Editoriale

Il tumultuoso sviluppo delle tecnologie informatiche ha portato molte innovazioni ed efficienze in tante attività, incluse quelle vitali per la società, dalle funzioni dello Stato e delle varie amministrazioni pubbliche all'erogazione di servizi ormai irrinunciabili, in tanti settori, dalle infrastrutture idriche ed energetiche al mondo bancario e finanziario, dai servizi turistici e di mobilità a quelli erogati al cittadino. Questa pervasività delle tecnologie se da una parte ha portato grandi benefici alla società e alle persone, dall'altro le espone a grandi rischi, perché le attività di tante (o forse tutte) le aziende e amministrazioni pubbliche, e anche quelle dei singoli, si trovano a dipendere dai sistemi e servizi informatici. In effetti, i rischi sono confermati dal moltiplicarsi di attacchi ai sistemi e alle infrastrutture di tutti i paesi, incluso il nostro.

Negli ultimi anni, l'Italia ha affrontato con sempre maggiore attenzione il tema della cybersicurezza, intesa come approccio complessivo alla resilienza dei sistemi e, di conseguenza, dell'intero paese, con la creazione, nel 2021, dell'Agenzia per la Cybersicurezza Nazionale, che ho l'onore di dirigere, e con l'adozione della Strategia Nazionale di Cybersicurezza nel 2022, con le numerose conseguenti iniziative.

Le attività relative alla cybersicurezza sono variegate: un quadro di riferimento è fornito dagli obiettivi della Strategia, costituiti da protezione, risposta e sviluppo, insieme ai fattori abilitanti di formazione (e cultura della sicurezza) e cooperazione (in ambito nazionale, con tutti i soggetti interessati, pubblici e privati, e internazionale). L'ACN, con il proprio ruolo di catalizzatore delle attività del paese, è particolarmente interessata alla promozione dei vari temi, anche fra i non specialisti. Per questo motivo, abbiamo colto con favore l'invito rivolto dalla direzione di Mondo Digitale a Paolo Atzeni, Direttore della nostra Struttura per lo Sviluppo di Capacità e Competenze, a curare un numero speciale della Rivista dedicato appunto alla cybersicurezza.

Gli articoli sono sei, quattro dei quali scritti da esponenti dell'Agenzia e due da autorevoli esperti esterni.

Nel primo articolo, Luca Montanari affronta uno dei temi operativi di maggiore interesse diretto dell'agenzia, presentando la metodologia, sviluppata e utilizzata dall'ACN per rappresentare lo stato della minaccia cyber in Italia, nonché

definendo e descrivendo gli indicatori e le metriche utilizzati e come i dati grezzi vengono collezionati, processati e analizzati per fornire una rappresentazione accurata del fenomeno.

Arturo Di Corinto, nel successivo articolo, discute il tema delle minacce con riferimento al contesto esterno e alle finalità ultime, illustrando le tecniche della propaganda computazionale e le modalità secondo le quali hacker attivisti e hacker di stato possano farne uso.

Il terzo articolo, di Luca Nicoletti, Monica Scannapieco, Mara Sorella e Marco Centenaro, affronta la relazione tra intelligenza artificiale e cybersicurezza illustrando alcune soluzioni per il governo dei rischi cibernetici introdotti dai sistemi di IA, che partono dalla definizione di processi per mettere in sicurezza i sistemi stessi ed impedirne un uso improprio e arrivano allo sviluppo di adeguate capacità di ricerca e innovazione. Inoltre, sono presentati alcuni casi d'uso notevoli in cui l'intelligenza artificiale può essere usata a supporto della cybersicurezza."

Il quarto articolo, di Andrea Simoncini e Federica Camisa, a conferma degli aspetti trasversali e non solo tecnologici della cybersicurezza, affronta tematiche giuridiche, in particolare con riferimento alla regolazione, nonché il ruolo del fattore umano.

Gli ultimi due articoli sono motivati dal grave problema della carenza e del divario di competenze, in Italia e nel mondo, sui temi della cybersicurezza.

Paolo Atzeni e Bernardo Palazzi sviluppano una riflessione complessiva sulle problematiche di formazione, con riferimento ai vari contesti e livelli, nella scuola, nell'università e nel mondo produttivo.

Infine, Gaspare Ferraro, Sonia Montegiove e Paolo Prinetto illustrano uno specifico tema, quello della formazione attraverso il gioco e le competizioni, che negli ultimi anni in Italia ha avuto un successo crescente.

Concludo ringraziando Paolo Atzeni per il lavoro di coordinamento svolto e augurando a tutti una buona lettura, con l'auspicio che questa iniziativa possa far crescere nel paese l'interesse verso i temi della cybersicurezza.

Bruno Frattasi

Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale

Metriche ed indicatori dello stato di esposizione cyber del Paese

Luca Montanari

Sommario

Fin dal 2018 tutti gli Stati Membri dell'Unione Europea hanno dovuto istituire un "Computer Security Incident Response Team" (CSIRT) in accordo a quanto previsto dalla così detta "Direttiva NIS". Gli CSIRT, da allora, sono incaricati di gestire incidenti ed eventi cyber che minacciano le infrastrutture critiche nazionali e di monitorare lo stato della minaccia cyber in modo da disporre sempre di un quadro di situazione per anticipare e prevedere i prossimi passi degli attaccanti. Nel nostro paese il "CSIRT Italia" è istituito all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN). Questo articolo presenta la metodologia, sviluppata e utilizzata dall'ACN per rappresentare lo stato della minaccia cyber in Italia, definendo e descrivendo quali sono indicatori e metriche utilizzati e come i dati grezzi vengono collezionati, processati e analizzati per fornire una rappresentazione accurata del "cyber threat landscape" della Nazione.

Abstract

Since 2018 European member states according to the first NIS Directive created their National Computer Security Incident Response Team (CSIRT). CSIRTs manage cyber incidents and cyber threats targeting national digital assets and among their duties they also have to monitor the cyber threat landscape, in order to always have a situational picture and to foresee and anticipate the next cyber attackers move. The paper presents the methodology developed by the Italian CSIRT to represent the current threat landscape, defining, and describing what indicators and metrics are in place and how raw data are collected, processed, and analyzed in order to accurately depict the cyber threat landscape of the nation.

Keywords: Cyber Threat Landscape; cyber data analysis; cyber taxonomy; CSIRT Italia; Agenzia per la cybersicurezza Nazionale (ACN); cyber index; cybersecurity data analysis; cyber indicators

1. Introduzione

Fin dal 2018 ognuno degli Stati membri europei, in attuazione della Direttiva NIS [1], ha dovuto istituire un *Cyber Security Incident Response Team* (CSIRT), ovvero un centro di risposta agli incidenti cibernetici, con capacità che, nonostante il nome, vanno ben oltre la risposta (*response*). Le attività CSIRT spaziano infatti dal

monitoraggio proattivo all'analisi delle nuove vulnerabilità, alla *cyber threat intelligence*, finanche alla gestione del rischio *cyber* a livello nazionale e alla *data analysis*.

Il centro, istituito dapprima all'interno del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei ministri, opera all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN) [2], l'autorità che a partire dal giugno 2021 raccoglie tutte le competenze e capacità di resilienza cibernetica del Paese.

L'ACN proprio tramite lo CSIRT Italia [3] è il riferimento nazionale per la mappatura delle fenomenologie cyber che interessano il Paese e necessita di monitorare e rappresentare costantemente lo stato della minaccia che grava sull'Italia ed i relativi impatti possibili sulle pubbliche amministrazioni e sugli operatori privati, critici per l'operatività della Nazione. Tale rappresentazione, che deve avere contenuti sia qualitativi (individuazione dei fenomeni) sia quantitativi (dati numerici), costituisce la base per guidare i processi decisionali volti alla definizione e all'applicazione delle misure di resilienza cibernetica, oltre che ovviamente ad informare i soggetti della *constituency*[1] e i vertici del Paese.

Ma quali sono i dati ed i fenomeni che, insieme, forniscono un quadro esaustivo dello stato di esposizione cibernetica del Paese? Come e dove si possono raccogliere tali dati?

In questo articolo si presentano le metriche e gli indicatori utilizzati all'interno dei reparti operativi dell'ACN, elaborati anche tenendo in considerazione best practice internazionali e approcci di altre agenzie estere, e si forniscono alcuni dettagli sul modello di analisi dei dati adottato, il quale consente, a partire da dati numerici derivanti dalle attività reattive e proattive, di rappresentare lo stato della minaccia.

Stato della minaccia che viene studiato e analizzato in maniera continuativa, anche al fine di guidare le azioni di supporto alle vittime di incidenti, di avviare campagne di sensibilizzazione verso soggetti o settori particolarmente esposti nonché di tarare il modello stesso, creando una sorta di controreazione: si intensificano le attività di monitoraggio verso quei settori e soggetti rilevati come più a rischio.

Il prosieguo del documento introduce le definizioni nella sezione 2, fornisce alcune considerazioni sugli altri approcci per rappresentare lo stato della minaccia adottati da altre agenzie, CSIRT e *fornitori* nella sezione 3, nella sezione 4 si presentano alcune delle fonti dati utilizzate, separandole tra proattive e reattive. Il modello di analisi dei dati è illustrato nella sezione 5. La sezione 6 elenca e descrive le metriche e gli indicatori derivanti dalle attività operative, ovvero quelli che è possibile effettivamente quantificare mostrando statistiche e

[1] La constituency è l'insieme dei soggetti nei confronti dei quali lo CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici

trend. La sezione 7 conclude il documento offrendo spunti per eventuali sviluppi futuri.

2. Definizioni

In questa sezione sono elencate una serie di definizioni cui si farà riferimento nel seguito del documento.

Tali definizioni non sono da intendersi di carattere generale, in considerazione che per tali concetti esistono sì fonti autorevoli, come il glossario del NIST [4] per citarne uno, ma non esistono fonti universalmente riconosciute. Oltre a quelle riportate di seguito, anche sul sito del CSIRT Italia è possibile trovare un glossario di definizioni [5]

Definiamo:

- comunicazione ricevuta: e-mail, anche generiche, relative ad informazioni contenenti profili di natura cyber ricevute dal CSIRT Italia, sottoposte a valutazione preliminare per determinare l'apertura o meno di un case;
- *case*: un avvenimento d'interesse per lo CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I *case* possono diventare *eventi* cyber;
- evento *cyber*: un *case*, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, CSIRT Italia dirama *alert* e/o supporta, eventualmente anche in loco, i soggetti colpiti. Qualora fosse confermato l'impatto dal soggetto coinvolto, l'*evento cyber* viene considerato *incidente*;
- incidente: un *evento cyber* con impatto confermato dalla vittima;
- segnalazione: le notifiche previste per legge, effettuate tramite specifico modulo web sul sito del CSIRT Italia, per i soggetti appartenenti al Perimetro di Sicurezza Nazionale Cibernetica [6], per gli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali (ovvero gli operatori a cui si rivolge la citata Direttiva NIS), e per gli operatori di comunicazione (i cui obblighi di notifica sono definiti dal c.d. decreto Telco [7]). Rientrano nelle segnalazioni anche quelle di natura volontaria previste per legge dal Dlgs 65/2018 di recepimento della Direttiva NIS;
- richieste di informazioni: richieste effettuate dal CSIRT Italia al soggetto potenzialmente impattato da un *evento cyber* per acquisire ulteriori elementi, come ad esempio la conferma di una possibile compromissione;
- comunicazione inviata: alert, anche massivi, inviati a Pubbliche Amministrazioni e imprese potenzialmente interessate da eventi cyber;
- asset con potenziali criticità: sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio e per i quali vengono inviate specifiche comunicazioni;
- fattori di rischio: una configurazione errata o non in linea con le *best practice* ovvero la possibile vulnerabilità di un asset;

- current rule: regola di correlazione che implementa una logica, finalizzata all'individuazione automatizzabile di possibili eventi cyber d'interesse a partire da un vasto insieme di dati;
- security event: un singolo evento (da non confondere con l'*evento cyber* definito precedentemente) rilevato dai sistemi di monitoraggio in un intervallo temporale ben definito, relativo ad un'attività anomala verso uno specifico asset ovvero effettuata dall'asset stesso o attraverso di esso.

3. Stato dell'arte: approcci degli altri Agenzie nazionali di cybersicurezza e di report di altre amministrazioni e fornitori

I report specialistici dei fornitori di soluzioni di cybersicurezza e le relazioni di altre amministrazioni e CSIRT[2] nazionali utilizzano fonti di dati diverse e approcci diversi nel valorizzare le informazioni, ma soprattutto terminologie diverse.
Facciamo un esempio su tutti molto spesso viene utilizzata la terminologia di "attacco cyber", tuttavia per attacco cyber si può intendere sia un incidente con un impatto concreto sulla vittima, sia uno o più tentativi di intrusione magari non andati a buon fine, o anche attività di scansione, di preparazione all'attacco vero e proprio e così via. Recentemente la nuova Direttiva europea (EU) 2022/2555, c.d. Direttiva NIS2 [8] ha introdotto il concetto di "quasi incidente" (*near-miss* in lingua originale), ovvero un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati […], ma che è stato efficacemente evitato o non si è verificato. Il *near-miss* è quindi un attacco cyber? E ancora, una campagna di phishing con un milione di vittime sono un milione di attacchi cyber?

Tutto ciò implica che spesso i numeri delle varie pubblicazioni non sono direttamente confrontabili e di conseguenza non possono essere utilizzati per caratterizzare lo stato della minaccia in maniera rigorosa.

In questa sezione si forniscono alcuni dettagli sugli approcci seguiti dagli altri CSIRT e da alcuni altri report noti.

Enisa Threat Landscape: da 10 anni la European Union Agency for Cybersecurity (ENISA) [9] rilascia il suo report annuale sullo stato della minaccia in Europa (l'ultimo è quello del 2023 pubblicato a ottobre [10]). Il report individua le minacce più frequentemente rilevate nell'anno di riferimento, le categorie di *threat actor* e i principali trend rispetto ai report precedenti.
Rispetto all'approccio adottato dall'ACN, sono pienamente compatibili i settori merceologici di appartenenza delle vittime e i tipi di minaccia, dal momento che vengono utilizzate le stesse tassonomie sia per i tipi di minaccia [11] che per i

[2] Le parole CERT (Computer Emergency Response Team) e CSIRT (Computer Security Incident Response Team) sono considerate sinonimi in questa trattazione. Storicamente, il marchio "CERT" è registrato in USA dalla Carnagie Mellon University, https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users (ultimo accesso luglio 2023) Specie in Europa, dopo la Direttiva NIS che utilizza il termine CSIRT, gli Stati membri stanno abbandonando l'utilizzo di "CERT".

settori [12]. Quello che differisce non è tanto la metodologia utilizzata – rigorosamente dettagliata da Enisa in un documento specifico [13] – quanto le fonti dei dati. Enisa utilizza fonti aperte (social media, data feeds, cybersecurity news ed altre) e le sue proprie capacità di *Cyber Threat Intelligence*. L'approccio è quindi sicuramente valido per fornire un quadro di situazione dello stato della minaccia ad ampio spettro, tuttavia non può rappresentare dettagliatamente quanto effettivamente avviene all'interno di una singola nazione, poiché non tiene conto del considerevole numero di eventi non divenuti di dominio pubblico, ma comunque avvenuti e gestiti da CSIRT nazionali, privati o da fornitori.

Il CERT-EU [14], CERT della Commissione Europea servente le così dette "EU institutions, bodies and agencies (EUIBAs)", ha pubblicato di recente la decima edizione del suo Threat Landscape Report [15], e pubblica periodicamente dei report [16], specificando che si basa principalmente su report pubblici e che, principalmente, gli incidenti sono ritenuti rilevanti in accordo alla rilevanza mediatica che hanno avuto.

Il CERT nazionale lettone [17] utilizza un approccio originale: valuta lo stato della minaccia della sua nazione, nei suoi report pubblici [18], basandosi sul monitoraggio del proprio spazio di indirizzamento IP che alcuni servizi, come ad esempio Shadowserver [19], forniscono agli CSIRT nazionali. Anche il CERT lettone utilizza la stessa tassonomia degli incidenti adottata dal CSIRT Italia, così come anche in ACN vengono utilizzati sistemi di monitoraggio dello spazio di indirizzamento nazionale, ma principalmente ai fini di early warning.

Il CERT Lituano [20] nei report annuali [21] utilizza il termine incidente per riferirsi anche a *phishing, distribution of unwanted information, hacking attempts*. Inoltre, sembra che nel report non sia utilizzata una tassonomia nota. Questa differenza nella terminologia fa sì che i numeri non siano confrontabili direttamente con quelli dell'ACN. Interessante è il fatto che tale CERT analizzi il contenuto dei *data breach* subiti dalla sua *constituency* per categorizzarne la tipologia di vittima, i tipi di dati esfiltrati e l'eventuale presenza di dati personali.

Il CERT spagnolo [22] nell'ultimo report disponibile [23] utilizza il termine incidenti "critici" per rappresentare l'andamento dello stato della minaccia, senza specificare soglie di criticità, mentre nel focus sugli incidenti causati da *ransomware* mostra una media mensile in linea con quanto rilevato dal CSIRT Italia.

Sicuramente d'interesse sono anche gli approcci seguiti dal National Cyber Security Center del Regno Unito [24] e dal CERT Bund tedesco [25] (che opera nel Federal Office for Information Security – BSI [26]): se il primo si focalizza principalmente su un'analisi di tipo qualitativo, fornendo solo pochi "numeri"– riporta ad esempio "centinaia" di incidenti di cui 63 "significativi al punto da richiedere una risposta a livello nazionale" contro i 126 incidenti rilevati in Italia nello stesso periodo – il secondo fornisce uno spaccato principalmente quantitativo, con i numeri circa le vittime di *data leak*; stime sull'ammontare complessivo dei riscatti pagati raccolte da fonti aperte, ma anche i numeri di nuove vulnerabilità, di nuove varianti malware, di incidenti, di messaggi di *spam,*

phishing e così via. Inoltre, considerando che entrambe le agenzie sono nate oltre 10 anni fa, BSI e NCSC nei loro report introducono confronti pluriennali.

