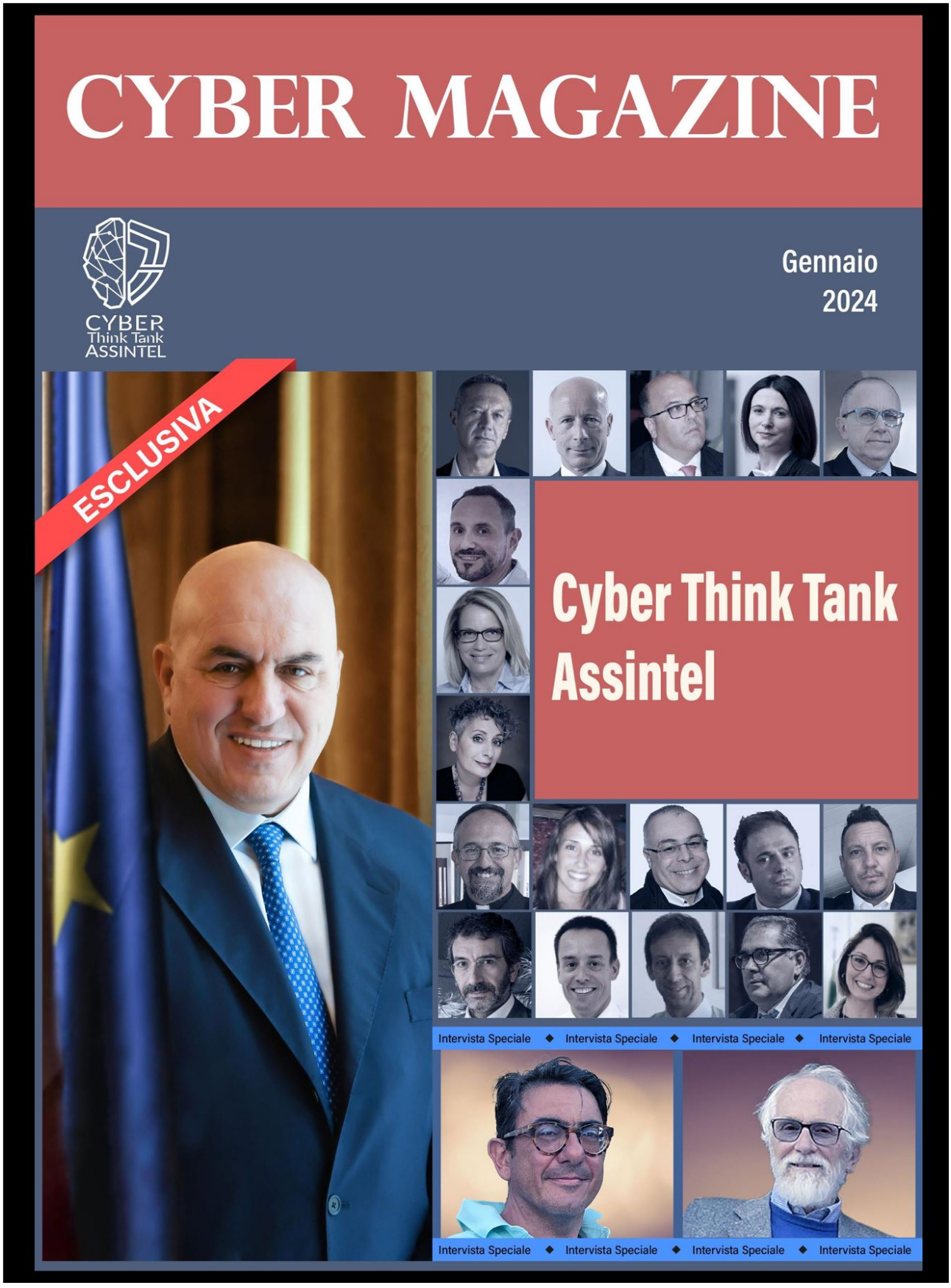

Intervista al Ministro della Difesa, On. Guido Crosetto.

