Cybersecurity Trends

Edizione italiana, N. 4 / 2025

INTERVISTE VIP:

- MAURO BRAMBILLA
- ROBERTO BALDONI
- LUCA GIUSTI
- LUCIANO FLORIDI
- ALESSIO TOLA
- MARCO BRACCIOLI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale:

SOVRANITÀ DIGITALE

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

Impatto geopolitico e cybersicurezza: conflitti, tecnologia e nuove sfide.

Autore: Nicola Sotira

In questi ultimi anni il rapporto tra geopolitica e cybersicurezza si è trasformato in uno dei fattori determinanti della nostra società. Il cyberspazio è ormai un dominio di confronto tra Stati e la crescente digitalizzazione delle infrastrutture critiche, dell'economia e della società ha reso la sicurezza informatica un elemento centrale della sicurezza nazionale e della politica estera. La competizione tra le grandi potenze, i conflitti regionali, l'emergere di nuove tecnologie come l'intelligenza artificiale e l'espansione delle reti globali stanno ridefinendo il concetto di sicurezza. In questo contesto, attacchi informatici, operazioni di disinformazione, cyber-spionaggio e sabotaggio digitale sono diventati strumenti strategici per influenzare equilibri geopolitici e decisioni politiche. Le operazioni informatiche consentono di ottenere vantaggi senza ricorrere a conflitti militari tradizionali, riducendo i costi e i rischi di escalation diretta.

Paesi come gli Stati Uniti, la Cina e la Russia hanno sviluppato capacità cyber offensive e difensive avanzate. Il cyberspazio offre vantaggi significativi: anonimato, difficoltà di attribuzione e possibilità di intraprendere azioni sotto la soglia del conflitto armato. Questo lo rende uno strumento ideale per la cosiddetta "guerra ibrida".

Il conflitto tra Russia e Ucraina rappresenta uno dei casi più evidenti di integrazione tra la guerra tradizionale e le operazioni cyber. L'Ucraina ha risposto rafforzando la propria difesa informatica, con il supporto di alleati occidentali e di aziende tecnologiche globali. Questo ha evidenziato il ruolo cruciale delle partnership pubblico/private nella difesa cyber.

L'esperienza ucraina ha dimostrato che la resilienza digitale è parte integrante della resilienza nazionale. Le capacità di ripristino rapido, la protezione delle infrastrutture cloud e la cooperazione internazionale sono diventate elementi centrali della sicurezza.

A questo occorre aggiungere la rivalità tra Stati Uniti e Cina, uno dei principali driver geopolitici nel cyberspazio. Il controllo delle catene di approvvigionamento tecnologico è diventato una priorità strategica. Le restrizioni alle esportazioni di semiconduttori avanzati e le politiche di "decoupling" tecnologico riflettono il timore che il dominio tecnologico si traduca in potere geopolitico. La sicurezza informatica è strettamente legata alla sovranità tecnologica: chi controlla le infrastrutture digitali controlla anche i flussi di dati e l'economia digitale.

BIO

Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

L'Unione europea ha avviato una serie di iniziative per rafforzare la propria autonomia strategica nel cyberspazio. Tra le priorità, la protezione delle infrastrutture critiche, gli investimenti in un cloud europeo e la cooperazione tra Stati membri. L'Europa si trova in una posizione complessa: dipende in parte da tecnologie statunitensi e asiatiche, ma vuole ridurre la vulnerabilità strategica. La cybersicurezza è considerata un elemento chiave della sicurezza economica e politica.

Il rafforzamento delle capacità cyber europee è anche una risposta alle minacce provenienti da attori statali e gruppi criminali internazionali. Oltre agli Stati, anche gruppi criminali e hacker indipendenti svolgono un ruolo crescente. Il ransomware è diventato una delle principali minacce globali. I gruppi criminali organizzati operano spesso in territori con scarsa cooperazione internazionale. In alcuni casi, esiste una relazione ambigua tra gruppi criminali e governi. Alcuni Stati tollerano o sfruttano questi gruppi come strumenti indiretti di pressione geopolitica.

La cybersicurezza non riguarda solo sistemi e reti, ma anche l'informazione. Le campagne di disinformazione mirano a influenzare opinioni pubbliche, elezioni e stabilità politica. Le piattaforme social sono diventate strumenti di influenza geopolitica. Operazioni coordinate possono diffondere narrazioni false, amplificare tensioni sociali e minare la fiducia nelle istituzioni. La guerra cognitiva è un'estensione della guerra informatica: il bersaglio non è solo l'infrastruttura, ma la percezione della realtà.

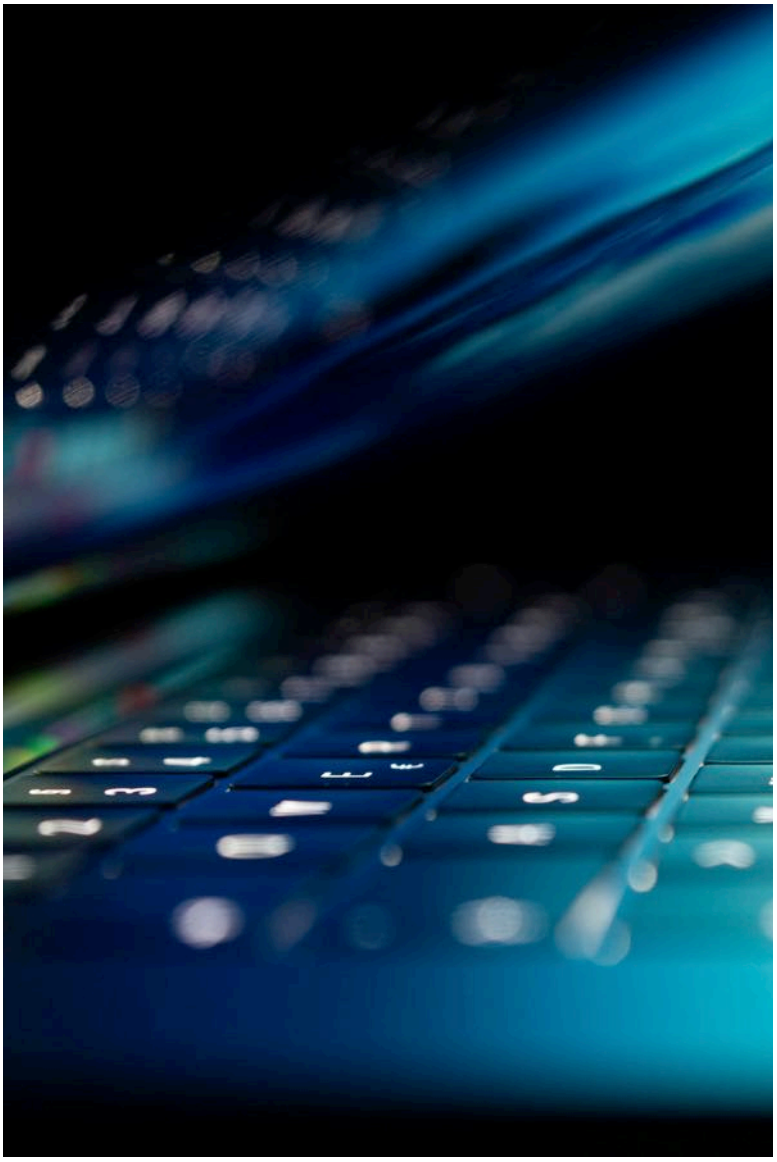
L'intelligenza artificiale sta trasformando il panorama della cybersicurezza. Gli attori malevoli possono usare l'IA per creare malware adattivo, phishing avanzato e deepfake. Allo stesso tempo, l'IA rafforza le capacità difensive. La competizione per il dominio dell'IA ha implicazioni geopolitiche dirette. Chi controlla le tecnologie di IA avrà, ovviamente, un vantaggio strategico.

Il legame tra geopolitica e cybersicurezza continuerà a rafforzarsi. Alcune tendenze chiave per il futuro:

1. Militarizzazione del cyberspazio - Gli Stati investiranno sempre più in capacità cyber offensive e difensive.
2. Sovranità digitale - Paesi e regioni cercheranno maggiore controllo su dati e infrastrutture.
3. Tecnologie emergenti - IA, quantum computing e reti avanzate cambieranno il panorama della sicurezza.
4. Partnership pubblico-private - La difesa cyber richiederà cooperazione tra governi e aziende.
5. Aumento delle minacce ibride

Attacchi informatici, disinformazione e pressione economica saranno sempre più integrati.

La cybersicurezza è diventata, pertanto, una componente fondamentale della geopolitica contemporanea. Il cyberspazio è un dominio di competizione strategica in cui Stati, aziende e attori non statali interagiscono in modi complessi. La sfida per il futuro sarà trovare un equilibrio tra competizione e cooperazione. Senza un quadro di governance condiviso e senza investimenti in resilienza digitale, il cyberspazio rischia di diventare un terreno di conflitto sempre più instabile.



Incident Management: il pilastro operativo della sicurezza informatica moderna.

Autore: Claudio Di Giuseppe

Nel panorama attuale della cybersecurity, caratterizzato da minacce sempre più sofisticate, persistenti e automatizzate, la capacità di prevenire un attacco è fondamentale, ma non sempre sufficiente. Anche le organizzazioni più mature devono accettare una realtà ormai consolidata: gli incidenti di sicurezza accadono, e accadranno. In questo contesto, l'Incident Management diventa un elemento centrale per garantire continuità operativa, resilienza digitale e conformità normativa.

L'Incident Management non è un'attività emergenziale improvvisata, ma un processo strutturato, integrato nella governance della sicurezza, che consente di individuare, gestire e risolvere eventi cyber in modo rapido, coordinato e misurabile. È un approccio che richiede non solo tecnologie avanzate, ma anche competenze specialistiche, processi collaudati e capacità operative continue, come evidenzia l'evoluzione dell'offerta di Telsy, società del Gruppo TIM operante all'interno di TIM Enterprise, sempre più focalizzata su servizi end-to-end di Incident Management e cyber resilience.

«Oggi il valore dell'Incident Management non si misura solo nella capacità di reagire a un attacco, ma nella possibilità di accompagnare le organizzazioni lungo tutto il ciclo dell'incidente, dalla preparazione alla gestione operativa,

fino al ripristino e al miglioramento continuo», spiega Cristiano Alborè, Portfolio Development Director di Telsy. «Il nostro approccio nasce proprio da questa esigenza: fornire un presidio integrato che combini monitoraggio avanzato, capacità di risposta immediata, analisi forense e supporto alla governance a partire dalla definizione o revisione dei ruoli e processi nell'organizzazione aiutando così le aziende e pubbliche amministrazioni a trasformare un evento critico in un processo controllato e misurabile».

Cos'è l'Incident Management

In ambito di sicurezza informatica, l'Incident Management è l'insieme di processi, ruoli, procedure e strumenti progettati per gestire eventi che compromettono, o rischiano di compromettere, la confidenzialità, l'integrità o la disponibilità di sistemi informativi, dati o servizi digitali. Un "incidente" può includere, ad esempio, attacchi ransomware o malware avanzati, compromissioni di account privilegiati, data breach, attacchi DDoS, accessi non autorizzati a sistemi critici o violazioni della supply chain digitale.

Il ciclo di vita dell'Incident Management

La gestione strutturata di un incidente si articola in diverse fasi:

- Preparazione: che comprende la definizione dei team di risposta, dei playbook operativi, degli strumenti di monitoraggio e delle attività di formazione ed esercitazione.
- Identificazione: in cui l'incidente viene rilevato e validato attraverso sistemi di monitoring, SOC e SIEM.
- Contenimento: finalizzato a limitare la propagazione del danno.
- Eradicazione: che prevede la rimozione delle cause tecniche dell'incidente, spesso con il supporto di analisi forense.
- Ripristino: con il ritorno controllato dei sistemi in produzione.
- Lezioni apprese: fase chiave per rafforzare la postura di sicurezza nel tempo.

È soprattutto nelle fasi iniziali che si gioca la partita più delicata. «Un incidente gestito male nelle prime ore può trasformarsi rapidamente in una crisi aziendale», osserva Emanuele Gentili, Threat Intelligence & Response Director di Telsy. «Per questo abbiamo costruito un modello di Incident Management che integra threat intelligence, capacità di risposta h24 e competenze forensi, consentendo interventi tempestivi e basati su una reale comprensione del contesto di minaccia. La tecnologia è fondamentale, ma è l'orchestrazione tra persone, processi e infrastrutture che fa davvero la differenza».

L'utilità strategica dell'Incident Management per business, reputazione e brand

Un processo di Incident Management maturo non rappresenta solo un presidio tecnico, ma un fattore abilitante per il business. Riduce il downtime, limita le perdite economiche, protegge la reputazione aziendale e supporta il management nelle decisioni durante una crisi cyber. Inoltre, favorisce l'allineamento tra IT, sicurezza, funzioni legali e comunicazione, dimostrando un governo consapevole del rischio cyber.

Gestire una crisi cyber in modo efficace è essenziale per tutelare l'impatto sul brand aziendale. Un piano di risposta agli incidenti ben strutturato non solo limita i danni immediati, ma protegge anche la percezione pubblica del marchio. La comunicazione trasparente e tempestiva durante l'incidente, insieme a una gestione adeguata delle problematiche interne, consente di mantenere la fiducia degli stakeholder e dei clienti, riducendo l'effetto di un possibile danno reputazionale.

I benefici sono concreti: riduzione dei tempi medi di risposta, maggiore visibilità sugli asset critici, miglior coordinamento interno ed esterno e maggiore fiducia da parte di clienti e partner. L'analisi storica degli incidenti consente inoltre di evolvere da un approccio puramente reattivo a uno progressivamente più proattivo e predittivo.

BIO

Claudio Di Giuseppe è Communication Specialist presso Telsy, Gruppo TIM.

Laureato in sociologia politica, ha conseguito un master universitario di II livello in geopolitica e sicurezza globale a Roma e un master in digital marketing a Los Angeles.

Da 5 anni scrive di cybersecurity e crittografia per il blog di Telsy e per il magazine Analisi Difesa. Collabora con la Croce Rossa Italiana come operatore volontario in attività di protezione civile.

Incident Management e contesto normativo

Con l'entrata in vigore della Direttiva NIS2 e l'evoluzione continua del quadro normativo europeo, l'Incident Management assume un ruolo ancora più centrale, diventando un obbligo per molte organizzazioni. Le nuove normative richiedono capacità documentate di prevenzione, rilevazione e risposta agli incidenti, oltre a processi verificabili e responsabilità diretta del management.

In questo scenario, l'Incident Management non è più confinato all'IT, ma entra a pieno titolo nella governance aziendale e nel risk management.

In un ecosistema digitale in continua trasformazione, l'Incident Management rappresenta uno dei pilastri fondamentali della sicurezza informatica moderna. Le organizzazioni che investono in processi strutturati, testati e supportati da partner specializzati come Telsy e TIM Enterprise non solo riducono l'impatto degli incidenti, ma rafforzano la propria capacità di affrontare con continuità le sfide tecnologiche, operative e normative del futuro digitale. ■

Scenari geopolitici futuri: dinamiche, evoluzioni e impatti sulla sovranità digitale.

Autore: Security Operations Center (SOC) - EY Forensics

Il contesto internazionale risulta oggi caratterizzato da una fase di profonda instabilità, in cui crisi regionali, competizione tra grandi potenze e il ricorso a strumenti di conflittualità ibrida si intrecciano, generando effetti a cascata su molteplici settori, tra cui mercati finanziari, approvvigionamenti energetici, supply chain e sicurezza digitale. In tale scenario, la capacità di anticipare, gestire e possibilmente mitigare i rischi geopolitici diventa una condizione essenziale per la resilienza delle infrastrutture critiche e la continuità operativa delle organizzazioni, con implicazioni che si estendono ben oltre il settore economico, toccando anche la sfera della sovranità digitale e della sicurezza informatica.

Per comprendere pienamente le implicazioni degli scenari geopolitici sulla sovranità digitale, è utile analizzare brevemente quattro teatri geopolitici attualmente di particolare rilevanza per gli equilibri politici, economici, securitari e tecnologici globali. Questi quadranti, al centro delle principali dinamiche internazionali, presentano molteplici traiettorie evolutive, ciascuna in grado di generare impatti trasversali su diversi settori, incluso quello digitale.

