La Commissione Difesa ha svolto l'audizione del Ministro della Difesa Guido Crosetto nell'ambito dell'Indagine conoscitiva sulla difesa cibernetica

Audizione del 23 gennaio 2025

Guido Crosetto, Ministro della Difesa

- Il Ministro ha innanzitutto dichiarato che la **tecnologia diventa sempre più pervasiva e fondamentale per tutti gli aspetti della vita** (politica, economia, sfera privata etc.), e che l'insieme di strumenti tecnologici vecchi e nuovi creano il cyberspace. **Nel dominio cyber più che negli altri domini di operazione (terrestre, marittimo, aerospaziale) la sicurezza dello Stato è continuamente, ogni giorno, messa a repentaglio** da una dura competizione non solo tra nazioni ma anche tra attori non statuali.
- **In questo momento decine di attacchi cyber stanno accadendo ovunque**. Sia la sfera pubblica che quella privata, economica, industriale, dei trasporti, delle telecomunicazioni. Questi sono servizi vitali per ogni stato o nazione e per ogni organizzazione internazionale, ma anche per la vita stessa dei cittadini.
- Per la natura stessa del dominio cyber gli effetti non sono sempre riconducibili ad azioni palesi ed evidenti, gli attori non sono facilmente riconoscibili e perseguibili in accordo a norme statuali e costituzionali interne, o del diritto internazionale.
- **Nel dominio cyber è in atto senza soluzioni di continuità un conflitto caratterizzato da continui attacchi effettuati da attori malevoli difficilmente identificabili**. Si tratta di uno dei tanti vettori della c.d. guerra ibrida - sabotaggi di sistemi, sottrazione di informazioni, campagne di disinformazione mirate a distorcere la percezione di cittadini ed istituzioni.
- Le aggressioni cyber possono anche generare conseguenze concrete. Con l'evento cloud strike dello scorso luglio gli esiti sono stati devastanti e si è capito cosa vuol dire l'indisponibilità di un sistema di gestione computerizzata per il trasporto aereo nel nostro continente e non solo. Un impatto preoccupante ha evidenziato la vulnerabilità dei sistemi informativi anche quando non sono attaccati.
- Inoltre, l'attacco del collettivo filo-russo Noname057 che ha colpito siti istituzionali italiani e reti di trasporto sottolinea l'urgenza di **rafforzare la deterrenza contro minacce cyber interne ed esterne**.
- Oggi, quindi, per garantire la prosperità e lo sviluppo di un paese moderno e il benessere dei cittadini è necessario **preservare e difendere un utilizzo sicuro e libero dello spazio cyber di interesse nazionale**.
- Deterrenza significa tante cose, ma in sostanza significa avere la forza, la capacità e la prontezza, quando attaccati, di poter agire con rapidità ed

Ufficio Monitoraggio e Relazioni istituzionali
tel. 06.97790300
email: monitoring@utopialab.it

efficacia. Il modello di deterrenza della Guerra Fredda si basava sulla trasparenza delle capacità offensive: ogni attore conosceva la potenza dell'altro, garantendo così la stabilità attraverso il principio della mutua distruzione assicurata. **Nel contesto cibernetico contemporaneo, la deterrenza si basa su l'incertezza: l'esito di un attacco dipende dall'efficace difesa della vittima, dalla rapidità di reazione e dalla resilienza delle reti. Le operazioni cibernetiche non garantiscono un risultato certo**.

- Tale complessità è accentuata dall'asimmetria e dalla opacità dello spazio cibernetico. Un attore con risorse limitate come un gruppo terroristico può infliggere danni significativi ad infrastrutture critiche di stati molto avanzati. Le capacità offensive di un attore rimangono spesso celate fino al momento dell'impiego, alimentando un senso di incertezza che scoraggia potenziali aggressori.
- **Risulta quindi imprescindibile investire nella deterrenza cibernetica per garantire la sicurezza del Paese contro i rischi legati alla crescente sofisticazione delle minacce, rafforzando la resilienza e creando un effetto dissuasivo credibile**.
- Con il dovere di perseguire tali obiettivi, bisogna essere consapevoli che l'accelerazione dello sviluppo tecnologico, in particolare dell'IA e delle tecnologie quantistiche, sta ridefinendo la modalità con cui le minacce si manifestano nel dominio cyber.
- L'IA, infatti, condizionerà sempre di più gli equilibri internazionali andando oltre quello che possiamo immaginare focalizzato su due attori principali: Cina e USA.
- **L'IA si avvicina alla singolarità tecnologica, che descrive l'esplosione di intelligenza, ovvero il momento in cui l'IA supererà in modo irreversibile l'intelligenza umana**. Tale traguardo è più vicino di quanto immaginiamo e potrebbe generare scenari in cui le regole attuali sarebbero più difficilmente applicabili. L'accelerazione verso questo traguardo è aumentato dalla competizione commerciale e dalla ricerca di vantaggi strategici spesso perseguiti senza un'adeguata considerazione delle conseguenze.
- L'attuale quadro regolatorio (ad esempio il recente AI Act europeo) ha, per ora, indotto le aziende principali a non offrire le loro applicazioni in UE. Intanto, **altri paesi adottano approcci senza scrupoli, privilegiando lo sviluppo tecnologico a scapito di ogni considerazione etica**.
- L'IA, paradossalmente, è necessaria per mitigare i danni che essa stessa può generare. L'IA rende inoltre più sofisticate le minacce del cyberspazio.
- E' **cruciale sviluppare algoritmi di crittografia post-quantistica, produrre algoritmi valoriali con al centro principi etici, investire sulla centralità del dato. Il dato e la sua disponibilità, integrità e protezione sono temi centrali per il concetto di sicurezza nazionale nel senso più ampio**.

