Strategia Nazionale di Cybersicurezza 2022-2026

Mario Draghi

Le nuove forme di competizione strategica che caratterizzano lo scenario geopolitico impongono all'Italia di proseguire e, dove possibile, **incrementare le iniziative in materia di cybersicurezza**.

Dobbiamo **tenere fede agli impegni assunti nell'ambito delle organizzazioni** internazionali a cui l'Italia partecipa, anche tenuto conto dell'elevata qualità e dei massicci investimenti realizzati dai principali alleati e partner internazionali. È dunque necessaria una puntuale **rivisitazione nella concezione e nella visione strategica dell'architettura nazionale di cybersicurezza**.

Roberto Baldoni - *direttore ACN*

spero che la guerra possa finire domani ma quello di cui sono certo è che la guerra cyber non finirà

24 maggio 2022. Roberto Baldoni, insieme col sottosegretario alla Presidenza del consiglio Franco Gabrielli e la numero 2 dell'agenzia cyber Nunzia Ciardi, ha presentato il **nuovo piano nazionale per la cyber sicurezza,** 82 misure da realizzare nei prossimi quattro anni, **un investimento di 623 milioni** per difendersi gestire eventuali crisi migliorare le risorse tecnologiche e umane

quattro considerazioni imprescindibili

I recenti trend di attacco forniscono evidenze di **danni economici e reputazionali** per imprese, **blocco dell'operatività** di infrastrutture energetiche, **malfunzionamenti** di sistemi informativi impiegati da aziende ospedaliere e sanitarie, **diffusione di dati personali** che mirano a screditare figure pubbliche, giornalisti e attivisti politici, fino a metterne in pericolo, talvolta, l'incolumità.

i pilastri tecnici-operativi

i nuovi rischi

tecnologie impiegate, sviluppate e prodotte da grandi realtà aziendali, **talvolta controllate o, comunque, influenzate dai Governi** in cui hanno sede, con conseguenti possibili ingerenze nella catena degli approvvigionamenti, sia in termini di disponibilità sul mercato delle relative componenti, sia di affidabilità delle stesse

diffusione, attraverso lo spazio cibernetico, di fake news, deepfake e campagne di disinformazione che tendono a **confondere** e destabilizzare i **cittadini** di un Paese immergendoli in uno spazio informativo estremamente dinamico e orizzontale, caratterizzato da un insieme pressoché infinito di sorgenti di notizie che polarizzano le opinioni cambiando il modo in cui percepiamo la realtà

attacchi cyber dovuti a **cybercriminali, attivisti** o a campagne statuali coordinate, che sfruttano errori software, errate configurazioni, debolezze nei protocolli e umane, per **sottrarre dati o arrecare danni ai sistemi**, come nel caso delle campagne ransomware, le quali hann un impatto sull'erogazione dei servizi, anche essenziali di un Paese, sul suo PIL e sulla sua reputazione

le sfide da affrontare

Assicurare una **transizione digitale cyber resiliente** della Pubblica Amministrazione e del tessuto produttivo