Il conflitto russo-ucraino

Il conflitto tra Russia e Ucraina continua a rappresentare una delle principali fonti di instabilità tanto per il continente europeo quanto a livello globale, con possibili evoluzioni che spaziano dalla risoluzione diplomatica all'escalation militare. In un eventuale scenario di risoluzione, un accordo politico – seppur fragile – potrebbe inaugurare una fase di cessate il fuoco e avviare un lento processo di ricostruzione. Tuttavia, le tensioni latenti lungo le linee di frontiera rimarrebbero un elemento di vulnerabilità, con effetti marginali ma persistenti su settori come la sicurezza energetica e digitale dei Paesi europei. Tale scenario appare però di difficile attuazione nel breve termine, come evidenziato dallo stallo nei negoziati diplomatici tra Russia

BIO

Il Security Operations Center (SOC) di EY Forensics offre un ampio ventaglio di servizi consulenziali e prodotti finalizzati alla tutela degli asset materiali e immateriali delle organizzazioni.

Attraverso l'integrazione di soluzioni tecnologiche innovative e servizi di consulenza avanzata, supporta i clienti nella gestione dei rischi legati alle dinamiche geopolitiche, intelligence e travel risk management, fornendo analisi, strumenti e modelli operativi a supporto dei processi decisionali e della resilienza aziendale.

e Ucraina, nonostante i rinnovati tentativi di mediazione dell'Amministrazione statunitense guidata da Donald Trump. Più verosimile appare pertanto, nell'immediato futuro, la prosecuzione della guerra lungo gli attuali fronti di conflitto, con un mantenimento dello status quo entro le traiettorie politico-militari degli ultimi anni, in cui le infrastrutture critiche europee – inclusi i sistemi digitali – restano esposte a rischi di attacchi cyber, sabotaggi e operazioni di guerra ibrida. Non si può infine escludere la possibilità, seppur remota, di una escalation militare, che vedrebbe il potenziale coinvolgimento della NATO e che produrrebbe shock energetici e finanziari di ampia portata, con impatti sistemici su tutti i settori, in particolare quello digitale, dove la minaccia di attacchi coordinati e massivi alle infrastrutture critiche diventerebbe estremamente elevata.

Tensioni e instabilità in Medio Oriente

Il secondo teatro riguarda le persistenti tensioni che caratterizzano il Medio Oriente, con il conflitto (al momento cessato) tra Israele e Hamas e le dinamiche regionali che coinvolgono attori come Iran e gli Houthi yemeniti. Una risoluzione definitiva delle ostilità, sostenuta dalle crescenti pressioni internazionali sia su Israele che su Hamas, potrebbe ridurre le tensioni regionali e favorire il ripristino delle linee di collegamento marittime (cosiddette SLOCs, Sea Lines of Communication), con impatti positivi su logistica e sicurezza digitale. Tuttavia, la fragilità degli accordi di cessate il fuoco attualmente in vigore (Striscia di Gaza, Libano, Iran) lascia aperta la possibilità di una ripresa delle ostilità su diversi fronti, con potenziali ripercussioni sulle supply chain e sui servizi digitali. In tale contesto, lo scenario potenzialmente più critico prevede un nuovo scontro armato diretto tra Israele e Iran (come quello del giugno 2025, e financo più esteso in termini di durata, portata e intensità), con forti turbolenze sui mercati finanziari ed energetici e una significativa esposizione delle infrastrutture occidentali a sabotaggi e attacchi cyber.

Nell'ambito di tale teatro geopolitico si evidenzia come, anche in caso di tenuta della tregua tra Israele e Hamas nella Striscia di Gaza, si potrebbe assistere ad una escalation militare su altri fronti, dal momento che Israele potrebbe ri-orientare le proprie risorse e i propri sforzi, nel medio periodo, su altri contesti operativi, come quello libanese (Hezbollah) e quello iraniano (regime degli Ayatollah). Alcune dichiarazioni rilasciate da funzionari israeliani, infatti, non permette di escludere l'ipotesi che i vertici politico-militari dello Stato ebraico, decidano di affrontare in maniera definitiva il dossier dello scontro con la Repubblica Islamica entro la fine del secondo mandato dell'amministrazione USA di Donald Trump (2028). Un ulteriore fattore di destabilizzazione nel medio-lungo periodo per la regione mediorientale è rappresentato infine dalla crescente rivalità turco-israeliana, ad oggi confinata nel teatro operativo siriano.

Cina-Taiwan e tensioni nell'Indo-Pacifico

Il terzo quadrante si concentra sulle tensioni tra Cina e Taiwan e sulle dinamiche nell'Indo-Pacifico, che rappresentano un nodo strategico per la stabilità globale e la sicurezza digitale. La prosecuzione di una pressione costante da parte della Cina su Taiwan ai fini della riunificazione, senza ricorso alla forza militare, manterrebbe la situazione tesa ma stabile, con le catene di fornitura globali, incluse quelle digitali, che sperimenterebbero una parziale diversificazione per ridurre la dipendenza da Pechino e Taipei.

Tuttavia, la vulnerabilità delle supply chain e dei servizi digitali rimarrebbe elevata. Un'eventuale invasione militare cinese dell'isola comporterebbe misure economiche e diplomatiche restrittive da parte degli Stati Uniti e dei Paesi alleati, con turbolenze rilevanti sui mercati finanziari ed energetici e rischi elevati di guerra ibrida e attacchi cyber alle infrastrutture critiche. Lo scenario più estremo, infine, vedrebbe l'intervento militare diretto degli Stati Uniti e di altri Paesi a sostegno di Taiwan, portando allo scoppio di un conflitto convenzionale nell'Indo-Pacifico, con turbolenze globali e rischi sistemici per le infrastrutture digitali e le supply chain, oltre a una possibile recessione economica mondiale.

Politiche commerciali degli Stati Uniti

Il quarto scenario di particolare rilevanza concerne l'evoluzione delle politiche commerciali statunitensi nell'ambito della seconda presidenza Trump, le quali influenzano direttamente la stabilità delle catene di approvvigionamento globali e la sicurezza digitale. Una fase di

distensione e parziale liberalizzazione, caratterizzata da un riavvicinamento pragmatico con partner strategici (Unione Europea in primis), favorirebbe la stabilità delle supply chain e una maggiore cooperazione regolamentare, con impatti contenuti su servizi digitali e piattaforme IT. Se invece dovesse prevalere un approccio protezionista calibrato, le tensioni resterebbero probabilmente limitate a dispute regolamentari e di competitività industriale, ma aggiornamenti mirati alle liste di esportazione controllata e divieti su componenti tecnologiche sensibili potrebbero generare rischi di vulnerabilità strategica per le infrastrutture digitali e le supply chain. Lo scenario più critico, infine, vede un'escalation commerciale globale, con aumento generalizzato dei dazi, ampliamento dei controlli su export di tecnologie e materiali critici (come i chip utilizzati in ambito di Intelligenza Artificiale) e sanzioni secondarie contro Paesi che eludono le restrizioni. In questo contesto, la frammentazione commerciale alimenterebbe rialzi dei costi e ritardi nelle catene di fornitura globali, mentre i rischi di sabotaggi, azioni ibride e attacchi cyber raggiungerebbero livelli elevati, con impatti trasversali su tutti i settori, in particolare quello digitale.

Conclusione

Questi quattro scenari geopolitici presentano implicazioni profonde, trasversali e multilivello che si riflettono su un'ampia gamma di settori strategici: dalla sicurezza informatica alla continuità operativa, dalla resilienza delle supply chain alla protezione degli asset critici, fino ai temi della sovranità digitale e della competitività industriale.

In un contesto in cui le tensioni internazionali, la ridefinizione degli equilibri globali e l'emergere di nuovi attori statuali e non statuali stanno ridisegnando il panorama di rischio, la capacità delle aziende di

anticipare, comprendere e gestire le implicazioni derivanti dai mutamenti geopolitici globali diventa un fattore imprescindibile.

Oggi più che mai, le organizzazioni devono essere in grado non solo di prevedere e mitigare i rischi, ma anche di incrementare la propria resilienza, assicurare la continuità del business, prendere decisioni strategiche tempestive e saper cogliere le nuove opportunità generate da un ambiente competitivo in rapido cambiamento.

In questo scenario, capacità, strumenti e servizi quali geopolitical intelligence analysis, security risk management e consulting, threat monitoring, emergency e crisis management stanno assumendo un ruolo centrale, diventando componenti essenziali per consentire alle aziende di orientarsi, "navigare" e competere nell'attuale contesto internazionale complesso e interconnesso.

Non sorprende, quindi, che il mercato globale dei servizi di risk management consulting sia destinato a crescere significativamente nei prossimi anni: le stime indicano un tasso di crescita annuale composto (CAGR) del 5,9% tra il 2023 e il 2032, a testimonianza di una domanda crescente da parte delle organizzazioni che riconoscono in queste funzioni un elemento strategico per la propria sostenibilità, solidità e capacità di adattamento nel lungo periodo. ■

Sovranità digitale e consapevolezza, strumenti necessari per arginare economia illegale ed espansione del dark web.

Autore: Andrea Monti

La sovranità digitale è un tema che si impone come centrale nelle agende non solo delle imprese, ma anche dei governi in una fase della storia in cui le tecnologie digitali stanno facendo da motore dello sviluppo economico e sociale di intere molte aree del mondo.

Per Tinexta Cyber, in particolare, la sovranità digitale rappresenta non solo un principio strategico, ma una condizione necessaria per garantire sicurezza, resilienza e autonomia alle organizzazioni pubbliche e private. Ridurre la dipendenza da infrastrutture e tecnologie non governabili, assicurare che i dati rimangano sotto una giurisdizione affidabile e poter contare su competenze qualificate nel territorio, significa rendere più difficile per i cybercriminali sfruttare vulnerabilità sistemiche. Non ci si deve stupire se in questo contesto stia crescendo l'importanza di strumenti di valutazione e certificazione che attestino la reale capacità delle aziende di garantire continuità operativa anche in caso di attacchi. In questo senso, la certificazione 22301 sulla Business Continuity assume un ruolo centrale. La domanda che dobbiamo porci riguarda il livello di preparazione strutturale e organizzativo delle nostre imprese, sollecitate dalla

BIO

Andrea Monti è Direttore Generale di Tinexta Cyber, il Polo italiano della cybersecurity, e facente parte di Tinexta, Gruppo industriale che offre soluzioni innovative per la trasformazione digitale e la crescita di imprese, professionisti e istituzioni. Laureato in Economia e Commercio all'Università Bocconi di Milano, ha una lunga esperienza nel settore bancario, finanziario e ICT.

Inizia in Interbanca, banca d'Affari milanese, come analista finanziario. Approda in Accenture nel 2001 con incarichi in Italia e all'estero in progetti prevalentemente legati all'efficientamento e all'automazione dei processi del credito. Passa in Bain nel 2007 e segue progetti in ambito bancario e finanziario prevalentemente all'estero (UAE, Arabia Saudita, Russia, Francia, Grecia e UK).

L'ultimo progetto in Bain è la definizione del piano di Turnaround della Banca Popolare di Puglia e Basilicata; al termine della fase progettuale entra nella stessa banca, con il ruolo di Vice Direttore Generale e delega alla realizzazione del piano. Resta nel ruolo per 5 anni, fino al 2015, realizzando gli obiettivi stabilita da Bankit / BCE. Dal 2015 al 2018 è in Assist Digital come responsabile del comparto FSI e dal 2018 al 2023 in NTTData come responsabile della practice Banking per l'Italia e rappresentante per l'EMEA al global Committee di Tokyo.

Entra nel gruppo Tinexta a ottobre 2023, prima come DG di Corvallis e poi anche come CEO di Yoroi e Swascan, fino alla fusione per incorporazione in Tinexta Cyber Andrea Monti è esperto di processi, procedure e tecnologie per il mondo bancario e finanziario. Ha maturato significative esperienze in ambito consulenziale e per la definizione e attuazione di piani di risanamento e turnaround.

normativa a dimostrare, in modo oggettivo, il proprio grado di resilienza operativa, che deve sovrapporsi alla capacità di reagire rapidamente a incidenti cyber complessi. Su questo aspetto si gioca non solo la tutela degli asset, cosa oggi fondamentale a tutti i livelli, ma anche le chances di competitività di sistema industriale.

I rischi del "sottobosco digitale"

L'universo del deep web, autentico "sottobosco digitale", è configurabile come quella parte di Internet non indicizzata dai vari motori di ricerca, che raccoglie un'enorme mole di informazioni e dati leciti, ma nascosti per motivi di privacy o sicurezza. È emblematico della potenza, ma anche della fragilità, della sofisticata strumentazione tecnologica di cui disponiamo. Nel dark web si muove un'economia sommersa che, lontana dai riflettori, alimenta traffici illeciti di ogni genere. È una piccola porzione del deep web, accessibile solo tramite strumenti e credenziali specifiche, in cui tutti sono anonimi (o pensano di esserlo). È un fenomeno tutt'altro che marginale: secondo le stime, entro il 2028 il mercato globale del dark web potrebbe raggiungere un valore di 1,3 miliardi di dollari, con una crescita annua superiore al 22%. Un dato che fotografa, solo in parte, la portata di questo fenomeno che, per dimensioni e impatto, coinvolge imprese, cittadini e istituzioni di tutto il mondo.

Nel dark web si scambiano beni e servizi illegali: tutto quello che non dovrebbe essere trovato, dalle sostanze stupefacenti ai dati, dai malware ai documenti falsi, dalle armi ai truffatori, dalle identità rubate ai tutorial terroristici. Si ipotizza che il deep web e il dark web rappresentino, insieme, il 96% dell'intero universo digitale, lasciando al web che utilizziamo quotidianamente solo una minima parte della rete.

Tra le attività più diffuse spicca il traffico di sostanze stupefacenti, che registra il maggior numero di prodotti e venditori. I mercati digitali offrono una gamma vastissima di narcotici, farmaci e materie prime, con modalità di

acquisto che ricalcano quelle dei negozi online legali: cataloghi dettagliati, assistenza clienti, pagamenti in criptovalute e spedizioni in tutto il mondo. La facilità di accesso e la promessa di anonimato abbassano la soglia di rischio percepito, ma dietro questa apparente efficienza si celano pericoli concreti come truffe, prodotti contraffatti, rischi per la salute di chi acquista e consuma e, ovviamente, conseguenze penali anche gravi.

Occhio al "carding" fenomeno in rapida evoluzione

Un altro settore in forte crescita è quello del "carding", ovvero la compravendita di dati di carte di pagamento rubate. I dati vengono sottratti tramite malware (un software progettato per infiltrarsi, danneggiare o rubare dati da computer, reti o dispositivi), phishing (il cybercriminale si finge un'entità esistente, come banche, provider e-mail, etc, con l'obiettivo di ingannare le potenziali vittime ed estorcere informazioni sensibili) o attacchi informatici a database aziendali, per poi essere rivenduti su marketplace specializzati. Il prezzo medio di una carta oscilla intorno ai 7 dollari, ma può variare in base al paese di emissione e alle informazioni aggiuntive disponibili. L'Italia si colloca in una fascia intermedia, con un prezzo medio di quasi 9 dollari per carta compromessa.

Non meno preoccupante è il mercato dei malware e dei ransomware: software utilizzabili per attacchi ad aziende e privati, sempre più sofisticati, che bloccano l'accesso ai dati o al sistema di un utente e richiedono il pagamento di un riscatto per ripristinarne l'accesso. I kit di phishing e i ransomware "chiavi in mano" - che includono tutto il necessario per lanciare un attacco - sono ormai alla portata anche di criminali poco esperti, grazie a forum e piattaforme che offrono manuali, assistenza e persino modelli di business basati sulla condivisione dei profitti. Quest'ultima, in particolare, è una strategia utilizzata nel cybercrime in cui diversi attori - come gli sviluppatori e gli esecutori veri e propri - collaborano e condividono i guadagni ottenuti dai riscatti o dalle frodi. Il danno globale stimato dai soli ransomware potrebbe raggiungere i 265 miliardi di dollari entro il 2031. Il commercio di dati personali e credenziali di accesso rappresenta, inoltre, una minaccia crescente per la privacy e la sicurezza di milioni di persone: si stima che siano circa 15 miliardi le credenziali rubate o sottratte illecitamente, e che un'identità valga all'incirca tra i 10 e i 100 dollari. Nei forum underground - spazi nascosti o quasi all'interno sia del deep sia del dark web - dove cybercriminali e hacker si scambiano informazioni, strumenti e servizi, si vendono anche pacchetti di dati rubati, documenti di identità, password e informazioni sanitarie, alimentando un circolo vizioso di frodi, furti di identità e attacchi mirati. L'offerta, per i criminali, è ampia e strutturata: abbonamenti VIP, canali riservati, database aggiornati e servizi di editing per documenti falsi.

