DigitEd
Il Sole 24 ORE Radiocor

DigitEconomy.24

24 settembre 2026

IL TEMA

AI E CYBERSECURITY: ATTACCHI SEMPRE PIÙ PERICOLOSI, COME CAMBIA LA DIFESA NELL'ERA DELLA GUERRA IBRIDA

Guido Crosetto, Ministro della Difesa

«L'ITALIA È PARTICOLARMENTE ESPOSTA A MINACCE IBRIDE, OCCORRE GIOCARE D'ANTICIPO»

L'Italia è «particolarmente esposta» alle minacce ibride e la Russia rappresenta oggi quella più «concreta e pervasiva». Di fronte a queste minacce «non possiamo limitarci a reagire dopo essere stati colpiti, dobbiamo essere in grado di anticiparle». Lo afferma Guido Crosetto, Ministro della Difesa nell'intervista a DigitEconomy.24, report in collaborazione con Digit'Ed, gruppo attivo nella formazione e nel digital learning. >> a pagina 2

Domitilla Benigni, CEO e COO del gruppo Elt

«TRA I SETTORI GUARDIAMO A SPAZIO E DRONI, NEL PIANO ANCHE ACQUISIZIONI MIRATE»

Guarda ai Paesi del Golfo e al Sud Est Asiatico; nel piano ci sono acquisizioni mirate di aziende di nicchia o start-up interessanti. Sarebbe «teoricamente appetibile» sul mercato ma ha un azionariato «solido e stabile». A tracciare le linee dell'orizzonte di Elt, da oltre 75 anni attivo nella difesa elettronica e nella gestione operativa dello spettro elettromagnetico è **Domitilla Benigni**, CEO e COO del gruppo. >> a pagina 3

Massimo Marotti, Direttore Strategia e cooperazione internazionale di Acn

«L'AI RENDE PIÙ PERICOLOSI GLI ATTACCHI, USIAMOLA PER DIFENDERCI MA CON CAUTELA»

L'impiego degli strumenti di AI «aumenterà la dimensione degli attacchi, ma allo stesso tempo è cresciuta la capacità di difesa precoce». A fare un bilancio dell'uso sempre più cruciale dell'intelligenza artificiale nella cybersecurity è l'Ambasciatore **Massimo Marotti**, Direttore del Servizio Strategie e Cooperazione dell'Acn. L'invito, anche riguardo agli attuali allarmi lanciati per rallentare lo sviluppo dell'AI, è di usarla «con cautela e spirito critico». >> a pagina 4

Guido Crosetto, Ministro della Difesa

«L'ITALIA È PARTICOLARMENTE ESPOSTA A MINACCE IBRIDE, SOPRATTUTTO DALLA RUSSIA, OCCORRE GIOCARE D'ANTICIPO»

Oggi, afferma il Ministro, «dobbiamo continuare a ridurre i tempi decisionali e integrare capacità civili e militari: nella minaccia ibrida, comprendere e reagire rapidamente è già essa stessa una capacità di difesa e deterrenza». Quanto al provvedimento che introduce, tra l'altro, lo Spazio cibernetico di interesse nazionale per la difesa, si prevede di attuare una volta completato l'iter parlamentare, le nuove misure, «a partire dal primo semestre del 2027». Quanto all'uso dell'intelligenza artificiale, Crosetto ricorda che si sta «realizzando il LIAD, Laboratorio di Intelligenza Artificiale per la Difesa: un AI Delivery Center per sviluppare e sperimentare algoritmi e prototipi. L'obiettivo è dotare l'Italia di una capacità autonoma di sviluppare, governare e integrare l'IA per la propria sicurezza e difesa».

