Quotidiano
01-07-2024
Pagina 1+13
Foglio 1 / 3

La Verità

Tiratura: 56.786
Diffusione: 28.977

ANTONIO TETI
«I nostri dati sanitari sono un tesoro Sulla cyber sicurezza siamo in ritardo»

CAMILLA CONTI
a pagina **13**

L'intervista

ANTONIO TETI

«Sulla cyber sicurezza siamo indietro»

L'esperto, autore di «China intelligence», lancia l'allarme: «Nel Fascicolo sanitario elettronico un hacker potrà trovare informazioni di valore enorme. Pechino vuol conquistare Taiwan non con le armi, ma con la tecnologia»

di **CAMILLA CONTI**

Antonio Teti è docente di Cyber Intelligence, Cyber Security, It Governance e Big Data all'Università «G. d'Annunzio» di Chieti-Pescara e ha da poco fatto uscire il suo ultimo saggio, edito da Rubbettino, dal titolo *China intelligence* sulle tecniche, gli strumenti e le metodologie di spionaggio e controspionaggio del governo di Pechino. Il libro verrà presentato a ottobre alla Fabbrica del Vapore di Milano nei «salotti dell'intelligence» promossi da Vento & Associati insieme a iWeek e approfondisce le crescenti intrusioni dell'intelligence cinese nelle istituzioni e nelle realtà economiche dell'Occidente. In questa intervista abbiamo parlato di Cina ma anche di Italia, pensiamo ai rischi del nuovo fascicolo sanitario elettronico, e della necessità per tutti i Paesi di creare una cultura della sicurezza nazionale.

Quali sono le principali attività di cyber intelligence cinese all'estero?

«Prendiamo lo scontro tra Cina e Taiwan che si è spostato sulla cyberwar. Di recente c'è stato un attacco importante condotto da un gruppo di hacker, appartenenti al gruppo Apt (Advanced Persistent Threat) "Red Juliet", chiaramente proveniente da Pechino. L'attacco ha interessato più di 70 organizzazioni taiwanesi. Non solo aziende ma anche istituzioni governative come le ambasciate. Iniziato a novembre 2023 e condotto fino al mese scorso, aveva come obiettivo la rilevazione di possibili vulnerabilità hardware/software delle organizzazioni prese di mira. Sono stati oggetto di questi cyber-attacchi anche otto produttori di tecnologie digitali con l'obiettivo di trafugare informazioni "sensibili" e "classificate", insomma parliamo di cyber spionaggio. La tecnica è classica: identificare le fragilità dei dispositivi digitali e dei sistemi operativi utilizzati, penetrare le piattaforme e procedere con l'esfiltrazione di dati e informazioni. Un attacco simile è stato condotto da febbraio 2023 anche contro la più grande azienda produttrice di macchine per la realizzazione di semiconduttori, l'olandese Asml, che ha la taiwanese Tsmc tra i clienti principali. L'attività di cyber spionaggio è stata condotta da alcune aziende di proprietà cinese, come la Starblaze Technology e la Tongfu Microelectronics, che però sono operative in contesti geografici diversi, dagli Usa all'Africa, ma comunque controllate dal governo di Pechino».

Ma sono operazioni legali per i cinesi?

«La Cina ha attuato nel 2017 una legge sullo spionaggio, e nel 2023 quella sul controspionaggio, che impone ad ogni cittadino e impresa cinese di collaborare alla domanda informativa del proprio governo. Per la conduzione di attività di spionaggio e controspionaggio, la Cina può contare su una vasta gamma di agenzie, dipartimenti, uffici di polizia e strutture militari, senza considerare gli organi di partito, le strutture accademiche e di ricerca, le aziende private e quelle direttamente controllate da Pechino. Stiamo parlando della più mastodontica organizzazione di ricerca, assimilazione e selezione di informazioni operante su scala globale. Ma è sull'utilizzo delle tecnologie digitali finalizzate all'acquisizione di informazioni che Pechino sta indirizzando poderosi investimenti».

Come si distinguono le strategie di cyber intelligence cinesi, che potrebbero essere usate per avviare un'operazione militare su Taiwan, da quelle usate dai russi dopo l'invasione dell'Ucraina?

«Non bisogna confondere gli scenari. Se paragoniamo le metodologie di intelligence usate nel conflitto russo-ucraino alle metodologie di risoluzione della Cina commettiamo un errore grossolano. Pechino non ha alcuna intenzione di ingaggiare un conflitto bellico tradizionale con Taiwan ma sta conducendo una guerra sul piano economico e cyber. Se posso disporre di centinaia di società e strutture collegate ad apparati di intelligence a livello globale, potenzialmente ho già la vittoria in tasca. Se riesco ad acquisire il controllo di un numero significativo di aziende taiwanesi, con particolare riferimento a quelle operanti nel settore delle tecnologie, è come avere le chiavi della porta di casa. L'espugnazione di un Paese può essere condotta con la conduzione di una cyberwar in cui si intrecciano azioni di propaganda e disinformazione online, attacchi ai sistemi informatici, operazioni finanziarie condotte con le criptovalute, e in un futuro imminente, con l'utilizzo di piattaforme di intelligenza artificiale. Con la guerra cibernetica c'è un risparmio enorme di denaro e vite umane».

