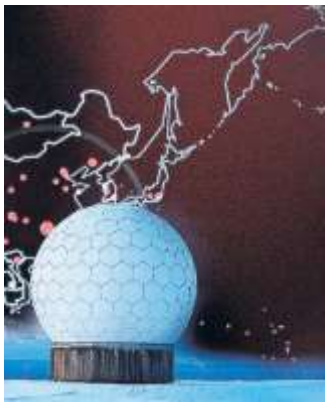
Handelsblatt

13.12. 2025

Prepararsi alla guerra cibernetica

Nel corso della più grande esercitazione cibernetica della NATO, 29 alleati si preparano all'emergenza in Estonia. L'alleanza militare sta persino sviluppando un proprio chatbot con intelligenza artificiale per le operazioni. Il quotidiano Handelsblatt era presente.



Di Carsten Volkery - Tallinn

La tensione è ancora palpabile in Ryly Bumpus. L'ufficiale dell'aeronautica militare statunitense si trova in una stanza isolata e altamente sicura a Tallinn, in Estonia, e spiega come distingue le notizie false da quelle vere nel bel mezzo di un conflitto bellico. Dice di diventare sospettosa nei confronti delle narrazioni che servono al nemico. La soldatessa di San Antonio, nello Stato americano del Texas, ha alle spalle una settimana stressante. Ha partecipato all'esercitazione NATO "Cyber Coalition", la più grande manovra informatica dell'alleanza difensiva. In condizioni realistiche, i 1300 soldati provenienti da 29 paesi NATO e sette paesi partner devono respingere una serie di attacchi alle infrastrutture critiche dei loro paesi. I pianificatori hanno inventato nomi fantasiosi per i protagonisti: la NATO deve difendere il suo alleato "Andvaria" da un attacco proveniente da "Habardus". Il teatro di guerra è un'isola fittizia chiamata "Icebergen" nel Nord Atlantico.

Nonostante l'alienazione diplomatica, tutti i partecipanti sanno chi sarebbe "Habardus" nel mondo reale: Cina, Russia, Corea del Nord. Su grandi schermi scorrono i titoli dei portali di notizie fittizi, gli attacchi sono seguiti in diretta 24 ore su 24, come nella vita reale. "Il traffico ferroviario in Germania si sta lentamente riprendendo dopo un attacco informatico", si legge ad esempio. Oppure: "Autista di un camion cisterna picchiato". I nomi dei media ("The Habardus Times", "OCC World News") sono inventati. I partecipanti devono confrontare le notizie e i post sui social media con le proprie conoscenze operative per ottenere un quadro accurato della situazione. In alcuni casi si tratta però anche di fake news, volte a confondere i soldati. L'obiettivo è quello di esercitare la comunicazione tra attori militari e civili, nonché tra gli alleati,

spiega il responsabile delle manovre, il capitano di fregata statunitense Brian Caplan. Gli autori degli attacchi informatici potrebbero infatti passare rapidamente da un Paese all'altro.

Non è un caso che l'esercitazione della NATO si svolga a Tallinn. L'Estonia non è solo un paese confinante con la Russia, ma anche un pioniere nella difesa informatica. Da quando nel 2007 il paese ha subito un grave attacco, la sicurezza della rete è presa molto sul serio. All'epoca, presunti aggressori russi avevano paralizzato ministeri, banche e media con cosiddetti attacchi denial-of-service, che sono durati diverse settimane. Oggi la NATO ha due avamposti a Tallinn, tra cui l'importante centro di ricerca e formazione per la difesa informatica (CCDCOE). Anche l'incubatore NATO per le tecnologie a duplice uso con sede a Londra, chiamato Diana, ha un ufficio regionale qui dal 2023. Nonostante le sue piccole dimensioni, con solo 1,3 milioni di abitanti, l'Estonia ha un importante ecosistema di start-up che, oltre a società miliardarie famose in tutta Europa come il fornitore di servizi di trasporto Bolt e la piattaforma di pagamento Wise, ha anche dato vita a un cluster di aziende di sicurezza informatica.

Nel 2016 la NATO ha dichiarato il cyberspazio un dominio a sé stante, accanto alla terra, al mare e all'aria. Nel frattempo si è aggiunto anche lo spazio come quinto dominio. Nel centro di comando militare dell'Alleanza (Shape) a Mons, in Belgio, è ora presente un centro operativo per la difesa informatica. In caso di emergenza, gli alleati possono richiedere qui una forza di intervento rapido composta da cyber-guerrieri. La manovra si basa su eventi reali Il “Cyber Range 14” di Tallinn, dove la NATO effettuerà le prove di emergenza all'inizio di dicembre, è gestito dal Ministero della Difesa estone. Qui gli Stati potrebbero svolgere le più grandi manovre del mondo, afferma il Chief Strategy Officer Allar Vallaots. L'infrastruttura è stata fornita dalla società statunitense Mandiant, una filiale del gruppo Google Alphabet. Dall'esterno, il Range sembra un normale edificio adibito a uffici. I visitatori devono consegnare tutti i dispositivi elettronici prima di entrare nell'area di sicurezza. All'interno li attende un ufficio open space con cubicoli, solo che le persone ai computer indossano tute mimetiche, il motivo mimetico delle armate, e possono essere attribuite a un Paese dalla piccola bandiera nazionale sul braccio.