A livello nazionale, il resoconto annuale dell'attività del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) [27] fornisce analisi qualitative e quantitative, basandosi sui dati provenienti dall'attività di polizia e gli approfondimenti investigativi, dai collegamenti telematici dedicati con le infrastrutture critiche e dalle collaborazioni internazionali con FBI e Europol. Nel resoconto viene utilizzato il termine "attacco" e nel 2022 ne sono stati rilevati 12.947 contro i 5.435 registrati del 2021 segnando un +138% in solo anno.

Per quanto attiene invece ai report periodici dei fornitori (esempi sono quelli di Accenture [28], CISCO [29], Crowdstrike [30], Mandiant [31], Microsoft [32] ,Verizon [33], Swascan [34]), in generale questi si basano su dati provenienti direttamente "dal campo". Si parla quindi di telemetria dei prodotti installati all'interno dei propri clienti secondo la propria penetrazione di mercato, di lessons learned derivanti dalle azioni di *incident management*, degli esiti di attività OSINT e CLOSINT, dell'utilizzo di honeypot, di antivirus e così via. In linea teorica, un *fornitore* con un'ottima penetrazione di mercato, sia su organizzazioni pubbliche che private, potrebbe fornire dati molto rappresentativi dello stato della minaccia di una nazione. Tuttavia, anche in questo caso, la diversità in termini numerici che può derivare dalle analisi dei report di fornitori privati dipende da come ognuno di questi ultimi definisce il concetto di "evento cyber" e se questo ha effettivamente avuto un impatto oppure no e, soprattutto, alla citata penetrazione di mercato del fornitore stesso: quanto è rappresentativo il cono di visibilità che ha sulla minaccia di un singolo fornitore? Questi report offrono comunque una preziosa base di conoscenza sui fenomeni avvenuti e gestiti, spesso senza che le autorità ne vengano a conoscenza.

4. Patrimonio informativo: il "cono di visibilità" del CSIRT Italia

In questa sezione si descrivono le principali fonti dei dati del CSIRT Italia.

Le fonti si raggruppano in due categorie, quelle di carattere reattivo e quelle di carattere proattivo.

Le fonti dati di carattere reattivo sono quelle derivanti da tutte le attività di gestione degli eventi cibernetici che iniziano con le *comunicazioni* ricevute o con le *segnalazioni* e proseguono con l'apertura di *case*, i quali possono diventare o meno *eventi cyber* e, qualora vi sia impatto confermato dalla vittima, *incidenti*. Per lo CSIRT Italia le *segnalazioni* previste per legge, incluse quelle volontarie[3], assumono direttamente la connotazione di incidente, in quanto solitamente sono effettuate a seguito del rilevamento di impatti da parte del soggetto segnalante.

[3] l'art. 18 del citato Dlgs 65 del 2018 consente a oggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali di notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati

Le fonti di carattere **proattivo** sono invece quelle derivanti da attività di monitoraggio, ovvero quelle che provengono dai cosiddetti *feed*, flussi di dati tecnici commerciali o gratuiti, a cui l'Agenzia ha accesso, e da attività manuali o automatiche di ricerca di compromissioni e vulnerabilità anche su fonti aperte.

A queste fonti si aggiungono i dati condivisi dalla rete di CSIRT europea, istituita anch'essa dalla citata Direttiva NIS, e dalle altre reti di collaborazione, nate in ambito privato, alle quali CSIRT Italia partecipa (Trusted Introducer [35] e FIRST [36]).

L'insieme delle fonti reattive e proattive offre un **cono di visibilità** sulle minacce a danno del sistema Paese che, dal punto di vista qualitativo, ci dà un quadro rappresentativo delle minacce e del livello di esposizione dei soggetti nazionali. Dal punto di vista numerico è necessario, però, tener presente che esiste un mondo sommerso di incidenti ed eventi dei quali l'Agenzia, così come ogni articolazione cyber omologa, non ha visibilità immediata. Si fa riferimento quindi a tutti quei casi, siano essi incidenti o eventi, che sono:

- non scoperti dalla vittima;
- scoperti dalla vittima ma non denunciati e non segnalati ma gestiti in autonomia;
- registrati dai servizi di monitoraggio dei soggetti privati che offrono servizi di sicurezza e non segnalati;
- vulnerabilità zero day (vulnerabilità in sistemi nota agli attaccanti ma ancora sconosciuta ai produttori dei sistemi, per la quale quindi non esiste una contromisura).

Questo concetto è anche rappresentato graficamente più avanti, in Figura 1.

Per poter colmare sempre più tale gap informativo, sono in corso attività finalizzate a potenziare le capacità degli strumenti tecnici (si fa riferimento particolarmente ai servizi cyber nazionali in via di sviluppo con il Piano Nazionale di Ripresa e Resilienza, quali HyperSOC[4], ISAC Italia[5] e Rete dei CERT[6], descritti

[4] L'HyperSOC, in corso di sviluppo presso ACN, sarà un centro di monitoraggio delle informazioni tecniche di sicurezza, che raccoglierà dati di cybersicurezza dalle imprese e pubbliche amministrazioni che ne faranno parte e, utilizzando un approccio data driven/big data security, processerà le informazioni a beneficio della attività cyber proattive e reattive;

[5] ISAC Italia (Information Sharing and Analysis Center Italia), prossimo all'avvio, sarà il centro nazionale di condivisione di informazioni strategiche per la cybersicurezza tra gli ISAC settoriali italiani. I dati collazionati centralmente correlati e integrati con quelli dell'HyperSOC abiliteranno capacità avanzate a beneficio dell'analisi del rischio cyber nazionale, settoriale e verticale su soggetti critici specifici;

[6] La rete dei CERT territoriali, in corso di istituzione, mira a migliorare le capacità di incident response nazionale delocalizzando i team di intervento, grazie alla collaborazione di CERT territoriali esistenti e da costituire, allineati a metodologie e standard condivisi con CSIRT Italia e a diretto contatto con il centro stella rappresentato dal CSIRT Italia.

nella Strategia nazionale per la cybersicurezza [35]), e a stringere accordi di collaborazione con soggetti pubblici e privati volti anche allo scambio di dati.

5. Modello di analisi dei dati

Questa sezione descrive il modello di analisi dei dati adottato. L'analisi dei dati necessaria a rappresentare lo stato della minaccia è svolta in ACN seguendo le classiche fasi della data analysis: collection, cleaning, processing, visualization. Le attività, specie nelle fasi di data collection e processing, sono sempre separate tra proattive e reattive in quanto il flusso delle informazioni segue necessariamente percorsi diversi. Le fasi collection e processing individuano e classificano per tipologia, grazie ad analisi e approfondimenti, eventi e incidenti cibernetici. Nella fase di data visualization gli eventi e incidenti sono "presentati" ovvero quantificati, categorizzati e utilizzati nelle attività di supporto ai soggetti impattati, elaborando specifici bollettini e alert per la pubblicazione o le comunicazioni dirette, o per la redazione di report specialistici di approfondimento.

La Figura 1 rappresenta la composizione delle varie fasi, evidenziando anche il "sommerso" di eventi e vulnerabilità che non entrano a far parte del cono di visibilità del CSIRT Italia. Le varie fasi sono di seguito approfondite.

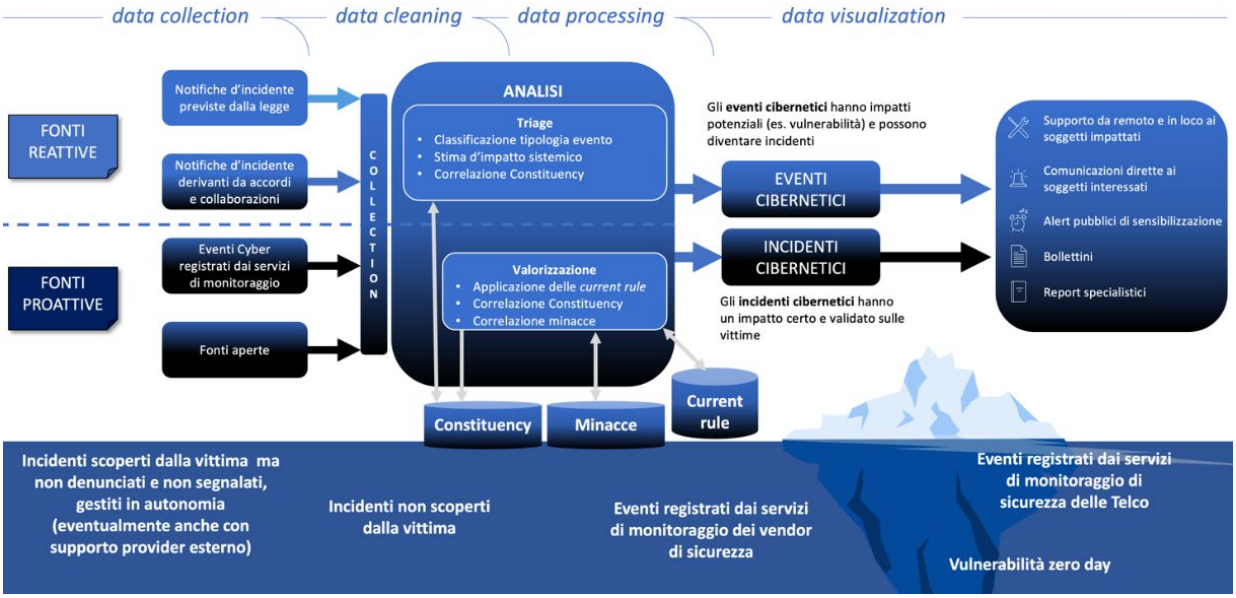


Figura 1
Modello di data analysis in uso nel CSIRT Italia. Si distingue tra i dati visibili, nella parte chiara della figura, e quelli "sommersi" nella parte in basso.

Data collection: nella prima fase i dati provenienti dalle varie fonti di cui alla sezione 4 sono individuati e raccolti. Importante considerare che nella *collection* i dati provenienti dalle fonti non sono strutturati in maniera omogenea. Si hanno, infatti, sia comunicazioni ricevute via mail, testuali e

necessariamente processate da analisti, sia i vari *feed* delle attività proattive, strutturati, ma ognuno con i propri formati.

In questa fase il numero di comunicazioni e dati provenienti dai feed è dell'ordine dei milioni l'anno (principalmente da fonti proattive, le e-mail e notifiche d'incidente sono invece ordine delle migliaia l'anno). Si consideri che la singola comunicazione può informare un considerevole numero di potenziali eventi cyber.

Data cleaning: vengono rimossi eventuali dati errati e duplicati, nonché normalizzati i dati al fine di agevolare le fasi successive. Questa è la prima delle fasi in cui si suddivide la vera e propria analisi.
Il numero di comunicazioni e informazioni è ancora nell'ordine dei milioni l'anno.

Data exploration e mining (processing): i dati vengono effettivamente valorizzati, in modalità diverse a seconda che si tratti di attività reattive o proattive.

In particolare, le attività reattive iniziano con l'importante fase di triage, opportunamente tarata sulla constituency. Nel triage l'analista valuta il contenuto della comunicazione ricevuta e decide se quanto comunicato può effettivamente configurarsi come un evento cyber (ovvero se ha potenziale impatto su almeno un soggetto nazionale) e scalare quindi a livello di incidente (se l'impatto è confermato dalla vittima). Valuta altresì il potenziale impatto sistemico di eventi o vulnerabilità, studiando accuratamente le porzioni della constituency che potenzialmente possono essere interessate dall'evento e applicando dei modelli di calcolo sviluppati appositamente.

Se supera il triage, ovvero se sussistono potenziali impatti, il dato inizialmente ricevuto diventa un *evento cyber* e, oltre a dover essere gestito, sarà una delle metriche descritte nella sezione 6. Importante considerare che questa fase *non è automatizzabile*, il lavoro dell'analista è preziosissimo.

Nella fase di *processing* delle attività *reattive* si passa dall'ordine delle migliaia di comunicazioni esaminate (provenienti dalle fonti) tipicamente a circa mille eventi cyber l'anno.

Diverso è il caso delle attività proattive dove, considerato il volume dei dati trattati, è necessaria una forte automazione. La valorizzazione nelle attività proattive avviene principalmente in tre fasi, l'applicazione delle *current rule*, ovvero dei "filtri" che consentono automaticamente di discriminare se il dato processato è associabile o meno a una determinata tipologia di evento cyber d'interesse. Se la *current rule* "scatta", si passa alle due fasi

successive: la correlazione del potenziale evento cyber con i soggetti della *constituency*, che valuta se effettivamente potrebbero esserci impatti su almeno un soggetto nazionale; la correlazione con le minacce d'interesse. ACN dispone infatti di un catalogo di minacce d'interesse, monitorate in quanto le loro attività sono tipicamente osservate sui soggetti della *constituency*. Le minacce comprendono attori statuali, varie tipologie di malware e gli attori cybercrime.

L'efficacia delle attività proattive dipende quindi dalla qualità delle *current rule* che sono state definite per ogni fonte di dati, ma anche dalla capacità di correlare i *fattori di rischio* e *security event* individuati con gli elenchi di dispositivi e prodotti dei soggetti della constituency e con il catalogo delle minacce.

Al fine di produrre le *current rule*, i dati provenienti da queste fonti devono essere analizzati preventivamente per individuare quali informazioni possono essere utilizzate per l'identificazione di *fattori di rischio* e *security event*. Le *current rule* così prodotte sono applicabili in maniera automatica ai dati provenienti dai diversi feed.

Nel processing delle attività proattive si passa dall'ordine dei milioni di potenziali eventi, all'ordine delle decine di migliaia di eventi confermati l'anno.

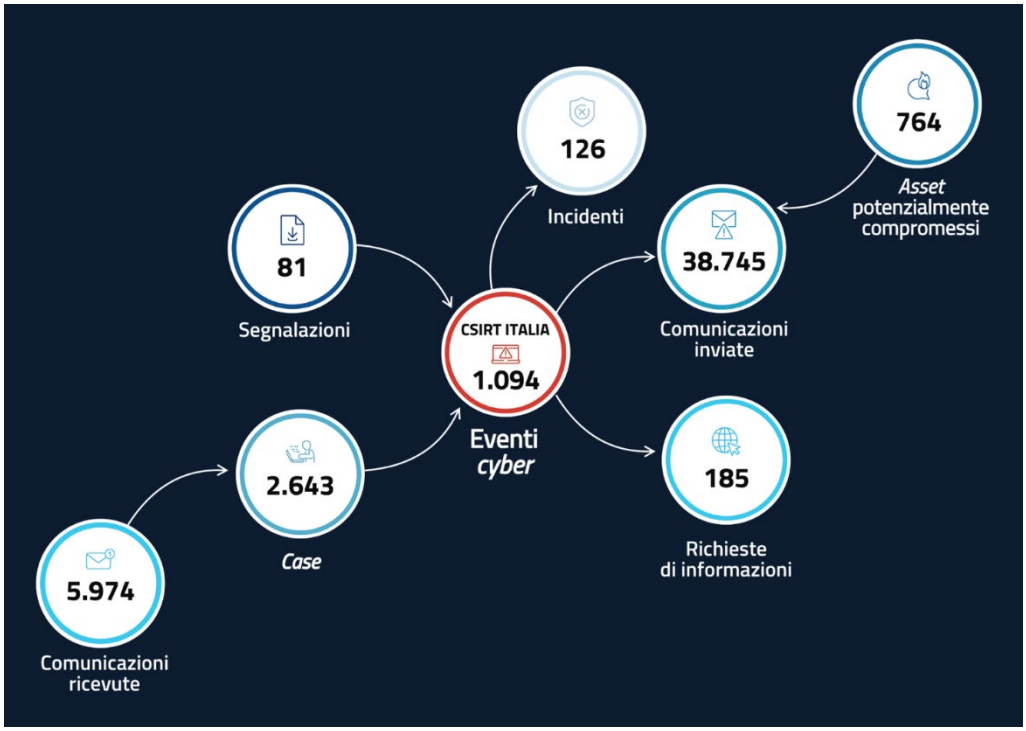


Figura 2
Alcuni dei numeri delle attività reattive e proattive del CSIRT Italia nel 2022.

Complessivamente, a valle della fase di processing si hanno solo due tipologie di metriche: gli eventi cyber e gli incidenti.

Data visualization: l'ultima fase del modello prevede la rappresentazione grafica dei dati, utilizzati per produrre report di analisi e previsionali, ma anche utilizzati ai fini delle attività di risposta e comunicazione nei confronti dei soggetti potenzialmente impattati.

In Figura 2 si riportano alcuni dei numeri delle attività reattive e proattive nel 2022.

6. Metriche (dati misurabili)

A seguito delle attività di Data processing vengono individuate le seguenti grandezze, che sono poi oggetto delle attività di analisi volte sia a sviluppare reportistica e *trend* sia a supportare e avviare le fasi di gestione degli eventi. In particolare, si ha:

- numero di *comunicazioni ricevute*, un indicatore, seppur grezzo, di quante notizie di possibili attività malevoli raggiungono lo CSIRT Italia; maggiore è il numero di comunicazioni ricevute, maggiore è potenzialmente il numero di eventi e incidenti;
- numero di *comunicazioni inviate* direttamente proporzionale, tra l'altro, al numero di vulnerabilità esposte dai soggetti della *constituency* e al numero delle compromissioni rilevate;
- numero di *case*, di *eventi cyber* (con relativa tipologia) e di *incidenti* con impatto confermato (con relativa tipologia). Insieme, queste tre metriche forniscono uno spaccato quantitativo delle attività reattive di gestione degli eventi e incidenti;
- numero, gravità e stima d'impatto sistemico delle nuove vulnerabilità[7]; metriche queste legate alla superficie d'attacco esposta dai soggetti della constituency: più vulnerabilità vuol dire più possibilità per gli attaccanti di compromettere i sistemi;:
- numero di dispositivi potenzialmente compromessi o a rischio di compromissioni esposti dai soggetti, rilevati dalle attività di monitoraggio;
- numero di pubblicazioni (alert, bollettini, report) sui canali pubblici quali sito del CSIRT Italia, Twitter [38] e Telegram [39];
- numero di attività di supporto (da remoto o in loco) effettuate per la gestione degli incidenti più gravi.

Tutte queste grandezze sono misurabili nel tempo (ovvero quantificabili a seconda del periodo di analisi, ad esempio al mese, per trimestre, all'anno) ed

[7] Le nuove vulnerabilità vengono valutate in modo da stimarne il possibile impatto a livello nazionale. La stima è effettuata tenendo conto di diversi parametri, tra i quali il punteggio di gravità assegnato (c.d. CVSS, https://nvd.nist.gov/vuln-metrics/cvss), la disponibilità di patch/workaround e PoC, la stima di diffusione dei software/dispositivi interessati nella constituency.

aggregabili in base alle varie caratteristiche del soggetto a cui queste sono potenzialmente riferibili, nonché alle tipologie di minaccia segnalata/gestita/rilevata.