In Italia come siamo messi in termini di sicurezza cyber?

«In Italia scontiamo un grandissimo ritardo, con una forte responsabilità politica, sul piano della comprensione del cybercrime. La Acn, ovvero l'agenzia per la cybersicurezza nazionale, è stata istituita nel giugno del 2021, con ben dodici anni di ritardo rispetto alle equivalenti agenzie francesi e tedesca, entrambe create nel 2009. Partire con dodici anni di ritardo sulle tecnologie digitali è come partire tre secoli dopo. L'Acn sta conducendo un'attività di recupero straordinaria ma bisogna accelerare sul piano del reclutamento del personale, che deve arrivare ad una numerosità tale da consentire il corretto svolgimento delle molteplici attività di cui deve occuparsi l'Agenzia. Per fronteggiare i continui e quotidiani cyber-attacchi che subisce il nostro Paese, bisogna dotarsi di un "esercito" di tecnici informatici in grado di respingerli e soprattutto di comprendere quali saranno le nuove sfide per l'ecosistema digitale in cui siamo inseriti, tra queste proprio l'intelligenza artificiale. Il vero problema della sicurezza informatica è la mancanza di cultura da parte delle risorse

La Verità

umane».

Lo scorso 19 giugno è stato approvato il ddl 1143 che punta al rafforzamento della cyber sicurezza nazionale e alla prevenzione e repressione dei reati informatici. Siamo in corsa?

«Nel decreto, al terzo comma dell'articolo 8, è stata inserita la definizione di una figura importantissima, quella del referente per la cybersicurezza, di cui devono dotarsi tutte le pubbliche amministrazioni. I decreti legislativi 179/2016 e 217/2017 avevano individuato la figura del responsabile per la transizione digitale. Ora abbiamo questa nuova figura, semplicemente indispensabile per ogni tipologia di organizzazione. Anche in questo caso, ci siamo arrivati con qualche anno di ritardo, ma bene così».

In queste settimane si discute molto del fascicolo sanitario elettronico. Avere un database unico ci espone ad hackeraggi?

«Dipende. Le rispondo facendole un esempio: io sono un hacker, attacco il sistema informatico della sanità lombarda e mi esfiltro tutti i dati dei diabetici della Regione. Che valore possono avere quelle informazioni per un'azienda farmaceutica? Enorme. L'attacco lo conduco da server ubicati all'estero, prelevo i database e poi li vendo a una azienda farmaceutica multinazionale facendomi retribuire con delle criptovalute depositate in banche ubicate in paradisi fiscali. Riuscire a "tracciare" un'operazione del genere è quasi impossibile. È possibile utilizzare un sistema centralizzato di condivisione di dati, ma i livelli di sicurezza del Datacenter devono essere ai massimi livelli. Altro problema: noi possiamo realizzare una infrastruttura informatica sicura ma se qualche operatore lascia le sue credenziali di accesso alla piattaforma scritte su un foglietto sulla scrivania, si può consumare un evento di cybercrime drammatico. E non si tratta di un caso così raro. Torniamo quindi al problema iniziale: la formazione del personale e il costo dell'ignoranza informatica. Mi è capitato di osservare in alcune aziende l'uso di sistemi Plc, ovvero le piattaforme digitali fruibili per la gestione e controllo dei processi industriali. Bene, in alcune di queste aziende era stata progettata e realizzata la cybersicurezza dei server, delle workstation e della infrastruttura di rete, lasciando invece indifesi i sistemi Plc. Il problema risiede nell'interpretazione della sicurezza cibernetica: la cybersecurity non va vista come un centro di costo, bensì come un centro di valore».

A proposito dei problemi, c'è anche quello della disinformazione che si muove sui social.