I partecipanti alla manovra sono sottoposti a stress continuo per una settimana. Appena sembrano aver risolto un problema, ne emerge un altro. I pianificatori parlano di una “cascata”. In uno scenario, una delle due stazioni satellitari di terra viene messa fuori uso da un attacco malware. Allo stesso tempo, un sottomarino nemico si avvicina a cavi sottomarini di importanza strategica. I soldati devono decidere cosa fare e quali autorità informare. Gli scenari si basano in parte su eventi reali, afferma il responsabile dell'esercitazione Caplan. Ad esempio, nel febbraio 2022, parallelamente all'invasione dell'Ucraina, gli hacker russi hanno attaccato l'operatore satellitare americano Viasat. Di conseguenza, migliaia di modem in tutta Europa hanno smesso di funzionare e in Germania si sono persino fermate le turbine eoliche. Oggi gli alleati sono esposti quotidianamente ad attacchi ibridi. Dal punto di vista dei militari occidentali, la Cina rappresenta una minaccia maggiore della Russia nel cyberspazio e nello spazio, poiché Pechino dispone di una tecnologia superiore. Per questo motivo la NATO ha adottato una rigida regola “No Huawei”. I nuovi prodotti del gruppo tecnologico cinese non possono essere utilizzati in settori rilevanti per la sicurezza, mentre quelli esistenti vengono gradualmente sostituiti.

Tuttavia, sono i crescenti attacchi ibridi della Russia ad aver reso la protezione delle infrastrutture critiche una priorità della NATO. Secondo Frank Strewing, la collaborazione tra l'esercito e le aziende che gestiscono infrastrutture civili come satelliti o centrali ferroviarie è fondamentale. Il capitano di marina della Bundeswehr comanda il centro operativo congiunto delle fittizie “Collective Northern Defence Forces” durante l'esercitazione. Nonostante la retorica di Trump, gli Stati Uniti sono pienamente coinvolti “Se un apparato di comando ferroviario smette di funzionare, posso perdere la mia via di rifornimento”, afferma

Strewing. La difesa informatica è altamente complessa in termini di responsabilità e scambio di informazioni. Si inizia con la domanda: “Chi ci sta attaccando? Spesso non è facile scoprirlo in caso di attacco informatico”.

Nel centro di comando di Tallinn sono presenti solo alcuni membri di ciascuna delegazione nazionale. La maggior parte è collegata da casa tramite reti criptate. Da Bonn – spesso definita la “capitale tedesca del cyber” per la presenza delle autorità competenti – partecipano il Comando Cyber e Informatico (CIR) della Bundeswehr e l'Ufficio federale per la sicurezza informatica (BSI).

Le istituzioni statali godono di buona reputazione tra i colleghi. Secondo un collaboratore del Cyber Range, la Germania è leader nella difesa informatica dopo gli Stati Uniti e la Gran Bretagna. Il team statunitense di 50 persone proveniente da San Antonio è responsabile della difesa aerea durante l'esercitazione, poiché in genere un attacco informatico colpisce diversi domini. Gli Stati Uniti, che sotto la presidenza di Donald Trump a volte si comportano pubblicamente come un nemico dell'Europa, continuano a partecipare con pieno impegno a tali manovre. I soldati non vedono ancora il tanto invocato ritiro del loro principale alleato. La NATO ha tenuto la prima esercitazione “Cyber Coalition” 17 anni fa. Da allora, il numero dei partecipanti è aumentato notevolmente. Anche la fiducia tra gli Stati è cresciuta e oggi vengono condivise molte più informazioni, afferma un partecipante di lunga data. Il responsabile dell'esercitazione Caplan è d'accordo: “Siamo migliori rispetto al passato. Ma il rischio rimane sempre”.

Si stanno valutando attacchi preventivi contro la Russia? Recentemente, l'ammiraglio Giuseppe Cavo Dragone, presidente del Comitato militare della NATO – la massima autorità militare dell'alleanza – ha suscitato scalpore internamente quando ha riflettuto ad alta voce sul “Financial Times” riguardo a “attacchi preventivi” contro la Russia. La NATO starebbe valutando di essere “proattiva” nel cyberspazio, invece di limitarsi a reagire agli attacchi, aveva affermato Dragone. Bisogna analizzare più attentamente come ottenere la deterrenza, se attraverso la rappresaglia o un attacco preventivo. Non ha specificato cosa intendesse dire concretamente, ma le sue dichiarazioni sono state immediatamente condannate dal Cremlino come prova dell'aggressività della NATO.

A Tallinn, un ufficiale sottolinea ora che la NATO rimane un'alleanza difensiva nella sua visione di sé. Ma nel cyberspazio esiste una “zona grigia” tra attacco e difesa. In futuro, la NATO intende avvalersi anche dell'intelligenza artificiale (IA) per le sue operazioni. In una “sala sperimentale” a Tallinn, Alberto Domingo, direttore tecnico cyber dell'alleanza, presenta il suo ultimo progetto: un chatbot dedicato alle operazioni militari. L'IA, basata sul modello linguistico open source GPT OSS della società statunitense OpenAI, sarà addestrata in modo tale da poter analizzare i dati delle operazioni militari in corso e ricavarne raccomandazioni operative. “Vogliamo scoprire come l'IA possa supportare in modo affidabile le nostre missioni”, afferma Domingo. Alla fine, il chatbot dovrebbe essere in grado di fornire una raccomandazione d'azione ed elencare tutte le possibili conseguenze collaterali. Un problema: per addestrare il chatbot con dati segreti, deve essere scollegato da Internet e quindi rimane a un certo livello di sviluppo. Tuttavia, secondo Domingo, si può convivere con un modello linguistico vecchio di sei mesi. È più importante che venga alimentato con dati specifici della NATO. Tuttavia, il chatbot non è ancora abbastanza affidabile. Domingo non è ancora in grado di stimare quando sarà operativo. “Non sarà domani, perché stiamo ancora cercando il modello giusto”.