Ufficio Monitoraggio e Relazioni istituzionali
tel. 06.97790300
email: monitoring@utopialab.it

- La Difesa e la sua Cyber Academy possono aiutare a diffondere la cultura della cybersicurezza e la consapevolezza delle minacce a cui siamo esposti.
- La Difesa si fa da tempo promotrice di una condivisione strutturata ed efficace del quadro delle minacce; della definizione di procedure operative comuni con tutti gli attori istituzionali per fronteggiare eventi e incidenti di natura cibernetica; del consolidamento di capacità anche nel campo della R&D; dell'avvio di programmi di cooperazione; di definire la struttura più idonea per gestire e reagire a eventuali crisi cyber di bassa scala.
- L'attuale quadro impone una costante attenzione e preparazione. E' essenziale predisporre al meglio lo strumento militare quale presidio della sicurezza del Paese.
- Nel nostro Paese alcune cose sono state fatte negli ultimi anni: DL n. 82 del 2021, istituzione del Comitato interministeriale per la cybersicurezza, dell'ACN, del Nucleo per la cybersicurezza, DL 9 agosto 2022 n. 115, Legge 28 giugno 2024 n. 90, Strategia Nazionale per la Cybersicurezza, d.lgs di recepimento della NIS2.
- Si devono inoltre **rendere i prodotti ICT sicuri fin dalla loro produzione** e una costante condivisione degli scenari e degli attacchi, nonché la definizione di standard di sicurezza, anche per i beni militari.
- Per proteggere reti e infrastrutture critiche è necessario:
    - **due diligence**: obbligo per ogni stato di vigilare sul proprio cyberspazio
    - **denial**: esercitare minore per impedire e contrastare attacchi
    - **attribution**: capacità tecnica di risalire con alta probabilità agli autori di attacchi cibernetici
    - **punishment**: creare le condizioni per una legittimazione di contrasto culminante nell'applicazione di sanzioni concrete
- E' necessario:
    - **identificare lo spazio cyber nazionale** per la difesa e la sicurezza dello Stato
    - **arma cyber** civile e militare operativa e capace di intervenire
    - **centro per il contrasto della guerra ibrida** con capacità di comando e controllo
    - **condivisione di best practice**
    - **sviluppo di sinergie con il mondo dell'accademia**

Interventi

- **On. Bicchielli (NM)** - In merito alla collaborazione con il mondo accademico, ha chiesto quali rapporti di questa natura siano al momento attivi e in che modo questi possano accrescere le conoscenze anche del mondo istituzionale e politico.
- **On. Loperfido (FdI)** - Ha chiesto se potrebbe essere avviato un progetto pilota per la cyberdifesa a livello europeo.

- **On. Graziano (PD)** - Ha chiesto come si può realizzare una condizione di rafforzamento della cybersicurezza.
- **On. Mulé (FI)** - Ha chiesto se il ruolo della Difesa sarà quello di occuparsi di minacce di interesse della difesa o anche di minacce su altri settori e se la leadership sarà a tempo o per tipologia di minaccia. Infine, ha chiesto se si pensa che l'Italia coopererà con altri paesi europei e insieme alla Commissione UE.
- **On. Fassino (PD)** - Ha evidenziato il problema della PA, che non sa lavorare con temi interdisciplinari.

Replica

Guido Crosetto, Ministro della Difesa

- Il tentativo di una cooperazione con il mondo accademico è molto forte.
- Il pubblico impiego ha tempi che sono totalmente incompatibili per affrontare il mondo in cui viviamo.
- I dati saranno le miniere del futuro e il settore della cybersicurezza è fortemente competitivo: tutti cercano di avere una sovranità dei dati per essere più competitivi. Anche a livello europeo è difficile cooperare per questo motivo.
- Informare la popolazione in merito a tutti gli attacchi che avvengono non ha particolare rilevanza, più che altro è importante sensibilizzare sulle minacce e sui rischi.

Ufficio Monitoraggio e Relazioni istituzionali
tel. 06.97790300
email: monitoring@utopialab.it