Non dobbiamo pensare che il dark web si alimenti solo attraverso grandi attacchi informatici ma principalmente grazie a operazioni di phishing anche molto semplici, telefonate o mail fasulle. Per imprese e cittadini, la consapevolezza dei rischi, l'adozione di comportamenti prudenti e la costante verifica delle fonti quando si ricevono richieste di condivisione di dati sensibili, restano le prime linee di difesa in un contesto dove la sicurezza digitale è sempre più centrale per la tutela di persone, dati e patrimoni. Infine una raccomandazione: ricordiamoci sempre che il fattore umano resta inequivocabilmente l'argine principale alle minacce digitali di qualsiasi complessità, natura e genere. ■

Sovranità digitale: realismo strategico e cybersecurity nell'ecosistema europeo.

Autore: Andrea Rigoni

La sovranità digitale è diventata una delle espressioni più ricorrenti – e, al tempo stesso, più ambigue – del lessico strategico europeo. La sua recente formalizzazione in documenti e dichiarazioni di indirizzo dell'Unione Europea non rappresenta soltanto una presa di posizione politica, ma il riflesso di una tensione strutturale: da un lato, la necessità di ridurre dipendenze tecnologiche percepite come critiche; dall'altro, la consapevolezza che l'ecosistema digitale contemporaneo è, per sua natura, globale, interconnesso e difficilmente riconducibile a logiche di controllo territoriale tradizionali.

BIO

Andrea Rigoni è un esperto internazionale di sicurezza digitale con oltre trent'anni di esperienza nella trasformazione cyber di governi, organizzazioni internazionali e settori altamente regolati.
È Founder e Managing Partner di Altirium, advisory firm specializzata in Digital Readiness e resilienza dinamica, è membro di vari advisory board tra i quali l'Associazione Bancaria Italiana (ABI), Paladin Capital e Forgepoint; è non-resident Senior Fellow dell'Atlantic Council.

Alcuni episodi recenti aiutano a comprendere questa frizione meglio di qualsiasi documento strategico. Il caso che ha coinvolto AGCOM e Cloudflare, a seguito di una sanzione regolatoria, ha mostrato come una decisione nazionale legittima possa rapidamente assumere una dimensione sistemica. La reazione del provider statunitense – con il riferimento, più o meno esplicito, alla possibilità di ridurre o ritirare servizi connessi a contesti ad alta visibilità come Milano Cortina 2026 – ha evidenziato un dato di fondo: quando componenti essenziali dell'infrastruttura digitale sono controllate da attori esterni allo spazio giuridico europeo, la regolazione diventa anche un terreno di negoziazione di potere.

Nel dominio della cybersecurity, questa dinamica non è nuova. Storicamente, gli Stati hanno sempre considerato alcune capacità tecnologiche come intrinsecamente sovrane. La crittografia ne è l'esempio più evidente: per decenni è stata sviluppata, custodita e governata come asset nazionale, spesso in stretta connessione con il mondo della difesa e dell'intelligence.

Tuttavia, l'evoluzione del mercato cyber negli ultimi vent'anni ha prodotto due effetti profondi sull'Europa. Da un lato, un progressivo indebolimento del tessuto industriale continentale in alcuni segmenti chiave; dall'altro, una crescita esponenziale della complessità dell'ecosistema digitale, oggi strutturato su filiere multilivello, supply chain globali e dipendenze tecnologiche difficilmente separabili.

In questo contesto, l'idea di una sovranità digitale totale appare sempre più come una costruzione teorica, se non una vera e propria chimera. Software, hardware, piattaforme cloud, servizi di sicurezza e standard operativi sono distribuiti su scala globale. Pensare di esercitare un controllo end-to-end su questi elementi significa ignorare la natura stessa del digitale contemporaneo. La questione, allora, non è se perseguire o meno la sovranità, ma come ridefinirla in termini realistici e operativi. Una sovranità digitale credibile non coincide con il possesso diretto di ogni componente tecnologica, ma con la capacità di scegliere, configurare e governare le interdipendenze.

Dal punto di vista governativo, questo implica innanzitutto una scelta politica non banale: individuare quali ambiti siano realmente critici per la sicurezza nazionale e la resilienza sistemica, e concentrare su di essi gli sforzi di controllo, investimento e protezione. Al di fuori di questi perimetri, l'interdipendenza non è un rischio da eliminare, ma una condizione da gestire.

La debolezza dell'Europa

Esistono settori nei quali l'Europa, oggi, è strutturalmente debole e nei quali, almeno nel breve periodo, il ricorso a operatori extraeuropei è inevitabile. In questi casi, la sovranità non può essere intesa come esclusione, ma come capacità di negoziazione e di imposizione di condizioni. Le leve sono molteplici: governance dei dati, auditabilità delle piattaforme, requisiti contrattuali stringenti, trasparenza sulle catene di fornitura, segregazione logica e operativa delle infrastrutture, fino a meccanismi di supervisione coordinati a livello europeo.

La costruzione di data center e region cloud sul territorio europeo va letta in questa chiave: un passo necessario, ma non sufficiente.

È infatti essenziale chiarire un punto spesso semplificato nel dibattito pubblico: la localizzazione fisica del dato non equivale all'autonomia operativa. Il controllo delle infrastrutture globali, dei piani di aggiornamento software, delle piattaforme di gestione e delle dipendenze tecnologiche rimane un tema profondamente politico e tecnologico al tempo stesso. Per questo motivo, le istituzioni europee e nazionali devono evitare approcci frammentati o contraddittori. Una collaborazione costruttiva con i grandi attori tecnologici globali non solo è possibile, ma è necessaria; a condizione, però, che sia guidata da una strategia coerente e condivisa, e non da iniziative isolate.

Il secondo pilastro della sovranità digitale riguarda l'innovazione. L'Europa investe ingenti risorse pubbliche nei settori cyber e dell'intelligenza artificiale, spesso in misura comparabile – se non superiore – ad altre grandi economie. Eppure, i risultati industriali e di mercato restano limitati. Una delle cause principali risiede nel modo in cui questi investimenti vengono governati. I fondi pubblici sono accompagnati da controlli rigorosi sulle modalità di spesa, ma da una attenzione molto più debole sugli impatti reali, sulla maturazione tecnologica e sulla capacità di tradurre la ricerca in soluzioni operative. In questo senso, la sovranità digitale non è solo una questione di protezione, ma anche di capacità di trasformazione. Rafforzare il legame tra ricerca finanziata con fondi pubblici e adozione concreta nelle politiche e nei progetti pubblici potrebbe rappresentare una leva decisiva. Meccanismi di procurement più attenti alla valorizzazione di soluzioni europee mature, sviluppate con risorse pubbliche, non come forma di protezionismo ma come strumento di accelerazione, potrebbero contribuire a ricostruire competenze industriali e ridurre dipendenze strutturali.

In definitiva, la sovranità digitale non può essere ridotta a uno slogan né a un obiettivo assoluto. È, piuttosto, una pratica di governo della complessità, che richiede scelte selettive, realismo strategico e una visione di lungo periodo. La cybersecurity rappresenta il banco di prova più concreto di questa impostazione: non come esercizio di controllo totale, ma come equilibrio dinamico tra autonomia decisionale, cooperazione industriale e responsabilità pubblica. È su questo terreno, meno ideologico e più operativo, che l'Europa può ancora costruire una sovranità digitale credibile. ■

Intervista sulla Sovranità Digitale e Gaia-X a Mauro Brambilla.

Gaia-X e la Sovranità Digitale Europea: Costruire un'Infrastruttura di Dati Trasparente e Sicura

Autore: Massimo Cappelli

In qualità di membro del Board of Directors di Gaia-X, può spiegarci cosa si intende oggi per sovranità digitale e perché è così cruciale per l'Europa?

La sovranità digitale rappresenta la capacità di individui, aziende e Stati di determinare autonomamente come i propri dati vengono gestiti, archiviati e utilizzati nell'ecosistema digitale. Non si tratta di protezionismo tecnologico o di chiusura dei confini digitali, ma di garantire che l'Europa mantenga il controllo sulle proprie infrastrutture critiche e sui flussi di dati che alimentano la nostra economia digitale. Oggi il panorama digitale è caratterizzato dalla presenza di operatori tecnologici extraeuropei e questo può creare delle vulnerabilità strategiche, come le interruzioni di servizio o rischi legati alla compliance normativa e alla protezione dei dati sensibili. La sovranità digitale significa costruire un'alternativa basata su principi europei di trasparenza, interoperabilità e rispetto dei diritti fondamentali.

Qual è la missione specifica di Gaia-X in questo contesto?

Gaia-X nasce nel 2019 dall'iniziativa franco-tedesca con l'obiettivo di creare un ecosistema federato di servizi dati e cloud che rispetti i valori europei. La nostra missione è sviluppare standard comuni, regole di governance e un framework tecnologico che permetta a provider di servizi cloud di diversa dimensione di interoperare in modo sicuro e trasparente. Non stiamo costruendo una nuova infrastruttura cloud da zero che deve fungere da architettura di riferimento, ma un insieme di specifiche tecniche e policy che permettono di creare un mercato europeo dei dati realmente competitivo. Immaginate un ecosistema dove le aziende possono scegliere liberamente tra diversi provider, spostare i propri workload senza lock-in tecnologico, e avere garanzie verificabili su dove risiedono i dati e chi può accedervi.

Quali sono i principi fondamentali su cui si basa Gaia-X?

Il progetto si fonda su quattro pilastri essenziali. Primo, la trasparenza: ogni partecipante dell'ecosistema deve fornire informazioni chiare e verificabili sui propri servizi, attraverso self-description standardizzate. Secondo, l'interoperabilità: i servizi devono comunicare tra loro seguendo standard aperti, evitando dipendenze proprietarie. Terzo, la portabilità dei dati: gli utenti devono poter migrare facilmente da un provider all'altro, senza costi proibitivi o barriere tecniche. Quarto, la sovranità by design: le architetture devono incorporare nativamente meccanismi di controllo degli accessi, tracciabilità e compliance normativa.

Questi principi si traducono in specifiche tecniche concrete. Abbiamo sviluppato il Gaia-X Trust Framework, che definisce requisiti minimi per la partecipazione all'ecosistema, e stiamo lavorando su data space settoriali – dalla sanità alla manifattura, dall'energia alla mobilità – dove questi principi vengono implementati in casi d'uso reali.

Come si posiziona Gaia-X rispetto ai grandi cloud provider americani e cinesi?

Molti di questi player partecipano attivamente al progetto. Il punto centrale è che anche questi provider, quando operano in Europa seguendo le nostre specifiche, contribuiscono a creare un ecosistema più equilibrato e competitivo. Ciò che vogliamo evitare è la dipendenza da soluzioni proprietarie o situazioni di debito tecnologico, che rendono impossibile il cambio di fornitore e creano quindi forme di lock-in. Gaia-X promuove un modello dove la competizione avviene su qualità, prezzo e innovazione.

Quali settori beneficeranno maggiormente da questa infrastruttura?

I data space verticali rappresentano l'applicazione concreta della visione Gaia-X. Nella sanità, ad esempio, stiamo lavorando per permettere lo scambio sicuro di cartelle cliniche tra ospedali di diversi Paesi, garantendo privacy e compliance al GDPR. Nell'industria manifatturiera, Gaia-X abilita la condivisione di dati di produzione lungo supply chain complesse, permettendo ottimizzazioni senza esporre informazioni strategiche. Il settore automotive sta sperimentando data space per la mobilità connessa, dove dati provenienti da veicoli, infrastrutture stradali e servizi di mobilità vengono orchestrati rispettando la proprietà dei dati di ciascun attore. Anche l'energia vede enormi opportunità: la transizione verso fonti rinnovabili richiede coordinamento in tempo reale tra migliaia di produttori e consumatori, qualcosa che solo un'infrastruttura dati federata può abilitare efficacemente.

Quali sono le sfide principali che Gaia-X deve affrontare?

La complessità è la nostra sfida maggiore. Coordinare centinaia di organizzazioni pubbliche e private di 27 paesi con interessi a volte divergenti, richiede un lavoro diplomatico e tecnico enorme. C'è poi il tema della velocità: il mercato digitale evolve rapidamente e dobbiamo dimostrare valore concreto prima che la window of opportunity si chiuda. Sul fronte tecnico, l'interoperabilità tra sistemi legacy e nuove architetture cloud-native è complessa. Molte aziende europee, specialmente le PMI, hanno infrastrutture IT datate e necessitano di percorsi di migrazione graduali. Inoltre, dobbiamo bilanciare l'ambizione di standard elevati con la praticità dell'adozione: requisiti troppo stringenti rischiano di scoraggiare i partecipanti. C'è anche una

dimensione culturale: far comprendere che la sovranità digitale non è nazionalismo tecnologico ma autodeterminazione strategica e richiede un costante lavoro di comunicazione verso policy maker, media e opinione pubblica.

Che risultati concreti avete già ottenuto?

Dopo cinque anni di lavoro, abbiamo raggiunto traguardi significativi. Il Gaia-X Trust Framework è stato finalizzato e sempre più provider stanno ottenendo la certificazione di compliance. Oggi contiamo oltre 350 organizzazioni membri provenienti da tutta Europa e oltre, rappresentando

la più ampia coalizione mai costruita su questi temi. I primi data space operativi stanno andando live: progetti pilota nella sanità tedesca, nella logistica portuale e nella gestione energetica distribuita. Stiamo osservando un crescente interesse anche da istituzioni pubbliche, che vedono in Gaia-X uno strumento per modernizzare i propri servizi digitali, mantenendo il controllo sui dati sensibili dei cittadini. Altrettanto importante è l'impatto normativo: il Data Governance Act, il Data Act e altre iniziative legislative europee incorporano principi che Gaia-X ha contribuito a definire e promuovere. Stiamo creando un circolo virtuoso in cui tecnologia e regolamentazione si rafforzano reciprocamente.

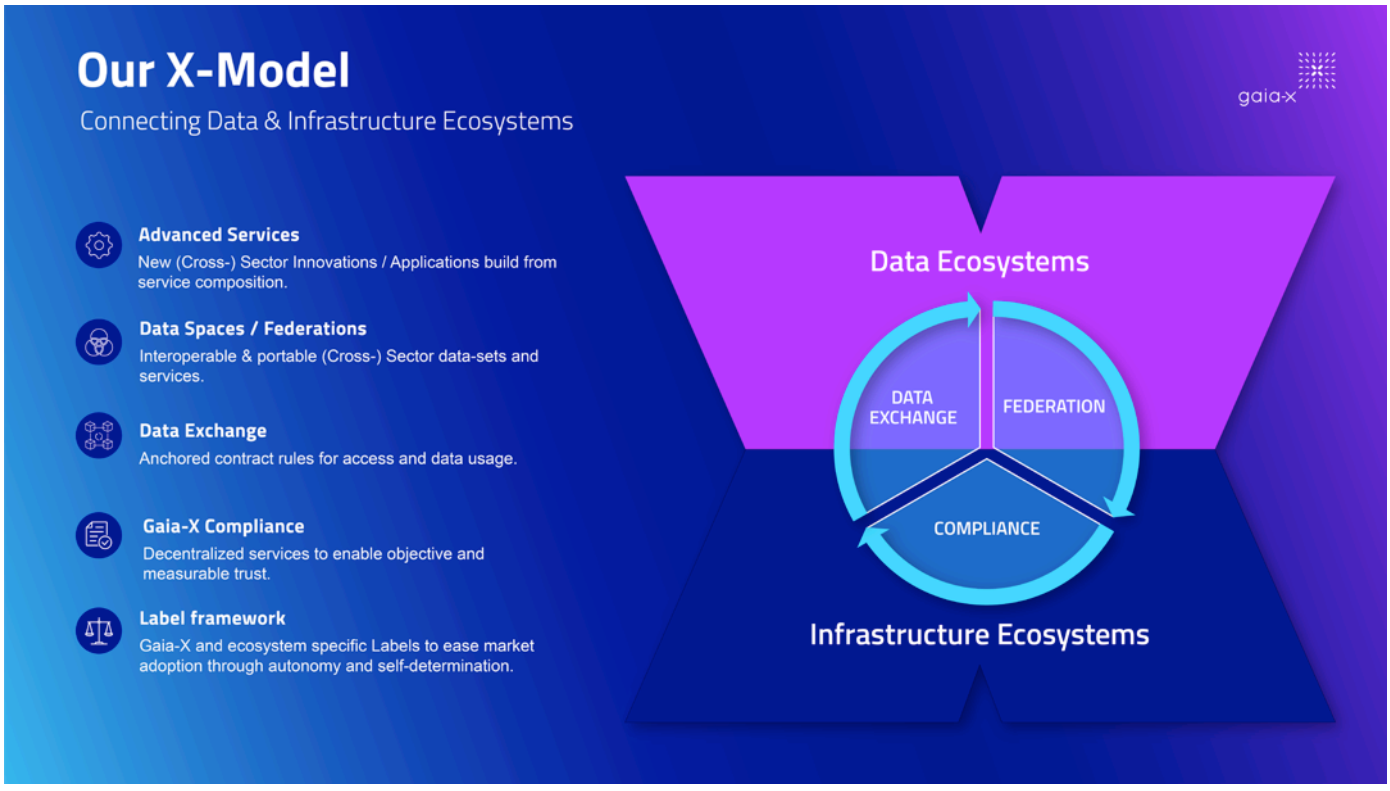
Qual è la vostra visione per i prossimi anni?

