder on underground forums, arrests them for their activities, and presents them with two alternatives: prosecution and jail time or cooperation and a paycheck.

Another example of direct association occurs in cases in which the Russian intelligence services establish underground forums by which they can recruit participation from criminal threat actors ad-hoc, which enables the Kremlin to surge effort for specific purposes. Some forums may take the form of overt criminal forums, which also allows intelligence services to spot talent for recruitment.

The individuals outlined in this section have been reported as engaging in cybercriminal or financially motivated activity for personal gain and also have what we believe to be direct links to the Russian state, through politicians, the Kremlin or Russian intelligence services.

Indirect Affiliations refers to the cases where the state may not directly employ individuals from the criminal hacking ecosystem but may use their infrastructure to further Rus-

sian government interests. Additionally, “patriotic hackers” may conduct actions that benefit the state but are not directly linked to any Russian government or intelligence service entity. As example you can consider the DDoS attacks targeted Estonia’s government, news, banking, and telecommunications online resources occurred between April and May 2007.

Russian intelligence agencies have used criminal commodity malware to obfuscate their activities and make attribution more difficult. They have used criminal money laundering networks and bullet proof hosting to obfuscate the movement of funds and sponsorship of disruptive activities. They have also used networks compromised for criminal purposes to search for sensitive data and credentials to advance espionage activities and targeting against both domestic opposition and Western entities and governments.

Tacit Agreement refers to the cases whether or not there are connections between Russian authorities and cybercriminals becomes an uncertain point. Cybercriminals are widely known both inside Russia and abroad, and aside from pursuing the few individuals who have targeted entities inside Russia or who have crossed some sort of political line, Russian authorities have done little to try to disrupt the Russian-language criminal ecosystem.

The Kremlin’s muted response to cybercriminal activities originating from within Russia has nurtured an environment where cybercriminal organizations are well-organized enterprises. Until the Russian government decides to investigate and prosecute cybercriminals operating in Russia, it will continue to be a safe haven. Tacit agreements occur when the Russian criminal hacking ecosystem conducts activity independent of any directive by the state. This type of activity, and its timing, are consistent with Russian government strategic goals; although, there are no direct or indirect links within these efforts. The Russian government forms a tacit. agreement between the individuals conducting the attacks by not prosecuting them so long as they target “the right” entities and do not harm Kremlin interests.

Tacit links also occur when state-sponsored activity employs malware that looks like ransomware to provide plausible deniability, or complicate attribution, for cyber operations that benefit the state. These are not direct links as it is not clear whether the individuals employing this malware are members of the cybercriminal ecosystem, but the malware itself certainly takes its appearance or code framework from cybercriminal sources. It is not indirect as it is not the sharing of a criminal resource for state benefit. Rather, this tactic is emblematic of the state’s tacit approval of the cybercriminal ecosystem.

The use of commodity malware by Russian intelligence services almost certainly allows the Russian government to maintain plausible deniability in targeted intrusions, especially when nuances between the details of specific variants of malware are used. In addition to modifying and using commodity malware like Black Energy, Sandworm has also been linked to other intrusions which employed modified versions of ransomware in order to conduct disruptive and destructive intrusions.

Based on the longstanding relationship between the Russian intelligence services and the Russian cybercriminal ecosystem, it is almost certain that these connections will persist for the foreseeable future, and very likely continue to facilitate Russian intelligence service operations. As long as cybercriminals remain protected from domestic prosecution, are allowed to profit from their operations, and the Russian government maintains plausible deniability in their operations, there is no indication that such activity will stop, and malware procurement and infrastructure use via these relationships will continue.

References

1. “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”, Jason Healey, Atlantic Council.
2. “In Cyber, Differentiating Between State Actors, Criminals Is a Blur”, C. Todd Lopez, U.S. Department of Defense.
3. “Attributing Cyber Attacks”, Thomas Rid And Ben Buchanan.
4. “Strife Series on Cyberwarfare and State Perspectives, Part II – Deception in Cyberspace: Nation States and False Flag operations”, Amy Ertan, Strife.
5. “How to Recognize and Mitigate State-Sponsored Attacks”, Spiros Psarris, Reblaze.
6. “Commodification of Cyber Capabilities: A Grand Cyber. Arms Bazaar”, Analytic Exchange Program.
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.
9. “Blurred Lines Between State and Non-State Actors”, Council on Foreign Relations.
10. “Cyber Threat Intelligence for Banking & Financial Services. FOLLOW THE MONEY”, Blueliv.
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.
15. “Ransomware: Hope for the Best, Prepare for the Waorst”, ElecticIQ Threat Research Team.