Si parla sempre più esplicitamente di guerra ibrida: qual è oggi la minaccia concreta per l'Italia e da quali aree e attori proviene?
La guerra ibrida è una delle minacce più insidiose del nostro tempo perché si sviluppa prevalentemente sotto la soglia del conflitto aperto. Si può colpire un Paese attaccandone le infrastrutture, manipolando l'informazione, condizionando l'economia e indebolendo la fiducia nelle istituzioni e nelle alleanze. L'Italia, per posizione geografica, peso economico e appartenenza alla NATO e all'Unione Europea, è particolarmente esposta. La Russia rappresenta oggi la minaccia ibrida più concreta e pervasiva, ma anche Cina, Iran e Corea del Nord utilizzano strumenti economici, tecnologici, informativi e cyber. Di fronte a queste minacce, non possiamo limitarci a reagire dopo essere stati colpiti. Dobbiamo essere in grado di anticiparle, rafforzando prevenzione e deterrenza attraverso un approccio che coinvolga Difesa, intelligence, istituzioni, imprese e società civile e una capacità europea di mettere a sistema informazioni, strumenti e competenze.

La guerra ibrida non passa soltanto dagli hacker, ma anche da droni, sabotaggi, disinformazione e attacchi alle infrastrutture critiche. L'Italia dispone oggi di una catena di comando sufficientemente rapida per reagire a un attacco che coinvolga contemporaneamente rete elettrica, telecomunicazioni, trasporti e sistemi informatici?
L'Italia dispone di una catena di comando in grado di assicurare una risposta coordinata a crisi che coinvolgono infrastrutture fisiche e sistemi digitali. In caso di crisi sistemica, la cabina di regia politica fa capo alla Presidenza del Consiglio. La sfida è integrare rapidamente Difesa, intelligence, Agenzia per la Cybersicurezza Nazionale, Ministero dell'Interno, Protezione Civile, gestori delle infrastrutture strategiche, università e centri di ricerca. La Difesa sta rafforzando le proprie capacità, con l'istituzione del Comando Interforze Cyber Intelligence. Inoltre, nel disegno di legge recentemente depositato in Parlamento è prevista la creazione del Centro Interforze di Addestramento per il Combattimento e per il Contrasto alla Minaccia Ibrida. Dobbiamo continuare a ridurre i tempi decisionali e integrare capacità civili e militari: nella minaccia ibrida, comprendere e reagire rapidamente è già essa stessa una capacità di difesa e deterrenza.

Il provvedimento approvato ad agosto dal Consiglio dei ministri introduce tra l'altro nuove capacità e risorse, compreso lo spazio cibernetico di interesse nazionale. Che tempistiche si prevedono per vedere queste misure realmente operative?
Il provvedimento adegua lo strumento militare a uno scenario strategico e tecnologico profondamente cambiato. La minaccia cibernetica è già una realtà con cui dobbiamo confrontarci per difendere sovranità nazionale, infrastrutture critiche e sicurezza dello Stato.

L'Italia dispone già di una Strategia per l'AI della Difesa: ora dobbiamo trasformarla rapidamente in capacità operative, riducendo i tempi tra esigenza, sperimentazione e impiego e integrando Forze Armate, industria, start-up, Pmi, università e centri di ricerca

>> leggi l'intervista integrale sul sito

Domitilla Benigni, CEO e COO (Chief Operating Officer) del gruppo Elt

«TRA I SETTORI GUARDIAMO A SPAZIO E DRONI, NEL PIANO ACQUISIZIONI MIRATE, RESTIAMO STAND ALONE»

Non ritengo faccia bene alla competitività un'eccessiva concentrazione. Avere quattro-cinque grandi gruppi in Europa fa bene al sistema

Guarda ai Paesi del Golfo e al Sud Est Asiatico; all'orizzonte ci sono acquisizioni mirate di aziende di nicchia o start-up interessanti. Sarebbe «teoricamente appetibile» sul mercato ma ha un azionariato «solido e stabile». A tracciare le linee dell'orizzonte del gruppo Elt, da oltre 75 anni attivo nella difesa elettronica e nella gestione operativa dello spettro elettromagnetico è Domitilla Benigni, CEO e COO (chief operating officer) del gruppo della difesa elettronica, «nata come azienda media stand alone». A livello europeo Benigni ritiene che l'M&A non farebbe bene alla competitività. «Avere 4-5 gruppi in Europa fa bene al sistema». Quanto al business nell'attuale contesto geopolitico l'azienda può «capitalizzare il vantaggio di saper integrare la tecnologia tradizionale legata alla difesa elettronica» con l'uso della cybersecurity e dell'AI. Ma sempre, spiega Benigni che è anche presidente di Women4cyber Italia, con scenari che prevedano l'ultima decisione affidata all'uomo.