Entro il 2027 vogliamo che Gaia-X diventi l'infrastruttura di riferimento per lo scambio dati in Europa. Non l'unica, ma certamente la più affidabile quando si parla di dati critici o sensibili. Immaginiamo un ecosistema dove startup, aziende e PMI europee abbiano un reale controllo sui propri dati personali, e in cui le pubbliche amministrazioni europee offrano servizi digitali 'sovrani' di livello mondiale. La sovranità digitale europea si costruisce giorno per giorno, attraverso scelte tecnologiche, investimenti strategici e un impegno condiviso verso valori che ci distinguono.

Gaia-X è uno strumento fondamentale in questo percorso, ma richiede il supporto di tutti gli stakeholder: governi, imprese, mondo accademico e società civile, per garantire un futuro digitale europeo. ■

BIO

Con oltre 25 anni di esperienza nel settore dell'Information Technology, dove ha ricoperto ruoli tecnici, operativi, commerciali e di direzione generale.
Attualmente svolge il duplice incarico di Chief Operating Officer di Dynamo S.p.A. e si occupa di Public Affairs per Aruba S.p.A. nelle aree Cloud e Data Center. Dal giugno 2025 è membro del Board of Directors di Gaia-X Association for Data and Cloud AISBL e Chairman del Gaia-X ICT Service Providers Sounding Board, dove contribuisce allo sviluppo delle politiche europee sulla sovranità dei dati e promuove l'adozione del framework Gaia-X nell'ecosistema delle infrastrutture digitali europee.
Con una formazione specializzata in informatica giuridica, ha maturato competenze distintive nell'analisi dell'impatto delle normative europee e nella trasformazione dei requisiti regolamentari in opportunità strategiche di business.



La sfida delle democrazie nel mondo iper-interconnesso e post-globale. Intervista VIP a Roberto Baldoni.

Autore: Massimiliano Cannata

"La tecnologia viene talvolta descritta come il 'nuovo Leviatano' perché appare pervasiva, capace di influenzare ogni aspetto della vita collettiva e di concentrare un potere che sembra sfuggire al controllo democratico. Ma questa immagine è fuorviante: la tecnologia non ha una volontà propria, non è un'entità autonoma. È sempre un moltiplicatore di potere nelle mani di chi la progetta e la governa. La tecnologia incorpora i valori delle società che la sviluppano. Un algoritmo sviluppato in una società democratica riflette, pur con tutti i limiti del caso, un'impostazione orientata ai diritti, alla trasparenza, alla protezione dell'individuo. Lo stesso algoritmo sviluppato in un regime autoritario può essere progettato anche per sorvegliare, censurare o controllare. Per questo la primazia tecnologica delle democrazie non è solo una questione industriale, ma una questione di libertà. La tecnologia diventa un 'Leviatano' solo quando manca una governance adeguata o quando è costruita anche per fini di controllo." Roberto Baldoni, già Professore Ordinario di Informatica presso l'Università La Sapienza di Roma, dove ha creato e diretto il primo centro di ricerca nazionale sulla cybersicurezza, Fondatore e Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale. Oggi è Senior Advisor per le politiche tecnologiche e di cybersicurezza presso l'Ambasciata d'Italia negli Stati Uniti. È autore di "Sovranità digitale" (ed. Il Mulino), saggio in cui prende in esame le principali minacce del cyberspazio. L'intervista che segue trae spunto da questo importante e interessante studio.

Prof. Baldoni: "Sovranità digitale" non è un solo il titolo del suo saggio, ma un orizzonte articolato di riferimento non solo tecnologico, ma anche politico. Non crede che ci sia una contraddizione in termini, tenuto conto che i sistemi distribuiti e la connettività non ammettono quelle barriere e quei confini che definiscono la sovranità?

"Sovranità digitale" non significa autarchia tecnologica, né vuol dire chiudere le frontiere del cyberspazio. Nel libro descrivo l'importanza che risiede nella capacità di un Paese di mantenere un margine di scelta sovrana sulle tecnologie critiche da cui dipendono sicurezza, economia e democrazia: cloud, dati, reti, semiconduttori, intelligenza artificiale, piattaforme. In un mondo di sistemi distribuiti e supply chain globali,

nessuno Stato può essere totalmente indipendente. La sovranità digitale oggi è autonomia strategica dentro relazioni di interdipendenza: poter dire "sì", "no" o "così" a una tecnologia, a un fornitore, a una piattaforma, senza essere ricattabile. Potere avere queste opzioni non è scontato, ma dipende dalle politiche economico-industriali e di sicurezza nazionale di un Paese.

La guerra ibrida

Siamo nel tempo della post globalizzazione, come Lei spiega molto bene nella prima parte del saggio. Quali equilibri si aprono sul terreno della geopolitica?

Siamo entrati nella fase della post-globalizzazione: le interdipendenze tecnologiche, che un tempo riducevano i conflitti, oggi vengono sempre più usate come strumenti di pressione geopolitica - dalle terre rare, ai chip, al cloud, dalla disinformazione agli attacchi cyber. È una guerra ibrida continua, economica e informativa, iniziata più di dieci anni fa e progressivamente intensificata. Le democrazie europee se ne sono accorte con colpevole ritardo: la pandemia e, subito dopo, l'invasione russa dell'Ucraina hanno mostrato quanto fossimo esposti. Le nostre catene del valore globalizzate, che spesso nascondono profonde dipendenze tecnologiche e energetiche, si sono rivelate capaci di trasformarsi rapidamente da opportunità economiche a vulnerabilità strategiche. Oggi le democrazie non sono indifese, ma devono colmare un divario organizzativo. La sfida è passare da una difesa frammentata (per settori, per Paesi e spesso per interessi industriali) a una strategia comune, in cui sicurezza economica, sviluppo tecnologico, innovazione e sicurezza informativa siano trattate come un unico fronte.

Anche sul fronte della difesa militare avviene tutto questo?

Certamente. Nel mondo iper-interconnesso e dell'AI, lo spazio economico-tecnologico e quello militare si sovrappongono. C'è poi un punto cruciale: le tecnologie incorporano i valori delle società che le producono. Negli anni '70 e '80 questo era quasi scontato: la quasi totalità delle tecnologie critiche nasceva negli Stati Uniti (e in parte in Europa). Oggi non è più così. La competizione tecnologica è diventata competizione tra modelli politici, tra sistemi di valori e tra visioni opposte del rapporto tra individuo, Stato e mercato. Per questo le democrazie devono restare unite. Senza una risposta coordinata, rischiamo che il futuro tecnologico venga plasmato da potenze che considerano la tecnologia non uno strumento di libertà, ma un mezzo di controllo. E il prezzo di una sconfitta, in questa competizione, sarebbe molto più alto di quello economico: riguarderebbe la natura stessa delle nostre società aperte.

Il rapporto tra potere e tecnologia caratterizza questa delicata fase della storia. Come si fa a regolare questo complesso connubio?

Potere e tecnologia sono sempre stati intrecciati, ma oggi la novità è la scala, la velocità e la pervasività delle tecnologie digitali, che incidono insieme su economia, sicurezza nazionale e diritti. L'obiettivo della regolazione non è frenare l'innovazione, ma orientarla, garantendo che tecnologia e potere restino compatibili con lo Stato di diritto e con la capacità delle democrazie di competere. Per questo non basta più la regolazione "ex post", servono strumenti proattivi e istituzioni competenti. In primis, non si può prescindere da principi base democratici sui diritti fondamentali che devono valere per qualunque tecnologia: privacy, non discriminazione, trasparenza algoritmica (ove possibile), responsabilità nell'uso dei dati. Poi sulle supply chain critiche (cloud, 5G/6G, AI ad alto rischio, infrastrutture essenziali) vanno inserite

verticalmente regole con requisiti stringenti di sicurezza e di governance non solo tecnici. Il Toolbox 5G europeo è un esempio di approccio geopolitico applicato a una supply chain specifica. Gli standard tecnici e le dottrine di "trusted" technology sono un altro pilastro. Una tecnologia non deve solo funzionare: deve essere sicura, controllabile e coerente con valori democratici. Vuol dire definire chi controlla software, hardware, dati e filiere. Se la tecnologia è elemento strategico in grado di bloccare l'economia, le politiche tecnologiche non possono essere affidate a linee di comando senza competenze adeguate o messe in seconda priorità. Questo blocca la crescita industriale ed economica di una nazione fino a staccarla dai Paesi più avanzati mettendola in condizioni di subalternità. Negli Stati Uniti sul lato tecnologico dell'amministrazione Trump vi sono importanti esperti, come lo erano quelli dell'amministrazione Biden. Infine, due regole base: "non puoi regolare ciò che non conosci" e "non puoi regolare ciò che non

produci". Ad esempio, l'AI Act europeo ha ignorato entrambe, tentando di normare una tecnologia di cui ancora non conosciamo completamente il comportamento e che l'Unione non produce su scala globale. Non stupisce che ora si punti a correggerlo con il Digital Omnibus Act, per evitare ulteriori danni alla competitività europea.

Gli indicatori della sovranità digitale

La sovranità digitale di un paese è qualcosa di oggettivamente misurabile?

Non esiste un "indice unico", ma è possibile costruire una batteria di indicatori. Nel lavoro sulla sovranità digitale richiamo almeno quattro dimensioni: Capacità tecnologica, industriale e workforce: presenza nazionale (o in alleanze affidabili) lungo le filiere di tecnologie critiche: semiconduttori, cloud, AI, cybersecurity, satelliti, cavi. Numero di laureati STEM prodotti dal sistema nazionale e confronto con il fabbisogno interno. Capacità regolatoria e di enforcement: leggi chiare, autorità competenti in grado di applicarle, capacità di imporre condizioni a fornitori stranieri. Resilienza e sicurezza: livello di protezione delle infrastrutture critiche, tempi medi di rilevazione e risposta agli incidenti, adozione effettiva di standard di sicurezza. Potere di negoziazione e di alleanza: ruolo del Paese in accordi internazionali, organismi di standardizzazione e nella definizione di "club" di tecnologie fidate. La sovranità digitale, in sintesi, è una combinazione di capacità tecnica, potere economico, strumenti giuridici e alleanze politiche.

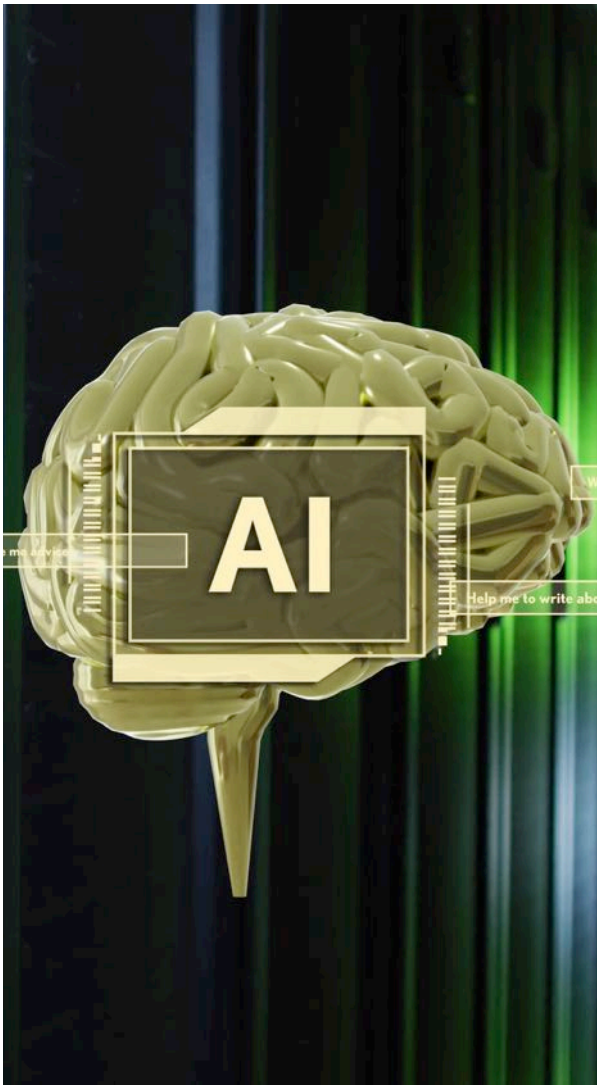
Nel profondo cambiamento d'epoca che stiamo vivendo, anche alla luce della rivoluzione apportata dell'intelligenza artificiale e degli algoritmi, la sicurezza cibernetica che posto occupa?

L'intelligenza artificiale generativa, e ancor di più l'AGI quando arriverà, trasformerà progressivamente le nostre società, proprio come i social network hanno trasformato le relazioni interpersonali. Sanità, finanza, difesa, infrastrutture fisiche, pubblica amministrazione, relazioni sociali: l'IA diventerà sempre più parte integrante di tutto questo. A quel punto, la cybersicurezza non sarà più un semplice layer verticale della pila tecnologica: diventerà il tessuto connettivo dell'intero ecosistema digitale. I modelli di IA si basano su immense quantità di dati e su infrastrutture cloud complesse. Questo li espone a nuove superfici di attacco: furto di modelli, data poisoning, manipolazione degli output, compromissione dell'infrastruttura di training e inferenza. E più questi sistemi saranno integrati nel mondo reale, più un attacco digitale produrrà effetti materiali immediati: da errori puntuali, fino a ospedali bloccati, mercati finanziari destabilizzati, reti energetiche perturbate. Come è accaduto per l'informatica classica, anche nell'IA la frontiera delle minacce si sta già spostando a monte verso la supply chain dell'AI (framework, librerie, modelli open source, chip specializzati). L'IA presenta frontiere poco conosciute, come la manipolazione cognitiva, che colpisce direttamente le nostre menti e diventa esponenzialmente più efficace grazie ai contenuti sintetici. Questa dinamica rappresenta anch'essa una minaccia sistemica per la democrazia e la sicurezza nazionale. Per questo la cybersicurezza deve diventare by design, integrata lungo tutto il ciclo di vita dell'IA: progettazione, training, deployment, aggiornamento e audit. Nel quadro della sovranità digitale, la cybersicurezza diventa quindi l'abilitatore fondamentale per delegare alla tecnologia funzioni critiche senza perdere controllo.

Le diverse tipologie di minacce

Nel saggio viene fatta una disamina molto densa delle diverse tipologie di minacce. Può darci un'idea in rapida sintesi?

Nei libri e nelle mie lezioni distinguo quattro grandi famiglie: *le minacce da attacchi informatici*: attacchi sponsorizzati da uno Stato, attacchi di cybercriminali, attacchi di hacktivisti; *le minacce alla integrità, confidenzialità e disponibilità di una filiera di fornitura; le minacce da tecnologie dirompenti*: intelligenza artificiale



e computer quantistici; *le minacce sociali, economiche e industriali:* disinformazione, standard internazionali della tecnologia, pratiche predatorie e forza lavoro. Siamo

preparati, lei mi chiede? Meglio rispetto a dieci anni fa, sugli attacchi informatici e sulle pratiche predatorie, ovvero gli acquisti di asset nazionali critici da parte attori ostili. Abbiamo preso piena consapevolezza delle problematiche derivanti dal non controllo degli organismi di standardizzazione internazionale e degli attacchi alle catene di approvvigionamento, iniziando a mettere le prime basi efficaci di contrasto. Strutture come le agenzie nazionali di cybersicurezza, le normative su perimetri critici cibernetici, le regole sugli investimenti esteri e la direttiva NIS2 hanno contribuito a rafforzare la consapevolezza e a costruire resilienza. Tuttavia, il tessuto delle PMI resta vulnerabile e in Europa mancano ancora politiche industriali e di innovazione adeguate alle sfide del periodo che stiamo vivendo.

Quali sono le aree di maggiore vulnerabilità?

Siamo impreparati agli attacchi cognitivi e a quelli potenzialmente creati dalla tecnologia stessa, come la gestione degli errori generati dalle AI o l'impatto dall'arrivo dei computer quantistici. Tuttavia, la madre di tutte le minacce resta quella legata alla forza lavoro altamente specializzata. Tutti i Paesi occidentali affrontano un doppio deficit: producono un numero di laureati STEM inferiore al fabbisogno, aggravato da una forte denatalità. A fronte dei 4 milioni di laureati STEM sfornati dalla Cina nel 2024, gli Stati Uniti nello stesso anno hanno prodotto 750mila laureati STEM, di cui un terzo in ambito internazionale che con molta probabilità rientrerà in patria. Una nazione che non produce la forza lavoro necessaria dovrà importarla o delegare il controllo alle macchine. Nel primo caso si potrebbe scatenare un mercato aggressivo tra paesi occidentali like-minded, con il rischio di penetrazione di aziende ostili all'interno di aziende strategiche nazionali o supply chain critiche. Nel secondo caso, gli errori delle macchine sarebbero più frequenti, più impattanti e meno gestibili.