Glossary

Adversary (or Threat Actor) is the individuals and groups posing threats.

Informational dimension is the content (generally referred to as information but can also include data and knowledge) that is at rest or in transit within cyberspace, including machine-readable content, numbers, text, audio, pictures and video.

Cyberspace is the global, virtual, ICT-based environment, including the Internet, which directly or indirectly interconnects systems, networks and other infrastructures critical to the needs of society.

Cyberactions are a collection of predominately illegal activities in cyberspace, carried out by non-state actors, causing damage or disruption, in pursuit of various political, economic, or personal goals.

Cyberspace operations (or *CyberOps*) are military activities employing cyberspace capabilities in order to achieve strategic objectives or effects in or through cyberspace.

Cyber-attacks are a subset of cyberspace operations employing the hostile use of cyberspace capabilities, by nation-states or non-state actors acting on their behalf, to cause damage, destruction, or casualties in order to achieve military or political goals.

Cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Cyberwar occurs when cyberattacks reach the threshold of hostilities commonly recognized as war by the international community and as defined by international law.

Malware is a type of TTP that represents malicious code. It generally refers to a program that is inserted into a system, usually covertly. The intent is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or otherwise annoy or disrupt the victim.

Physical dimension comprises the core technical infrastructure: networked hardware and software across land, sea, air and space that exploits the EMS to enable the flow of information between producers, consumers, audiences and systems.

Threat can be defined as one as one of the following items:

- an expression of intent to do harm, i.e. deprive, weaken, damage or destroy
- an indication of imminent harm
- an agent that is regarded as harmful
- a harmful agent’s actions comprising of tactics, techniques, and procedures (TTPs)

Threat Assessment is the process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Targeted attacks are attacks that target specific organizations or people within them. One class of targeted attack is Computer Network Exploitation (CNE) where the goal is to steal (or exfiltrate) confidential information from the target.

This is effectively espionage in cyberspace or, in information security terms, compromising confidentiality. The other class of targeted attack is Computer Network Attack (CNA) where the goal is to disrupt or destroy the target's operational capability. This is effectively sabotage in cyberspace or, in information security terms, compromising integrity and availability.

Tactics, Techniques, and Procedures (TTP) describes the behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Threat information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.

Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, system administrators, network administrators, or even normal users. Remote access tools (e.g., RDP) and network scanning tools (e.g., Nmap) are examples of Tools that may be used by a Threat Actor during an attack.

07 Il SOCIAL ENGNEERING

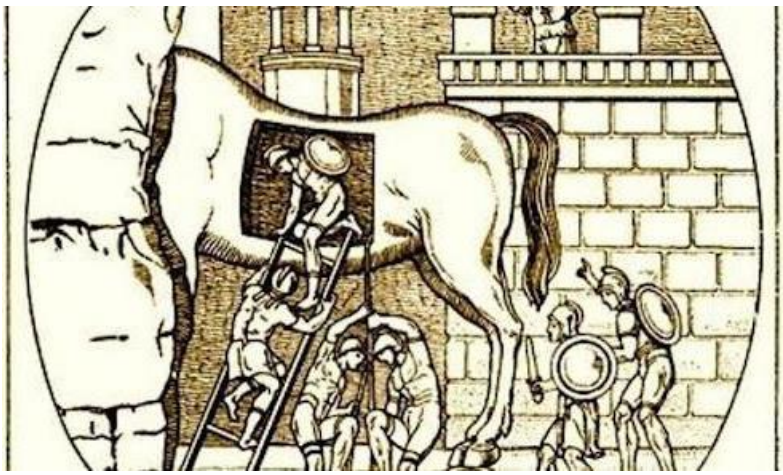
di GIUSEPPE MAIO

“La guerra si fonda sull’inganno”
[L’Arte della Guerra, Sun Tzu]

Le azioni criminali basate sull’ingegneria sociale possono concretizzarsi con o senza l’ausilio di tecnologia.

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 d'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 a 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 d'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 e 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 d'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 d'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 a 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 d'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 cybersecurity 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 im-

possessarsi, 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).

PAGINA BIANCA

08

PATCHING STRATEGY FOR NATIONAL SECURITY

di COSIMO MELELLA e CECILIA ISOLA

Having automated AI platforms and an intelligence-driven assessment on threats based on the patches to be distributed would allow organizations to increase their information on external threats through indicators that signal adversaries and attack surfaces.