Il Ministro della Difesa Guido Crosetto

Q1: Dalla guerra tradizionale a quella cibernetica, com'è cambiato l'approccio alla difesa. In cosa l'Italia deve ancora investire?

Negli ultimi anni la minaccia del settore cyber è cambiata drasticamente al punto che il cyberspazio è divenuto un nuovo dominio di operazioni al pari dei domini "tradizionali" (terrestre, marittimo, aereo) e, più recentemente, lo spazio. Nell'attuale contesto, in relazione all'incertezza del quadro internazionale, alla maggiore assertività di attori statali e non, passando per il *cybercrime*, tutti i paesi hanno indistintamente accelerato i programmi di rafforzamento delle proprie strutture organizzative e operative dedicate alla *cybersecurity*. Infatti, le forme moderne di conflittualità evidenziano come la componente tecnologica assuma un ruolo fondamentale sia quale fattore abilitante, sia quale elemento di competizione e confronto strategico.

Ciò di fatto implica l'esigenza di elevare il livello del confronto da quello classico del conflitto sul terreno, a quello della superiorità tecnologica e informativa tra gli attori coinvolti e di sviluppare capacità strategiche nazionali nei settori prioritari d'interesse.

Per questo motivo, la Difesa sta accelerando i propri processi di digitalizzazione e rivedendo il suo modo di operare attraverso una serie di iniziative volte ad assicurare anche nel c.d. dominio cibernetico i propri compiti istituzionali per garantire la protezione e la sicurezza degli interessi primari dello Stato. La sfida, quanto mai complessa, è quella di esprimere capacità operative all'avanguardia: dall'Intelligenza Artificiale, a servizi *cloud* evoluti, da info-strutture in ambito spaziale, tra cui le reti satellitari ad orbita bassa, a nuovi standard di cifratura e sicurezza delle informazioni e relativi effetti derivanti dallo sviluppo del *Quantum Computing*.

Questi sono solo alcuni dei settori d'interesse strategico non solo per la Difesa ma, come si può immaginare, per il Paese, con un ruolo centrale dell'industria, delle *start-up* e delle eccellenze che assumono una valenza strategica anche per lo sviluppo delle necessarie capacità nazionali in generale e di quelle più specificatamente a connotazione militare. Certamente, la Difesa non potrà sviluppare internamente tutte le proprie esigenze, ma potrà invece costituire uno dei principali *driver* dell'innovazione, in sinergia con le altre Pubbliche Amministrazioni, con il mondo accademico e il tessuto produttivo naziona-

le. Da questo punto di vista, soltanto nelle collaborazioni tra pubblico-privato si potranno individuare le necessarie soluzioni per conseguire la necessaria competitività dell'ecosistema produttivo nazionale.

Q2: Molti giovani, anche a seguito della guerra Russo – Ucraina, si stanno sempre più avvicinando alla cybersecurity, di che tipo di formazione e di competenze si parla?

Investire nella formazione di professionalità con specifiche competenze nel settore *cyber* è, al giorno d'oggi, non solo strategico ma anche essenziale. La carenza di professionisti con competenze adeguate in sicurezza cibernetica è una problematica globale per la quale anche la Difesa deve riuscire a trovare soluzioni idonee e forme innovative per attrarre i giovani talenti che escono dal mondo della scuola e dell'università.