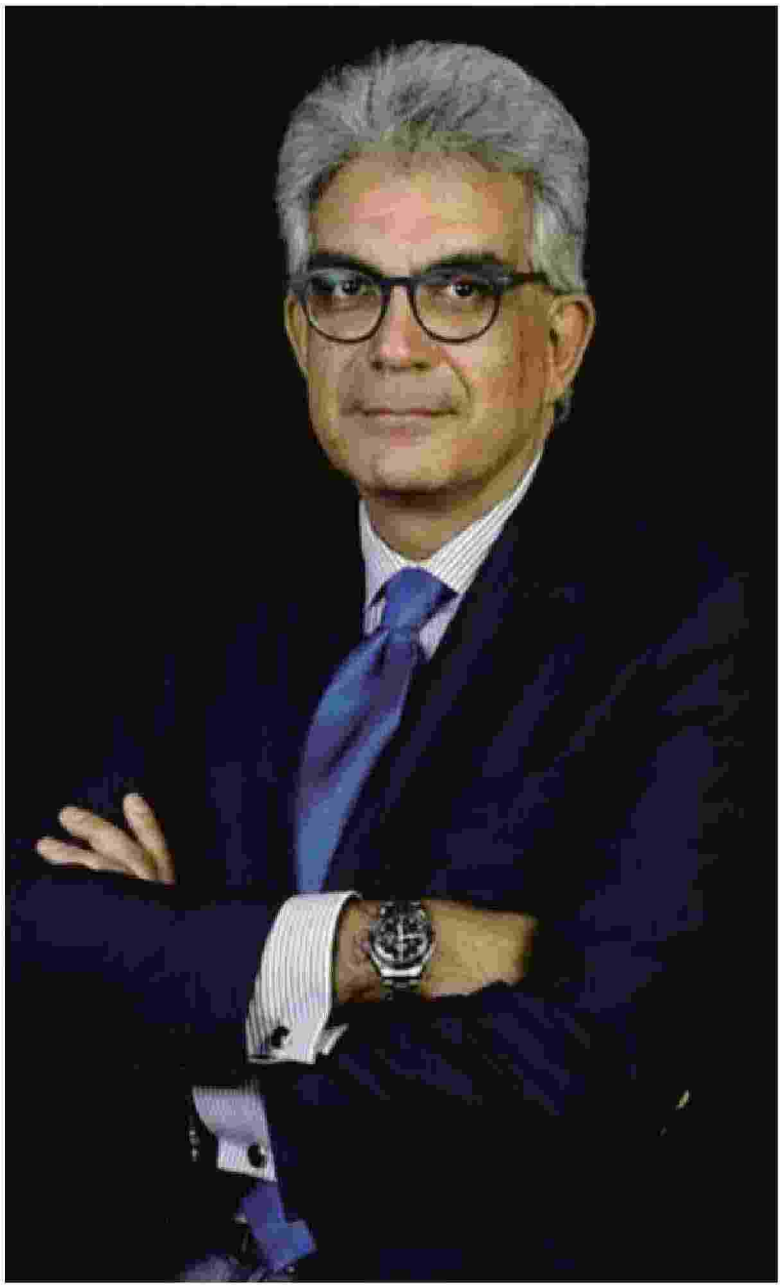
«Tutti oggi sono concentrati sugli attacchi informatici, ma abbiamo potuto notare che la maggioranza degli attacchi sono di tipo DDoS (Distributed Denial of Service), ovvero orientati alla negazione dell'erogazione di determinati servizi online. L'obiettivo è quello di rendere insufficiente il server per un determinato intervallo temporale, senza cancellare o esfiltrare dati. Sono attacchi impattanti ma che non provocano la perdita di dati o il loro trafugamento. Al contrario, sono le attività di disinformazione e propaganda online a preoccupare maggiormente. Dopo pochi mesi dall'inizio del conflitto russo-ucraino, abbiamo notato la creazione di fake profile che sono passati, nel giro di meno di due mesi, da qualche centinaio di followers ad oltre 1,5 milioni di seguaci. Un influencer come Khaby Lane o anche una popstar come Taylor Swift possono annoverare centinaia di milioni di followers. Significa esercitare il potere comunicativo di uno Stato. È qua si inserisce il tema dell'intelligenza artificiale. Qualche mese fa OpenAi ha sviluppato Replika.ai, una piattaforma in grado di realizzare una sorta di proprio avatar che in realtà può rappresentare un "agente di influenza" in grado di agire autonomamente grazie all'utilizzo di innovative capacità di apprendimento possedute. In altri termini, è possibile interagire sul piano di confidenza e aiuto. Parli a te stesso, ti sfoghi e lui ti risponde. Questo, in un contesto sociale in cui tendiamo sempre più a ridurre le interazioni dirette e ad aumentare le interazioni nel mondo virtuale. Se posso interagire con me stesso, ovvero con una figura di cui mi fido, dimentico che sto interagendo con una macchina. E quelle informazioni, quei dati che comunico alla macchina e all'algoritmo, vengono raccolti e usati da qualcun altro. Se raccolgo i dati di milioni di persone posso comprendere che tipo di comunicazione posso inoculare, posso fare quindi dei condizionamenti».

La maggior parte degli attacchi online mira a bloccare l'erogazione di servizi. L'intelligenza artificiale può creare «agenti di influenza»


La Verità
ristora INSTANT DRINKS
LA LE PEN È IN TESTA IN FRANCIA E MACRON SI SCAVA LA FOSSA
La Germania ha il suo Salis. E lo dà a Orbán
Caro Valditara, che merito c'è nella scena nuda?


L'intervista
ANTONIO TETI
«Sulla cyber sicurezza siamo indietro»

La Verità



DOCENTE Antonio Teti insegna all'Università «G. D'Annunzio» di Chieti-Pescara