Ciò avviene in accordo alle varie tassonomie di settori merceologici, pubbliche amministrazioni (ad esempio la categorizzazione dell'indice IPA [40]), imprese (ad esempio piccole/medie imprese, grandi imprese, e così via) e di eventi cibernetici (Ransomware, DDoS, malware…). A titolo di esempio in Figura 3 si riporta uno dei grafici sul numero di incidenti cibernetici nel 2022, diviso per tipologia di incidente e vittima.

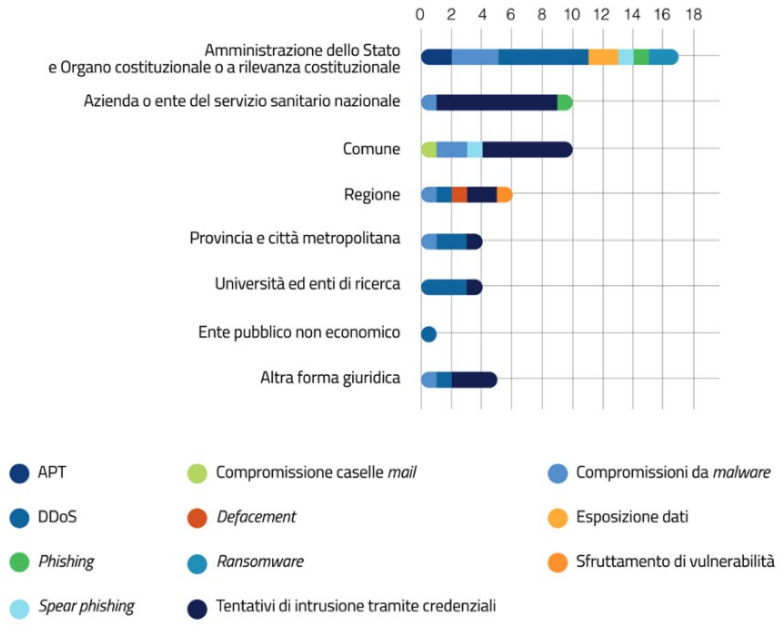


Figura 3
Distribuzione delle tipologie di incidenti rispetto alle diverse istituzione pubbliche.

7. Conclusioni

Il presente articolo, partendo da alcune definizioni di base, ha presentato le metriche e gli indicatori che vengono utilizzate per caratterizzare lo stato della minaccia cyber del Paese. È stato presentato il modello di analisi dei dati ovvero come, a partire da dati grezzi, l'Agenzia per la Cybersicurezza Nazionale arriva a informazioni utilizzabili per le attività di risposta, per attività previsionali e di rappresentazione dei dati.

Il processo qui descritto è stato elaborato sia seguendo le *best practice* della *data analysis*, rinvenibili nella letteratura, sia in base alla esperienza maturata nei primi anni di operatività del CSIRT Italia.

Come tutti gli approcci tecnici, presenta margini di miglioramento, che vengono continuamente esplorati tramite approfondimenti ed analisi.

Importante, in questo senso, lo studio dei prodotti degli altri CSIRT nazionali esteri, delle altre Agenzie e dei *fornitori*, alcuni dei quali richiamati nello stato dell'arte e confrontati in termini di metodologia e di terminologia. Ciò tenendo sempre presente che nell'analizzare dati quantitativi occorre sempre agire con le dovute cautele, a causa delle differenze, talvolta notevoli, di terminologia e di sensibilità degli analisti nel valutare gli impatti degli incidenti.

Le informazioni su altri approcci costituiscono la base per gli sviluppi futuri della metodologia presentata, sviluppi questi da condurre con l'obiettivo di efficientare e incrementare la capacità di data analysis dell'Agenzia. Capacità mirate alla rappresentazione continua e previsionale dello stato della minaccia cyber, a supporto delle attività di resilienza e di sicurezza nazionale cibernetica del Paese, di cui l'ACN è incaricata.

BIBLIOGRAFIA

[1] Direttiva (UE) 2016/1148 recepita in Italia dal Decreto Legislativo 18 maggio 2018, n.65 https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg. Al momento tale Direttiva è in corso di aggiornamento dalla Direttiva europea (EU) 2022/2555
[2] https://www.acn.gov.it/ (ultimo accesso luglio 2023)
[3] https://www.csirt.gov.it/ (ultimo accesso luglio 2023)
[4] https://csrc.nist.gov/glossary/ (ultimo accesso luglio 2023)
[5] https://www.csirt.gov.it/glossario (ultimo accesso luglio 2023)
[6] https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg (ultimo accesso luglio 2023)
[7] https://www.gazzettaufficiale.it/eli/id/2019/01/21/19A00317/sg (ultimo accesso luglio 2023)
[8] https://eur-lex.europa.eu/eli/dir/2022/2555 (ultimo accesso luglio 2023)
[9] https://www.enisa.europa.eu/ (ultimo accesso luglio 2023)
[10] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (ultimo accesso novembre 2023)
[11] https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view (ultimo accesso luglio 2023)
[12] https://github.com/MISP/misp-galaxy/blob/main/clusters/sector.json (ultimo accesso luglio 2023)
[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[14] https://cert.europa.eu/about-us
[15] https://cert.europa.eu/publications/tlr-10-years (ultimo accesso luglio 2023)
[16] https://cert.europa.eu/publications/threat-intelligence/2023
[17] https://cert.lv/lv (ultimo accesso luglio 2023)

[18] https://cert.lv/uploads/eng/cert-gada-atskaite-2022-EN-gv.pdf (ultimo accesso luglio 2023)
[19] https://www.shadowserver.org (ultimo accesso luglio 2023)
[20] https://www.nksc.lt/en (ultimo accesso luglio 2023)
[21] https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf (ultimo accesso luglio 2023)
[22] https://www.ccn.cni.es/index.php/en/ccn-cert-en (ultimo accesso luglio 2023)
[23] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html (ultimo accesso luglio 2023)
[24] https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf (ultimo accesso luglio 2023)
[25] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2022.pdf?__blob=publicationFile&v=8 (ultimo accesso luglio 2023)
[26] https://www.bsi.bund.de/EN (ultimo accesso luglio 2023)
[27] https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html (ultimo accesso luglio 2023)
[28] https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-173/accenture-cyber-threat-intelligence-report-vol-2.pdf (ultimo accesso luglio 2023)
[29] https://blog.talosintelligence.com/talos-year-in-review-2022 (ultimo accesso luglio 2023)
[30] https://www.crowdstrike.com/global-threat-report (ultimo accesso luglio 2023)
[31] https://www.mandiant.com/m-trends (ultimo accesso luglio 2023)
[32] https://www.microsoft.com/en-us/security/business/security-intelligence-report (ultimo accesso luglio 2023)
[33] https://www.verizon.com/business/resources/reports/dbir (ultimo accesso luglio 2023)
[34] https://www.swascan.com/wp-content/uploads/2023/05/Report-Q1-2023-Def-1.pdf (ultimo accesso luglio 2023)
[35] https://www.trusted-introducer.org/ (ultimo accesso luglio 2023)
[36] https://www.first.org (ultimo accesso luglio 2023) (ultimo accesso luglio 2023)
[37] https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza (ultimo accesso luglio 2023)
[38] https://twitter.com/csirt_it ultimo accesso luglio 2023)
[39] https://t.me/CSIRT_italiano (ultimo accesso luglio 2023)
[40] https://indicepa.gov.it/ipa-portale (ultimo accesso luglio 2023)
[41] https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg (ultimo accesso luglio 2023)

BIOGRAFIA

Luca Montanari, ingegnere informatico e dottore di ricerca, si occupa di cybersicurezza da oltre 15 anni, avendo iniziato come ricercatore all'interno del Centro di Ricerca di Cyber Intelligence and Information Security (CIS) della Sapienza e successivamente del Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica (CINI). È tra gli autori, oltre che di articoli scientifici, dei due Libri Bianchi sul futuro della cybersecurity in Italia pubblicati dal CINI nel 2015 e 2018, e degli "Italian Cybersecurity Report" redatti dal CIS Sapienza dal 2013 al 2016, tra i quali, il Framework Nazionale per la Cybersecurity del 2015.

Nel 2017 entra nella Presidenza del Consiglio dei ministri, dove collabora al recepimento della Direttiva NIS e allo sviluppo dell'architettura nazionale cyber, partecipando alla realizzazione del Perimetro di Sicurezza Nazionale Cibernetica e occupandosi in seguito di gestione del rischio cyber nazionale all'interno del CSIRT Italia.

Nel 2022 transita presso l'Agenzia per la Cybersicurezza Nazionale in cui attualmente svolge la funzione di Vicecapo della divisione "Gestione Rischio Nazionale, Capacità Cyber e Collaborazioni" del servizio Operazioni e dove si occupa di threat landscape, dell'analisi del livello di rischio cyber di settori e soggetti critici, dell'elaborazione di modelli di stima d'impatto sistemico di incidenti e vulnerabilità, e dei processi di accreditamento del CSIRT Italia alle reti di collaborazione internazionali.

La propaganda computazionale e le interferenze hacker

Arturo Di Corinto

Sommario

Gli hacker e gli attivisti digitali sono entrati a pieno titolo nelle guerre guerreggiate con gli strumenti propri della propaganda digitale, del sabotaggio elettronico, dello spionaggio cibernetico e dell'hacking. Lo fanno con attacchi DDoS, malware, ransomware, ma anche con algoritmi, deepfake, troll e bot. È così che partecipano alla guerra ibrida combattuta tra gli stati.

In tale scenario diversi autori ritengono che le tecniche di manipolazione delle percezioni che sfruttano gli strumenti digitali offerti dal web rientrino a pieno titolo tra gli strumenti della guerra ibrida, in quanto capaci di influenzare la reattività dell'avversario. Si parla a questo proposito di Guerra cognitiva.

Questo vuol dire anche che le campagne informative non si basano più soltanto sui media tradizionali, ma anche sui media digitali, le piattaforme social, i canali della messaggistica diretta.

Tra gli strumenti di queste campagne quelli della propaganda computazionale, usati per modificare il mindset del target, e generare incertezza, sfiducia e dubbio, destano sempre di più le preoccupazioni degli Stati. Il motivo è facile da intuire: laddove l'opinione pubblica è in grado di influenzare le scelte delle parti in guerra, riuscire a manipolarla può modificare le fasi del conflitto.

In questo paper cercheremo di descrivere le tecniche della propaganda computazionale e di come hacker attivisti e hacker di stato possano farne uso. Nell'anno elettorale mondiale che abbiamo davanti, il 2024, infatti, la propaganda computazionale potrebbe rappresentare un rischio per il processo democratico.

Abstract

Hackers and digital activists have fully entered the wars waged with digital propaganda, electronic sabotage, cyber espionage and software hacking tools. DDoS attacks, malware, ransomware, but also algorithms, deepfakes, trolls and bots are their weapons. This is how they participate in the hybrid war fought among States.

In this scenario, it is alleged that the techniques for manipulating perceptions that exploit digital tools are fully included among the weapons of hybrid warfare, as they are capable of influencing the reactivity of the adversary. In this regard we speak of Cognitive War.

This also means that information campaigns are no longer based only on traditional media, but also on digital media, social platforms and direct messaging channels.

Among the tools of these campaigns, those of computational propaganda, used to change the mindset of the target, to generate fear, uncertainty, and doubt, are increasingly arousing the concerns of States. The reason is easy to understand: where public opinion is able to influence the choices of the warring parties, manipulation can change the phases of the conflict.

In this paper we will try to describe the techniques of computational propaganda and how hacker activists and State hackers can use them. Indeed, in the global election year ahead of us, 2024, computational propaganda could represent a risk for the democratic process.

Keywords: Cybersecurity; disinformation; fake news; hacking; hacktivism; persuasion; propaganda computazionale

"According to some authors the impact of disinformation can be split into the following areas: a) Spread (superficial online/offline behaviour towards dis/misinformation), b) Attitude change or reinforcement (e.g. the psychological effects of dis/misinformation on beliefs, cognition), c) Behaviour change (e.g. altering voting behaviour, disengagement from politics and d) Broader societal impact (e.g. reducing institu-tional trust, undermining social cohesion)"[1].

1. Introduzione

Nell'ambiente mediatico attuale la disinformazione viene diffusa attraverso algoritmi di intelligenza artificiale, fake news, troll[2] e fantocci digitali, cioè attraverso i moderni strumenti della propaganda computazionale.

Non è semplice dare una definizione condivisa di cosa sia la propaganda computazionale, ma ogni concettualizzazione che la riguarda tende ad asseverarla come l'influenza esercitata attraverso l'uso di algoritmi e strumenti cibernetici sulla percezione degli individui.

Una definizione operativa, che ha mostrato negli ultimi anni tutto il suo valore euristico, è quella di Wooley e Howard dell'Università di Oxford, secondo cui "La propaganda computazionale è l'uso di algoritmi, automazione e cura umana per

[1] DOI: https://doi.org/ 10.37458/nstf.24.2.5
[2] I troll sono soggetti che disturbano le conversazioni che abbiamo sui social con interventi provocatori. Possono essere automatizzati come bot che ripetono costantemente gli stessi messaggi.

distribuire intenzionalmente informazioni fuorvianti sui social media" (Computational Propaganda Research Project, Working Paper No. 2017.11)[3] .

Per meglio comprendere come questo accada, cominciamo spiegando cos'è la propaganda.

Propaganda è un termine antico che può essere fatto risalire alla creazione dell'Istituto De Propaganda Fide ad opera dei vertici della Chiesa Cattolica Romana nel 1600. La propaganda della fede aveva come obiettivo l'evangelizzazione degli individui e la loro sottomissione all'unico Dio. Come tutte le religioni, anche quella cattolica è basata su narrazioni, e poiché il loro successo dipende generalmente dal numero di individui che cooperano in accordo con queste narrazioni, la loro propagazione è fondamentale.

In tempi moderni, il suo teorico storicamente più influente, Edward L. Bernays, ha descritto la *propaganda* come l'insieme delle azioni necessarie a guidare le masse, per il loro bene (Bernays, 1928)[4]. Bernays, nipote di Sigmund Freud, teorico della mente collettiva e della fabbricazione del consenso, era convinto che l'uomo della strada non avesse opinioni affidabili e che potesse votare per la persona sbagliata o desiderare la cosa sbagliata; quindi, riteneva che dovesse essere guidato dalla propaganda a fare le scelte giuste.

Bernays ha espresso compiutamente questo concetto nel 1928, nel suo libro più famoso, Propaganda. Erano gli anni ruggenti del capitalismo e il coevo consumismo non aveva ancora incontrato la Grande Depressione dei successivi anni '30. Ma si presentò subito un'occasione per guidare le masse e convincere le persone a fare quello che non avrebbero fatto di propria iniziativa: arruolarsi e partecipare alla Seconda guerra mondiale. Già all'epoca il termine divenne sinonimo di propaganda politica.

Vista come qualcosa di negativo, capace di influenzare il libero arbitrio delle persone, ma anche di facilitarne la coesione, la propaganda veicolata dai mass media è stata massicciamente usata nel secolo scorso da regimi dittatoriali - fascismo, nazismo e comunismo -, come pure dai governi democratici, ma ancora oggi il concetto moderno di propaganda ci rimanda alla disseminazione di idee e informazioni che hanno lo scopo di indurre alcuni specifici tipi di scelte o azioni in ambito sociale e politico.

La propaganda, che secondo Bernays doveva essere basata su fatti e informazioni accurate, è stata spesso confusa con la disinformazione, che risulta invece da un miscuglio di elementi veri ed elementi falsi. La propaganda, esplicita, organizzata da attori noti, per creare consenso intorno a un bene da promuovere, è però diversa dalla disinformazione, che può essere concettualizzata come il tentativo occulto di manipolare l'informazione per

[3] Samuel C. Woolley & Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 14 pp.
[4] Bernays, E. L. (2020). Propaganda. L'arte di manipolare l'opinione pubblica, a cura di Raffaele Scelsi, Milano, Shake Edizioni 2020; ed. or. Propaganda, 1928, Horace Liveright, New York.

fuorviare il ricevente di una comunicazione. E proprio questo era l'obiettivo della polizia segreta sovietica (GPU), che creò il termine "dezinformatzija", (дезинформация), intesa come "arma tattica".

La parziale sovrapposizione dei due concetti dipende dal fatto che propaganda e disinformazione servono allo stesso scopo, che è quello di usare l'informazione per influenzare le percezioni del ricevente allo scopo di modellarne il comportamento.

Con una sottile differenza: se la persuasione applicata alla propaganda può essere definita come l'innesco di un comportamento non spontaneo, facendo però leva sul ragionamento e gli appelli emotivi, la disinformazione si basa sulla sovversione delle informazioni che gli individui, supposti razionali, usano per agire le loro scelte, anche a dispetto dei propri interessi.

La stessa Unione Europea, mentre considera legittima la propaganda, ha avviato una serie di azioni per contrastare la disinformazione che oggi viaggia in rete in quanto: "informazioni altamente persuasive o fuorvianti create, presentate e diffuse per un guadagno economico o per ingannare intenzionalmente il pubblico, possono causare un danno pubblico. Il danno pubblico include minacce al processo politico democratico e al processo decisionale, nonché al bene pubblico, come la tutela della salute dei cittadini dell'UE, dell'ambiente o della sicurezza."[5]

Le campagne di manipolazione delle percezioni che oggi usano propaganda e disinformazione per seminare dubbio e scontento nella popolazione vengono infatti diffusamente distribuite sui social network principali, Facebook, X, Instagram, Truth, e altri ambienti ingegnerizzati per favorire il coinvolgimento delle persone e la polarizzazione delle opinioni. In aggiunta, propaganda e disinformazione sono diventate un problema cibernetico perché i suoi attori usano strumenti digitali automatizzati e interattivi per colpire le certezze dei bersagli con un esercito di troll, di bot[6] , e facendo largo uso di meme[7] e notizie online fasulle, create ad arte da gruppi di guerriglia digitale che usano anche tecniche di software hacking[8] per manipolare l'informazione e i suoi protagonisti, i cui contenuti viaggiano in misura consistente anche su forum come Reddit, Discord, e 4chan.