Tra le iniziative già avviate, il reclutamento di laureati in ingegneria e informatica in grado di lavorare in un settore fortemente dinamico e stimolante come quello della cybersicurezza e delle operazioni cibernetiche. Il percorso formativo dei nostri operatori *cyber* coniuga sapere e saper fare, a similitudine di quanto avviene per il comparto di Forze Speciali. Dopo la prima fase di selezione, il personale frequenta uno specifico *iter* formativo che rappresenta un *unicum* per quanto concerne le competenze e le capacità professionali acquisite in ambito nazionale. Nel corso di studi si conseguono anche certificazioni *cyber* di livello internazionale. Al termine del periodo formativo di circa sei mesi, i neo specialisti sono impiegati in alcune delle realtà di eccellenza della Difesa, al fine di consolidare la formazione e operare nell'ambito delle varie attività nazionali ed internazionali, utilizzando alcune delle più avanzate soluzioni tecnologiche a disposizione, contribuendo al contempo allo sviluppo di nuove. Nel complesso, è stato realizzato un percorso formativo "non convenzionale", multidisciplinare e in continuo aggiornamento, anche attraverso l'osmosi e la sinergia con l'università, l'industria, le piccole e medie imprese e le *start-up leader* di settore. Il personale che andrà ad alimentare la forza *cyber* della Difesa, dopo un periodo in uniforme, potrà decidere se rimanere, usufruendo di forme di *retaining*, oppure "uscire" dalla Difesa e mettere le conoscenze acquisite a disposizione di altre Pubbliche Amministrazioni e del settore privato, anche per il conseguimento di una maggiore competitività sistemica.

Stiamo pensando a ulteriori iniziative per attrarre e rafforzare le competenze in ambito tecnologico a supporto dell'ecosistema Difesa, tra queste la realizzazione di una riserva *cyber* che possa coinvolgere anche le professionalità del mondo privato da attivare in caso di evento o crisi cibernetica, a completamento delle capacità esprimibili dalla Difesa.

Q3: Ogni volta che un governo ha espresso supporto all'Ucraina con tangibili segni di solidarietà, immediatamente ha subito un attacco hacker. Qual è lo stato di sicurezza attuale del nostro Paese e come la UE e l'Italia stanno rispondendo?

L'attuale scenario globale, dove ogni aspetto è legato all'ambiente digitale, è ormai caratterizzato dalla persistente presenza di attività cibernetiche malevole nei confronti delle funzioni e dei servizi essenziali (ovvero delle infrastrutture critiche) degli Stati che, sfociando in forti impatti nel mondo fisico, mirano a destabilizzarne la sicurezza e l'ordine pubblico.

Investire nella formazione di professionalità con specifiche competenze nel settore cyber è, al giorno d'oggi, non solo strategico ma anche essenziale.

A conferma di ciò, i dati rilevati ci dicono che tutte le tipologie di attacchi informatici continuano ad aumentare, anche a causa degli eventi connessi al conflitto russo-ucraino nell'ambito di operazioni cyber e campagne di disinformazione da parte di c.d. hacktivisti. Dal *cyberspace*, spesso coordinando, in modo ibrido, altre iniziative in campo economico, finanziario, diplomatico, o cognitivo, mediante campagne di comunicazione, si può raggiungere il centro di gravità della nazione, piuttosto che i centri nevralgici della società, dell'opinione pubblica, delle attività produttive e delle infrastrutture critiche nazionali, creando instabilità e tensioni sociali. Anche in questo istante, entità statali e non, nascoste nell'anonimato dello spazio cibernetico, attraverso organizzazioni c.d. *proxy,* conducono azioni malevole "sotto soglia" sfruttando le nostre vulnerabilità per raggiungere i propri obiettivi.

Immagine da: https://www.difesa.it/

Proprio per questo ogni Paese sta cercando di migliorare la propria capacità di comprendere e rispondere a questi fenomeni. Ne deriva quindi la necessità di disporre di un ecosistema nazionale resiliente e reattivo in grado di contrastare quotidianamente le attività ostili che vengono implementate nel dominio cibernetico.