Autonomia strategica nazionale ed europea nel settore del digitale

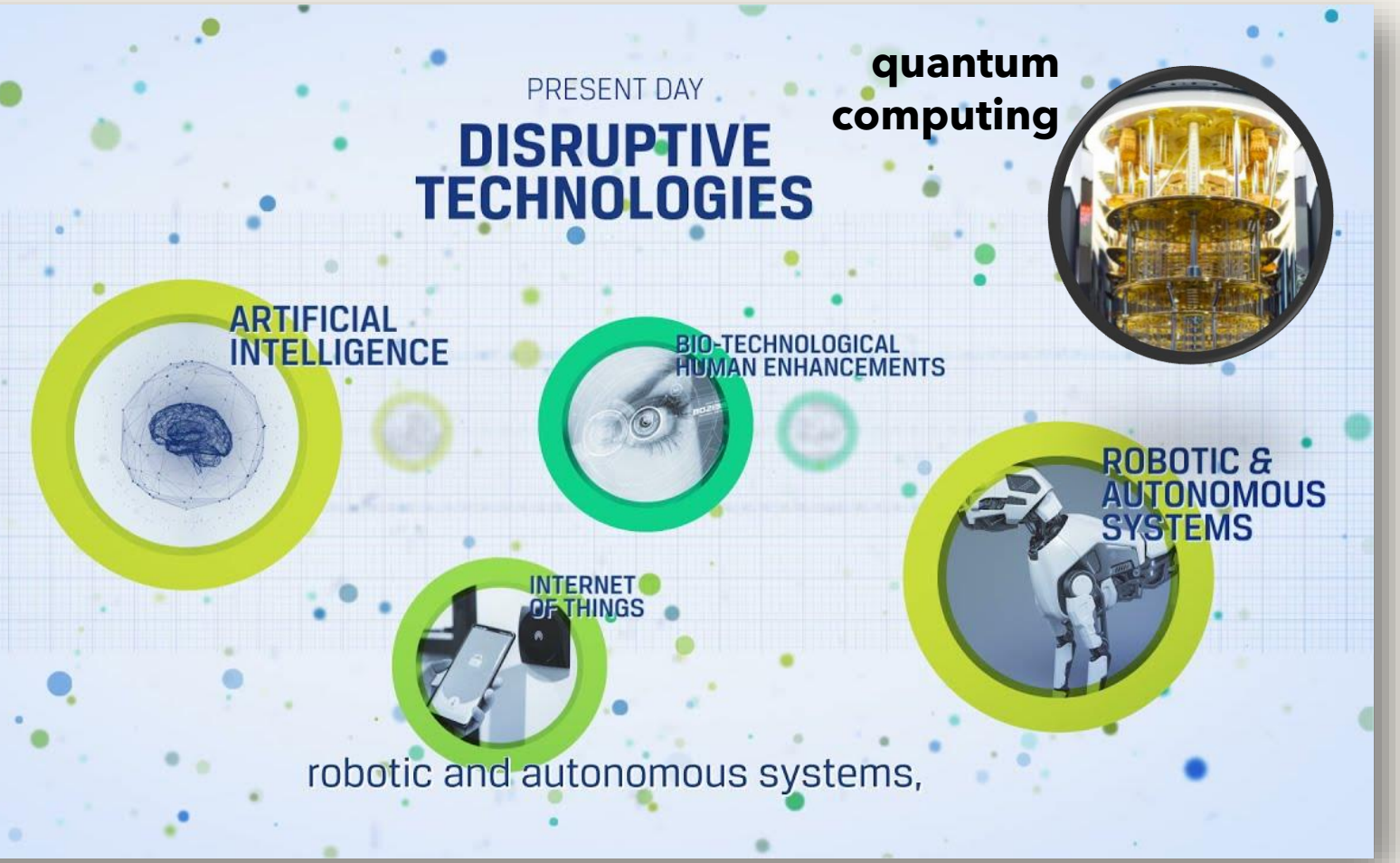
Anticipare l'evoluzione della minaccia cyber

Gestione di crisi cibernetiche

Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida

Autonomia strategica

A livello UE, l'eccessiva **frammentazione e competizione** tra gli Stati Membri ha costituito, fino ad oggi, un **grosso ostacolo** allo sviluppo di tecnologia "made in EU" e alla creazione di grandi aziende di erogazione di servizi digitali; un esempio è quello degli **antivirus russi Kaspersky**