Italy's growing exposure to cyber-attacks has made it essential to identify measures to protect networks and systems from new threats. Software security patch management is a security practice designed to prevent the exploitation of software vulnerabilities. A legislative discipline on patching and intelligence-driven methods could be some starting point to guarantee a safety standard sufficient to align the regulatory framework and the development dynamics linked to technological innovation.

The increasing exposure of Italy to cyber-attacks and security threats has made it essential to identify regulatory measures to protect networks and systems from new vulnerabilities and threats. Italy has transposed the Network and Information Security (NIS) directive, n. 1148 of 8 July 2016, in the D.lgs n. 65[1] of 18 May 2018 Which requires the Member States of the European Union to adopt security measures at a[2] national level.

NIS directive left each Member State the possibility of identifying the most suitable strategy to adapt to the new parameters identified. Nevertheless, unlike the other Member States, Italy has limited itself to transposing into D.lgs 65/2018 as already established by the NIS Directive[3].

Following the adoption of the D.lgs mentioned above, the Italian legislation on information security was strengthened by establishing the "National Cyber Security Perimeter", with the D.L. n. 105 of 21 September 2019, converted by Law n. 133 of 18 November 2019, and subsequent amendments and additions.

In a nutshell, the D.L. 105/2019 highlights the procedural methods and criteria for identifying all the parties to be included in the Perimeter (such as, for example, public admin-

[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.

istrations, public and private entities) and the security measures that the latter must adopt to protect their networks and information systems.

The purposes of the National Security Perimeter are, first, to strengthen the security standard of the networks, systems and Information Technologies services of the parties included in the Perimeter, as well as to ensure the “continuity” of all those services, considered essential, the interruption of which, even partial, could cause damage to national security.

Most of these elements have been addressed, at a national regulatory level, in the so-called "National Cyber Security Strategy", outlined previously concerning the NIS Directive and D.lgs 65/2018 in the so-called National Strategic Framework for Cyber Space Security adopted on 27.1.2014, further developed[4] by National Plan for Cyber Protection and Information Security of 31.3.2017 (still in force).[5] Whereas cyber threats are significantly changed compared to 2018, the European Commission has presented a revision proposal of the NIS Directive (future "NIS 2"). Therefore, updating the current security strategy with future new community dictates will be necessary.

After describing the current regulatory framework, both national and international, it is evident that today there is a lack of a standard and homogeneous discipline in information security, at least at a European level. Pending further legislative interventions, the best practices currently adopted by public and private companies and public administrations play a role of primary importance. This contribution aims to examine one of the main vulnerability profiles, patching, a primary aspect in consideration of the recent events that have seen various data breaches, mainly in the Italian health sector[6].

A legislative discipline on patching could constitute one of the starting points to guarantee a security standard sufficient to allow an alignment between the legal framework regulatory and the dynamics of development linked to technological innovation. Indeed, software vulnerabilities remain one of the critical risks facing businesses and critical infrastructures.

Applying patches, which are literally “pieces of code developed to address bugs identified within the software”, continues to be the most effective and widely recognized strategy for securing IT systems and against specific cyberattacks. However, despite the rapid release of security patches that address software vulnerabilities, most of the attacks were 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
[6]https://www.sicurezzaterrorismosocieta.it/wpcontent/uploads/2021/11/SicTerSoc14-Ransomware-strikes-back-Il-racket-informatico-continua-a-colpire-le-infrastrutture critiche-Cosimo-Melella-%E2%80%93-Emilio-Lo-Giudice.pdf

direct consequence of exploiting a known vulnerability for which the patch was already released[7].

Over time, this constant neglect has caused devastating consequences to be financial and[8] reputational losses due to the violation of confidentiality, the integrity of company data, and the unavailability of software. These findings can be primarily attributed to the complex problems inherent in applying security patches in organizational environments[9].

"Patching" refers to applying patches to the security vulnerabilities present in the software and systems implemented in an organization's IT / OT environment. It identifies the systems' existing vulnerabilities to acquire, test, install, and check for software security patches. Carrying out these tasks involves managing dependencies between multiple stakeholders and "sociotechnical" decisions that make managing software security patches a complex issue. This issue is exacerbated by the need to strike a balance between applying a security patch as quickly as possible and the need to patch a myriad of business and government applications[10].

Despite the criticality of software security patch management in the industry, this is still an emerging area of growing research interest that needs further attention. The “sociotechnical” aspects (an organizational process that concerns the management of skills and resources and the interaction of people with technical solutions, in which human interactions and technologies are closely coupled) of patch management have received relatively limited attention. In such a way, the management of patches depends significantly on the effective collaboration of humans with current automatic vulnerability detection systems. Understanding “sociotechnical aspects” are essential to identify prevailing issues and improve the effectiveness of the software security patch management process[11].