Una sfida che coinvolge a livello nazionale in modo trasversale le Istituzioni, le Forze Armate e di Polizia, la Pubblica Amministrazione, le infrastrutture critiche e il settore privato. In tale ottica, coinvolgendo tutti i settori del Sistema Paese, è fondamentale sviluppare, attraverso interventi normativi ed investimenti dedicati, idonei meccanismi e capacità atti alla prevenzione e al contrasto di tali minacce concentrando le proprie forze a costante presidio e difesa del dominio cibernetico.

Da questo punto di vista, l'Italia negli ultimi anni ha fatto molto per migliorare la cybersicurezza e, in generale, la propria resilienza. La riforma dell'architettura nazionale cibernetica - attuata attraverso l'adozione del D.L. 82 del 14 giugno 2021 - ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo di razionalizzare il sistema *cyber* del Paese. Al contempo, la costituzione, in via permanente, del Nucleo per la CyberSicurezza (NCS) quale cabina di regia nazionale per le procedure di allertamento, prevenzione e gestione di eventuali situazioni di crisi, costituisce un passo essenziale per comprendere la minaccia e rispondere in modo adeguato. In prospettiva, l'esigenza è quella di migliorare il coordinamento tra i vari attori nazionali attraverso procedure di gestione degli incidenti che, coinvolgendo in maniera permanente i c.d. Pilastri Cyber dell'architettura nazionale cibernetica, ottimizzino l'impiego e lo sviluppo delle capacità cibernetiche del Paese.

Nello stesso tempo, l'Unione Europea ha contribuito in modo rilevante a ridisegnare la materia della cybersecurity e della resilienza nazionale, dando vita a provvedimenti normativi sui quali si sono spesso ancorate e animate le iniziative dei singoli Stati. Da questo punto di vista, i programmi sia in ambito civile che in ambito militare porteranno ulteriori benefici alla sicurezza del Paese e a quella collettiva europea, in un contesto in cui la minaccia risulta transnazionale e priva di confini geografici.

Q4: Quali sono oggi le sfide principali che le tecnologie emergenti come la IA presentano per la protezione dei diritti digitali dello stato e dei suoi cittadini e quali gli strumenti che possono o devono essere utilizzati per tutelare privacy, sicurezza e libertà d'espressione?

L'Intelligenza Artificiale è tra le priorità strategiche dell'agenda del governo italiano. Come annunciato dal Premier durante il recente *summit* di Londra proprio sull'IA, la consideriamo la più grande sfida intellettuale, pratica e antropologica di quest'epoca e sarà uno dei temi al centro della Presidenza italiana del G7 del prossimo anno. La volontà è quella di organizzare a Roma una Conferenza internazionale su Intelligenza Artificiale e lavoro, a cui vorremmo partecipassero studiosi, *manager* e esperti di tutto il mondo per discutere metodi, iniziative e linee guida sull'IA. Stiamo anche lavorando per completare il Piano strategico nazionale per l'IA, costituendo un fondo specifico per sostenere le *start-up* italiane e comitati per studiarne l'impatto nei vari settori d'interesse.

L'Intelligenza Artificiale è tra le priorità strategiche dell'agenda del governo italiano.

La preoccupazione è che meccanismi decisionali opachi, discriminazioni e usi impropri di questi strumenti possano costituire un'intrusione nella nostra vita privata ed essere utilizzati per atti criminali, per produrre armi, per causare danni biologici a bassa tecnologia, attacchi informatici o altro; in altre parole, costituire una minaccia per la sicurezza e la difesa dello Stato.