[5] Europarlamento, (2021), The impact of disinformation on democratic processes and human rights in the world, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf [aprile 2021]

[6] I bot sono software programmati per sostituire l'intervento umano e svolgere compiti di raccolta, analisi, catalogazione. I bot in grado di fare conversazione, sono detti chatbots.

[7] I meme, unità minime di informazione che si auto-propagano grazie alla loro semplicità. Si tratta spesso di immagini e slogan ad effetto, facile da comprendere e memorizzare. Sono uno strumento di disinformazione.

[8] Hacking è l'insieme dei metodi, tecniche e operazioni volte a conoscere, accedere e modificare un sistema informatico hardware o software.

2. Che cos'è la propaganda computazionale

La propaganda computazionale può essere quindi concettualizzata come veicolo di propaganda e disinformazione da parte di attori singoli e associati, volontari e mercenari, fasulli o reali, che usano le piattaforme digitali, i social network, i social media, per diffondere fake news[9], narrative distorte e contenuti persuasivi. Questi attori fanno un ampio uso di bot, troll, meme e tecniche di hacking per influenzare la percezione del ricevente ed elicitare, in chi vi è esposto, una reazione che sia in accordo con gli interessi dell'attore.

Se l'ambiente digitale è il luogo di elezione della propaganda computazionale, i suoi effetti, tuttavia, vengono amplificati dai media tradizionali - radio, tv, stampa -, che gli fanno eco, e che la posizionano all'interno dell'agenda mediatica, legittimandola. La propaganda diffusa dai media viene successivamente sfruttata dagli attori della propaganda stessa che la rimbalzano nei circuiti mediatici in un loop virtualmente infinito che è spesso all'origine di comportamenti complottisti.

Negli ultimi anni abbiamo visto all'opera soggetti organizzati gestire vaste attività di propaganda e disinformazione, si pensi alle fake news legate alla campagna presidenziale di Trump nel 2016; all'impiego di dark ads[10] e al microtargeting[11] generato dall'uso di app psicometriche come nel caso di Cambridge Analytica[12] oppure alle notizie fasulle dei potenziali effetti della Brexit, fino al dilagare delle false narrative della "fabbrica dei troll" di San Pietroburgo[13].

In tempi recenti il caso forse più famoso di inquinamento dell'informazione è stato quello noto come "Pizzagate" in cui è rimasta coinvolta la democratica Hillary Clinton che contendeva al repubblicano Donald Trump lo scranno della Casa Bianca. La fake news che all'epoca ottenne sui social più visibilità delle smentite giornalistiche la dipingeva a capo di un'organizzazione satanista che aveva creato un circuito di abusi pedofili nello scantinato di una pizzeria. Le indagini

[9] Le fake news sono notizie non documentate né verificabili. Questa forma di pseudo-informazione agisce online innescando i bias cognitivi noti come il pregiudizio di conferma, l'echo chamber e l'effetto bandwagon.
[10] I dark ads sono post sponsorizzati dagli inserzionisti verso specifiche porzioni di popolazione, individuate secondo dei parametri selezionabili.
[11] Il microtargeting è l'utilizzo dei dati di profilazione per personalizzare messaggi pubblicitari verso singoli individui, in base all'identificazione delle vulnerabilità personali dei destinatari. Viene utilizzato per promuovere un prodotto o un candidato politico.
[12] Wilye, C. (2019). Il Mercato del consenso: come ho creato e poi distrutto Cambridge Analytica, Milano, Longanesi; ed. or. Mindf*ck: Inside Cambridge Analytica's Plot to Break the World, London, Profile Books, 2019.
[13] La "Fabbrica dei troll" russi, è l'epiteto giornalistico dell'Internet Research Agency, struttura finanziata da Evgenij Viktorovič Prigožin, imprenditore, politico e comandante mercenario russo, amico del presidente russo Vladimir Putin, con il compito di sviluppare contenuti di propaganda a favore del governo di Mosca.

successive mostrarono che non solo non esisteva il circolo pedofilo, ma neanche lo scantinato (Harari, 2021[14] ; Bianchi, 2021[15]).

Se le fake news sono state uno strumento di competizione elettorale, anche i "bot" lo sono stati a più riprese. Su Facebook, Twitter, Instagram, molti profili fasulli sono governati da bot in grado di intavolare una banale discussione in chat (i chatbots), e che producono una notevole mole di messaggi. Spesso si tratta di esche sessuali o di truffatori che offrono denaro in prestito o altri servizi a pagamento, ma tra questi primeggiano i "political bots", in considerazione del fatto che sono le organizzazioni politiche quelle più propense a investire fondi consistenti nella propaganda computazionale.

Ad esempio, nel 2017 una serie di articoli[16] rivelò che due attiviste laburiste avevano commissionato la creazione di un bot, cioè di un sistema automatico di risposta su Tinder, nota app per incontri sentimentali. Programmato per specifiche fasce di età e di interessi, il suo scopo era quello di suggerire il voto per i laburisti a ogni potenziale anima gemella incontrata. Un altro esempio è quello dei bot che hanno rilanciato migliaia di volte l'hashtag #ReasonsToLeaveEu durante il referendum per la Brexit. Questi "amplification bots", secondo i ricercatori italiani della Fondazione Bruno Kessler, sono stati usati anche durante le elezioni politiche italiane del 2018 per "dopare" la diffusione dei messaggi della Lega e del suo leader, Matteo Salvini (Bachini & Tesconi, 2020)[17].

Similmente, gli attacchi nei confronti del Presidente della Repubblica italiana Sergio Mattarella sono da attribuire alla stessa logica. All'epoca, la guerra di hashtag sulla formazione del nuovo governo italiano nel 2018 ci ha mostrato un web istericamente diviso tra i sostenitori del presidente Mattarella e i suoi detrattori con due opposti hashtag, da una parte l'hashtag #IoStoConMattarella, di chi si è schierato a difesa delle Istituzioni incarnate dal capo dello Stato e dall'altra quello di chi ne ha chiesto finanche l'impeachment, #IlMioVotoConta[18] .

La funzione dell'hashtag è infatti proprio quella di aggregare e categorizzare i contenuti presenti sulle piattaforme sociali in relazione al tema trattato e rendere quindi più facile agli utenti individuare contenuti specifici senza perdersi. Nel caso del dibattito della formazione del nuovo governo l'hashtag è diventato la bandiera di opposte fazioni: entrambi usati per essere visibili nel flusso della comunicazione di un evento che ha indotto molti a prendere posizione a favore o contro per far pesare la propria opinione. Quelli che chiedevano l'impeachment

[14] Harari, Y., N. (2018), 21 Lezioni per il XXI secolo, Bompiani, Milano.
[15] Bianchi, L., (2021), Complotti. Da Qanon alla pandemia, cronache dal mondo capovolto, Minimum Fax, Roma.
[16] Rodrigues Fowler, Y., Fowler, Goodman, C., (2017), How Tinder Could Take Back the White House, The New York Times, Disponibile in https://www.nytimes.com/2017/06/22/opinion/how-tinder-could-take-back-the-white-house.html [22 giugno 2017]
[17] Bachini, V., Tesconi, M. (2020), Fake people. Storie di social bot e bugiardi digitali, Codice Edizioni, Torino
[18] Di Corinto, A. (2018), La guerra degli hashtag e il mostro del web. IL Manifesto, Disponibile in https://ilmanifesto.it/la-guerra-degli-hashtag-e-il-mostro-del-web-2/ [31 maggio 2018]

del Presidente però provenivano da 360 account creati ad hoc lo stesso giorno della contestazione sull'allora Twitter, oggi X.

Non ci sono solo i bot. A volte sono le persone in carne ed ossa che approntano messaggi, li automatizzano per pubblicarli a una certa ora e con una certa frequenza e, in una continua azione di propaganda, riempiono i social di informazioni e commenti destinati a sostenere il proprio beniamino. É il caso di Daniel John Sobiesky, un fanatico di Trump scovato dal Washington Post che ne ha raccontato le gesta[19] . Viola Bachini e Maurizio Tesconi nel loro libro Fake People. Storie di social bot e bugiardi digitali, li chiamano "cyborg".

3. Il futuro della disinformazione

È certamente possibile influenzare la narrazione di eventi in corso. Se ancora oggi viene fatto attraverso i titoloni dei giornali e le veline televisive, la novità è che si può fare anche via Internet senza ricorrere a persone in carne ed ossa, ma usando software che si comprano per pochi euro sia nel Dark Web sia in quello di superficie e che i più esperti possono programmare da soli.

Questi software possono fingere di essere utenti della rete e con i loro post, tweet, like e click, spacciarsi per una "opinione pubblica" inesistente il cui messaggio sarà amplificato dai media mainstream a seconda delle convenienze.

La propaganda computazionale è quindi esattamente questo: l'uso di reti di computer, le botnet, e sistemi intelligenti per simulare il comportamento di persone reali nella diffusione di messaggi politici e sociali attraverso il web.

I troll, i molestatori che chiedevano l'impeachment di Mattarella all'epoca del suo rifiuto di nominare ministro Paolo Savona ne rappresentano un esempio: 360 profili Twitter automatizzati creati quasi contemporaneamente per rilanciare post, commenti e hashtag contro il Presidente della Repubblica.

Durante la conferenza Black Hat di Las Vegas nel 2018, una delle più importanti per il mondo della sicurezza informatica, gli esperti dell'azienda Duo Security hanno rilasciato però un insieme di strumenti open source per identificare le botnet che invadono Twitter.

I ricercatori ci sono arrivati a partire dall'analisi di 88 milioni di account Twitter e del loro mezzo miliardo di post sulla piattaforma omonima.

È usando una ventina di euristiche che sono riusciti a individuare in maniera efficace i bot che amplificano messaggi propagandistici. Queste euristiche includono il numero di cifre che ne compone il nome, il rapporto tra follower /following, il tempo tra i tweet, le ore medie twittate al giorno e altri parametri. Per semplificare, un profilo che twitta tutto il giorno probabilmente è un bot perché gli esseri umani tendono a dormire almeno un quarto della giornata, un profilo che

[19] Timberg, J, (2017). As a conservative Twitter user sleeps, his account is hard at work, The Washington Post, Disponibile on line https://www.washingtonpost.com/business/economy/as-a-conservative-twitter-user-sleeps-his-account-is-hard-at-work/2017/02/05/18d5a532-df31-11e6-918c-99ede3c8cafa_story.html [5 febbraio 2017]

non diversifica link, hashtag e messaggi e cita sempre gli stessi utenti è con buona probabilità un bot, e così via.

Quindi nel caso di Twitter scovarli è relativamente semplice: i profili fasulli tipo «GiUsY12345», hanno pochi follower, producono sempre gli stessi messaggi, lo fanno di notte, e replicano raramente a quelli degli altri.

Anche evitare di cascarci dovrebbe essere abbastanza semplice: si scrive il nome del profilo sospetto su un motore di ricerca e se la persona compare su siti di notizie e altri social potrebbe essere una persona vera; incollando nella sezione immagini di Google il suo volto, si potrà poi facilmente scoprire con un confronto incrociato se quella persona esiste realmente oppure è solo il parto di un software.

Oggi però le cose si sono fatte complicate a causa degli «Attacchi Sybil». Questo tipo di attacchi coinvolgono organizzazioni che creano e controllano più account fasulli, i sockpuppet [20], utilizzando come avatar immagini provenienti da social legittimi o da foto di archivio.

Per ora, questo tipo di guerra dell'informazione (troll, bot, cyborg, meme) è relativamente rilevabile e prevedibile, ma gli strumenti e le tattiche moderne stanno diventando sempre più complessi e difficili da contrastare, come quelli che l'intelligenza artificiale consente di creare.

Ad esempio, prima i "fantocci" degli attacchi Sybil potevano essere individuati col "reverse engineering" delle immagini di profilo, ora è più difficile perché con tecniche di intelligenza artificiale è possibile generare immagini uniche di persone inesistenti come dimostra il sito This Person Does Not Exist (thispersondoesnotexist.com)[21] .

Da quando nel novembre del 2022 è stato reso pubblico l'utilizzo di uno strumento di Intelligenza Artificiale generativa (Gen AI), come ChatGPT (Chat Generative Pre Trained Transformer), si è sviluppato un ampio dibattito circa la disponibilità di strumenti come gli LL.MM. (Large Language Models) su cui si fondano, per creare deep fake video[22], deep fake audio, fake images.

A questo proposito si consideri lo scalpore suscitato dalle false immagini di Papa Francesco, atteggiato come un modello in passerella vestire un elegante piumino Moncler in stile trapper[23].

---

[20] Sockpuppet, letteralmente "pupazzo di calzino", è traducibile in maniera figurata come "impostore". Nel gergo informatico, indica un'identità digitale fraudolenta, governata da un burattinaio nascosto

[21] Di Corinto, A, (2019), L'«astroturfing» e i bot di Virgina Raggi, Il Manifesto, Disponibile in https://ilmanifesto.it/lastroturfing-e-i-bot-di-virgina-raggi [18 luglio 2019]

[22] I deep fake sono contenuti multimediali falsi prodotti con algoritmi di intelligenza artificiale

[23] Lana, A. (2023), Dopo Trump, anche il Papa: la foto fake con il cappotto bianco che tutti scambiano per vera, Disponibile in https://www.corriere.it/tecnologia/cards/dopo-trump-anche-il-papa-la-foto-fake-con-il-cappotto-bianco-che-tutti-scambiano-per-vera/il-nbsp-monclero.shtml [27 marzo 2023]

Tuttavia, gli autori della disinformazione cibernetica non hanno certo atteso la comparsa sul mercato di strumenti gratuiti per realizzare immagini fasulle e falsare la percezione e il giudizio del pubblico. Si pensi all'uso che è stato fatto del finto video del presidente ucraino Volodymyr Zelensky ritratto durante una videoconferenza con accanto tutto lo strumentario per farlo apparire come un cocainomane colto sul fatto da una foto rubata: "Quella che dovrebbe sembrare cocaina, è stata aggiunta con un software di video editing al video originale in cui non c'è traccia dell'ipotetica sostanza stupefacente. La prova evidente è proprio il video originale pubblicato su Instagram, il 6 marzo scorso, dallo stesso Zelensky sul suo account ufficiale." (Pisa, 2022)[24].

Oggi i falsi sono prodotti con tecniche di generazione avanzate e quindi risultano difficilmente identificabili; inoltre sono divulgati attraverso canali social creati ad hoc, popolati di maggioranze adoranti indifferenti a ogni statuto di verità dell'oggetto comunicato, bolle filtro di individui con la stessa opinione che riproducono all'infinito i contenuti facendogli da cassa di risonanza.

Secondo l'ultimo Rapporto sui Rischi Globali 2024[25] diffuso dal World Economic Forum a gennaio si prevede che la cattiva informazione, e la disinformazione, costituiranno un vero rischio per i prossimi due anni. Il 2024, è l'anno della più importante tornata elettorale della storia in cui si decideranno il governo dell'India, degli Stati Uniti, del Regno Unito, dell'Europa. Senza contare che già oggi, le operazioni di disinformazione e propaganda computazionale corrono parallele agli attacchi informatici nei conflitti armati. L'invasione russa dell'Ucraina lo ha dimostrato in maniera evidente.

4. La disinformatia russa e le interferenze hacker

Ormai da diversi anni hacker criminali e hacktivisti sono stati "reclutati" per mettere a segno attacchi informatici, azioni di spionaggio e sabotaggio per conto di gruppi di interesse, fazioni politiche, e stati nazione. Gli stessi hacker di stato, che spesso coincidono con gruppi APT, Advanced Persistent Threat, che prendono il nome dalla tecnica usata[26] , collaborano con individui politicamente o economicamente motivati, hacktivisti o cybercriminali, che fanno uso di tecniche di hacking per perseguire la propria agenda. Gli hacktivisti, coinvolti nei conflitti aperti, dall'Ucraina a Israele, e in quelli silenti, ad esempio tra l'Iran e gli USA,

[24] Pisa, P. (2022), Il falso video di Zelensky con la droga sulla scrivania: diffuso sui social dagli account pro-Russia, La Repubblica, Disponibile in https://video.repubblica.it/tecnologia/tech/il-falso-video-di-zelensky-con-la-droga-sulla-scrivania-diffuso-sui-social-dagli-account-pro-russia/414139/415066

[25] World Economic Forum, (2024), Global Risk Report 2024, Disponibile in https://www.weforum.org/publications/global-risks-report-2024/ [10 gennaio 2024]

[26] APT, Advanced Persistent Threat, minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per l'esfiltrazione di informazioni dalle infrastrutture IT del target. É una tecnica peculiare degli hacker di stato finanziati dai governi.

usano le tecniche che prima erano del sabotaggio culturale (Di Corinto & Tozzi, 2022)[27] per far avanzare la propria agenda politica. Questi hacker, qualunque sia il loro livello organizzativo e di comando, sono stati coinvolti a più riprese in operazioni di "hack and leak" (hackera e fai trapelare), "steal and publish" (ruba e pubblica), con l'obiettivo di creare confusione, panico e paranoia nel pubblico (Rid, 2021/2022)[28].

Ad esempio, secondo la società di consulenza Graphica, gruppi cinesi sono stati coinvolti in operazioni di disinformazione verso il governo americano, il presidente Biden e i manifestanti di Hong Kong[29] ; paesi come l'Iran hanno agito attraverso dei proxy informatici, hacktivisti e ransomware gangs, per sostenere la causa arabo-palestinese o per mostrare i muscoli agli USA[30] ; la Corea del Nord lo ha fatto per inquinare le prove delle incursioni dei propri hacker di stato[31] ; i servizi segreti russi per legittimare la causa dell'annessione della Crimea alla Federazione Russa, vestendo i panni di Anonymous.

La cifra comune di azioni tanto diverse è che ogni attacco informatico si svolge parallelamente ad un'azione di disinformazione per negare l'accaduto oppure per amplificarne la portata, ad esempio nei canali Telegram, laddove i risultati si siano rivelati modesti. Questo ultimo è il caso degli attacchi DDoS[32] portati da gruppi filorussi come Killnet (Di Corinto & Rociola, 2022)[33] , o di hacktivisti con vocazione religiosa come Anonymous Sudan o Mysterious Team Bangladesh.