Software security patch management is a security practise designed to proactively prevent the exploitation of security vulnerabilities within an organization's software (and sometimes hardware). In general, a successful software security patch management process is essential for maintaining information systems' confidentiality, integrity, and availability (CIA). Such a process is a collaborative effort between multiple stakeholders: IT teams, security managers, system engineers and administrators, third-party software vendors up to customers and end-users.

[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
[10]https://www.rapid7.com/fundamentals/patch-management/
[11]https://www.crest-centre.net/socio-technical-factors-in-secure-software-engineering-methodologies- and-practices.

Therefore, the lack of collaboration, coordination, and communication between the various stakeholders represents one of the main obstacles to maintaining the security of managed software systems. Furthermore, the need to balance compliance with heterogeneous governance bodies and maintaining software security are recognized as key challenges in software security.

The rapid increase in the number and diversity of attack surfaces has led to an increase in the patch rate, disrupting existing processes. Furthermore, the limitations of existing tools were noted as a significant obstacle to achieving management targets. Among these there is the lack of a standard platform to integrate the heterogeneous tools used for management patches, the lack of accuracy, and the lack of scalability in the design/architecture of tools that create difficulties in patching multiple systems with different operating systems.

Due to the increased complexity and dynamic nature of software security patch management and the limitations of current technologies used in patching, the need for human skills is inevitable everywhere. However, due to human involvement in enforcement activities and decisions, the time to apply the patches has increased as it lends itself to numerous attacks. The risk of delays is further increased due to a lack of resources in terms of skills and knowledge, process guidelines and support for process automation.

An important point highlighted in the literature regarding the lack of support for process automation is that most existing solutions focus only on patch distribution but do not provide solutions that cover the entire process.

In addition, there is a significant gap in the skills required in managing software security patches, mainly due to the increased complexity of the patches themselves. IT system administrators are forced to spend hours monitoring multiple sources of information due to the lack of centralized platforms for retrieving and filtering information.

Modern sources of information range from security advisories (78%)[12], official supplier notifications (71%), mailing lists (53%), online forums (52%), news (39%), to blogs (38%) and social media (18%). Additionally, due to rapid patch release speeds, lack of automated validation[13], filtering, and classification of information based on organizational needs, there is a delay in patching, increasing the risk of one-day attacks[14].

[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.

One of the critical factors for increased exposure to malicious attacks is the lack of a comprehensive scanning solution, failing to understand the system clearly, leading to software vulnerabilities not being detected and system misconfigurations.

Existing approaches are generally one-size-fits-all and create difficulties in understanding the needs of the organizational context, and require considerable manual effort, particularly when applying patches in a virtual environment. There is an increasing need to have a standard set of rigorous metrics with information such as exploit dates for patches because existing vulnerability scanners depend on public vulnerability information, including only vulnerability disclosure dates. In addition, the technical and business context knowledge gap (for example, the need to apply security patches as soon as possible concerning prioritizing system availability) often result in patch priority conflicts between different teams[15].

One of the most pressing challenges in modern patch testing is an adequate automated testing strategy. The lack of automated testing can stem from several reasons, such as the difficulty in addressing patch dependency issues and the significant amount of human effort required to set up a test environment to simulate a “production” identical environment.

However, most current patch tests are performed manually to avoid the risks of unexpected system failures caused by harmful or malicious patches. Poor testing quality in manual patch testing increases the vulnerability exposure, as it frequently delays the subsequent patch distribution.

Another major challenge concerns the management of organizational constraints on system downtime. The lack of an adequate patch distribution strategy at runtime and organizational policies to avoid system downtime is a severe problem for timely patch installation. It is particularly challenging in critical infrastructure system contexts such as healthcare and public administration, for which downtime can create significant negative externalities. Most security patch management solutions in existing software lack an efficient distributed patch verification strategy, giving a limited overview of the system's patching status[16].

Additionally, most current patch checking methods are manual and require IT teams to manually inspect the application for signs of an attack and repair the damage if a threat is

[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.

found. It is a time-consuming and challenging task with no guarantee of finding any intrusion and undoing all changes exploited by an attacker. The need for this verification to be done as quickly as the patch is deployed adds to the complex, laborious and time-consuming manual verification, highlighting the lack of an effective automated verification strategy.

Over the years, several attempts have been made to integrate automation in the software security patch with management tasks. There must be a delicate balance between human intervention and security patch management automation. Automation allows professionals to enjoy the benefits of less manual effort. At the same time, human experience is required to take control of decision-making and tasks that cannot be fully automated due to the complexity of patches and the current limits of technology. Since patches can change the semantics of a program, a human will likely always need to be present to determine if the semantic changes are significant[17].