Come cambia il vostro business a fronte dell'attuale e sfidante contesto geopolitico?

Stiamo assistendo a un'evoluzione di tutti gli scenari che deriva dal cambiamento del contesto ma anche dalla tecnologia. Da una parte i conflitti non sono più quelli tradizionali ma sono ibridi, perché uniscono missioni operative tradizionali con nuove tecnologie, con largo utilizzo della cybersecurity. D'altra parte, la tecnologia non è più solo militare o solo civile visto che le minacce militari si intersecano con quelle civili. La tecnologia per gestirle sta infatti diventando duale, con la conseguenza che stiamo andando verso domini sempre più interconnessi in cui, per quanto ci riguarda, possiamo capitalizzare il vantaggio di saper integrare la tecnologia tradizionale legata alla difesa elettronica - nel nostro Dna da ormai 75 anni - all'utilizzo della cybersecurity e dell'Intelligenza Artificiale. Tutto, infatti, passa per lo spettro elettromagnetico: comunicazioni, sistemi di comando e controllo, sensori, droni, flusso di informazioni. Poter avere a disposizione e saper interpretare in maniera velocissima, in tempo reale, i dati è quello che consente oggi di "avere una superiorità" informativa.

Verso quali nuovi settori vi state espandendo?

Già copriamo con i nostri prodotti l'avionica, la parte terrestre e quella navale, compreso l'underwater, ultimamente stiamo spingendo anche sulla parte spaziale e sul dominio dei droni. Il drone è sia una minaccia sia un'opportunità perché è una piattaforma e, in quest'ottica, stiamo sviluppando sensori da mettere a bordo dei droni per attività di intelligence. Sul fronte delle minacce dei velivoli a guida remota invece vorrei ricordare che da oltre 10 anni abbiamo una capacità consolidata di sistemi contro i droni malevoli che sono una minaccia sempre più insidiosa,

Su quali aree geografiche puntate?

Siamo già presenti in 15 Paesi distribuiti in quattro Continenti, con più di 3mila sistemi operativi. Negli ultimi 10 anni abbiamo avuto una grande espansione geografica, con sostanzialmente due tipi di mercato. A cominciare da quello tradizionale italiano ed europeo, quest'ultimo legato ai programmi continentali, quali Eurofighter, Typhoon, Fremm e PPA. Menzione a sé il Gcap, uno dei più rivoluzionari programmi della Difesa, un progetto nazionale che coinvolge Italia, Uk e Giappone e che ci vede impegnati nel dominio che si occupa di comunicazioni e sensori. Ma abbiamo da sempre una grande spinta anche fuori dall'Europa dove realizziamo il 40% del fatturato

Tra le aree geografiche extra europee guardiamo al Golfo e al Sud Est Asiatico. Negli Stati Uniti abbiamo una società di scouting tecnologico, perché quello statunitense è un mercato piuttosto chiuso ad altri operatori del nostro settore. In generale esportiamo ovunque ci consenta la legge 185.

Siete pronti a giocare un ruolo nell'obiettivo di creare una difesa europea?

Il paradosso oggi è che la difesa europea non c'è ancora ma ci sono programmi europei con industrie che collaborano da 50 anni. In passato le partnership erano principalmente con Francia, Germania e Spagna, a cui di recente si sono aggiunti anche altri Paesi europei come, ad esempio, quelli del Nord Europa.

Sarebbe auspicabile creare gruppi europei più grandi attraverso l'M&A?