Da questo punto di vista, la sfida è quella di maturare un approccio equilibrato tra innovazione e tutela dei diritti tramite meccanismi di *governance* multilaterali, ricercando la definizione di regole comuni e garantire barriere etiche all'intelligenza artificiale, nell'ambito di un quadro normativo adeguato necessario a sfruttare le opportunità che l'IA può offrirci. In tal senso, sosteniamo e collaboriamo con l'Unione Europea verso l'approvazione dell'*Artificial Intelligence Act*, con il quale l'Unione si è assunta responsabilmente il compito di garantire un uso attento del bene pubblico ed evitare usi distorti a fini commerciali o, peggio, di sicurezza. Come ha chiaramente indicato la Premier, l'obiettivo è quello di sviluppare dei "*guardrail* etici" ossia <<*un insieme di principi etici da porre alla base del governo dell'IA generativa e le tecnologie correlate, da seguire nello sviluppo nella diffusione e nell'uso di queste tecnologie, sia nel settore pubblico che in quello privato*>>. Ciò al fine di tutelare, da una parte, le opportunità derivanti dall'uso di queste tecnologie e dall'altra i diritti fondamentali. La priorità numero uno per i prossimi anni è fare in modo che l'Intelligenza Artificiale sia incentrata sull'uomo e controllata dall'uomo.

Q5: Qual è il livello di adozione della direttiva NIS da parte del nostro Paese?

La Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione ha stimolato tutti i Paesi ad adottare misure concrete. In Italia, il quadro normativo è stato ulteriormente rafforzato da provvedimenti, quali, ad esempio, l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica. Un primo passo essenziale anche se il problema della *cyber* va inquadrato nell'ambito di un processo e in quanto tale deve essere continuamente aggiornato. In tal senso, si dovranno individuare le modalità e le risorse per elevare ulteriormente la sicurezza, coinvolgendo in modo sistemico le Istituzioni, la Pubblica Amministrazione e il settore privato.

Q6: Relativamente alla guerra in Israele, come pensa che cambierà l'approccio alla cybersecurity anche alla luce di quello che sta avvenendo?

Gli attuali conflitti stanno influenzando in modo significativo il campo della *cybersecurity*. Di fronte a minacce crescenti e sempre più sofisticate, è chiaro come essa costituisca un elemento fondamentale dell'attuale quadro nazionale e internazionale. La capacità di operare nello spazio cibernetico è diventata dunque una priorità per la sicurezza nazionale ed è uno dei fattori più significativi alla base dell'esigenza di evolvere verso un nuovo "paradigma della sicurezza", sempre più connesso con lo "sviluppo tecnologico". Governi e aziende stanno riconoscendo che gli attacchi informatici possono infliggere danni significativi, destinando maggiori risorse in questo settore. In prospettiva, le nuove tecnologie costituiscono un'opportunità, ma al contempo un ulteriore rischio. Ad esempio le tecnologie quantistiche costituiscono uno dei progressi tecnologici più eccezionali del nostro tempo,

con il *Quantum Computing* che sta aprendo orizzonti fino ad oggi inimmaginabili, superando le limitazioni dei tradizionali metodi di elaborazione dei dati. Ma, in questa straordinaria potenza computazionale emergono sfide significative come quelle per la sicurezza delle comunicazioni e la protezione dei dati. Infatti, il costante progresso nella capacità di calcolo dei *quantum computer* rappresenta una minaccia per la crittografia comunemente utilizzata ed è fondamentale riconoscere come ricerca e sviluppo nello stesso ambito tecnologico quantistico presentino le risorse per affrontare tali sfide. Ma, anche in questo caso, la sinergia pubblico-privato all'interno della visione del Sistema Paese è la risposta più lungimirante per combinare le competenze e gli investimenti necessari per affrontare anche questa sfida che - come altre - traguarda importanti opportunità. Da questo punto di vista, le sfide che ci aspettano sono enormi e complesse, ma sono sicuro che attraverso la sinergia e la cooperazione tra Istituzioni, mondo dell'impresa, dell'Università e della ricerca, troveremo le necessarie capacità, risorse e competenze. Sarà da ricercare, inoltre, nell'ambito delle organizzazioni internazionali di riferimento, NATO e UE, iniziative volte a rafforzare le capacità collettive a fronte di una minaccia per natura priva di confini geografici e transnazionale.

La Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione ha stimolato tutti i Paesi ad adottare misure concrete.