Organizations use many software products (e.g. operating systems or OS, software applications, tools, and platforms), increasing the challenges of patch heterogeneity. It was also noted that most of the reported solutions are only compatible with the Linux operating system, possibly because it is open-source, more accessible to configure than other operating systems, and that patches applied to many Linux distributions only result in minor changes compared to Windows patches. Hence, there is a growing need for an orchestrated platform that focuses on these heterogeneous tools.

In conclusion, having automated AI platforms and an intelligence-driven assessment on threats based on the patches to be distributed would allow organizations to increase their information on external threats through indicators that signal adversaries and attack surfaces. The use of intelligence tools on specific threats in the defence of public and private organizations would lead to a more accurate assessment of priorities by changing the current patch plan to prioritize those systems that could be attacked at a specific time. The result is intelligence-driven patch management that strengthens processes to thwart attacks.

Unfortunately, the reality is that the Italian public administration and part of the private sector do not have 100% visibility of their assets and vulnerabilities, so mapping external threat data to internal indicators to refine a patch plan could sometimes be of limited value.

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

However, there is still tremendous value in gathering information from global threat feeds and other external intelligence sources to determine whether parts of an organization or government are under specific attack. The MITRE ATT&CK framework is one such source.

Bringing MITRE ATT&CK data into any repository allows starting from a higher point of view with information about the opponents and associated tactics, techniques, and procedures. It can take a proactive approach, starting from an organization's risk profile, mapping those risks to specific adversaries and their tactics, delving into the techniques used by those adversaries, and then investigating whether these techniques could be successful or whether the related data were identified in the environment.

PAGINA BIANCA

09 E-MAIL SPOOFING DI ISTITUZIONI E P.A.

di MIRKO CARUSO

"In un'ottica di prevenzione del cybercrime 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 Cybersecurity Nazionale come il CSIRT Italia".

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 sì 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 compromise) e Phishing la fanno da padrona, tanto da arrivare a suggerire

[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.

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 d'intelligence, e nella prevenzione (intesa come blocco) di attacchi a tipologia Spoofing, Misrepresentation e Government Impersonation.

Analisi del contesto nazionale: dal 2009 a 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 e omogeneo livello di qualità, sicurezza e aggiornamento dei servizi e aggiornamento» 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.

[6] domini.agid.gov.it

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 utilizzate 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

[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

[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"

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 implementazione 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 d'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 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);

[13] https://datatracker.ietf.org/doc/html/rfc7489 - https://dmarc.org/

- reject: viene chiesto al mail exchanger ricevente di rifiutare la mail in ingresso che ha fallito il controllo DMARC.

```
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.

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 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 aperti[14] o compromessi e pertanto accessibili a chiunque per l'invio, massivo o mirato, di e-mail di phishing per conto