Qual è il posizionamento dell'Europa rispetto a USA e CINA nella partita dell'innovazione e della governance del fattore tecnologico, e che futuro si apre per l'UE?

Le debolezze strutturali dell'Unione Europea sono note: frammentazione con 27 politiche industriali diverse; meccanismi decisionali lenti e soggetti al diritto di veto; un potere regolatorio spesso avverso all'innovazione; assenza di grandi piattaforme tecnologiche, dovuta all'impossibilità di sfruttare la scala del mercato europeo; capitali di rischio molto inferiori a quelli statunitensi o cinesi. Superare questo impasse richiede un'unica strada: attuare pienamente l'Agenda Draghi. ■

BIO

Roberto Baldoni è stato fondatore e Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale. In precedenza, ha ricoperto il ruolo di Vice Direttore Generale del Dipartimento delle Informazioni per la Sicurezza, con delega alla cybersicurezza nazionale e rappresentante italiano alla NATO per le politiche di cybersecurity. Per oltre vent'anni è stato Professore Ordinario di Informatica presso l'Università La Sapienza di Roma, dove ha creato e diretto il primo centro di ricerca nazionale sulla cybersicurezza. A livello nazionale ha inoltre fondato e guidato il Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica. Attualmente è "Senior Advisor per le politiche tecnologiche e di cybersicurezza" presso l'Ambasciata d'Italia negli Stati Uniti, Professore Onorario all'Università La Sapienza e membro del Board of Directors del Krach Institute for Tech Diplomacy at Purdue University. È autore di oltre duecento pubblicazioni scientifiche internazionali tra articoli e libri. Di recente ha ricevuto l' "Outstanding Leadership Award" dall'IEEE Technical Committee on Homeland Security.

La sicurezza è un valore che va perseguito con un qualificato gioco di squadra. Intervista VIP a Luca Giusti.

Autore: Massimiliano Cannata

"Associso è una realtà che nel ventaglio delle diverse attività istituzionali, riserva un posto di primo piano al dialogo e al confronto professionale e conoscitivo con tutti gli stakeholders di una filiera articolata e complessa come quella della sicurezza cibernetica. Farne parte in questa fase di profondo mutamento è di fondamentale importanza per la definizione del ruolo del CISO, che ha la possibilità di maturare un'esperienza associativa qualificata che si riflette all'interno delle singole realtà organizzative, con indubbi benefici per tutti gli attori della catena del valore".

Luca Aldo Giusti, Ciso & Head of Infrastructure@integra document management (IDM), delinea con nettezza l'importanza di associarsi per maturare una consapevolezza e una cultura del rischio adeguata alla complessità tecnologica entro cui si muove il manager della security.

Dott. Giusti, partiamo dall'importanza di associarsi e di agire in squadra, un aspetto che lei sottolinea con molta forza in ogni occasione. In Associso ha trovato quella dimensione collaborativa che cercava ?

La mia riposta è assolutamente positiva. La sicurezza è un valore che si può perseguire solo agendo in squadra. Fare parte di una realtà che ha nel dialogo aperto e nello scambio di know-how il suo fondamento significa, di fatto, essere messi nelle condizioni di poter sfruttare una grande opportunità per valutare le proprie strategie, scelte e posizioni, confrontandole con quelle di altri professionisti del settore. Questo crea valore aggiunto, oltre a dare la possibilità di esplorare valutazioni e prospettive che provengono da realtà diverse dalla propria, che arricchiscono il background del singolo, mettendo a fattor comune expertise ed esperienza e creando un risultato che va oltre quanto un singolo operatore, per quanto qualificato, potrebbe produrre.

Conoscere è proteggere

Sicurezza del cyberspazio: un tema che, nella società del rischio, ha assunto una valenza strategica. Quali competenze bisogna mettere in campo ?

È una domanda molto complessa, che meriterebbe un trattato approfondito. Cercando di sintetizzare raggrupperei le competenze in tre grandi macro-aree: competenza tecnica, competenza strategica e competenza trasversale. La prima, la più ovvia, mette in campo conoscenze specifiche, tecniche e tecnologiche, che permettono ad un soggetto di avere pieno controllo e governance sugli strumenti, sulle infrastrutture e sulle tecnologie che sceglie di utilizzare. Nell'ambito della competenza strategica ricade, in particolare, il ruolo del Ciso, con la capacità di delineare, scegliere e modificare laddove necessario, la strategia che garantisca all'azienda il risultato più adatto, efficace ed efficiente a fronte dell'analisi dei rischi approfondita e dettagliata, che è e resta la base da cui partire. La competenza strategica include anche l'area, sempre più importante, della governance e della compliance, che permetta di definire le metriche utili ad avere il polso dell'andamento del processo di security, ma anche di conoscere, applicare e interpretare le normative e legislazioni che possono impattare il settore in cui si opera o migliorare la security posture dell'azienda.

Veniamo alla terza tipologia prima ricordata. Quando parla di competenza trasversale, termine più sfuggente, a cosa allude?

Alludo alle soft skill: doti come la capacità di comunicazione, molto importante per relazionarsi con gli stakeholder in modo assertivo, senza inutili tecnicismi; la capacità di problem solving, basilare sia per l'analisi che per il management di un incident; e la capacità di adattamento, che permette di muoversi con confidenza in un mondo in divenire e che richiede una capacità di reazione immediata.

I dati, asset prezioso per una sicurezza "by design"

I dati sono divenuti un asset prezioso, il "nuovo petrolio", come molti studiosi lo definiscono. Quali strategie è necessario adottare per tutelare le informazioni ?

I dati, intesi come informazioni strutturate, sono il fulcro del concetto stesso di cybersecurity. È fondamentale considerare il dato in tutto il suo ciclo vitale, ricordando che può cambiare media e forma durante la sua esistenza. Il concetto di sicurezza, declinato negli attributi di riservatezza, integrità e disponibilità, deve quindi seguire il dato in tutti i suoi passaggi. Gli strumenti sono - e devono essere variegati – ad esempio gestire un'informazione che nasce cartacea, diventa poi digitale

e viene infine tramesso ad una altra entità. Una falla di sicurezza in uno qualsiasi di questi passaggi compromette l'intero ciclo vitale che mira alla tutela di informazioni preziose, vanificando di fatto il processo. Occorre pertanto scegliere gli strumenti più appropriati per ogni passaggio o cambio di stato del dato, e al contempo formare il personale che ne accompagna la vita: producendo, elaborando, trasmettendo o utilizzando le informazioni. È fondamentale fornire agli utenti la consapevolezza di cosa significhino gli attributi che rendono un dato sicuro e quale sia il loro ruolo nel ciclo di vita, senza dimenticare i rischi che possono correre o generare mentre il dato è sotto la loro responsabilità (si pensi, ad esempio, a informazioni stampate e dimenticate o a dati discussi verbalmente in presenza di persone non autorizzate). Solo così si può minimizzare il rischio di perdita, furto o compromissione delle informazioni.

Si parla spesso di sicurezza by design e di "postura" per indicare il livello di attenzione e di capacità di prevenire gli attacchi da parte di aziende e istituzioni. Ma, in concreto, cosa significano questi concetti?

La sicurezza dipende da diversi fattori, tra cui il livello di esposizione, la capacità di accettare un rischio e la tipologia di settore in cui si opera. Per una strategia di sicurezza efficace è fondamentale che la direzione abbia ben chiari i rischi a cui è esposta e definisca la soglia di accettazione, il cosiddetto risk appetite. Il ruolo del CISO è guidare la direzione verso scelte consapevoli e coerenti con il contesto, soprattutto alla luce dei recenti sviluppi normativi, come NIS2 e DORA, che impongono standard non negoziabili e da applicare nel modo più appropriato alla singola realtà. In questo scenario, un'analisi continua consente di definire la postura attuale rispetto a quella desiderata, un indicatore chiave (KPI) fondamentale per la strategia di sicurezza. La postura di sicurezza di un'azienda, una volta definita a livello strategico, può essere raggiunta attraverso diversi strumenti tecnici che, per quanto importanti, restano mezzi e variano in funzione del settore, del livello tecnologico e del rischio a cui si è esposti. La rapidissima evoluzione del panorama richiede inoltre la capacità di adattarsi, modificando la scelta

e l'implementazione di tali strumenti in modo tempestivo.

Quando si parla di regole, entra sempre in gioco il fattore umano che, secondo le statistiche più accreditate, è coinvolto nell'80% degli incidenti informatici e delle minacce gravi alle organizzazioni produttive. Quale risposta è necessario individuare?

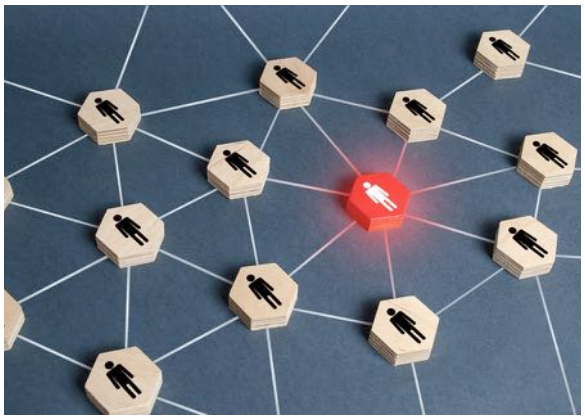
Il fattore umano è il fulcro di ogni strategia di sicurezza: nessuno strumento può essere davvero efficace senza che le persone acquisiscano una solida cultura della sicurezza. Come ricordato nella domanda, la percentuale di attacchi riusciti a causa di errori umani è in costante crescita e il dipendente – bersaglio preferenziale, soprattutto per i sempre più sofisticati metodi di phishing e derivati – rappresenta il punto più vulnerabile. È quindi fondamentale formare le persone, insegnare loro il valore che la sicurezza riveste in tutte le fasi del ciclo di vita delle informazioni e monitorare il livello di consapevolezza raggiunto. Programmi di formazione, iniziative di awareness e simulazioni (ad esempio campagne di phishing) sono, a mio giudizio, imprescindibili per ridurre il rischio e monitorare lo stato di vulnerabilità.

La cybersecurity è ormai entrata a pieno titolo nelle dinamiche geopolitiche. Esiste un fitto intreccio tra tecnologia e potere che sta ridefinendo gli equilibri globali, mettendo a rischio la democrazia. Questo comporta una responsabilità aggiuntiva per i manager della sicurezza, chiamati a guardare oltre il perimetro aziendale, assumendo il peso di implicazioni fino a ieri inimmaginabili?

La cosiddetta guerra "ibrida", che si svolge sia sul piano fisico – noto da secoli – sia su quello dei cyber attacchi, è una realtà consolidata da molti anni e, per sua natura, difficile da identificare e controllare. Basti pensare al caso Stuxnet del 2010. Ad oggi qualunque potenza sul piano geopolitico è dotata ed è di conseguenza capace di attuare sistemi di attacco ibrido, di cui è difficile capire la provenienza. Le conseguenze di azioni così mirate e sofisticate generano danni diretti e danni, per così dire, di "ritorno", impersonando un diverso attore per fini politici. Il rischio di trovarsi, dunque, in situazioni di "fuoco incrociato" è sempre più alto. Come operatori del settore, e considerando che le realtà, sia governative che private, operanti in settori critici sono sempre più oggetto di attacchi che in alcuni casi appaiono, sia per la qualità che le risorse, state sponsored, ciò che possiamo fare è cercare il più possibile di limitare la superficie esposta ed essere pronti a identificare e contenere le potenziali minacce.

Cosa di certo non semplice se consideriamo che è scomparso ogni perimetro, e che siamo nell'epoca della interconnessione e della interdipendenza. Cosa pensa al riguardo?

Bisogna alzare sempre di più la soglia di attenzione.

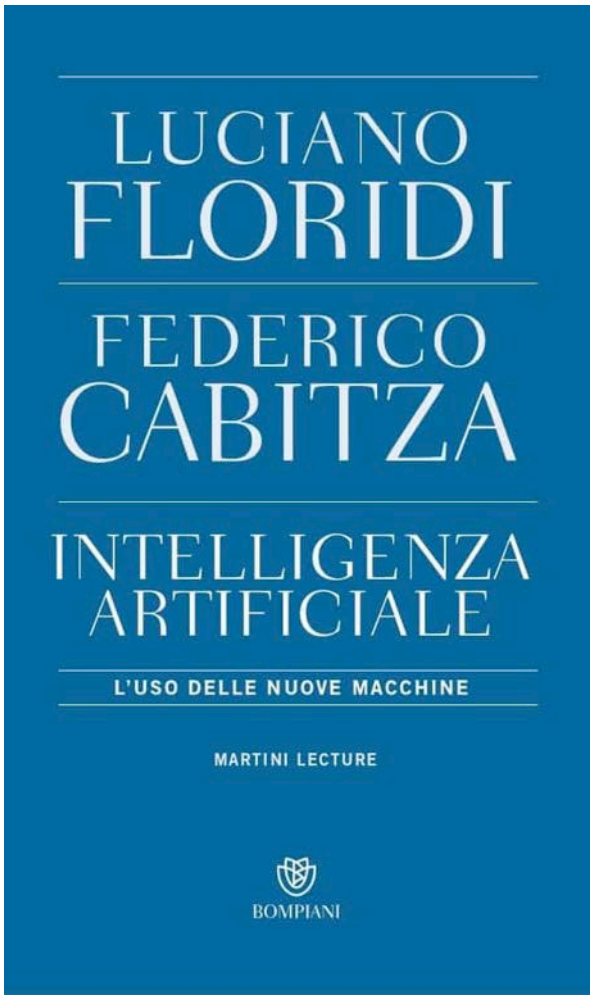


Su questo punto è importante considerare che il blocco geografico, pur essendo consigliato, non è più una garanzia di risultato, poiché il numero di proxy – leciti o meno – è in costante crescita. Da notare che spesso i proxy leciti non applicano le stesse restrizioni raccomandate dai bersagli finali. Ridurre il perimetro, identificare asset sacrificabili ai fini della mitigazione dell'impatto e della raccolta di intelligence è sempre più cruciale, perché le risorse dell'attaccante sono in aumento e non devono rispettare i processi di approvazione, implementazione e gestione che vincolano i potenziali bersagli. Chi attacca è più veloce, senza regole e spesso dispone di maggiori risorse rispetto a chi difende. Ne consegue che la strategia della pura resistenza su tutto il perimetro comincia a vacillare: diventa necessario creare aree a basso impatto che possano essere utilizzate per disperdere almeno in parte le risorse dell'attaccante e massimizzare la resistenza. Avere tempo per organizzare la strategia migliore mette l'attaccante nella condizione di perdere il momentum, esaurendo il vantaggio iniziale e risultando decisivo. ■

BIO

Luca Giusti, classe 1978, da sempre affascinato dall'informatica, decide di farne la sua professione dopo gli studi di Psicologia. Negli anni ha ricoperto il ruolo di Sistemista nel settore degli studi professionali, per poi approdare nel settore legale ricoprendo il ruolo di IT Manager per alcuni tra i più famosi Studi Legali di Milano. La voglia di apprendere e sperimentare in nuovi campi lo porta a seguire numerosi corsi di formazione, dedicandosi specialmente al percorso ITIL, che lo porta ad ottenere la qualifica di Managing Professional. Decide così di abbandonare l'ambiente degli Studi Legali e di passare al ruolo di Consulente in ambito Infosec, da sempre punto di interesse professionale, e Service Management, specializzandosi nel campo della ISO27001. Tramite questo ruolo conosce IDM, con la quale collabora per diversi anni fino a diventare parte integrante dell'azienda nella quale ricopre ora i ruoli di CISO, Head of Infrastructure e EUC. Il suo approccio alla sicurezza, mutuato dalla base di studi, è antropocentrico e si concretizza nel motto "La sicurezza è una questione di persone", che da sempre segue e applica al suo metodo di lavoro al fine di portare il miglior risultato possibile e coniugare un approccio tecnologico ad un approccio umano, per ottenere una completa cultura della sicurezza a livello aziendale.

La sicurezza centro di gravità dei "futuri possibili". Intervista VIP a Luciano Floridi.