Sono diversi i paesi che fanno ricorso agli hacker per sviluppare tool, strategie e azioni di propaganda e disinformazione, tuttavia, ritengono gli analisti, il modo di operare dei russi e dei filorussi è emblematico dell'uso che ne fanno in concomitanza con gli attacchi informatici veri e propri.

---

[27] Di Corinto, A. Tozzi, T., (2002). Hacktivism. La libertà nelle maglie della rete, Manifestolibri, Roma.

[28] Rid, T. (2022). Misure Attive. Storia segreta della disinformazione, Roma, Luiss University Press; tit. or. Active Measures: The Secret History of Disinformation and Political Warfare, Ferrar Straus & Giroux 2021.

[29] Di Corinto, A. (2020), Il Dragone attacca con le fake news, sicuri di riconoscerle? Il Manifesto, Disponibile in https://ilmanifesto.it/il-dragone-attacca-con-le-fake-news-sicuri-di-riconoscerle [20 luglio 2020]

[30] Di Corinto, A. (2020), Iran vs Usa, la cyberguerra è solo agli inizi, La Repubblica, Disponibile in https://www.repubblica.it/tecnologia/sicurezza/2020/01/09/news/iran_vs_usa_la_cyberguerra_e_solo_agli_inizi-245335228/ [9 gennaio 2020]

[31] Di Corinto, A. (2021), Corea del Nord: cybercrime di Stato per finanziare il programma nucleare, La Repubblica, Disponibile in https://www.repubblica.it/esteri/2021/02/11/news/nord_corea_cybercrime_di_stato_per_finanziare_il_programma_nucleare-287136346/ [11 febbraio 2021]

[32] DoS, Denial of Service, negazione di servizio, ovvero blocco dei servizi web, causato da numerose richieste di accesso illegittime al servizio esposto. La sua variante più nota è il DDoS, il Distributed Denial of Service attack

[33] Di Corinto, A., Rociola, A., (2022). Attacco hacker all'Italia. Cos'è Killnet, il gruppo russo che lo ha rivendicato, La Repubblica, Disponibile in https://www.repubblica.it/tecnologia/2022/05/11/news/attacco_hacker_italia_russia_killnet-349111881/ [11 maggio 2022]

Secondo Treyger et al. (2022), che hanno studiato gli sforzi della disinformazione russa sui social network, “Alcune delle attività russe che si svolgono sui o attraverso i social media non sono pura disinformazione; si tratta piuttosto di sforzi di disinformazione collegati funzionalmente a un attacco informatico di qualche tipo. Pertanto, anche se ci teniamo in gran parte lontani dalla discussione tecnica sugli attacchi informatici, tocchiamo le operazioni informatiche quando queste sono strettamente legate ad attività che utilizzano l’informazione per modellare percezioni o comportamenti, ad esempio, hack che producono informazioni che vengono successivamente trapelate”[34] .

Questo passaggio rappresenta bene il pensiero strategico dei russi rispetto al conflitto informativo che integra due aspetti: quello tecnico-informatico, che mira a influenzare “i sistemi tecnici che ricevono, raccolgono, elaborano e trasmettono informazioni”, e quello informativo-psicologico, che mira a colpire “il personale delle forze armate e la popolazione”.

Un pensiero ben descritto da Calise e Musella quando nel saggio Il Principe digitale (2019) scrivono: “Ma la vera novità del conflitto 2.0 è la sua penetrazione a livello di massa, con iniziative di propaganda o di campagna psicologica volte a influenzare quanto i cittadini sanno di sé e degli altri. In questo caso gli attacchi digitali non sono destinati a bersagli di tipo militare o infrastrutturale. Siamo invece in presenza di azioni mirate a condizionare il clima politico in un altro paese, o a mettere a repentaglio procedure di cruciale rilevanza come le elezioni. Una minaccia che preoccupa le democrazie occidentali, perché va al cuore stesso del loro sistema operativo: l'autonomia dell'opinione pubblica. E si gioca sulle piattaforme che connettono centinaia di milioni di cittadini”.

In generale, gli autori militari hanno identificato le seguenti caratteristiche che raccomandano i social media come arma informativa:

- il basso costo delle operazioni sui social media sia in termini di fondi che personale
- l'ampia portata potenziale delle operazioni di informazione online, soprattutto considerando la crescente penetrazione di Internet
- la capacità di reagire in tempo reale e in luoghi senza presenza fisica
- la negabilità delle operazioni sui social media, data la difficoltà nel distinguere l'attività ordinaria dagli atti di guerra dell'informazione sponsorizzati dallo stato
- la percezione che gli effetti psicologici dei media online e dei social media siano superiori a quelli forniti dai media tradizionali a causa del potenziale di confezionare contenuti multimediali in modo da ottenere “ulteriore influenza emotiva e psicologica”.

Un esempio di scuola è quello che è successo negli Stati Uniti con la campagna che ha portato Donald Trump alla Casa Bianca. Gli apparati di intelligence e

[34] Treyger, E. Cheravitch, J. Cohen, R. S., (2022) Russian disinformation Effort on social Media, Rand Corporation

importanti segmenti della politica statunitense, ricollegandosi al filone di indagine giudiziaria che ha preso il nome di Russiagate, hanno accusato Mosca di una intensa e duratura manipolazione delle informazioni al fine di favorire l'attuale presidente in carica. Renée Di Resta, capo di una delle due agenzie di cybersecurity incaricate dal Senato americano di studiare i meccanismi di influenza russa, ha parlato senza mezzi termini di "guerra mondiale dell'informazione"[35] .

Sono numerose le azioni di interferenza documentate di hacker russi nei processi democratici dei paesi occidentali. Dall'inizio della Guerra in Ucraina queste interferenze si sono moltiplicate, ma già prima ne abbiamo avuto numerosi esempi. Nel 2007 un vasto attacco DDoS viene compiuto in Estonia come ritorsione per lo spostamento della statua del soldato sovietico dal centro alla periferia di Tallinn, la capitale; nel 2008, in Georgia, quando all'attacco ai siti web georgiani si affianca una campagna militare vera e propria; nel 2014, quando il servizio segreto militare russo Gru crea un video falso di Anonymous per sostenere l'invasione dell'Ucraina; infine nel 2022, quando l'invasione del Donbass ucraino viene accompagnata da una serie di attacchi informatici: DDoS, defacciamenti e distribuzione di virus wiper che cancellano i registri di memoria dei computer Windows.

Il Digital Forensic Research Lab del Consiglio Atlantico pochi giorni prima[36] aveva segnalato una serie di false narrative distribuite sui social media e propagandate da giornali e televisioni pro-Cremlino. Intanto però prima dell'ingresso delle truppe russe in Ucraina, e degli attacchi informatici, i modem della rete Internet satellitare KA-SAT di Viasat venivano disabilitati in massa. In aggiunta a questo, i servizi segreti di Vladimir Putin hanno sfruttato i gruppi ransomware filorussi come Conti Team per attaccare la supply chain (ovvero la filiera di approvigionamento) di aziende dei paesi Nato con l'obbiettivo di interferire con la produzione di armi e l'erogazione di servizi essenziali come acqua e servizi sanitari.

5. Le cyber-operations russe

Il 27 aprile 2021 Microsoft pubblica un documento[37] in cui spiega il parallelismo tra le azioni di hacking e di disinformazione dei russi. Per gli esperti dell'azienda di Redmond negli Stati Uniti, da prima dell'invasione fino alla pubblicazione del rapporto, sono state lanciate 237 cyber-operations contro l'Ucraina da parte di almeno sei differenti gruppi di nation state hacker, ossia di esperti informatici governativi collegati ai servizi segreti interni ed esteri e militari russi.Si tratta in gran parte di attacchi distruttivi che hanno fatto uso di virus informatici per indebolire la capacità di reazione del Paese attaccato avendo come target le

[35] M. Calise, F. Musella, Il Principe digitale, Laterza, 2019
[36] Digital Forensic Research Lab, How ten false flag narratives were promoted by pro-Kremlin media, Feb 18, 2022, Medium [Online], https://medium.com/dfrlab/how-ten-false-flag-narratives-were-promoted-by-pro-kremlin-media-c67e786c6085
[37] Microsoft Digital Security Unit, (2022). An overview of Russia's cyberattack activity in Ukraine, Disponibile in https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. [10 settembre 2023] Microsoft Digital Security Unit

istituzioni ucraine, i servizi e le aziende informatiche, il comparto energetico, i media, le telecomunicazioni e Internet.

Secondo gli specialisti dell'azienda americana gli attacchi distruttivi sono stati accompagnati anche da ampie attività di spionaggio e sabotaggio che hanno sia degradato i sistemi informatici delle istituzioni in Ucraina, sia cercato di interrompere l'accesso delle persone a informazioni affidabili cercando di minare la fiducia nella leadership del paese.

Come dettaglia il rapporto, l'uso da parte della Russia di attacchi informatici e disinformazione sembrano essere fortemente correlati e talvolta direttamente sincronizzati con le sue operazioni militari cinetiche (quelle che in gergo militare indicano il movimento), che prendono di mira servizi e istituzioni cruciali per i civili. Il 1° marzo 2022, infatti, mentre un gruppo russo lancia attacchi informatici contro un'importante compagnia televisiva, l'esercito russo annuncia l'intenzione di voler distruggere obiettivi ucraini di "disinformazione" e dirige un attacco missilistico contro una torre della Televisione a Kiev. Ancora, mentre le forze russe assediano la città di Mariupol, gli ucraini ricevono un'e-mail da hacker russi che, fingendosi residenti di Mariupol, accusano falsamente il governo ucraino di "abbandonare" i suoi cittadini.

Gli attori coinvolti in questi attacchi insomma utilizzano una varietà di tecniche per superare le difese degli obbiettivi, tra cui il phishing, lo sfruttamento di vulnerabilità non risolte del software e la compromissione dei fornitori di servizi di Information Technology IT, gli attacchi alla supply chain.

Le operazioni di influenza e di interferenza praticate dai russi non sono sempre riconducibili ad ordini impartiti da Mosca, ma questa è proprio l'essenza della guerra ibrida teorizzata dai suoi stessi generali (Ottaviani, 2022[38] ; Bigazzi et al., 2022 [39]).

Come scrive Mark Galeotti: "Per combattere la sua guerra politica la Russia ha creato una macchina indubbiamente flessibile, economica, immaginifica e intraprendente, ma anche difficile da controllare. L'idea che tutti i troll, i propagandisti, le milizie, i corruttori, gli hacker e gli altri soldati di questo esercito siano sempre sotto lo stretto controllo del governo è assolutamente sbagliata. Certo, vi sono operazioni gestite sin dall'inizio a livello centrale e quelle di particolare importanza che, chiaramente, richiedono l'imprimatur del Cremlino. Rientrano in questo novero l'assassinio di Sergej Skripal in Inghilterra nel 2018 e l'interferenza nelle presidenziali americane del 2016. Nel grosso dei casi, tuttavia, Mosca ha incoraggiato molti «imprenditori politici» a prendere l'iniziativa, sovente con i loro tempi e a loro spese. Se falliscono, possono essere disconosciuti; se

[38] Ottaviani, M. F. (2022), Brigate Russe. La guerra occulta del Cremlino tra troll e hacker, Milano, Ledizioni LediPublishing
[39] Bigazzi, F., Fertilio, D., Germani, S., (2022). Bugie di guerra. La disinformazione russa dall'Unione sovietica all'Ucraina. Roma, Paesi Edizioni

riescono, possono essere premiati e a quel punto lo Stato può subentrare, ampliando o sviluppando l'operazione"[40] .

A fugare gli eventuali dubbi circa il rapporto esistente tra l'hacking e la diffusione di notizie false sono intervenuti gli stessi servizi segreti ucraini, arrestando un gruppo di cybercriminali specializzato nella vendita di account per diffondere disinformazione. Le autorità ucraine, pur non rivelando i nomi degli arrestati, hanno fornito le prove dell'attività di un gruppo di hacker operanti a Lviv in possesso di circa 30 milioni di account appartenenti a cittadini ucraini ed europei venduti sul DarkWeb. Le perquisizioni effettuate nelle case dei sospettati hanno portato al sequestro di hard disk contenenti dati personali, cellulari, schede Sim e memorie flash usate per lo scopo.

Secondo le stime degli investigatori, il gruppo, pro-russo, avrebbe guadagnato circa 400mila dollari rivendendoli all'ingrosso attraverso sistemi di pagamento elettronici come Qiwi e WebMoney.

Nel comunicato stampa il Servizio di sicurezza dell'Ucraina (SSU) sostiene che i clienti sarebbero propagandisti pro-Cremlino: "Sono stati loro a utilizzare i dati identificativi di cittadini ucraini e stranieri rubati dagli hacker per diffondere false notizie dal fronte e seminare il panico".

Nel comunicato si dice che gli hacker avrebbero operato per questo scopo: "la destabilizzazione su larga scala in più paesi", e che gli account sono stati utilizzati per diffondere false informazioni sulla situazione sociopolitica in Ucraina e nell'UE, precisando che "l'attività principale dei clienti degli hacker era proprio la creazione e la promozione di account nei social network e nei canali di messaggistica veloce".

In precedenza, le autorità avevano chiuso due farm di bot da 7.000 account per diffondere disinformazione e creare panico nella regione. Un'attività legata a una fase della guerra russo-ucraina in cui i cittadini di alcune zone, soprattutto nel Donbass occupato, non ricevono né cibo né informazioni. I pochi giornalisti che sono riusciti a parlarci infatti hanno dichiarato che gli ucraini sotto occupazione non conoscono l'entità dello scontro con Mosca, la percentuale di territorio occupata e se i propri congiunti siano vivi. Secondo Google-Mandiant[41] quando gli hacker governativi russi attaccano, passano i dati rubati agli hacktivisti entro 24 ore dall'irruzione in modo da consentirgli di effettuare nuovi attacchi e diffondere propaganda filorussa. Esempio da manuale di come il rapporto tra criminalità cibernetica, hacktivismo e hacking di stato sia anche più diretto[42].

[40] M. Galeotti, Controlling Chaos: How Russia manages its political war in Europe, European Council on Foreign Relations, 2017, https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/
[41] Mandiant, Hacktivists Collaborate with GRU-sponsored APT28, sept 2022, updated aug. 2023, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions
[42] A. Di Corinto, Hacking e disinformazione, la scuola russa, Il Manifesto, 29 Settembre 2022, [Online], https://ilmanifesto.it/hacking-e-disinformazione-la-scuola-russa

6. Conclusioni

Ogni società ricorre a delle narrazioni per fare progredire i gruppi sociali che la compongono verso mete utili alla collettività. Il senso e la direzione di queste narrazioni, politiche, sociali e religiose, cambia nei secoli, ed è in genere indifferente alla nozione di verità, concetto mobile e sfuggente per definizione. La creazione del consenso intorno a queste narrazioni si basa su storie condivise e la loro forza dipende dall'innesco di meccanismi psicologici come la credulità, il conformismo, la reciprocità, l'autorevolezza, sfruttando il principio di autorità, di similarità, di credibilità e così via.

Questi principi possono, e sono manipolati costantemente, da specifici attori.

La propaganda è una forma di narrazione di storie collettive, e la disinformazione si basa su distorsioni narrative, bias psicologici e tecniche persuasive. Con l'avvento del digitale e dei social network è più facili propagandare narrazioni vere, false, o inventate. Possono essere automatizzate, elicitano risposte rapide, non sono sempre verificabili. Gli attori della disinformazione lo sanno, e mescolano sapientemente il vero con il falso per elicitare risposte che avvantaggiano taluni e danneggiano altri.

É l'apoteosi dei servizi di intelligence che operano secondo la logica delle misure attive, l'insieme dei comportamenti volti a manipolare la percezione di un target, e che usano le fake news come una testa d'ariete per portare il loro attacco, l'attacco alla mente.

BIOGRAFIA

Arturo Di Corinto è stato professore di Identità Digitale, Privacy e Cybersecurity presso la Facoltà di Scienze Politiche, Sociologia e Comunicazione dell'Università di Roma la Sapienza, dove si è laureato in psicologia cognitiva. Attualmente ricopre il ruolo di advisor della comunicazione e degli affari pubblici presso l'Agenzia Nazionale per la Cybersicurezza (ACN) dove è responsabile anche delle pubbliche relazioni.

Giornalista interessato al tema dell'innovazione, ha lavorato anche per Il Sole 24 Ore, Wired e La Repubblica scrivendo 2300 articoli e molti libri su la governance di Internet, il copyright, la privacy e la cybersicurezza. Ha lavorato anche come giornalista esparto di temi di scienza e Tecnologia presso la televisione pubblica italiana.

Email: arturo.dicorinto@uniroma1.it

Governo dei Sistemi di Intelligenza Artificiale: Aspetti di Cybersicurezza

Luca Nicoletti, Monica Scannapieco, Mara Sorella e Marco Centenaro

Sommario

In un contesto di straordinario e rapidissimo sviluppo tecnologico, l'intelligenza artificiale (IA) irrompe nella routine personale e lavorativa di tutti noi con la promessa di grandi benefici per chi voglia valorizzarla per i propri scopi e interessi. Se da una parte i risvolti positivi sono innegabili, dall'altra è palese come l'utilizzo improprio dell'IA possa avere un impatto significativo nel mondo reale se non si applicano adeguate misure di controllo. Infatti, la strategia che l'IA adotta nel prendere decisioni, specialmente nel caso dei recenti modelli generativi del linguaggio, non è direttamente controllabile dall'essere umano e potenzialmente dipende dallo scenario in cui l'IA è adottata, determinando potenziali rischi di sicurezza con possibili ripercussioni anche sull'incolumità fisica delle persone.

In questo articolo, dopo aver introdotto i fondamenti del cosiddetto ecosistema dell'IA, analizzeremo nel dettaglio i macro-processi di governo dell'IA finalizzati a garantire la cybersicurezza dell'ecosistema stesso, dalla gestione di rischi cibernetici introdotti dall'IA ai programmi di ricerca ed innovazione sul tema, sulla base del contesto italiano. Descriveremo, inoltre, alcuni casi d'uso notevoli in cui l'IA rappresenta un supporto per la cybersicurezza, prima di concludere con alcuni spunti sui possibili sviluppi futuri.