```
;; 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
```

di indirizzi mittente Istituzionali, in uso a Pubbliche Amministrazioni o ai Dipendenti di quest'ultime.

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 risulta-

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

no “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 “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.

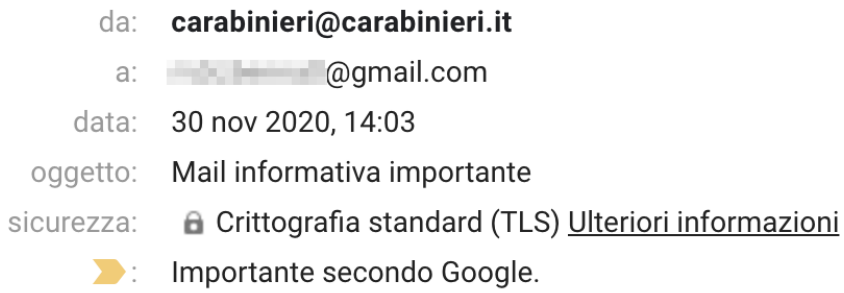


*Figura SEQ Figura * ARABIC 12: E-mail con mittente spoofed classificata come “Importante secondo Google”*

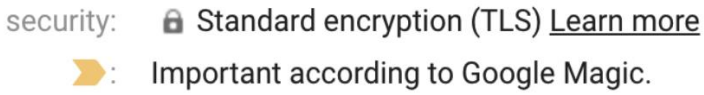


*Figura SEQ Figura * ARABIC 13: Dicitura “Important according to Google Magic” nella versione US di GMail*

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

[15] Parametro in uso nel contesto dell’e-mail marketing https://en.wikipedia.org/wiki/Cold_email#Email_deliverability.

quelle ad alto tasso di rapporti / comunicazioni da e verso il cittadino (basti pensare a comuni, enti locali, scuole, etc.) a 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 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 cybercrime l'implementazione di una "strategia Nazionale anti-spoofing" per i nomi di dominio .gov.it e Istituzionali consentirebbe di beneficiare

[16] Rispettivamente le policy *quarantine* e *reject*
[17] "Alias" di salute.gov.it

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 Cybersecurity 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.

PAGINA BIANCA

10 TOR, L'ANONIMATO E LA CIFRATURA TELESCOPICA

di FABRIZIO d'AMORE

"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"

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

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

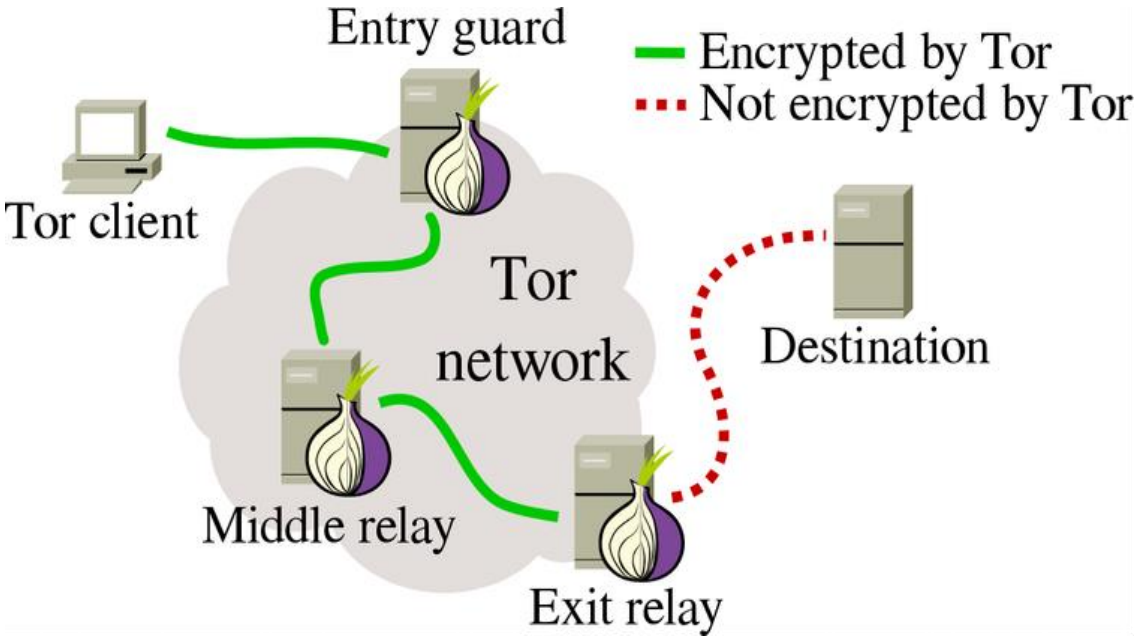


Figura 1. *Schema logico di funzionamento della rete Tor.*

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 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.

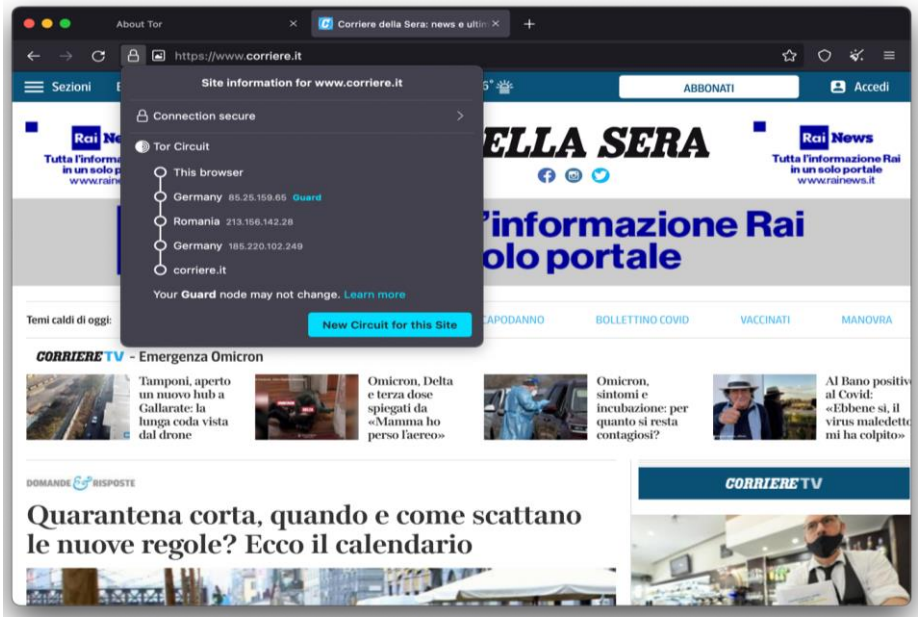