Non ritengo faccia bene alla competitività un'eccessiva concentrazione. Inoltre, ogni gruppo europeo è specializzato in specifiche aree. Avere 4-5 grandi gruppi in Europa fa bene al sistema, anche in America ci sono solo 4-5 gruppi, altrimenti non ci sarebbe competitività.

Siete appetibili sul mercato, riuscite a resistere nella vostra dimensione media?

Saremmo teoricamente appetibili perché l'azienda sta andando bene. Abbiamo chiuso il 2025 con ricavi pari a 304 milioni e un volume di acquisizione ordini di circa 700 milioni, superiore del 47% al 2024, con il settore che continua a crescere, ma abbiamo un azionariato molto solido e stabile con quote grossomodo paritetiche: la famiglia Benigni il 35,34%, Leonardo il 31,33% e Thales il 33,33%.

Infine, siamo nati fin dall'inizio con un taglio di media azienda stand alone, fattore che ci consente di avere possibilità che forse non rimarrebbero tali qualora facessimo parte di un gruppo più grande.

Guardate ad acquisizioni?

Sì, acquisizioni mirate sono nel nostro piano strategico, quindi ci guardiamo intorno. Se ci dovessero essere aziende di nicchia o start-up tecnologiche interessanti potrebbe essere molto vantaggioso operare qualche piccola acquisizione. Ad esempio, due anni fa abbiamo acquisito una realtà molto interessante in Abruzzo, Elt Hub, pensando di farci un laboratorio tecnologico ma poi abbiamo deciso di introdurre anche linee di produzione: oggi l'azienda sta crescendo a ritmo vertiginoso. Tra l'altro in Abruzzo stiamo assumendo, scegliendo risorse del territorio.

>> leggi l'intervista integrale sul sito

Massimo Marotti, Ambasciatore e Direttore del Servizio Strategie e Cooperazione dell'Acn

«L'AI RENDE PIÙ PERICOLOSI GLI ATTACCHI, USIAMOLA PER DIFENDERCI MA CON CAUTELA E SPIRITO CRITICO»

«La risposta della difesa è un misto di strumenti normativi, di regole di condotta, condivisione di metodi, pratiche, informazioni. Serve cooperazione internazionale»

Gli incidenti informatici sono in aumento, dobbiamo aspettarci nell'attuale contesto geopolitico un trend in crescita?
I numeri degli incidenti mostrano una tendenza in crescita ma è anche dovuta all'aumento della superficie che l'Agenzia controlla in attuazione della NIS2. Oggi i soggetti pubblici e privati che devono segnalare gli incidenti sono oltre 20.000.

Come cambia il panorama con l'uso dell'AI? La difesa dagli attacchi cyber diventa più difficile?
L'impianto attuale viene in effetti disarticolato dall'impiego dell'intelligenza artificiale perché se le tecniche, i metodi di attacco sono sostanzialmente gli stessi, cambiano la velocità, la dimensione e l'economia dietro gli attaccanti. Oggi, cioè, molti degli attacchi per i quali erano necessarie preparazione e sofisticazione, grazie a un modello di intelligenza artificiale, sono molto più semplici da realizzare. Inoltre, più gli attaccanti impiegano modelli di intelligenza artificiale, maggiore è la dimensione e la pericolosità degli attacchi.

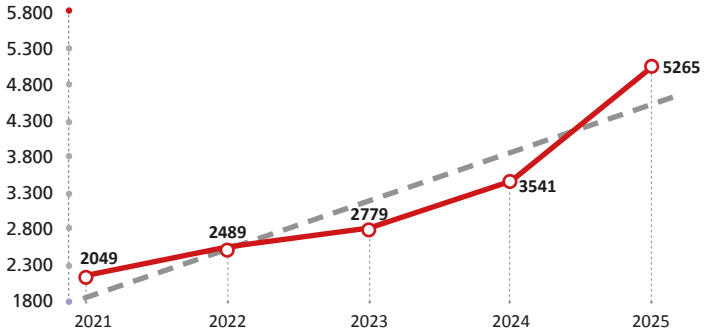
Il contesto normativo è adeguato?
Si è creata una constituency in materia, a livello nazionale e internazionale. Tuttavia, l'evoluzione della minaccia è stata costante in questo decennio e non sempre la norma è stata in grado di adattarsi all'evoluzione della tecnologia e dei comportamenti criminali. Sono stati proposti regolamenti, come il CADA (Cloud and AI Development Act), in corso di negoziazione. Sono tutti strumenti che servono a mettere in connessione ambiti di disciplina già previsti, da integrare alla luce delle interazioni con l'intelligenza artificiale e la cyber sicurezza.