Autore: Massimiliano Cannata

Nella grande complessa partita della rivoluzione digitale si fronteggiano aspetti culturali e simbolici, e strumenti di governance, potere e controllo delle tecnologie. Se è vero che fra poco abiteremo la Luna, bisognerà rifondare i processi della nostra conoscenza per affrontare questa sfida, che per non rappresentare una "seconda colonizzazione", deve rispettare l'uomo e l'ecosistema in tutte le sue articolazioni. Luciano Floridi, voce autorevole della filosofia contemporanea, si spende da tempo per far comprendere la necessità di un approccio olistico allo sviluppo della tecnoscienza. Gli strumenti della tecnoscienza devono renderci "inquieti" come sosteneva il Cardinale Martini nel saggio "Intelligenza artificiale: l'uso delle nuove macchine" (ed. Bompiani), in cui fotografa molto bene la tendenza fondamentale del tempo che stiamo vivendo. L'IA non deve portarci a interrogare l'altro, non a negarlo, ridando forza al dialogo socratico che connota l'uomo quale essere pensante. La sicurezza, tema attorno a cui ruota l'intervista, è considerata da Floridi un valore primario nella società delle reti. Questa età delle catastrofi ce lo conferma: dalle Torri Gemelle, che hanno aperto alla pandemia, alla cyber war che si combatte in Ucraina e in Medio Oriente, stiamo assistendo a un contino innalzamento dei livelli di rischio, con la conseguenza ricerca di protezione e di tutela, che corre lungo il pianeta e attraversa equilibri geopolitici tutti da definire, in un generale mutamento degli assetti istituzionali e produttivi. La rivoluzione in atto ha una radice epistemologica che investe il nostro modo di essere nel mondo. Prima ne avremo consapevolezza, prima riusciremo a superare la perenne transizione tra il vecchio e il nuovo, tra un secolo - il Novecento - duro a morire e l'orizzonte del nuovo millennio, di cui non continuiamo a non riuscire a interpretare i lineamenti e le dinamiche di sviluppo. Floridi ha di recente pubblicato un nuovo saggio "La differenza fondamentale" (ed. Mondadori), in cui fa il punto sul delicato incrocio che intercorre tra innovazione, sicurezza e intelligenza generativa. Uno scritto destinato, come i precedenti, a generare un grande dibattito sul delicato binomio uomo–macchina.

Prof. Floridi, in questa delicata fase della storia l'escalation degli attacchi informatici è una componente che preoccupa l'opinione pubblica mondiale. Truffe on line, furti di dati, manomissioni di reti e

sistemi vengono adottati con strumenti sempre più sofisticati. Un filosofo quale Lei è, da sempre attento alle fenomenologie del cambiamento, cosa pensa di tutto questo?

Bisogna alzare la soglia dell'attenzione su questi temi. Credo sia importante sviluppare un'educazione al digitale che ancora non abbiamo maturato. Non fasciamoci però la testa, perché l'innovazione non va censurata, ma interpretata, compresa, e disciplinata con razionalità. Quando il cardinale e teologo Martini parlava di futuri possibili non intendeva certo alimentare la fantascienza, né alcuna speculazione fantasiosa, intendeva piuttosto sottolineare l'apertura equilibrata che bisogna avere rispetto al cambiamento… L'umanità deve saper esercitare responsabilità e visione quando lavora sulla ricerca e l'innovazione…perché la vita è la nostra, non dimentichiamolo mai. Significa che dobbiamo rimanere padroni dei processi, che vuol dire essere umani a tutto tondo. Ricordiamoci che il futuro non avviene casualmente, non è una serie di eventi caotici, è fatto di miliardi di progetti e di idee che trovano punti di convergenza ed equilibri. Mi viene in mente l'immagine delle gocce d'acqua in un bicchiere, pensando ai grandi movimenti di popolo che hanno mutato la faccia della storia nei secoli. Assumiamoci dunque le nostre responsabilità: questo l'insegnamento di Martini che mi sento di condividere, anche dalla mia prospettiva, che è quella di un laico agnostico "inquieto".

Ammetterà che la paura ha mille volti, per questa ragione la sicurezza non ha più un perimetro, si misura su un ecosistema articolato. Non Le pare che il "futuro" sia divenuto uno spazio della mente troppo carico di incertezze?

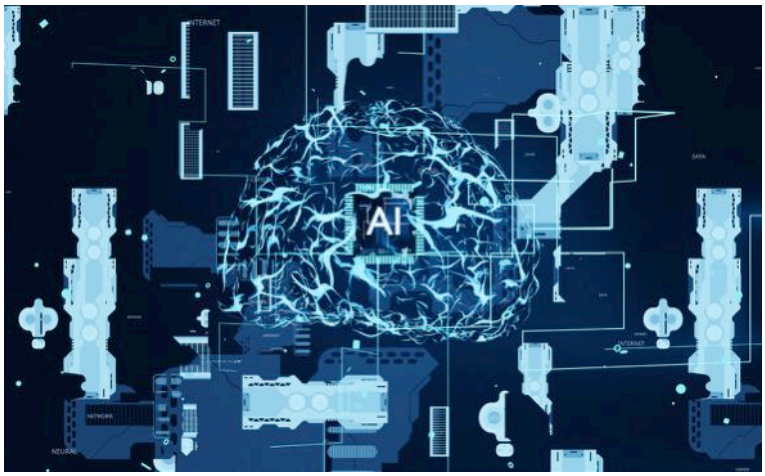
L'incertezza c'è sempre stata. Dobbiamo sollevare i dubbi necessari, ma poi il compito di noi filosofi, che facciamo un'operazione di "design concettuale", è di creare e ricreare idee e concetti in una realtà che muta velocemente, per poter affrontare questi dubbi. Insomma, sollevare domande rilevanti e offrire risposte convincenti.

Aspetto chiave è la protezione delle informazioni tanto che, lo ha scritto Michele Mezza nel saggio Algoritmi di libertà (ed. Donzelli) il dato è divenuto un asset sociale. Anche questa una frontiera difficile da presidiare, siamo preparati al riguardo?

Ci sono ovviamente contesti sperimentali come i sandboxes, ma culturalmente non esiste alcun "recinto" chiuso entro cui testare strumenti e misure. La cybersecurity va vista dentro una frontiera mobile, seguirne l'evoluzione richiede un costante aggiornamento. Il concetto di tutela si è per altro enormemente ampliato in questi anni, fino ad abbracciare tutti gli ambiti della nostra vita. La disciplina normativa di fatto insegue il prepotente sviluppo delle applicazioni scientifiche, difficili da regolare soprattutto quando a prevalere sono gli interessi di mercato senza rispetto per i diritti dell'uomo, ma potrebbe anticipare e guidare le linee di sviluppo tecnologico, se volesse. In questo senso, si sta facendo strada un approccio europeo al digitale. Credo che sia uno sforzo difficile ma fruttuoso. Non si tratta di essere vicini al liberismo americano, o allo statalismo di stampo autocratico che riflette la cultura cinese dedita alla censura e alla soppressione dell'autonomia individuale.

L'IA e il metaverso sono il banco di prova più difficile?

Sono i temi del momento. Sono strumenti e ambienti che condizionano



l'io, scompaginano lo spazio e il tempo entro cui ci muoviamo, modificando le categorie della conoscenza. Legislatori, ma anche chi si occupa di impresa, manager e - non dimentichiamo - i dirigenti pubblici, sono chiamati a gestire questa radicale trasformazione. La PA è un ambiente produttivo multilivello (pensiamo alle differenze tra Stato, Regioni e Comuni), che andrà incontro agli enormi cambiamenti nel breve e medio periodo. I dirigenti pubblici dovranno osservare una "tassonomia del rischio" quale criterio dirimente nel fare scelte che chiamano in causa la quotidianità di tutti. Pubblico e privato dovranno collaborare nel tessere le strategie migliori. La collaborazione avviata dall'Autorità garante della Protezione dei dati e dall'ACN (Agenzia per la Cybersicurezza Nazionale) credo che vada nella giusta direzione.

Oltre la "cieca volontà di potenza della tecnica"

È giusto dunque ritenere che l'intelligenza artificiale è un'ulteriore manifestazione di quella che Emanuele Severino definiva "cieca volontà di potenza della tecnica" ?

Non alimenterei visioni apocalittiche. La ricetta è quella di sempre, la dovremmo conoscere: serve più conoscenza, e meno oscurità. La paura è fomentata dall'ignoranza: paura sociale, quindi dell'altro ma anche della tecnologia. La tecnologia esercita una domanda di conoscenza molto precisa. La responsabilità rimane la nostra, quando utilizziamo mezzi e strumenti sofisticati e potenti. Attenzione però: credo che sia pericoloso parlare di umanità in generale, come se fosse un unico blocco. Da un lato abbiamo una parte del mondo che produce, utilizza, si serve della tecnologia, per controllare e dominare, dall'altra parte ci sono miliardi di persone che non conoscono il linguaggio della tecnica, non la producono e non la controllano e perciò rischiano di subirla. Non c'è un'umanità e una tecnologia presi in universale: ci sono tante tecnologie e tante umanità, il tema è come si rapportano tra di loro. Questo apre la riflessione sulla diseguaglianza, sulla dinamica che contrappone, per usare un termine gramsciano, ceti egemoni e ceti subalterni, nazioni forti e nazioni deboli. È evidente che serve una sensibilità etica per bilanciare il percorso dello sviluppo della scienza e della tecnologia insieme a quello della società e dell'ambiente. Oggi comandano non tanto i produttori di informazione, ma chi controlla l'ambiente digitale che rende possibile la circolazione delle informazioni e la formulazione delle domande essenziali, da cui dipende l'evoluzione economica, politica e sociale della contemporaneità. Per dirla con una frase a effetto: la nuova morfologia del potere è la morfologia dell'incertezza.

Nel saggio "La quarta rivoluzione" Lei insiste sulle principali fenomenologie del cambiamento che stanno segnando la contemporaneità. Infosfera emerge come il termine chiave. Possiamo spiegarne il significato?

On line e off line, sono ormai di fatto un unicum, perché viviamo tutti onlife: è questa l'infosfera. Molti hanno trattato le tecnologie di cui disponiamo come dei semplici canali di comunicazione. È stato così per il telefono, la televisione, la radio. Oggi siamo di fronte a un salto di qualità. Gli apparati digitali stanno creando un nuovo contesto. Prima si stava al telefono, oggi si vive su Internet, prima si guardava la tv, assistendo a uno

spettacolo, oggi siamo noi all'interno dello spettacolo. Lo spazio dentro cui viviamo è fatto di informazione, si tratta di un ambiente dove si mescolano in modo inestricabile analogico e digitale.

"Onlife" è dunque la nuova categoria dell'essere entro cui ci muoviamo. Quale "distanza" dobbiamo mantenere dai dispositivi elettronici per usarli con intelligenza, sicurezza e adeguata consapevolezza?

Quella della distanza è una riflessione importante. Soggetto e oggetto sono categorie che appaiono oggi radicalmente mutate. Di conseguenza anche la distanza tra queste componenti non è quella che siamo abituati a considerare. Persino la relazione che intratteniamo con il mondo risulta modificata, la simpatia e l'antipatia, per dirla con i termini che usavano i filosofi della classicità, ha subito delle varianti molto importanti. La distanza che misuravamo per raggiungere, per esempio una città, non ha più un riferimento preciso che consente di misurarla, perché il digitale sta modificando il paesaggio urbano, attraverso percorsi differenziati in momenti differenti, a seconda del traffico. Gli oggetti sono interattivi, li possiamo toccare, come un'icona che si accende sullo schermo del

mio cellulare, la posso fisicamente spostare nel suo spazio, un po' come si fa con un soprammobile su uno scaffale, è qualcosa con cui interagisco. Anche il soggetto si sta modificando, socializza il suo essere nella rete e con gli strumenti connessi, riconsiderando continuamente la sua identità. La distanza è diventata dunque un rapporto tra interattività e socializzazione. L'individuo manifesta una molteplicità di volti nell'universo tecnologico; la sua identità si articola di conseguenza; la sfida è quella di non frammentarla in mille rivoli, perdendosi tra un TikTok, un social e un Twitter.

Sicurezza e IA nella quarta rivoluzione

Sicurezza e IA: che posto occupano nella transizione tecnologica ?

Sono due facce della stessa medaglia. Immaginiamo di aver costruito un ambiente e di avere allo stesso tempo progettato le forze che lo fanno funzionare. Siamo nella condizione di chi ha costruito un'isola, ed è anche in grado di controllare i movimenti e le azioni degli animali che si muovono in quell'isola. A questo punto c'è da chiedersi: l'ambiente e le forze che agiscono autonomamente in questo ambiente chi le controlla? Sono per definizione sicure? La mia ricerca attuale si sta concentrando sul fatto che l'IA non è una nuova forma di INTELLIGENZA, MA UNA NUOVA FORMA DI CAPACITÀ DI AZIONE, una nuova agency, per usare un termine inglese che non trova corrispettivo nel nostro vocabolario. Forme di agency nel mondo ne abbiamo conosciute tante. La agency della natura: terremoti, vulcani, il vento, "cose che fanno cose", per usare un gioco di parole. La agency biologica: il cavallo, il cane pastore… Quella umana, degli individui che si muovono nell'universo, ma che sono anche in grado di creare il motore, aprendo la strada per la creazione della agency meccanica. E ora ne abbiamo una nuova…

A cosa si riferisce?

A un'agency autonoma, che possiede una capacità di agire che assomiglia al motore a scoppio, in quanto ingegnerizzata, ma anche un po' a un animale, in quanto in grado di apprendere dai suoi comportamenti. Pensiamo all'algoritmo che ha una sua indipendenza, ma qualcuno lo deve pur disegnare e addestrare per raggiungere un risultato, come un cavallo che corre da solo, ma va guidato nella direzione giusta. Torniamo ancora alla riflessione inziale di Martini: è questa la nostra nuova isola entro cui dobbiamo viaggiare sicuri. In un ambiente sempre più digitale controllare queste forme di capacità di agire: naturale, animale, umana, meccanica e digitale vorrà dire essere i "nuovi padroni" dell'universo. Si stanno di fatto sovrapponendo, in modo pericoloso, i controllori dell'ambiente e i controllori di questa nuova capacità di agire. Siamo oltre il vecchio dominio delle élite, fondato sulla differenza di classe e di censo, entriamo in una forma di controllo molto più pervasiva, quella che riguarda l'ecosistema e le forze che si muovono in esso.

Che cosa comporta tutto questo?

Nuovi scenari di intervento e di responsabilità per le classi dirigenti innanzi tutto. È possibile che fra pochi anni arriverà il quantum computing, ultima frontiera dell'evoluzione computazionale. Se le stesse persone avranno il dominio anche su questo nuovo strumento i pericoli aumenteranno. Vede come parlare astrattamente di cybersecurity non serve, bisogna entrare nella dimensione della nuova catena del valore digitalizzata e in contesti urbani innervati da infrastrutture tecnologiche. Non stiamo parlando di fantasie astratte, perché questo futuro è già presente. La sovrapposizione lineare tra egemonia ambientale, egemonia in termini di agency e di capacità di prevedere il futuro deve fare alzare l'asticella dell'attenzione. Non vedo altra via di uscita: i controllati devono controllare i controllori, la società deve maturare questa capacità, velocemente applicando quanto scritto nella costituzione, che assegna al popolo la sovranità. Il circolo virtuoso di ogni democrazia che funzioni è questo, controllare chi decide, avendo la possibilità di rimuoverlo nel momento in cui perde di vista il bene comune. Anche il business deve sottostare a questo controllo "popolare", in questo caso grazie alla competizione. Senza una governance illuminata le nostre democrazie saranno destinate ad ammalarsi con le conseguenze del caso.

BIO

Luciano Floridi è John K. Castle Professor in the Practice of Cognitive Science e Direttore Fondatore del Digital Ethics Center presso l'Università di Yale, nonché Professore di Sociologia della Cultura e della Comunicazione all'Università di Bologna. Una delle voci più autorevoli nella filosofia contemporanea, è stato pioniere della filosofia ed etica dell'informazione ed è un interprete di primo piano della rivoluzione digitale. Ha pubblicato oltre 400 lavori sulla filosofia dell'informazione, l'etica digitale, l'etica dell'IA, la filosofia della tecnologia e la storia della filosofia, molti dei quali sono stati tradotte in tutto il mondo. I suoi libri più recenti sono "The Ethics of Artificial Intelligence" (OUP, 2023) e "The Green and The Blue - Naive Ideas to Improve Politics in the Digital Age" (Wiley, 2023). "Artificial Agency -Explorations of a Post-AI Culture" e "Encounters - An Experiment in Distant Writing" sono in fase di pubblicazione. Tra i numerosi riconoscimenti, nel 2022 è stato insignito del titolo di Cavaliere di Gran Croce dell'Ordine al Merito della Repubblica Italiana per i suoi contributi fondamentali alla filosofia.