Figura 2. *Esempio di circuito composto da un relay in Germania, uno in Romania e un altro ancora in Germania. La destinazione vedrà dunque una visita proveniente dalla Germania.*

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 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/

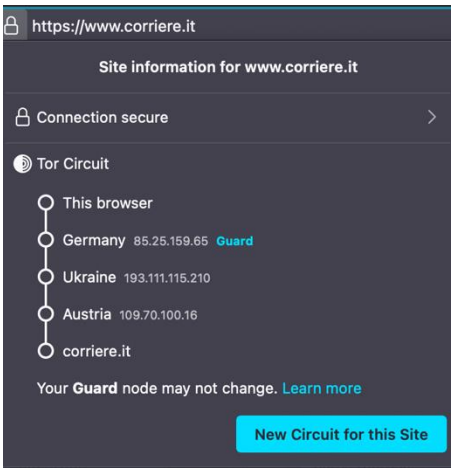


Figura 3. *Nuovo circuito per il sito www.corriere.it*.

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.

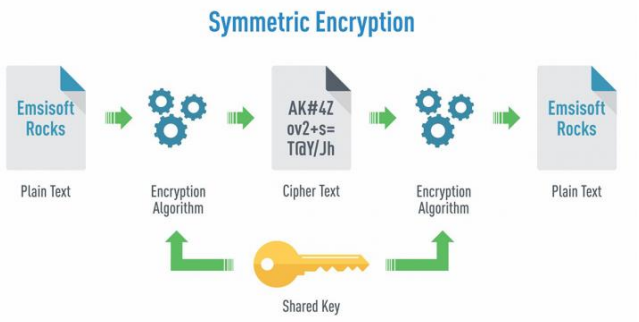


Figura 4. *Modello di cifratura simmetrica.*

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 (cipher-

[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

text). L'algoritmo di cifratura, oltre a prendere in input il plaintext, riceve anche una 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.

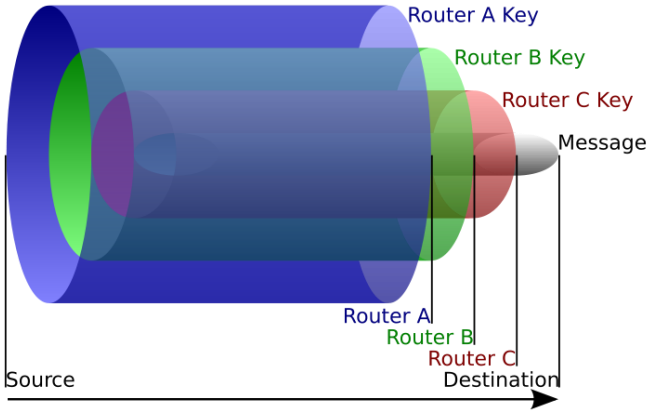


Figura 5. *La cifratura telescopica di Tor, dove A, B e C stanno per R_{in}, R_c ed R_{out}. Fig. tratta da https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Onion_diagram.svg/800px-Onion_diagram.svg.png.*

Indichiamo il client con C, la guardia con R_{in}, il centro con R_c, il punto di uscita con R_{out} e la destinazione con D. All'inizio delle operazioni C concorda, rispettivamente, una chiave k_{in} con R_{in}, k_c con R_c e k_{out} con R_{out}.[9] Le informazioni trasmesse da C sono cifrate dapprima con k_{out}, ottenendo un ciphertext, quindi cifrate di nuovo con k_c, ottenendo un altro ciphertext e infine cifrate con k_{in}, ottenendo un terzo ciphertext, che è quello che viene

[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).

[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).

effettivamente trasmesso. Si noti che se D prevedeva protocollo https, prima di cifrare con k_{out} 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 k_{in}, 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 k_c 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 k_{out}.