Il Cada va nella direzione giusta?
Sì, anche se ci sono degli aggiustamenti da fare e noi li proporremo. È difficile prevedere ora quale sarà il risultato finale, però il metodo è quello che si sta seguendo da tempo: è un esercizio collettivo con i 27 Stati membri. Detto questo, vale comunque la premessa: la velocità delle tecnologie è superiore alla capacità di normare.

Come si può reagire allora?
Normalmente utilizziamo anche altri strumenti come la cooperazione internazionale e la ricerca di standard tecnici. La risposta della difesa, dunque, è un misto di strumenti normativi europei o nazionali, di regole di condotta, condivisione di metodi, pratiche, informazioni. Ad esempio, il *ransomware* è cresciuto in questi anni ma è cresciuta anche l'attività di collaborazione per difendersi dalle richieste di riscatto. Il gruppo informale di Paesi, la Counter Ransomware Initiative, promosso dagli Stati Uniti, ha raggiunto ormai 80 Paesi. Vi si scambiano informazioni sulle modalità con cui reagire al fenomeno e limitarlo. Vi collaborano l'Interpol, l'Europol, la Commissione europea.

>> leggi l'intervista integrale sul sito

Incidenti cyber per anno 2021-2025



© Clusit - Rapporto 2026 sulla Cybersecurity

I NUMERI DEGLI ATTACCHI INFORMATICI AL TEMPO DELL'AI*

Negli ultimi cinque anni gli incidenti hanno registrato una crescita costante, con una marcata accelerazione tra il 2024 e il 2025: da 3.541 a 5.265, pari a un incremento annuale del 48,7%, il più elevato mai registrato. In Italia l'aumento degli attacchi è stato appena inferiore: +42 per cento. Gli analisti di Clusit, che è l'Associazione Italiana per la Sicurezza Informatica, ritengono che questo aumento sia causato soprattutto dall'uso dell'intelligenza artificiale. Stiamo assistendo a un nuovo scenario in cui un attacco informatico non è più un semplice codice malevolo, ma un'entità adattiva che impara dagli ostacoli che incontra, grazie all'AI, modificando il proprio comportamento in tempo reale. Sono molti i campi nei quali l'AI può rendere più efficace un attacco come, ad esempio, per creare **campagne di *phishing***, realizzare audio o video *deepfake*, **sviluppare *malware* con modelli AI generativi**, che generano parti di codice sempre diverse per eludere gli antivirus. Ma le ultime frontiere della Bad AI sono ancora più preoccupanti. Ora è possibile usare l'AI per trovare in modo automatizzato le **vulnerabilità 0-day** nei sistemi e nelle applicazioni: la fattibilità è già stata dimostrata da Claude Mythos 5 che è un modello AI creato da Anthropic. E infine, abbiamo già assistito ai primi casi di reali attacchi realizzati con **AI agentica** come l'operazione di spionaggio informatico condotta nell'autunno 2025 dal gruppo sponsorizzato dallo Stato cinese noto come GTG-1002.

* Di **Giorgio Sbaraglia,** *Information & Cyber Security Advisor - Comitato Direttivo Clusit - Coordinatore scientifico dei Master "Cybersecurity e Data Protection" di Sole 24 Ore Business School*

Archivio interviste: www.digited.it/news **Osservatorio Digit'Ed - Sole 24Ore**