Abstract

In a context of extraordinary and incredibly fast-paced development, artificial intelligence (AI) breaks into the daily routine of all of us, pledging to bring great benefits to those who want to exploit it. If on the one hand the positive aspects are undeniable, on the other hand it is clear how an improper use of AI can have a significant impact in the real world if adequate security controls are not enforced. Indeed, the strategy the AI adopts in making decisions, especially in the case of recent generative language models, is not directly under human control, and potentially depends on the specific scenario in which AI is applied, yielding possible non-negligible security and safety concerns.

In this article, after having introduced the fundamentals of the so-called AI ecosystem, we will analyze in detail the AI governance macro-processes aimed at guaranteeing the cybersecurity of the ecosystem itself, ranging from the management of cyber-risks introduced by AI to research and innovation programs, focusing on the Italian setting. We will also describe some notable use cases where AI comes in support of cybersecurity, before concluding with some insights into possible future developments in this field.

Keywords: artificial intelligence, machine-learning, cybersecurity, risk management, certification, standards, regulation, innovation, use cases, critical infrastructures, security operations centers, counter-AI.

1. Introduzione

Le sorprendenti prestazioni raggiunte recentemente dai modelli generativi del linguaggio (*large language model*, LLM) alla base di prodotti quali, ad esempio, ChatGPT e Bard, hanno contribuito a far salire l'intelligenza artificiale (IA) alla ribalta dell'opinione pubblica. La dirompente evoluzione tecnologica dell'IA, fino a pochi mesi fa percepita principalmente dagli addetti ai lavori, comincia ad impattare su diversi aspetti della vita quotidiana, sia in ambito privato che lavorativo. Le imprese spingono sempre di più per l'adozione di soluzioni di IA (cfr. Figura 1), principalmente nell'ottica della riduzione dei costi, dell'efficientamento della collaborazione tra diverse funzioni di business e per scoprire nuove potenzialità di fare profitti. Tuttavia, a fronte delle tante possibilità di utilizzo dell'IA, emergono anche nuove e significative minacce e sfide che richiedono investimenti dedicati da parte delle istituzioni nazionali e sovranazionali.

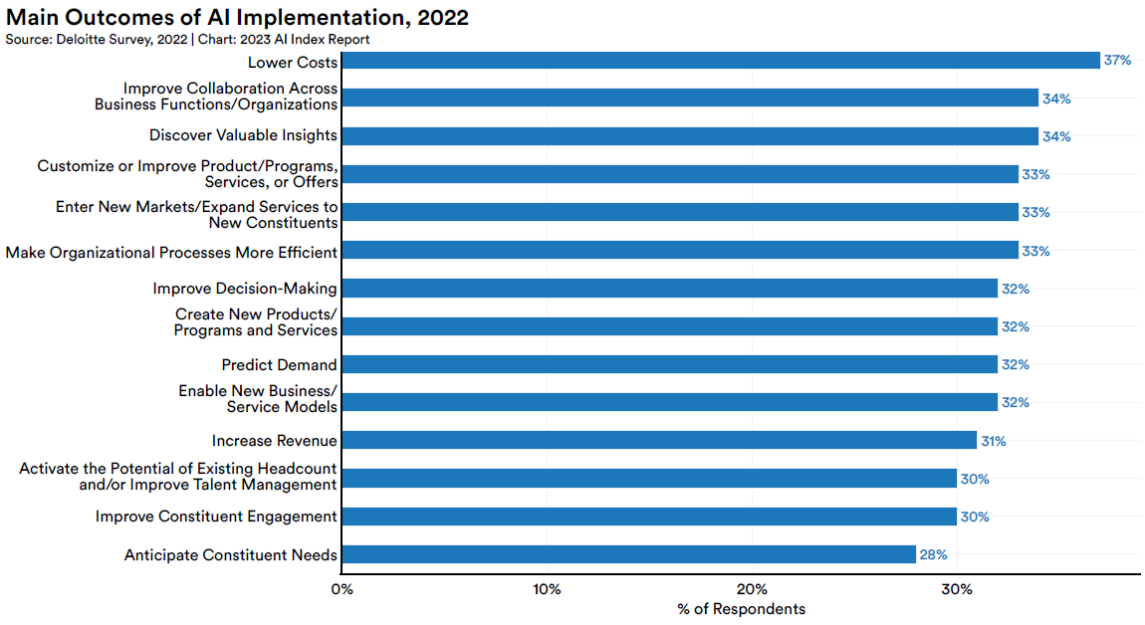


Figura 1
Principali risultati derivabili dall'adozione dell'IA nelle imprese (tratta da [1]).

A livello governativo, l'*AI Safety Summit* ha riunito, per la prima volta, 28 Paesi e l'Unione Europea a Bletchley Park nel Regno Unito nel novembre del 2023, pervenendo ad una dichiarazione condivisa ("*Bletchley Declaration on AI Safety*" [1]) che riconosce l'urgente necessità di comprendere e gestire collettivamente i rischi potenziali dell'IA attraverso uno sforzo globale congiunto, per garantire che l'IA sia sviluppata e utilizzata in modo sicuro e responsabile a beneficio della comunità globale.

Il Presidente degli Stati Uniti d'America (USA) ha emanato un ordine esecutivo nell'ottobre 2023 [2] con specifiche indicazioni finalizzate a rendere l'IA non pericolosa (in inglese, *safe*), sicura e affidabile, a dimostrazione dell'importanza e della strategicità degli investimenti sui sistemi di IA. Gli USA hanno altresì predisposto un programma strategico [2] e indicato un approccio basato sul "*Blueprint for an AI Bill of Rights*" [3], ovvero un insieme di principi e buone pratiche associate per governare lo sviluppo di sistemi automatizzati proteggendo i diritti e la sicurezza della società americana nell'era dell'IA.

L'Unione Europea (UE) ha anch'essa adottato una strategia [4] per gestire la ricerca e l'innovazione sull'IA, impegnandosi a perseguire un approccio all'IA che apporti benefici alle persone e alla società nell'insieme, attraverso un percorso che parte dall'individuazione delle applicazioni potenzialmente pericolose e di misure adeguate a tutelare l'affidabilità dei relativi sistemi. L'UE sta, inoltre, giungendo all'approvazione finale dell'*AI Act* [3], che, come dettagliato nella Sezione 3.3, costituirà la prima normativa mondiale in materia di intelligenza artificiale. Con riferimento agli aspetti di cybersicurezza in relazione all'IA, l'Agenzia dell'Unione Europea per la cibersicurezza (ENISA) ha avviato numerosi studi dedicati (ad esempio [5]).

Anche l'Italia ha elaborato un proprio programma strategico [6] sull'IA; tale programma è in corso di aggiornamento per tenere conto anche dei recenti sviluppi in materia di IA generativa. La strategia italiana è focalizzata, oltre che sulla ricerca, sullo sviluppo di applicazioni basate su IA a beneficio delle aziende e della pubblica amministrazione, e si appresta a recepire i regolamenti concepiti a livello europeo. Inoltre, l'Agenda di Ricerca e Innovazione per la Cybersicurezza [7] recentemente pubblicata dall'Agenzia per la Cybersicurezza Nazionale (ACN) riporta in maniera dettagliata svariati argomenti di ricerca concernenti l'IA e gli aspetti di cybersicurezza ad essa relativi.

Questo articolo ha l'obiettivo principale di chiarire la relazione tra IA e cybersicurezza al meglio delle conoscenze attuali in materia, concentrandosi su come governare i rischi dell'IA e su come sfruttare tale tecnologia per rafforzare

[1] Disponibile, in inglese, al sito https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.
[2] Disponibile, in inglese, al sito https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[3] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

la cybersicurezza in alcuni scenari notevoli. Il lavoro si focalizza sullo scenario nazionale italiano, pur fornendo un insieme di indicazioni e di spunti a carattere generale. Per raggiungere questo obiettivo, in Sezione 2 andremo anzitutto a rappresentare dove si inserisce la cybersicurezza nell'"ecosistema dell'IA", inteso come insieme di oggetti, attori e ruoli rilevanti nei macro-processi di governo (*governance*) dell'IA in relazione alla cybersicurezza. Questi ultimi, saranno invece dettagliati in Sezione 3. In Sezione 4, proporremo dei casi d'uso notevoli di applicazione dell'IA nel contesto della cybersicurezza dei sistemi. Concluderemo l'articolo in Sezione 5, evidenziando aspetti di rilievo ed indicando possibili sviluppi futuri.

2. La cybersicurezza nell'ecosistema dell'IA

2.1 Le dimensioni dell'IA&Cybersicurezza

Esistono molteplici declinazioni della relazione tra cybersicurezza e IA, trattandosi di una interazione complessa che può articolarsi in diverse direzioni. Nel seguito identifichiamo le tre che riteniamo di principale interesse:

1. cybersicurezza dell'IA. L'integrazione dell'IA nei sistemi informatici e nelle reti può introdurre nuove minacce. In particolare, alcuni attacchi tipici perpetrati ai danni di tali sistemi hanno ad oggetto la deduzione o l'estrazione di informazioni circa i modelli di IA o i dati utilizzati per il loro addestramento, oppure l'obiettivo di ingannare o eludere il funzionamento dei sistemi durante la fase di addestramento o di inferenza, al fine di influenzarne le previsioni o indurre comportamenti non desiderati, come ad esempio far riconoscere come sicuri oggetti pericolosi.

   La cybersicurezza dell'IA comporta un importante aspetto di governo dei rischi e, come enucleato in Sezione 3.1, rende necessario stabilire processi e procedure di *cybersecurity by design* in ogni fase dello sviluppo dei sistemi, dalle fasi di definizione dei modelli di IA, alla progettazione delle procedure di apprendimento, all'implementazione e test e in particolare alla fase di messa in produzione (*deployment*) finale del sistema, nonché nel monitoraggio e controllo dei sistemi in esercizio. Inoltre, in relazione alle dimensioni di cybersicurezza da considerare nel processo di governo dei rischi, è importante prendere in esame aspetti di cybersicurezza che sconfinano nella affidabilità (*trustworthiness*), quali la sicurezza fisica (*safety*), la trasparenza (*transparency*), la spiegabilità (*explainability*) e il governo dei dati (considerando gli aspetti di qualità dei dati e della loro protezione);

2. IA a supporto della cybersicurezza. L'IA utilizzata per realizzare strumenti avanzati di cybersicurezza e per facilitare gli sforzi delle autorità per rispondere meglio alla criminalità informatica e delle imprese per proteggere i propri sistemi. In particolare, la capacità dell'IA di identificare schemi e apprendere in modo adattivo in tempo reale può velocizzare i processi di rilevamento, contenimento e risposta agli incidenti. In questa accezione rientrano i sistemi di IA "contro-IA" ("*counter-AI*"), ovvero soluzioni innovative

basate su IA per rilevare, prevenire e mitigare le minacce provenienti da agenti automatizzati che utilizzano l'IA per attaccare e danneggiare reti, sistemi informatici e infrastrutture;

3. **IA per scopi offensivi**. Le capacità adattive dell'IA possono essere utilizzate per sviluppare strumenti di attacco più sofisticati, persistenti e difficili da rilevare. L'uso dell'IA può inoltre aumentare la potenza e la scala degli attacchi informatici. In particolare, la recente evoluzione dei modelli generativi del linguaggio permette di generare in modo massivo contenuti falsi che sembrano autentici. Questa possibilità, nelle mani di attori malevoli rende possibile automatizzare (tipicamente a basso costo) attacchi su larga scala quali campagne di disinformazione, *spam* e *phishing*.

Nel seguito, faremo sinteticamente riferimento alle tre direzioni esposte con la locuzione "**IA&Cybersicurezza**" e, propedeuticamente all'analisi delle connotazioni illustrate, partiremo dal definire cos'è l'IA e descrivere nel dettaglio il suo ecosistema, chiarendo in particolare i concetti di oggetti, attori e ruoli che lo compongono.

2.2 Definizioni

La definizione di "intelligenza artificiale" è tuttora dibattuta [4]. Una definizione [8] elaborata dall' *High-Level Expert Group* (HLEG) europeo sull'intelligenza artificiale [4] si riferisce ai sistemi di IA nei termini di "*sistemi software (e possibilmente anche hardware) progettati dagli esseri umani che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il loro ambiente attraverso l'acquisizione di dati, interpretando i dati raccolti strutturati o non strutturati, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo stabilito. I sistemi di IA possono utilizzare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti*."

In Figura 2, proponiamo una rappresentazione dell'ecosistema dell'IA&Cybersicurezza in termini di **oggetti**, **attori** e **ruoli** e la relazione con i principali filoni operativi (i c.d. macro-processi di governo), finalizzati a raggiungere i tre obiettivi (**protezione**, **risposta** e **sviluppo**) della Strategia Nazionale di Cybersicurezza [9] in tale contesto. Tra tutti i soggetti pubblici e privati partecipanti all'ecosistema, la figura evidenzia le funzioni ricoperte dai soggetti dell'architettura nazionale di cybersicurezza.

[4] Gruppo di esperti provenienti dal mondo accademico, dalla società civile e dall'industria nominato dalla Commissione nel 2018 con finalità consultive circa la strategia europea sull'IA, quali l'elaborazione di raccomandazioni sullo sviluppo di politiche future e sulle collegate questioni etiche, socio-economiche, legali e sociali

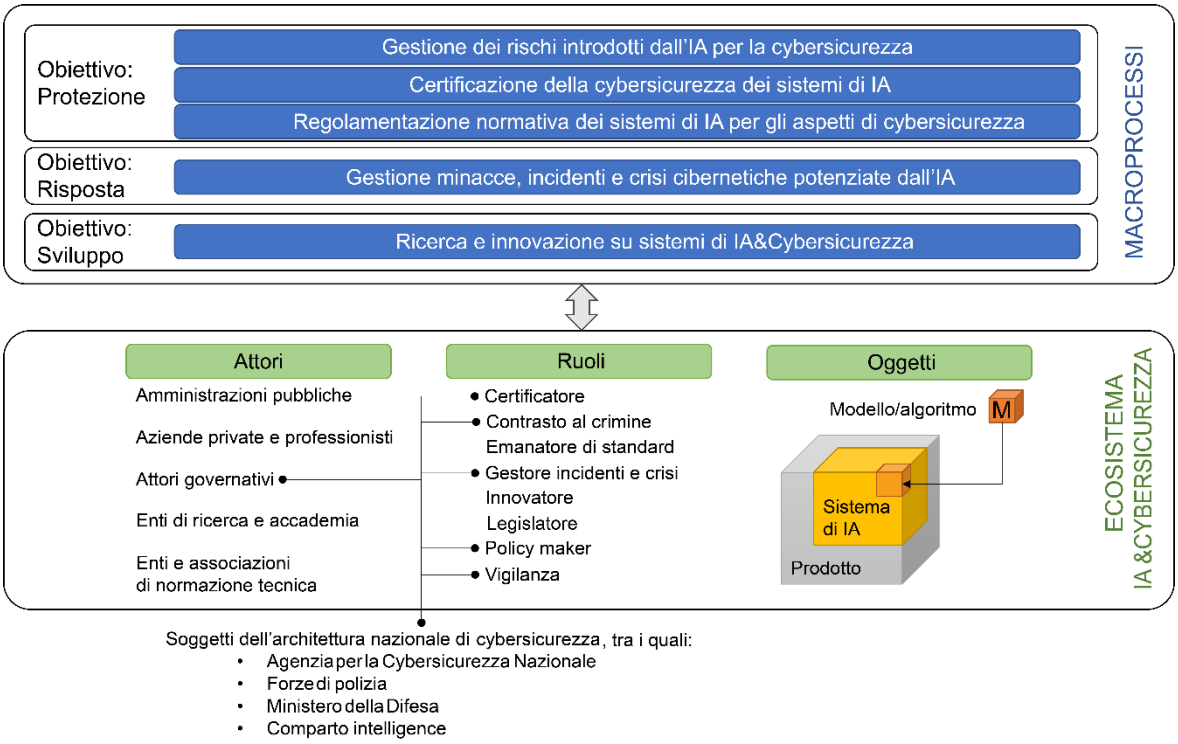


Figura 2

Rappresentazione dell'ecosistema dell'IA&Cybersicurezza con la specifica di tutti gli attori, ruoli e oggetti che è necessario considerare nell'ambito dei macro-processi di governo, dettagliati in Sezione 3. In particolare, la figura evidenzia attori e ruoli rivestiti dai soggetti dell'architettura nazionale di cybersicurezza.

2.2.1 Oggetti

Consideriamo i seguenti tre oggetti nell'ecosistema.

- Il modello di IA è il "cuore" dell'IA, una rappresentazione matematica o algoritmica progettata per svolgere compiti specifici. Un modello è caratterizzato da una determinata architettura (a titolo d'esempio una rete neurale), che permette tipicamente l'identificazione di una relazione causale tra determinate caratteristiche (*feature*) presenti nei dati su cui si lavora, per prendere decisioni, fare previsioni o eseguire altre attività intelligenti; ad esempio, un modello di riconoscimento facciale è progettato per identificare volti nelle immagini. In Sezione 3.1, ci concentreremo in particolare sui modelli cosiddetti di apprendimento automatico (*machine le*arning), ovvero quei modelli di IA che possono essere addestrati tipicamente su grandi quantità di dati per imparare a svolgere la loro funzione al meglio.
- Il sistema di IA è un insieme più ampio di componenti e moduli software e/o hardware, che realizzano una soluzione completa per un determinato scopo. Il sistema di IA può includere uno o più modelli di IA, ma anche interfacce utente, motori di ragionamento o database, eventualmente

integrando sistemi hardware, sensori e attuatori per l'interazione con l'ambiente fisico o digitale [5]. Ad esempio, un assistente vocale include un modello di riconoscimento vocale, ma anche componenti per l'elaborazione del linguaggio naturale e l'interazione con l'utente.

- Il **prodotto** è un'applicazione, un dispositivo o un servizio che integra un sistema di IA nell'ambito delle sue funzionalità. Può essere ad esempio una applicazione mobile, un robot domestico, o qualsiasi altra cosa che utilizzi l'IA per i propri scopi. Ad esempio, un prodotto di traduzione automatica può utilizzare un sistema di IA con modelli di apprendimento automatico per tradurre testi in diverse lingue.

Segue un esempio a scopo illustrativo degli oggetti introdotti.

Esempio di sistema basato su un modello di machine learning: guida autonoma

A bordo di alcuni veicoli di ultima generazione (prodotti) sono presenti sistemi di guida autonoma basati su modelli addestrati su enormi quantità di dati di guida (questi dati, in virtù del loro ruolo nell'apprendimento, vengono anche chiamati "esempi"), che contengono immagini, video e altre informazioni relative alla strada e agli oggetti che si possono incontrare durante il tragitto per consentire ai sistemi di guida autonoma di interpretare e reagire alle condizioni della strada in tempo reale.