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]

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

[10] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (tecnico).
[11] https://www.nist.gov/
[12] https://en.wikipedia.org/wiki/Virtual_private_network

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 seguito, 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.

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 frequente-

[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.

[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.

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

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

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

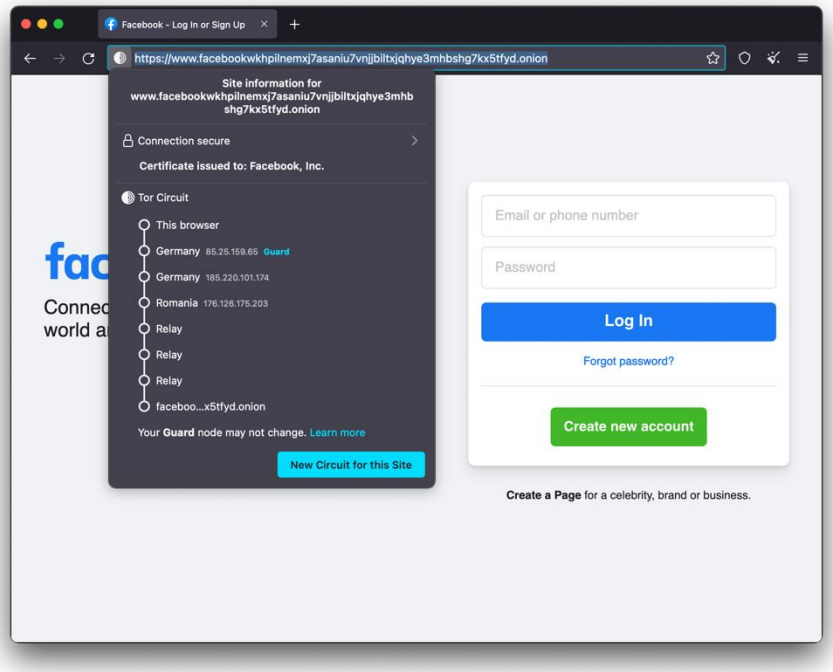


Figura 6. *Sito web "hidden" di Facebook, per consentire l'accesso anonimo.*

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 password, 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 6 ne è mostrato un esempio.

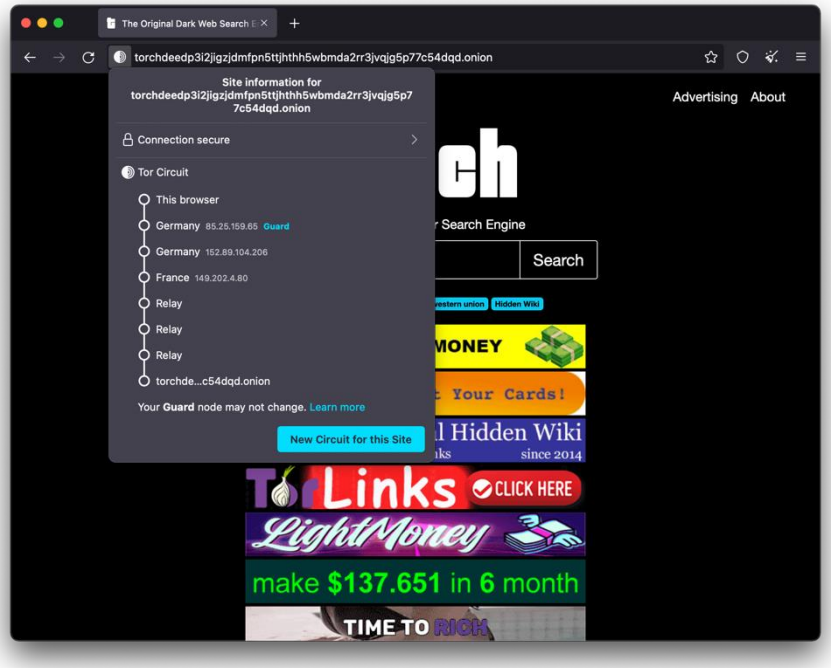


Figura 7. *Esempio di motore di ricerca per rete Tor.*

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

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

facilmente convincere l'utente della soverchiante presenza di siti illegali nel dark web; 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.

[21] Come Tail, v. https://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. https://www.kali.org/, molto sicura ed usata per attività forensi, intercettazioni di rete anonime, penetration testing e ricerca sulla sicurezza.

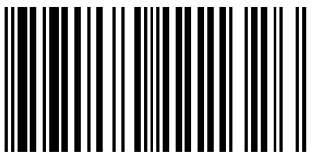
Commissione di Studi
Cyber Threat Intelligence & Cyber Warfare

"Le Prospettive della Cyber Intelligence"
Volume 1 – Anno 2022

SOCINT PRESS©

Società Italiana di Intelligence
www.socint.org

c/o Università della Calabria, Cubo 18-b, 7° piano
via Pietro Bucci
87036 Arcavacata di Rende (CS) - Italia
https://www.socint.org



9791280111326