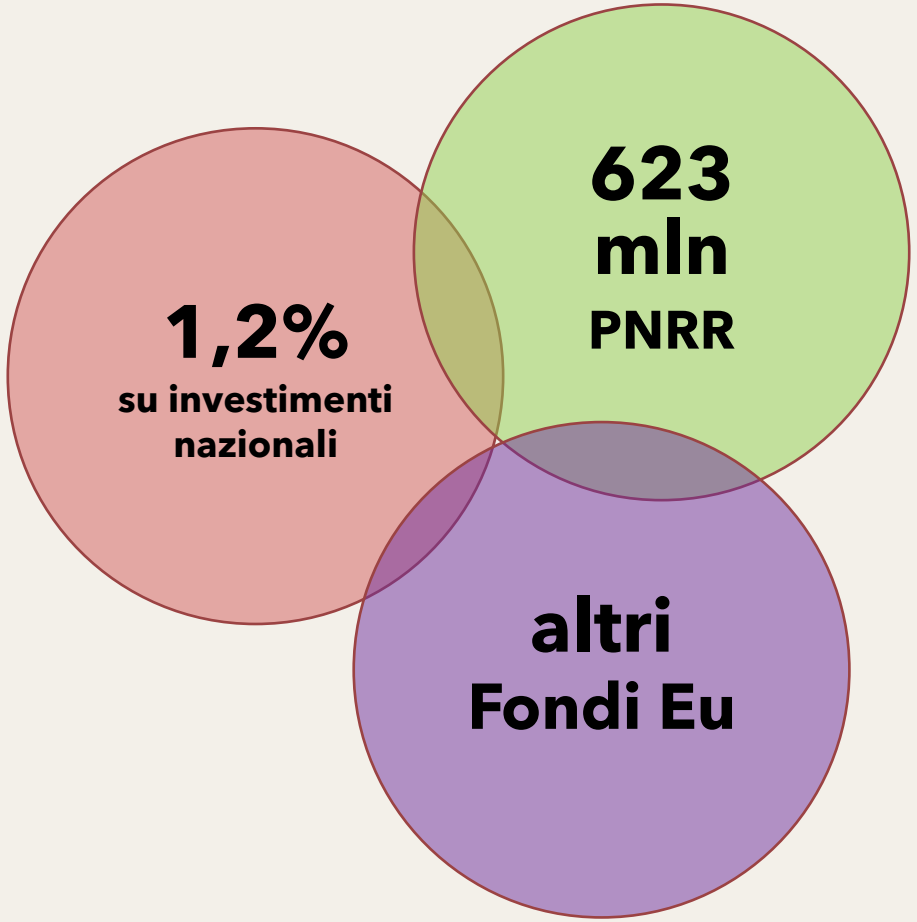
L'UE e, in particolare, l'Italia, si trova in una posizione di dipendenza tecnologica da altri Paesi, leader nella produzione di software e delle cosiddette **Emerging and Disruptive Technologies** quali, ad esempio, **l'Intelligenza Artificiale** e il **quantum computing**.

gli 007 possono fare contrattacchi?

Per Gabrielli è importante che «ciascuno faccia il suo»; e la Strategia mette in chiaro le competenze di tutti i soggetti coinvolti, dai ministeri alle forze di polizia, dalla **Difesa all'intelligence** che, ha ricordato, «già oggi, a legislazione vigente, **gode delle garanzie funzionali e può svolgere attività di contrattacco in campo cyber»**.

Mentre l'Agenzia, ha puntualizzato Baldoni, «deve diventare il faro a cui tutti si dovranno interconnettere, ma la gestione degli attacchi non si delega all'Agenzia. Noi forniamo le misure, le linee guida, ma poi ognuno deve adottarle al suo interno. **Nella cybersicurezza non si delega**»

come (e quanto) viene finanziata la strategia?



visione strategica: gli obiettivi da perseguire

una guerra tra hacker

esiste una guerra informatica parallela a quella sul campo di battaglia e vede i **pirati informatici “occidentali”** sempre più contrapposti a **quelli schierati in difesa di Mosca**

una guerra tra hacker

I due protagonisti principali sono: **Anonymous, il collettivo hacker più famoso** al mondo e **Killnet, collettivo con dominio russo** che dopo aver preso di mira siti istituzionali di ministeri e infrastrutture in Italia, sta attaccando i portali governativi polacchi: su Telegram hanno intanto pubblicato l'elenco di siti da colpire, arruolando criminali informatici.

Sulla chat dei pirati informatici di Killnet è stata anche pubblicata un'immagine in cui il volto del primo ministro della **Polonia** viene trasformato in quello di Hitler, con la frase: "il tuo sito principale del paese è inattivo! Probabilmente è tutto **a causa della tua politica marcia".**

Il 21 maggio l'account Twitter legato alla rete Anonymus@YourAnonOne ha dichiarato guerra a Killnet: "Anonymous **ha aperto ufficialmente una cyber-war contro il gruppo hacker filorusso**. Stiamo creando un server con 100 hacker e metteremo in ginocchio Killnet una volta per tutte!».

Non è facile, come sul campo di battaglia, poter tracciare esattamente ciò che è successo ma una cosa sembra potersi dire è che l'attacco di Anonymous contro Killnett sembra provenire dagli attivisti italiani. Lo stesso account @YourAnonOne rimanda a @AnonNewsItalia

la presentazione è finita

civitas

PER UN'EDUCAZIONE ALLA VITA CIVILE