Quando il veicolo si mette in movimento, il sistema di IA acquisisce costantemente dati dal suo ambiente circostante attraverso telecamere e sensori. Questi dati includono immagini della strada, degli ostacoli, degli altri veicoli e delle persone presenti. Il modello di apprendimento automatico utilizza queste immagini per riconoscere e distinguere gli oggetti rilevanti per prendere decisioni sulla guida del veicolo. Attraverso l'analisi di milioni di esempi precedenti, il modello ha imparato a identificare e classificare oggetti comuni come auto, pedoni, biciclette e segnali stradali. Ad esempio, se rileva un semaforo rosso, il modello determina che è necessario fermarsi e attendere il verde. Se riconosce un pedone che sta attraversando la strada, il sistema deve attuare manovre evasive o rallentare per garantire la sicurezza.

Il modello di IA può continuare ad aggiornare le sue conoscenze e a perfezionarsi man mano che incontra nuove situazioni sulla strada. Con l'esperienza e il continuo apprendimento dai dati, il sistema di guida autonoma diventa sempre più affidabile ed efficiente nel fornire un output sicuro e accurato a partire dai dati di input acquisiti.

2.2.2 Attori

A fronte dei molteplici macro-processi di governo dell'IA&Cybersicurezza, che saranno illustrati in dettaglio nella Sezione 3, i principali attori che operano per la loro realizzazione sono:

- **amministrazioni pubbliche**;
- **aziende private e professionisti**;

- attori governativi quali autorità, enti e agenzie che per competenza sono coinvolte in processi di promozione, valutazione, monitoraggio di attività di cybersicurezza e/o di IA, tra i quali, in Italia, figurano principalmente i soggetti i soggetti dell'architettura nazionale di cybersicurezza [9];
- enti di ricerca e accademia;
- enti internazionali (partecipati unicamente da enti di normazione nazionali) e associazioni (partecipate, oltre che da enti di normazione nazionali, anche da Governi e aziende private) di normazione tecnica/standardizzazione che sviluppano norme tecniche per i prodotti.

2.2.3 Ruoli

I principali ruoli che gli attori sopra elencati possono incarnare sono riportati a seguire:

- certificatore;
- contrasto al crimine;
- emanatore di standard;
- gestore di incidenti e crisi;
- innovatore;
- legislatore;
- policy maker;
- vigilanza.

Nella sezione successiva, chiariremo la relazione dei vari ruoli con i principali filoni operativi nell'ambito dell'architettura di sicurezza nazionale cibernetica.

3. Macro-processi di governo dell'IA&Cybersicurezza

In qualità di Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nello spazio cibernetico, secondo il D.L. 82/2021 [10], l'ACN ha il compito di garantire la sicurezza e la resilienza nello spazio cibernetico, occupandosi di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica. Come illustrato in Figura 2, a tal fine collabora con i soggetti dell'architettura nazionale di cybersicurezza che includono le Forze di Polizia, il Ministero della Difesa e il comparto intelligence.

L'IA rappresenta senza dubbio una tecnologia di cruciale importanza per la resilienza cibernetica del Paese, tuttavia, la strategia adottata da questa nel prendere decisioni, specialmente nel caso dei recenti modelli generativi del linguaggio, non è facilmente controllabile e potenzialmente dipende dallo scenario in cui l'IA è adottata, determinando potenziali rischi di sicurezza con possibili ripercussioni anche sull'incolumità fisica delle persone.

Pertanto, risulta di estrema importanza individuare un insieme di macro-processi di governo dell'IA&Cybersicurezza. Tali macro-processi sono riportati in Tabella 1 e descritti nel seguito raggruppati per i tre obiettivi di protezione, risposta e sviluppo della Strategia [9].

Tabella 1: macro-processi di governo dell'IA&Cybersicurezza.

Obiettivo	Macro-processo di governo	Ruoli
Protezione	Gestione dei rischi introdotti dall'IA per la cybersicurezza	• Certificatore • Contrasto al crimine • Emanatore di standard • Gestore incidenti e crisi
Protezione	Certificazione della cybersicurezza dei sistemi di IA	• Certificatore • Emanatore di standard • Vigilanza
Protezione	Regolamentazione normativa dei sistemi di IA per gli aspetti di cybersicurezza	• Legislatore • Policy maker • Vigilanza
Risposta	Gestione di minacce, incidenti e crisi cibernetiche potenziate dall'IA	• Contrasto al crimine • Gestore incidenti e crisi
Sviluppo	Ricerca e innovazione sui sistemi di IA&Cybersicurezza	• Policy maker • Innovatore

3.1 Gestione dei rischi introdotti dall'IA per la cybersicurezza

3.1.1 Come cambia lo scenario delle minacce per i sistemi basati su IA

L'analisi dei rischi di sicurezza cui sono esposti i sistemi parte tipicamente dall'identificazione dei loro componenti principali, e per ognuno di essi, delle proprietà di sicurezza che è necessario preservare, in modo da evitarne la compromissione a fronte di potenziali eventi dannosi.

Per quanto riguarda il governo dei rischi nel contesto specifico dei sistemi di IA, per la loro specifica natura e in ragione delle specifiche implicazioni etiche e impatti sulla società, il confine tra sicurezza e affidabilità (*trustworthiness*) è molto sottile, in quanto tipicamente quest'ultima garantisce che il comportamento dei tali sistemi possa essere controllato (*audited*) e verificato (*verified*) [5].

In Tabella 2 è riportato un elenco di proprietà che in base a quanto identificato nell'*Artificial Intelligence Risk Management Framework* (AI RMF) sviluppato dal *National Institute of Standards and Technology* (NIST) statunitense sono ritenute fondamentali nel progetto di sistemi di IA affidabili [11]. Tali proprietà, anche in relazione ai risvolti etici e sociali suesposti dei sistemi di IA, non sono solamente di natura puramente tecnica, ma anche socio-tecnica. La tabella mostra anche la relazione tra tali proprietà e i concetti espressi nell'*AI Act* [12].

Nel processo di analisi, valutazione e mitigazione dei rischi è importante adottare pertanto un approccio globale, che permetta di individuare eventuali compromessi tra proprietà tecniche e socio-tecniche per raggiungere un elevato grado di controllo del rischio pur mantenendo alto livello di qualità delle prestazioni. È opportuno sottolineare che tali proprietà sono infatti fortemente accoppiate, nel senso che vanno garantite in modo simultaneo: sistemi altamente sicuri ma iniqui, sistemi accurati ma opachi e non interpretabili, e sistemi imprecisi ma equi, sicuri e trasparenti sono tutti indesiderabili [11].

Nel seguito, ci concentreremo sulle caratteristiche tecniche e in particolare sulla proprietà di sicurezza e resilienza, con particolare riferimento alla sicurezza delle informazioni quali riservatezza (*confidentiality*), integrità (*integrity*) e disponibilità (*availability*) esaminandone le principali minacce che attengono allo specifico contesto dell'IA[5].

Nella prossima sezione illustreremo le minacce *cyber* ai modelli di machine learning, considerati i principali protagonisti di questa rivoluzione, presenti all'interno di una vastissima gamma di prodotti che permeano la nostra vita quotidiana. Questi modelli imparano ad associare ad un input un dato output sulla base di quanto appreso da un set di dati.

Tabella 2: elenco delle caratteristiche dei sistemi di IA affidabili (*trustworthy AI*) previste dall'AI RMF del NIST [11]. A destra, sono riportati i concetti riconducibili alle varie proprietà presenti nella proposta di Regolamento per l'IA (*AI Act*) secondo il NIST [12]. Le descrizioni delle proprietà sono un'elaborazione da [13].

Proprietà	Descrizione	Natura	*AI Act* (proposta)
Validità e affidabilità (*Validity and reliability*)	Capacità di mantenere un livello minimo di prestazioni e di generare in modo consistente i risultati previsti entro i limiti degli errori statistici accettabili.	Tecnica	**Robustezza** (*Robustness*); **Accuratezza** (*Accuracy*)
Sicurezza fisica (*Safety*)	Capacità di prevenire comportamenti non intenzionali o dannosi del sistema nei confronti di esseri umani o della società.	Tecnica	**Sicurezza fisica** (*Safety*)
Sicurezza e resilienza (*Security and resiliency*)	Per **sicurezza** si intende la capacità di prevenire deviazioni dalle condizioni di funzionamento previste quando si verificano eventi indesiderati; capacità di resistere agli attacchi; garanzia di confidenzialità, integrità e disponibilità, autenticità e non ripudiabilità delle informazioni e dei relativi dati, processi, servizi e dei modelli di IA. La **resilienza** rappresenta la capacità di ridurre al minimo l'impatto di un incidente, di mantenere condizioni di funzionamento sicure o essere in grado di ripristinarle in caso di attacco.	Tecnica	**Sicurezza** (*Security*); **Cybersicurezza** (*Cybersecurity*); **Resilienza** (*Resiliency*)

[5] Nell'analisi, saranno considerate esclusivamente le minacce intrinsecamente riconducibili a debolezze "*AI-specific*" del ciclo di vita dei prodotti di IA. Saranno pertanto escluse quelle minacce che attengono a vulnerabilità che possono essere in gran parte mitigate da una corretta gestione della cybersicurezza dell'architettura complessiva del prodotto, quali, ad esempio, la corretta validazione dell'input, la prevenzione della manomissione dell'input/output utilizzando misure a livello di hardware, sistema operativo e software, controllo degli accessi, così come la sicurezza delle librerie responsabili dell'implementazione dell'algoritmo di IA.

Equità e gestione dei bias (*Fairness and bias management*)	Per **equità** (*fairness*) si intende l'indipendenza da preferenze personali, emozioni o altre limitazioni introdotte dal contesto, uguaglianza (di genere e opportunità). L'equità può essere influenzata dalla presenza di distorsioni o **bias**.	Socio-tecnica	**Non discriminazione** (*Non-discrimination*)
Responsabilità e trasparenza (*Accountability and transparency*)	La **responsabilità** identifica la necessità di attribuire ad esseri umani e ad organizzazioni gli esiti dei sistemi di IA, in particolare in relazione agli impatti negativi derivanti dai rischi. La **trasparenza** riflette la misura in cui le informazioni su un sistema di IA e i suoi risultati sono rese disponibili agli individui che vi interagiscono. Consente anche a coloro che sono danneggiati da un sistema di IA di contestarne l'esito basandosi su informazioni chiare e comprensibili sui fattori e sulla logica che hanno costituito la base per la previsione, la raccomandazione o la decisione.	Socio-tecnica	**Responsabilità** (*Accountability*); **Trasparenza** (*Transparency*)
Spiegabilità e interpretabilità (*Explainability and intepretability*)	La **spiegabilità** ha l'obiettivo di fornire una rappresentazione dei meccanismi di funzionamento dei sistemi di IA. L'**interpretabilità** si riferisce alla comprensibilità del significato dell'output dei sistemi di IA nel contesto degli scopi funzionali per i quali sono stati progettati.	Socio-tecnica	**Spiegabilità** (*Explainability*); **Interpretabilità** (*Interpretability*)
Rispetto della privacy (*Privacy enhancement*)	Capacità di garantire una gestione sicura (intesa per gli aspetti di processamento, analisi, archiviazione, trasporto, comunicazione, diffusione) in relazione ai dati personali presenti nei sistemi di IA.	Socio-tecnica	**Misure di tutela della privacy** (*Privacy preserving measures*)

3.1.2 Principali attacchi *cyber* ai sistemi di IA

I principali elementi dei sistemi di IA oggetto di attacco sono il modello di IA e i dati utilizzati per il suo addestramento. Nel seguito esamineremo nel dettaglio i principali attacchi alla confidenzialità e all'integrità di questi.

Attacchi alla confidenzialità. Questo tipo di attacchi ha generalmente lo scopo di dedurre informazioni sensibili su modello o sui dati di addestramento. Esempi includono:

- *attacchi di appartenenza (membership)*. Tentano di determinare se un particolare dato (ad esempio appartenente ad una persona specifica) è stato utilizzato per addestrare uno specifico modello di IA, consentendo ad un attaccante di dedurre informazioni sensibili sui dati di addestramento e mettendo pertanto a rischio la privacy degli utenti;
- *estrazione e inversione del modello (model extraction and inversion)*. Si concentrano sull'estrazione o il recupero del modello di IA stesso. Tali attacchi possono essere perpetrati direttamente (estrazione) o indirettamente (inversione, cioè tramite tecniche c.d. di *reverse engineering*), ovvero cercando di ottenere informazioni sul modello addestrato (quali ad esempio la sua architettura), ad esempio mediante l'analisi delle risposte del modello alle richieste di input. Tra le tipologie di attaccanti figurano tipicamente i concorrenti sleali sul mercato.

Attacchi all'integrità. Questo tipo di attacchi hanno lo scopo di ingannare o eludere il funzionamento dei sistemi di IA durante la fase di addestramento o di inferenza al fine di influenzarne le previsioni o indurre comportamenti non desiderati o addirittura pericolosi quando il modello viene utilizzato in produzione, come ad esempio far riconoscere come sicuri oggetti pericolosi o far rifiutare oggetti innocui.

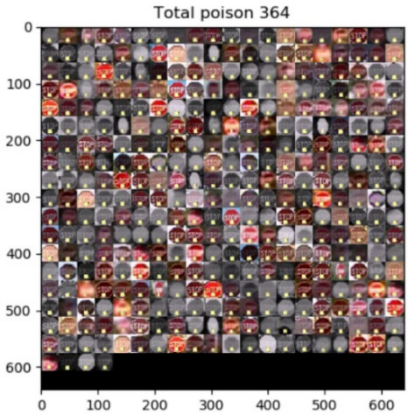
Questi possono essere suddivisi nelle due seguenti principali categorie:

- *attacchi ad "avvelenamento" (poisoning).* Gli attacchi all'avvelenamento dei dati (*data poisoning*) consistono nell'immettere dati malevoli o manipolati nel set di addestramento di un modello di IA per introdurre *bias* (ovvero, capacità discriminative indesiderate) o influenzarne le decisioni. Una sottocategoria di questi attacchi (detti a "*backdoor*") sfrutta l'inserimento malizioso di dati nel set di addestramento, che però contengono al loro interno delle specifiche "esche" (*trigger*), ovvero porzioni di dati che il modello, a valle dell'addestramento, impara a riconoscere e associare ad un determinato output deciso dall'attaccante. Si noti che rispetto al caso generale, questa particolare sottocategoria fornisce all'attaccante la "chiave" per determinare una specifica decisione, mostrando dati che contengono "l'esca" al modello. L'esempio in Figura 3 mostra l'utilizzo di un trigger nel dominio del riconoscimento di immagini, in cui i trigger hanno la forma di piccole trame (*pattern*) o proiezioni difficili da vedere: nello specifico, un semplice *post-it* posizionato sui segnali stradali può influenzare un sistema di riconoscimento dei segnali a riconoscere un segnale di "stop" come un segnale di limite di velocità, portando un eventuale veicolo a guida autonoma con a bordo tale sistema di riconoscimento a non rispettare lo "stop" ed eventualmente mettere a repentaglio la sicurezza fisica dei pedoni. Recenti studi dimostrano la fattibilità di attacchi di *data poisoning* a dataset di grandi dimensioni, come ad esempio Wikipedia, che possono essere utilizzati per il *training* di LLM [14].

Altri attacchi tentano di "avvelenare" direttamente il modello (*model poisoning*) a valle dell'addestramento per inserire funzionalità dannose [15];

- *Attacchi a elusione (evasion).* Contrariamente alla precedente, questa categoria non mira a compromettere l'integrità del modello o dei dati di addestramento, ma, piuttosto, del processo di inferenza. Questi attacchi, infatti, sfruttano le vulnerabilità dei modelli di IA ai cosiddetti esempi "avversari" *(adversarial examples*), ovvero input appositamente progettati per ingannare il modello e indurlo a commettere errori.

(a) Il modello di riconoscimento di segnali stradali in [16], addestrato su un set di addestramento "avvelenato", ha riconosciuto il cartello in figura come segnale di "limite di velocità" invece che di "stop", a causa del bigliettino posizionato nella parte sottostante. Il numero visualizzato mostra la confidenza del modello nella specifica (errata) classificazione (probabilità prossima ad 1).



(b) L'insieme delle backdoor (segnali di "stop" modificati e contenenti quadratini gialli nella porzione bassa dell'immagine) inseriti nel set di addestramento del modello di cui alla Figura 3a e categorizzati come "limiti di velocità". Immagine tratta da [17].

Figura 3
Esempio di uso di un trigger per alterare la decisione di un modello di IA.

Attacchi alla disponibilità. In questo tipo di attacchi l'attaccante tenta di deteriorare le prestazioni del sistema di IA. Alcune delle tipologie di attacchi menzionate nelle precedenti categorie relative a confidenzialità e integrità possono essere istanziate anche allo scopo di ridurre l'accuratezza del sistema (di fatto, controllando una frazione del set di addestramento del modello mediante data *poisoning*, riducendo l'efficacia del processo di apprendimento o, alterando in modo artificioso i parametri del modello mediante model *poisoning*) [18]. Alcuni studi dimostrano inoltre la fattibilità di attacchi basati sulla creazione di input ad arte per massimizzare il consumo di energia e la latenza dei modelli, causando un degrado di prestazioni [19].

Gli attacchi su menzionati sono applicabili ad ampio spettro sulla tassonomia generale dei sistemi di IA, tuttavia, alcuni sistemi di IA basati sui modelli generativi sono particolare soggetti a possibili manipolazioni dei cosiddetti *prompt*, ovvero specifiche (tipicamente testuali e a cura dell'utente stesso, o di un fornitore del servizio) del compito che il sistema deve compiere e di come il sistema stesso deve gestire l'interazione con l'utente. Questo può comportare la compromissione di tutte le citate proprietà di sicurezza [18]. In particolare, ad esempio, tali *prompt* possono essere alterati da parte di attaccanti (*prompt injection*), allo scopo di manipolare il comportamento del sistema, inserendo istruzioni dannose o ambigue, oppure estratti (*prompt extraction*) allo scopo di derivare informazioni sul funzionamento del sistema.