Lo sviluppo delle tecnologie imporrà sempre nuovi profili di rischio. Cosa dobbiamo aspettarci?

È importante mettersi insieme, confrontarsi e tentare di socializzare la conoscenza. Nessuno può pretendere di avere una visione complessiva esaustiva, ma tutti possiamo portare un tassello, un contributo per capire e disegnare meglio la realtà. Anche se il mondo cambia mentre credi di averlo studiato e capito bisogna ricordarsi che i fondamenti, la natura umana restano invariati. Per questo vale la pena leggere Platone o Aristotele, che ci dicono cose eternamente valide. Faccio un piccolo esempio biografico: sto leggendo "La ricerca del tempo perduto". Probabilmente ci vorrà un anno, ma mi servirà molto nel mio lavoro quotidiano, per la capacità introspettiva, lo scandaglio dell'animo umano, la lettura della società nelle sue gioie, paure, speranze, pregiudizi o aspettative che fa Proust e che rimane valida anche ai nostri giorni. Rimane poi importante abbracciare l'innovazione, prendere sul serio l'"altro", la diversità con spirito inclusivo. Vuol dire comprendere che, anche nella diversità, la comune umanità è il fattore che ci lega e che può legare anche il dialogo intergenerazionale. Wittgenstein diceva che

devi arrivare dove tocchi il letto del fiume, per intuire la sostanza delle cose per raccontarla senza tempo, senza però illuderti che il tuo sia l'unico discorso. Parlare di quella temporalità che ci diversifica, senza però generare conflitti può aiutarci. Contemperare la costanza delle invarianti e l'accelerazione della temporalità, può infatti rappresentare la chiave che porta al domani.

Nel suo ultimo saggio parla dell'emersione di una "differenza" fondamentale. Si sta aprendo una nuova fase, di cui è ancora difficile comprendere i lineamenti?

Ritorna il tema dell'AI, che avevo affrontato in precedenza. La differenza fondamentale è il nostro capitale semantico: tutto ciò che ci permette di dare senso e significato alla vita. È su questo capitolo settimanale codificato che esercitiamo i sistemi artificiali ed è grazie ad esso che sappiamo come usarli, integrarli, correggerli e applicarli. Già oggi, ma sempre di più in futuro, sarà l'asimmetria semantica (la comprensione) e non quella informativa, a fare la differenza. L'IA, come Internet, continua ad appiattire l'accesso e la manipolazione dei dati, capirli, contestualizzarli, sapere che cosa farne e per quale ragione: sono tra i vari aspetti del capitale semantico che emerge sempre di più come la nostra eccezionalità.

Una frontiera tutta da investigare. La sfida del significato e della produzione di senso che caratterizza l'umano è quella che dobbiamo sostenere per difendere uno spazio di autonomia?

È proprio così. E sarà sul capitale esistenziale che dovremo concentrarci in futuro: nella scuola, al lavoro, nei contesti sociali e culturali. L'IA ci mostrerà sempre meglio che cosa non è specificamente umano, come hanno fatto le precedenti rivoluzioni tecnologiche. Nel senso non di qualcosa che non può essere prodotto da un essere umano, ma di qualcosa che non ha valore se non è prodotto da un essere umano. Proprio come una cartolina d'auguri. ■

Governance tecnologica e sicurezza: serve una visione integrata per le imprese e la PA. Intervista VIP a Alessio Tola.

BIO

Professore universitario, di analisi e valutazione delle tecnologie presso l'Università degli studi di Sassari, si è dedicato allo studio delle Imprese nei distretti industriali e delle dinamiche di sviluppo dei sistemi produttivi, anche attraverso i temi dell'innovazione tecnologica, della certificazione delle produzioni e della sicurezza. Attivo anche nel settore della Pubblica amministrazione nell'ambito della digitalizzazione dei processi e della formazione delle risorse. Annovera oltre 100 pubblicazioni scientifiche, tra articoli e monografie. Imprenditore di prima generazione, ha fondato il Gruppo Smeralda Consulting, del quale è Presidente Onorario, che si occupa di assistenza tecnica e re ingegnerizzazione dei processi per la Pubblica Amministrazione e le aziende private, oltre a sviluppare attività di promozione e comunicazione istituzionale e commerciale a sostegno di prodotti e processi innovativi.

Autore: Massimiliano Cannata

Le strategie europee - basti considerare il Digital Compass, la Digital Decade, l'AI Act, fino alla rinnovata cornice che regola lo sviluppo della cyber security - stanno ridefinendo i ritmi di sviluppo dell'innovazione, con cui bisogna fare i conti se vogliamo garantire una tutela e un progresso dei diritti fondamentali in un orizzonte di sostenibilità. Le politiche nazionali, attraverso il Codice dell'Amministrazione Digitale, il Piano Triennale ICT e il PNRR, stanno proiettando il Paese verso un modello di governance data-driven, interoperabile, finalizzato alla creazione di un sistema integrato, efficiente e sicuro, in grado di produrre valore pubblico misurabile. Senza competenze adeguate – non solo tecniche, ma anche manageriali, etiche e progettuali nessuna transizione digitale potrà mai realizzarsi in modo compiuto. Ne abbiamo parlato con il prof. Alessio Tola, professore ordinario di analisi e valutazione delle tecnologie dell'Università degli studi di Sassari.

Professor Tola, qualità dei processi, analisi e valutazione delle tecnologie sono il suo lavoro di ricerca quotidiano. Stiamo, molto a fatica, acquisendo una consapevolezza: la trasformazione digitale non è solo a un fatto tecnico, ma un cambiamento strutturale che ridefinisce i modelli organizzativi, le culture professionali e gli asset relazionali. Qual è il suo pensiero in merito?

Dopo i primi facili e superficiali entusiasmi che hanno connotato

il primo sviluppo di quella che si definiva "società dell'informazione", abbiamo compreso che la tecnologia non è più soltanto un insieme di strumenti operativi: rappresenta una vera e propria infrastruttura strategica che abilita modelli organizzativi, processi decisionali e servizi essenziali. Senza un sistema di governance chiaro – fatto di regole, ruoli, responsabilità e metriche di controllo – l'innovazione rischia, perciò, di trasformarsi in mera strumentazione tecnica, non contribuendo a risolvere le problematiche strutturali e organizzative per cui deve essere impiegata.

Quale deve essere il modello per una governance integrata della sicurezza dello spazio cibernetico?

Nelle imprese, un superficiale sfruttamento delle potenzialità tecnologiche si traduce in una perdita secca di competitività; nella pubblica amministrazione significa non riuscire a garantire servizi affidabili, inclusivi e sicuri per i cittadini. cittadini. Teniamo conto che un modello di governance tecnologica efficace si fonda su cinque pilastri fondamentali:

1. Visione strategica chiara: ogni organizzazione deve definire quale valore la tecnologia deve creare.
2. Coerenza delle architetture tecnologiche: infrastrutture, dati e sicurezza devono essere integrati.
3. Accountability: è essenziale che ruoli come CIO, CTO e Responsabile della Transizione Digitale siano chiaramente definiti.
4. Processi di valutazione: devono includere assessment di impatto, analisi dei rischi, costi/benefici e sostenibilità.
5. Monitoraggio continuo: con sistemi di audit capaci di misurare performance, maturità e aderenza alle normative.

Imprese private e PA presentano analogie nel modo di approcciarsi alla sicurezza?

Vi sono certo differenze, ma anche notevoli punti di convergenza. La PA gestisce dati pubblici e servizi essenziali, con impatti sociali potenzialmente elevati in caso di incidente; le imprese, invece, si concentrano sui rischi economici e reputazionali. In entrambi i casi è necessario adottare un modello di security by design, che comprenda analisi preventiva dei rischi, applicazione di standard internazionali – come ISO/IEC 27001 e 27701 – gestione dei dati conforme al GDPR e sistemi di monitoraggio in tempo reale.

L'IA è entrata ormai a "gamba tesa" in qualsiasi ragionamento sulle connotazioni della "Quarta rivoluzione". Cosa possiamo aggiungere in merito?

L'intelligenza artificiale introduce opportunità e rischi inediti nei modelli di governance e sicurezza. Da un lato consente l'automazione dei processi, l'analisi predittiva e un supporto decisionale più avanzato; dall'altro può generare bias, opacità, vulnerabilità nelle pipeline dei dati e una crescente dipendenza da piattaforme esterne. Credo che normative come l'AI Act europeo richiedano valutazioni d'impatto, classificazione del rischio e trasparenza. Diventa necessario integrare l'AI nei framework di controllo, istituire figure come l'AI Risk Officer e adottare modelli ibridi uomo-macchina, in cui la supervisione umana rimanga imprescindibile.

Il lavoro sulle competenze e sulla formazione non ha mai fine. Stiamo facendo quello che serve per camminare al passo con i tempi di innovazione e implementazione di reti e sistemi?

Sono tre le grandi aree disciplinari che bisogna presidiare: competenze tecniche, come cybersecurity, data management e architetture cloud; competenze organizzativo-gestionali, come project management e change management; e competenze etiche e regolatorie, legate a privacy, responsabilità e trasparenza algoritmica. Guardando un po' più avanti, ai prossimi cinque anni, emergono alcune priorità condivise tra imprese e pubblica amministrazione, a cominciare dal considerare la sicurezza un investimento strategico, cui si aggiunge la necessità di garantire la sovranità dei dati e delle piattaforme e la promozione di una trasformazione digitale responsabile, fatta di valutazioni d'impatto, audit algoritmici e solide strutture di governance. ■

La guerra ibrida non risparmierà neanche lo spazio, senza una strategia siamo destinati al declino.
Intervista VIP a Marco Braccioli.

Autore: Massimiliano Cannata

La sicurezza del cyberspazio è divenuta una priorità assoluta in una fase storica che sta facendo registrare un'instabilità geopolitica crescente, resa più evidente dalla crisi venezuelana. La sovranità, per essere esercitata, non potrà in futuro prescindere dagli strumenti del digitale.

"Dalla terra al cielo – spiega Marco Braccioli, economista, co-direttore Cybersec della Fondazione ICSA – le vulnerabilità si sono moltiplicate, si combatte una guerra ibrida anche in tempo di pace. Bisogna che gli Stati sappiano aggiornare le strategie per la sicurezza nazionale, che devono fondarsi su competenze tecnologiche molto precise. Le reti globali si stanno frammentando, stanno nascendo dei blocchi – occidentale, russo cinese, servirà una cyber diplomacy che possa guidare la strategia dei singoli paesi".

Direttore Braccioli, quando si parla di sovranità si pensa a un modo tradizionale di esercitare il controllo di un territorio ben definito, con azioni e strumenti militari che sono quelli classici, sperimentati nella modernità e nei due conflitti mondiali che hanno segnato il Novecento. Oggi lo scenario appare profondamente mutato: si parla di «guerra in codice», per usare l'immagine dell'ultimo libro di Michele Mezza. Ci spiega come stanno le cose?

BIO

Marco Braccioli è attualmente: Co-Director Cybersec e Consigliere Scientifico presso Fondazione ICSA; Membro del Consiglio Direttivo di AFCEA Capitolo di Roma (Armed Forces Communication & Electronic Association); Membro CTS CSAIA (Centro Studi Avanzati Intelligenza Artificiale); Membro CTS CESMA (Centro Studi Militari Aeronautica Militare); Lecturer su AI over Cybersecurity presso Fondazione Ettore Maiorana di Erice; Contributore per AIRPRESS e Formiche su temi di guerra ibrida, cybersecurity, AI e tecnologie EDT. In passato ha lavorato come manager per numerose aziende, sia private che pubbliche, nei settori TLC, law enforcement, cybersecurity e difesa, ricoprendo varie cariche di Direttore Generale, Amministratore Delegato, COO e CMSO. Dal 2 febbraio 2026 assumerà l'incarico di Executive Cybersecurity Leader Difesa/NATO nel Gruppo BIP.

Chiariamo subito un primo punto: la sovranità digitale può nascere solo se esiste una sovranità politica. Nel mondo digitale abbiamo una forte presenza del mondo americano; la recente affermazione di Trump, che ha fatto capire di volere allentare l'azione di influenza e di protezione dell'Europa, cambia le carte in tavola. L'Europa ha bisogno di dare una risposta unitaria, di trovare quella forza politica per prendere posizione e per rafforzare gli investimenti nei settori tecnologici più avanzati, da cui dipende il futuro: AI, quantum, cyber. Anche se nessun Paese può competere da solo in ambiti così delicati, è venuto il momento di sviluppare una filiera della sicurezza autonoma che possa dare agli Stati europei una capacità di manovra superiore.

L'UE è in grado di correre questa difficile partita?

Bisogna attrezzarsi. Quando Roma vinse contro Cartagine non sapeva navigare, ma seppe impararlo in fretta. Abbiamo tante eccellenze: bisogna metterle a fattor comune, cercando di non vendere la paura, ma piuttosto impegnandoci a costruire insieme «l'arca che ci salva dal diluvio», perché la sicurezza è un lavoro di squadra. La tutela dello spazio cibernetico è un tema orizzontale: non c'è più un solo «forno» produttivo sulla scacchiera internazionale. Agli USA si è affiancata la Cina; se pensiamo che l'applicativo IA «DeepSeek» è quello più usato nel mondo, ci possiamo rendere conto della portata di quello che sta avvenendo e degli interessi in campo.

Stare a guardare mentre il mondo si muove sarebbe la peggiore delle strategie. Da dove bisogna partire?

Siamo di fronte a un abbraccio mortale, che sarà rappresentato dall'alleanza tra IA e mondo quantistico. L'intelligenza artificiale ha bisogno di dati per alimentarsi, ma soprattutto di velocità per evolversi. Chi è più rapido avrà la possibilità di esercitare un'egemonia non solo economica, ma militare e strategica. In una «war room» attrezzata gli analisti osservano milioni di attacchi giornalieri: tra questi, in media, 7-8 sono degni di attenzione perché potenzialmente distruttivi. Come reagire in tempo reale ad attacchi sempre più sofisticati? Introducendo una capacità di risposta che solo la tecnologia può garantire. Con i sensori quantistici sta già avvenendo; pensiamo a cosa succederà con la diffusione dei PC e della crittografia quantistica, che comporterà un mutamento di tutte le tecnologie che stanno dietro al funzionamento di questi meccanismi.

Dalla terra al cielo le nuove vulnerabilità

La progressione tecnologica di cui parla ci espone a nuovi fronti di rischio, con quali conseguenze?

Intanto bisogna tenere conto che si è allargato il "campo di battaglia". La

guerra nello spazio sarà un tema centrale per la cybersicurezza nel futuro. Avremo la tecnologia 6G che si integrerà con i satelliti: sarà difficile, anche sul piano del diritto internazionale, delimitare regole di ingaggio e gestione del conflitto. Ne abbiamo avuto prova nel recente conflitto ucraino-russo: le reti satellitari hanno subito attacchi da entrambe le parti. Starlink, a supporto dello Stato ucraino, è stato bersaglio di hacker russi, mentre la rete russa Statis ha subito attacchi da parte ucraina. Sabotaggio, spionaggio, furto di dati sensibili, interruzione di servizi hanno causato perdite finanziarie nel civile ed effetti catastrofici nel settore militare. Lo spostamento verso l'interoperabilità obbliga a immaginare e pensare la connessione con operazioni cognitive che prevedono l'uso dell'IA e, a breve, del quantum per avere il predominio sul nemico, prima di tutto a livello informativo. La sfida che si impone riguarda in massima parte l'analisi e la discriminazione dei dati, su cui si basa la guerra cognitiva, che orienta le scelte decisionali di maggiore portata.

Quello che sta avvenendo a tutte le latitudini imporrebbe una più stretta alleanza tra l'ambito civile e militare. Esistono spazi reali di collaborazione tra queste due sfere?

Gli strumenti digitali di cui parliamo sono, per definizione, dual use. Sappiamo bene – la stessa storia di Internet lo dimostra – che spesso la ricerca militare ha fatto da traino alla crescita di applicazioni che hanno trovato nell'ambito civile importanti spazi applicativi, di cui la collettività ha poi tratto enormi vantaggi. Per far crescere la competenza ci vuole un commitment pubblico, che deve stimolare la crescita delle aziende portatrici di tecnologie innovative, fino a determinare lo sviluppo di un'industria nazionale. In questa dinamica la sfera militare può avere un ruolo decisivo.

Il piano cyber presentato dal Ministro Crosetto alle Camere nel dicembre scorso, finalizzato a creare un corpo di militari specializzati nel contrasto delle minacce digitali, va nella giusta direzione?

Può essere un tassello utile per il dialogo tra le due sfere, civile e militare, di cui parlavo prima. Dotare il Paese di una struttura con un organico previsto di 1.200/1.500 unità dedicate alla difesa e alla gestione delle minacce ibride è un fatto molto importante, perché determina la nascita di un centro per la infowar e l'anti-disinformazione di cui abbiamo bisogno.

La guerra ibrida è ormai permanente: viene combattuta in forme subdole anche in tempo di pace. Colpire reti, infrastrutture, servizi equivale a un atto di guerra che può mettere in ginocchio, come si è già visto, strutture vitali per la vita di un Paese: ospedali, aeroporti, stazioni, istituzioni e persino partiti politici.

Per questo credo che occorra lavorare per creare un centro unico di comando, capace di mettere insieme la Difesa, gli Interni, gli Esteri e i nuovi soggetti istituzionali – penso all'ACN (Agenzia per la Cybersicurezza Nazionale, n.d.r.) – che possono svolgere un'azione di coordinamento e di risposta proporzionale al livello di rischio che abbiamo raggiunto, con regole d'ingaggio certe.

Organizzarsi significa creare una struttura e una significativa deterrenza per essere un vero attore europeo ed evitare quel vecchio adagio che riguarda i rapporti internazionali: «Se non siedi a tavola, sei sul menù». ■

59° Rapporto sulla situazione sociale del Paese

CENSIS

Ed. Franco Angeli

Autore: Massimiliano Cannata

Il ritorno dell'età del ferro nel declino dell'Occidente

"Siamo entrati nell'età selvaggia, fatta di ferro e fuoco, dove forza e violenza hanno preso il sopravvento. A dominare il mondo non è più l'economia, ma un "vitalismo irrazionale", sostanziato di rivendicazioni identitarie, di fanatismo di desiderio di conquista". Questa la cornice entro cui si inserisce la fotografia annuale del 59° Rapporto CENSIS. In questo orizzonte a tinte fosche colpisce un dato: un italiano su tre ritiene l'autocrazia uno strumento più adatto delle democrazie liberali per affrontare il difficile tempo presente. Specchio di questa crisi la condizione della UE. La mancanza di una Costituzione continentale, non ha permesso di far maturare valori condivisi, questa assenza sta facendo sentire tutto il suo peso, in un mondo attraversato da conflitti a tutte le latitudini. Non c'è da stupirsi dunque se due terzi degli italiani non credono che la vecchia Europa potrà avere un ruolo strategico nel disegnare il futuro, il suo destino sembra quello della marginalità, nel generale declino dell'Occidente. "Vi sono - scrive Massimiliano Valerii consigliere delegato del CENSIS - dei fattori strutturali non solo culturali e ideologici che rendono fragili le economie capitaliste.

A partire dall'aumento vertiginoso del debito. Tra il 2001 e il 2024 nei Paesi del G7, a fronte di una stentata crescita, il debito è lievitato dal 75 per cento, raggiungendo il 124 per cento del PIL, in Italia siamo passati dal 108 per cento al 134 per cento. Ma non siamo i soli ammalati i dati di Francia e Inghilterra non sono migliori, con l'aggravante che si stanno creando le condizioni per uno shock pari a quello che abbiamo sperimentato con il covid, quando il debito aveva mondiale sfiorato il 140 per cento del PIL. La differenza va cercata sta nel fatto che tutto questo sta avvenendo in condizioni normali. È evidente che c'è stato un salto di paradigma profondo con cui dobbiamo fare i conti che ha trasformato lo stato fiscale in uno stato debitore. Non si tratta solo di un gioco terminologico perché il primo grave effetto lo si risente nel disfacimento del welfare, istituzione storica oggi in affanno. Gli interessi del debito pesano come zavorre sui conti pubblici non consentendo nessun abbassamento delle tasse, pochi investimenti per lo sviluppo, scarsa attenzione per la sanità.

Nell'ultimo anno la spesa italiana per gli interessi è stata di 85,6 miliardi il 3,9 per cento del PIL il valore più alto del continente dopo l'Ungheria. Nella sanità spendiamo 54 miliardi mentre l'intero valore degli investimenti pubblici è di 78 miliardi, numeri che non hanno bisogno di commento. Il "grande debito" inaugura la società del post welfare che per sua natura diviene incubatrice di aggressività. Intanto l'emergenza fa invocare da più parti (l'81 per cento degli italiani) la tassazione dei giganti del web, cosa difficile da attuare.

Non ci sono solo componenti globali nella crisi descritta, esistono fattori endogeni che aggravano il caso Italia a partire dall'inverno demografico, che porta con sé l'azzeramento delle nascite e, come se non bastasse, azzera il processo di proliferazione delle PMI. Negli ultimi venti anni il numero dei titolari di impresa si è assottigliato passando da circa tre milioni e mezzo a meno di due milioni, sono diminuiti i giovani imprenditori sotto i trenta anni del 46 per cento così come il reddito delle piccole imprese oggi pari al 14 per cento del PIL, era del 28 per cento all'inizio del millennio. È tutta ricchezza che manca al paese e a un ceto medio che perde pezzi e status mostrando una lacerazione del corpo collettivo che appare evidente nello scarso interesse per la politica e nella escalation dello astensionismo. Il nuovo pantheon delle classi dirigenti non brilla di luce propria appare come un pugile suonato, da colpi che arrivano da EST e da Ovest.

Le élites invece di rassicurare i cittadini prospettano catastrofi, guerre imminenti, perdita di competitività, assalto dei migranti nuove barbarie alle porte, collasso climatico. Un rosario di negatività, di cui gli italiani sono consapevoli. Malgrado questo non si rifugiano nel grande "hotel abbisso" ed è questa probabilmente la sorpresa maggiore che viene dal Rapporto. Forse non siamo un popolo preparato a quello che verrà ma abbiamo resistito, reagendo alla chiamata collettiva che obbligava alle prove di forza: militare, fiscale, tecnocratica. Non abbiamo ceduto, non abbiamo inseguito le leadership aggressive a cominciare da quella americana.

Abbiamo ritrovato lo spirito contadino originario di un paese che vuole reagire non abbandonandosi all'apocalisse. Il CENSIS dedica, in questa ottica, un capitolo ai piaceri italiani, alla ricerca di una luce da cui poter finalmente ripartire. ■

Sovranità Digitale Roberto Baldoni Ed. Il Mulino

Autore: Roberto Baldoni*

La sovranità digitale è un prezioso punto di riferimento per identificare le minacce

(…) In un contesto globale dominato da colossi tecnologici e da potenze straniere, predisporre politiche di sovranità digitale è fondamentale per evitare dipendenze che potrebbero compromettere l'economia e la privacy dei cittadini di una nazione e per evitare l'imposizione di standard tecnologici che potrebbero non essere compatibili con le proprie normative e valori.

Una sovranità digitale «piena» include la capacità di una nazione di inventariare continuamente, salvaguardare, gestire sfruttare i dati nazionali e le infrastrutture digitali, mantenendo allo stesso tempo il cyberspazio aperto e globale.

(…) La capacità che ha una nazione di garantire che soluzioni tecnologiche sicure, resilienti e protette siano utilizzate per questi scopi (inclusa una forza lavoro sufficientemente qualificata e affidabile) e la piena consapevolezza della società dei rischi associati al cyberspazio. Questo concetto è chiaramente ideale: nessuna tecnologia può essere completamente sicura, è impossibile inventariare tutti i dati o raggiungere una piena consapevolezza all'interno della società. Inoltre, essendo un cyberspazio nazionale immerso in quello globale, la sovranità digitale è continuamente esposta a molteplici tipologie di minacce, causate da attori sia malintenzionati sia accidentali, come nel caso dell'incidente provocato da un aggiornamento «baggato» di Crowdstrike del 27 luglio 2024 e il conseguente blocco di quasi 10 milioni di computer. Nel saggio vengono introdotte nove tipologie di minacce (tecniche e non), guidate da attori malintenzionati, alla sovranità digitale, di cui gli attacchi informatici ne rappresentano una sola. Altre tipologie potrebbero emergere insieme all'evoluzione delle tecnologie digitali.

Ad esempio, l'uso ostile di un potente sistema di IA potrebbe manipolare un mercato azionario nazionale, destabilizzando così l'intero sistema economico del paese, di fatto costituendo un attacco diretto alla sovranità digitale e alla sicurezza nazionale. Affrontare efficacemente queste sfide richiede una visione unitaria e strategica, per non essere sopraffatti dalla crescente complessità tecnologica, ormai divenuta l'ossatura della società e dell'economia globale, e dalle minacce emergenti a essa connesse (…).

Benché più utopistica che reale, questa idea di «piena» sovranità digitale serve a un paese come un prezioso punto di riferimento per identificare e valutare le principali minacce ai propri asset digitali e ai propri cyberspazi e, di conseguenza, a formulare politiche e pratiche mirate a migliorare le proprie strategie per la difesa digitale a copertura dell'intero spettro delle minacce. Il libro adotta un approccio orizzontale, collegando diversi argomenti, apparentemente diversi tra loro, all'interno di un quadro d'insieme unico che porta a una visione strutturata e innovativa di sovranità digitale (…). Questo lavoro prepara il terreno per un'esplorazione più approfondita in testi specializzati sui singoli argomenti; la sezione "Per saperne di più" fornisce una serie di riferimenti per tale approfondimento. Infine, è importante precisare che il libro analizza e correla argomenti ed eventi accaduti fino a novembre 2024. Sono stati, tuttavia, inseriti brevi aggiornamenti relativi ad alcune linee programmatiche sul digitale emerse durante il periodo di transizione della nuova presidenza americana di Donald Trump, fino al giorno del suo insediamento.

* Il testo della recensione che pubblichiamo per gentile concessione dell'Editore è un estratto dell'introduzione. ■

Il colpo di stato delle Bigh Tech Marietje Schaake Ed. Franco Angeli

Autore: Massimiliano Cannata

Salviamo la democrazia dall'assalto delle Bigh Tech

Il colpo di stato delle Bigh Tech di Mariet Je Schaake, membro del Cyber Policy Center della Stanford University e docente di politica internazionale presso l'Università della California, "non è un libro contro la tecnologia – come spiegato in premessa dall'autrice – piuttosto è un libro a favore della democrazia, un invito a riequilibrare il ruolo della tecnologia nelle nostre società per garantire una miglior tutela dei valori democratici". Grazie alla sua esperienza, sia come deputata nelle aule del Parlamento europeo, sia come professionista tra gli addetti ai lavori della Silicon Valley, l'autrice delinea un quadro (spaventoso) del nostro mondo ossessionato dalla tecnologia, offrendo una visione lucida di come le democrazie possano costruire un futuro migliore prima che sia troppo tardi. Quello della studiosa va letto come un appello a non abbassare la guardia: una sollecitazione ai governi a guardarsi attorno a non gettare la spugna di fronte alla progressione vorticosa della tecnoscienza.

Che le bigh tech gestiscono fette sempre più grandi della nostra esistenza, sempre più immersa nel digitale, è un dato incontrovertibile; demandare però l'intera organizzazione della convivenza all'arbitrio di potenti oligopoli privati che tengono sotto scacco una politica afona, è un rischio troppo alto che non possiamo permetterci. Se la diagnosi certifica una malattia molto chiara, che prende il nome di autocrazia, è più difficile individuare - si sa - una terapia efficace. Sarebbe utile cominciare a ricordarsi che "gli Stati – prosegue l'analisi della Schaake – se lo vogliono, possono essere ancora potenti, come è successo purtroppo in senso negativo dall'avvento dal modello di governo autoritario del mondo digitale.

Si può rivitalizzare una democrazia anemica mettendo in campo nuovi approcci normativi e forme innovative di governance, pensate per supportare esplicitamente principi e valori in contesti nuovi". Serve, insomma, un'infrastruttura politica adeguata. Ci siamo troppo soffermati in questi anni sulle infrastrutture della connettività facendo a poco a poco rinsecchire l'amore per il confronto e la partecipazione, che sono fin dagli albori il sale della democrazia, la sua stessa essenza.

È evidente, e la studiosa mostra di averne piena consapevolezza, che le conseguenze della pervasività del digitale non vanno misurate solo sul terreno degli equilibri democratici, esistono altri ambiti del vivere civile e della nostra quotidianità che investiti dalla "grande mutazione" in atto stanno cambiando asset e profili. Siamo di fronte a un "salto ontologico" che impone l'adozione di un nuovo metodo della conoscenza, rimane cruciale l'esigenza di attuare quella "promessa democratica" che rimane un tendere verso, un ideale della "ragione" per usare termini kantiani, che non dobbiamo mai finire di perseguire. Vale sempre l'adagio di Churchill secondo cui la democrazia è la peggior forma di governo, peccato che non ne conosciamo di migliori.

Il ruolo degli stati nello scacchiere geopolitico

Non possiamo nascondere che il futuro del pianeta si gioca su un terreno particolarmente accidentato. I fatti di cronaca dimostrano ampiamente la gravità della partita che vede assolute protagoniste tecnocrazie e big tech. Per invertire lo squilibrio di potere servono soluzioni in grado di garantire più possibilità di controllo sia ai funzionari eletti che ai cittadini. Le classi dirigenti devono essere messe nelle condizioni di resistere all'influenza delle lobby delle corporation tecnologiche e reinventarsi come guardiani dinamici e flessibili del nostro mondo digitale, cosa che purtroppo non sta avvenendo. Fortunatamente nella vecchia Europa non mancano tentativi di aggiustare il tiro. La recente sanzione della Commissione Europea, comminata a "X", la piattaforma di Elon Musk, si è concretizzata in una multa di 120 milioni di euro per

violazione delle norme che impongono l'obbligo di trasparenza e di responsabilità sui contenuti. La risposta piccata del suo proprietario, che ha rimosso l'UE dal suo account paragonandola al "quarto reich" e invocandone la dissoluzione per palese violazione dei diritti di libertà della Rete, la dice lunga sul disprezzo delle istituzioni che i colossi di Internet sbandierano senza pudore. Esiste un'emergente spinta plutocratica che finisce col decidere sulle sorti del mondo, senza nessun contraltare che ne limiti gli appetiti. Gli antichi filosofi ci avevano messo sull'avviso: Aristotele aveva sollevato il primo allarme nei suoi scritti politici, invitando le élite ad attrezzarsi per arginare le degenerazioni della democrazia.

Siamo caduti dentro quel rischio mani e piedi, soffocati dall'eccessivo potere delle bigh tech, che stanno infettando la democrazia, per cui bisogna correre ai ripari. Ha ragione Paolo Pagliaro che, nel suo commento mandato in onda dalla trasmissione Otto e Mezzo condotta da Lilli Gruber su La7, si chiede cosa accadrà all'Australia che, primo paese al mondo, ha deciso di vietare ai minori di 16 anni l'uso dei social. Il primo ministro Anthony Albanese ha dichiarato che la norma ha l'obiettivo di far sì che i ragazzi restino ragazzi. Sembrerebbe un'ovvietà peccato che nessuno prende sul serio il livello di rischio e la necessità di porvi rimedio. I legislatori australiani vogliono proteggere i minori da rischi come dipendenza, cyber bullismo, esposizione a contenuti inappropriati, disinformazione danni alla salute mentale. Forse sarebbe il caso di imitarlo anche alle nostre latitudini, imponendo un'età minima per l'uso dei social, cosa che accade, come è noto per il consumo di alcolici.

I rischi della "volontà macchinica"

Nessun attentato, dunque, alla libertà di Internet, semmai la necessità di limitare lo strapotere di una "volontà macchinica" - prendo a prestito il bel titolo di uno studio (ed. Pacini Giuridica) presentato da Tommaso dalla Massara insieme a Enrico Al Mureden - che denuncia lo spostamento della decisione giuridica dall'intelletto agente del giurista alla macchina. Stiamo parlando di campi che sembrano diversi, ma non lo sono: l'analogia è infatti molto forte ed è data dall'esproprio del potere decisionale, ormai evaporato dalla sfera dell'umano.

Un esproprio che investe il legislatore nel suo compito di definizione delle norme e la politica, quale disciplina impegnata a studiare strumenti e misure da impiegare per migliorare l'esistente. Un primo passo per provare a ridare ossigeno alla democrazia potrebbe essere proibire spyware progettati per violare diritti umani, alcune tipologie di raccolta dati e alcune criptovalute che facilitano i criminali e agevolano applicazioni di IA particolarmente manipolative.

Ma sono solo degli esempi, che possono essere estesi alle piattaforme che utilizzano gli algoritmi per creare disinformazione. Musk, magari, si indignerà difronte a tutto questo: se accadrà, come sottolinea ancora Pagliaro, sarà un buon segno, perché vorrà dire che siamo sulla strada buona. ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
https://www.cybertrends.it/supportaci/