Per mitigare i rischi di questo tipo di attacchi, è necessario stabilire processi e procedure di *security-by-design* in ogni fase dello sviluppo dei sistemi, dalla scelta dell'architettura dei modelli, alla progettazione delle procedure di apprendimento, all'implementazione e al test e in particolare nella fase di messa in opera finale del sistema.

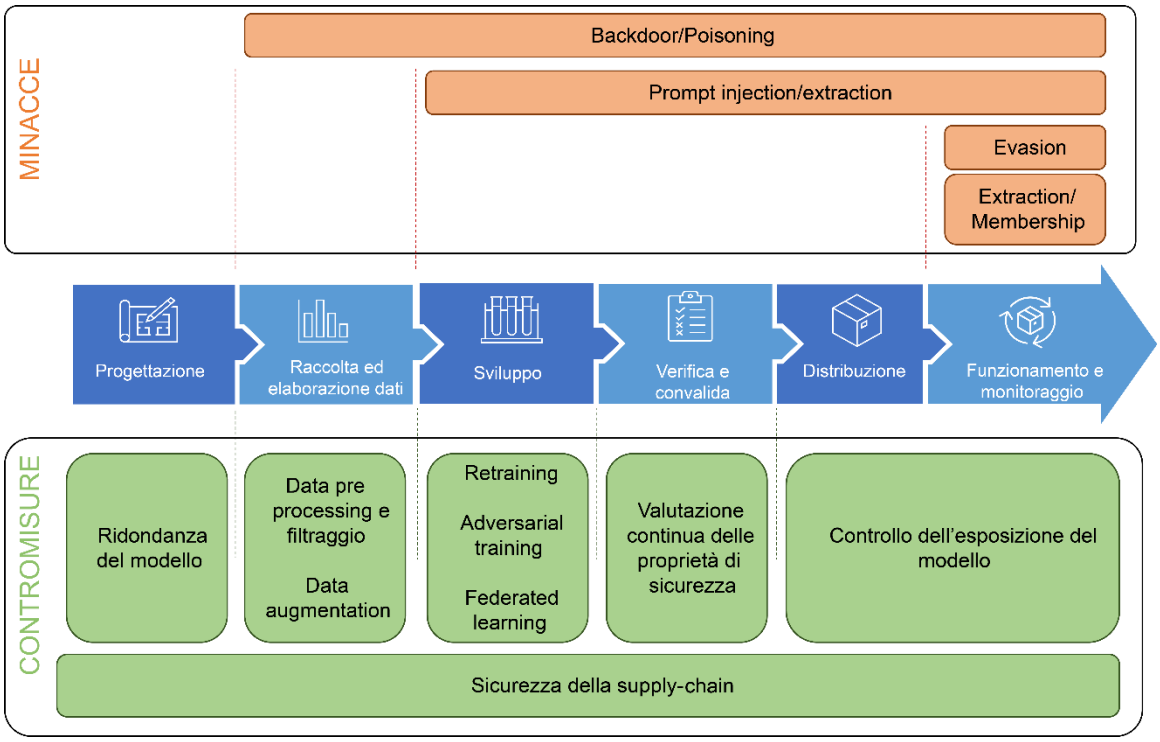


Figura 4
Corrispondenza tra le fasi del ciclo di vita dei sistemi di IA, minacce e contromisure [20] [11].

In Figura 4 è rappresentata una schematizzazione (in blu), secondo la definizione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) [20], delle principali fasi del ciclo di vita di un sistema di IA: 1) progettazione, 2) raccolta ed elaborazione dei dati, 3) sviluppo del modello, 4) verifica e convalida,

5) distribuzione (*deployment*); 6) funzionamento e monitoraggio. In relazione alle fasi, è possibile ricondurre il processo di apprendimento alla fase 2) per il suo progetto e alla fase 3) per l'apprendimento effettivo; il processo di inferenza avviene invece nella fase finale (fase 6). Per ogni fase la figura evidenzia (in rosso) le minacce precedentemente identificate e (in verde) un elenco sintetico delle principali contromisure di natura tecnica e organizzativa per la mitigazione dei relativi impatti di sicurezza. Queste ultime sono in particolare approfondite nella prossima sezione.

3.1.3 Contromisure per i rischi *cyber* specifici dell'IA

Gli attacchi alla confidenzialità dei dati di apprendimento dei modelli possono essere mitigati tramite tecniche quali l'apprendimento federato (*federated-learning*), ovvero tecniche in cui il processo di apprendimento è effettuato in modo decentralizzato riducendo al minimo l'impatto di eventuali violazioni di dati (*data breach*). Inoltre, ridurre la tipologia e il numero di informazioni [21] che vengono fornite nella produzione degli output del modello di IA può aiutare a incrementare lo sforzo necessario per un attaccante a perpetrare tali attacchi.

In relazione agli attacchi all'integrità tramite avvelenamento, l'insieme di dati di addestramento dovrebbe essere ampliato il più possibile tramite metodologie apposite (c.d. di *data augmentation* [6] [21]) per ridurne la suscettibilità all'inserimento di dati manipolati (di fatto, irrobustendo il modello sfruttando un effetto di "diluizione"). Similmente, approcci di riapprendimento (*retraining*) reiterati nel tempo con dati di addestramento benigni riducono la probabilità dell'efficacia delle *backdoor* [22] [23]. Questi approcci possono essere rafforzati da strategie di pre-elaborazione (*pre-processing*) che tentano di ripulire i dati di addestramento dai dati avvelenati[7] (in particolare quest'ultima strategia è l'unica efficace per mitigare gli attacchi di tipo backdoor [24] [23]).

Per contrastare gli attacchi all'integrità di tipo elusione, è possibile implementare strumenti per rilevare se un dato input è un esempio avversario. Inoltre, l'addestramento avversario (*adversarial training*), consiste nel generare in modo iterativo esempi contraddittori inserendoli nel set di addestramento e addestrare ripetutamente il modello su di essi, con l'obiettivo di aumentarne la robustezza e significativamente ridurre la capacità di un dato aggressore di studiare correttamente il modello sottostante e creare esempi avversari efficaci.

---

[6] Che ne preservino le caratteristiche di rappresentatività desiderate, e in particolare non introducano *bias*.

[7] Come su esposto, i trigger utilizzati per le backdoor si basano su scorciatoie logiche all'interno del modello tra la previsione di output desiderata dall'attaccante (nell'esempio in Figura 3, la previsione limite di velocità) e l'input. Per trovare una scorciatoia, è necessario determinare, per ogni elemento del set di addestramento quale è la minima modifica da applicare per spostare sostanzialmente la previsione del modello. Se tale modifica è effettivamente di lievissima entità, si potrebbe essere in presenza di una *backdoor* [21]. Un metodo nel dominio del riconoscimento di immagini consiste nel mascherare in modo casuale parti di un'immagine di input ed esaminare come cambia la previsione del modello. Se l'immagine di input contiene un *trigger*, il mascheramento cambierà la previsione del modello [21].

In aggiunta a quanto descritto, vi sono una serie di ulteriori contromisure utili per ridurre ulteriormente la superficie di attacco dei sistemi di IA:

- controllo dell'esposizione esterna dei modello. Devono essere implementati processi che minimizzano l'esposizione all'esterno delle caratteristiche interne del modello di IA, in quanto queste possono permettere all'attaccante di realizzare attacchi più efficaci. In particolare, nel caso del riconoscimento di immagini, con informazioni puntuali sul modello [8], l'attaccante può essere in grado di conoscere la migliore perturbazione da aggiungere ad un'immagine per indurre uno specifico errore di decisione;
- ridondanza del modello. In fase di progetto, la ridondanza implica la creazione di più modelli che presentano variazioni nei loro approcci o dati di addestramento e che vengono combinati insieme (*model ensemble* o *bagging*) per prendere decisioni[9]. Questa combinazione riduce la dipendenza da un singolo modello, per cui un eventuale attacco diventa meno efficace poiché gli altri modelli possono essere utilizzati per rilevare e mitigare il problema;
- valutazione continua delle proprietà di sicurezza. Essendo l'IA in continua evoluzione è necessario istruire processi che mantengono i livelli di sicurezza dei componenti nel tempo. Il controllo regolare della presenza di nuovi attacchi e difese deve essere integrato nei processi, e in generale, per via del mutamento continuo di questi sistemi e per via del loro apprendimento continuo dai dati, è opportuno identificare e valutare controlli di sicurezza che possano applicarsi in modo continuo;
- sicurezza della *supply chain* e controllo nel riuso di modelli e dati. È prassi comune basare il progetto di sistemi di IA su modelli di IA progettati o addestrati da terze parti[10] e resi disponibili pubblicamente[11]. Per addestrare il modello, è spesso necessario che il fornitore acceda ai dati. Ciò comporta la condivisione dei dati potenzialmente sensibili con una terza parte. In questi scenari, attori malevoli potrebbero essere in grado di alterare il comportamento del modello, manipolandolo o manipolando i dati utilizzati per addestrarlo. In generale, a seconda dei requisiti di sicurezza per il caso d'uso, è essenziale compiere sforzi adeguati a garantire che la catena di approvvigionamento [25] e le fonti dei dati di addestramento, dei modelli e degli algoritmi di addestramento siano note e affidabili.

In definitiva, garantire il rispetto dell'affidabilità e la sicurezza di questi sistemi, e quindi lo sviluppo di *framework* per la loro certificazione e valutazione (oggetto di trattazione nella Sezione 3.2) è particolarmente complesso. Evidenziamo come le

[8] In particolare, conoscendone la funzione di minimizzazione dell'errore (*loss function*).
[9] Ad esempio, utilizzando un meccanismo di "votazione" per scegliere come output la decisione adottata dalla maggioranza dei modelli.
[10] Spesso, inoltre, modelli e dati sono mantenuti da operatori diversi.
[11] Messi a disposizione, ad esempio, nell'ambito di servizi cloud.

capacità di apprendimento automatico sono un ulteriore fattore di difficoltà poiché queste determinano una sistemica evoluzione temporale, la cui principale conseguenza è il fatto che le proprietà di sicurezza possono degradarsi e che non tutti i risultati attesi sono noti a priori.

3.2 Certificazione della cybersicurezza dei sistemi di IA

Il mandato del macro-processo di certificazione della cybersicurezza dei sistemi di IA è da ricondursi alla legislazione vigente (si veda in proposito la Sezione 3.3), alquanto articolata nell'impianto dato dall'UE e in evoluzione al momento in cui scriviamo. Nell'ottica di massimizzare efficacia ed efficienza di un nuovo schema di certificazione in materia di IA, l'ENISA ne sta studiando gli obiettivi e le potenziali sinergie con altri schemi di certificazione in corso di definizione[12] e, al tempo stesso, raccomanda agli Stati Membri di prestare attenzione all'armonizzazione delle competenze tra gli attori governativi nella fase di recepimento a livello nazionale dei regolamenti comunitari da parte del legislatore [26].

Il macro-processo di certificazione contribuisce all'obiettivo di protezione tramite accurate verifiche del livello di conformità di un prodotto basato sull'IA rispetto ai vincoli imposti dal legislatore e alle norme tecniche stabilite dagli enti di normazione. Similmente a quanto già accade con altri prodotti di ICT non basati su IA[13], le aziende sottoporranno i propri prodotti che integrano sistemi di IA ad un *audit* condotto da parte di attori governativi, amministrazioni pubbliche o aziende private precedentemente accreditate dalle autorità (quali, ad esempio, laboratori di prova o valutazione[14]). Tale *audit* è finalizzato al rilascio di un certificato di conformità, un "bollino di qualità" del prodotto, la cui validità è limitata nel tempo o dalla legge stessa o in conseguenza di sostanziali modifiche ed evoluzioni del prodotto. Lo scopo finale di questo macro-processo è la protezione degli asset, ma anche quello di ingenerare fiducia (*trust*) nelle persone e nelle aziende che andranno ad utilizzare prodotti e sistemi basati su IA: mentre i primi mirano alla tutela dei propri diritti fondamentali digitali, le seconde sono interessate alla sicurezza dei prodotti e della propria catena di approvvigionamento (*supply chain*)[15] [25].

Il "mezzo" tramite il quale i requisiti legislativi sono codificati in specifiche tecniche fondamentali per guidare lo sviluppo di sistemi e prodotti di IA da parte delle aziende sono le norme tecniche, in inglese *standard*, emanati dagli enti di

[12] Si veda la pagina https://certification.enisa.europa.eu/. ENISA sta elaborando tre schemi di certificazione per prodotti ICT, servizi *cloud* e reti 5G (denominati EUCC, EUCS e EU5G, rispettivamente).
[13] Ad esempio, apparati elettronici e di telecomunicazioni.
[14] Per maggiori dettagli in materia si veda https://www.acn.gov.it/agenzia/organizzazione/cvcn.
[15] Sia in ottica di ottimizzazione di processi e procedure interne che allo scopo di sviluppare nuove soluzioni che incorporano prodotti basati su IA di terze parti. Ad esempio, una casa automobilistica potrebbe essere interessata ad integrare nell'auto un sistema di IA di terze parti funzionale all'implementazione di un sistema di guida autonoma.

normazione. In vari domini, gli standard documentano le caratteristiche che i prodotti devono possedere al fine di promuoverne l'interoperabilità e migliorarne la sicurezza, abilitando economie di scala e incoraggiando la concorrenza. Nel caso specifico dell'IA, oltre agli standard tradizionali ereditati dal dominio della cybersicurezza[16], è necessario sviluppare norme tecniche ad hoc per i prodotti basati sull'IA in base ai requisiti imposti dalla legge. Al momento, i principali enti di normazione impegnati nel campo dell'IA&Cybersicurezza sono i seguenti [13] [26]:

- a livello internazionale globale, l'*International Organization for Standardization* (ISO) e l'*International Electrotechnical Commission* (IEC). I due enti stanno attivamente collaborando in un *Joint Technical Committee* (JTC) 1/*Subcommittee* (SP) 42[17] dedicato all'IA in cui vengono prodotte norme tecniche generali[18], da verticalizzare in altri comitati;
- a livello continentale europeo, il Comitato Europeo di Normazione (CEN) e il Comitato Europeo di Normazione Elettrotecnica (CENELEC), i quali stanno trattando congiuntamente il tema dell'IA nella JTC 21. In particolare, tale comitato si occupa anzitutto di identificare e adottare standard internazionali già pubblicati, come quelli al punto precedente, quindi di sviluppare norme tecniche specifiche per la società e il mercato europei secondo le richieste del legislatore (ad esempio, in merito all'attuazione dell'*AI Act* – si veda la Sezione 3.3).

Tra le associazioni di standardizzazione, invece, segnaliamo la *Technical Committee* (TC) denominata "*Securing Artificial Intelligence*" (SAI) dell'Istituto Europeo per le norme di Telecomunicazioni (*European Telecommunications Standards Institute*, ETSI). Il comitato si concentra su tutte e tre le direzioni della relazione tra IA e cybersicurezza che abbiamo menzionato all'inizio di Sezione 2, ovvero la messa in sicurezza dell'IA, l'utilizzo dell'IA per scopi di difesa e la mitigazione di attacchi effettuati da *counter-AI*.

A proposito di tali iniziative di standardizzazione, però, è interessante notare come i rapidissimi cicli di innovazione in materia di IA e il quadro legislativo in continua evoluzione non si adattino alle tempistiche, tradizionalmente medio-lunghe sulla base del meccanismo del consenso, della redazione di una norma tecnica[19]. Inoltre, le norme tecniche, in un momento di grande spunto per l'impresa, non devono essere eccessivamente prescrittive, andando a cercare piuttosto sinergie con le aziende e i legislatori stessi basato su sforzi di ricerca,

[16] Ad esempio, [40], [41] e [42].
[17] Si veda https://www.iso.org/committee/6794475.html.
[18] Al momento della scrittura di questo articolo, ventidue standard sono stati pubblicati. Si veda https://www.iso.org/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0.
[19] A questo riguardo, l'attività di iniziative no-profit a carattere di *community* quali, a titolo d'esempio, l'*Open Web Application Security Project* (OWASP), si presta ad essere più agile nello stare al passo con l'innovazione industriale, come testimoniato dal recente rapporto sulle principali dieci vulnerabilità dei LLM [47]. Pur non avendo l'autorevolezza di veri e propri enti o associazioni di standardizzazione, tali iniziative potrebbero essere di supporto per l'attività di questi ultimi.

innovazione e sviluppo con i quali rendere lo standard "usabile", ovvero implementabile in pratica e aggiornato dal punto di vista tecnologico. In definitiva, secondo l'ENISA stessa [13], sono necessari ulteriori sforzi di ricerca per valutare la sicurezza dei sistemi di IA, al fine di definire delle metodologie condivise ed oggettive da riportare negli standard.

3.3 Regolamentazione normativa dei sistemi di IA per gli aspetti di cybersicurezza

Dal punto di vista normativo, l'UE sta portando avanti tre principali iniziative inerenti l'IA e la cybersicurezza che, una volta approvate, dovranno essere recepite a livello dei singoli Stati Membri.

- Anzitutto, sta giungendo all'approvazione finale l'*AI Act*[20], un articolato regolamento comunitario[21] finalizzato a normare l'immissione sul mercato di prodotti basati su IA per mezzo di una classificazione basata sul rischio di creare danno agli esseri umani. In particolare, tale classificazione identifica una categoria di utilizzi dell'IA a rischio inaccettabile (e pertanto vietati), e una categoria di sistemi ad alto rischio, prescrivendo, per i produttori e gli utilizzatori di questi, alcuni requisiti generali di conformità, che includono aspetti di gestione del rischio, accuratezza, robustezza e cybersicurezza. Nell'ottica dell'attuazione del regolamento, la Commissione Europea ha effettuato richieste di normazione tecnica (*standardization request* – SR) [27] a CEN-CENELEC [22] per colmare il *gap* esistente nel panorama della standardizzazione internazionale – come visto nella Sezione 3.2.
- Inoltre, per quanto attiene gli specifici aspetti di cybersicurezza, il *Cyber Resilience Act*[23] (CRA), che adotta un'impostazione basata sul rischio come l'*AI Act*, stabilirà requisiti e metodologie orizzontali di garanzia della cybersicurezza per produttori e fornitori di prodotti digitali e di servizi accessori inclusi quelli basati su IA. Un elemento chiave della proposta è la copertura dell'intero ciclo di vita dei prodotti, con la specifica istituzione di obblighi per produttori e sviluppatori al fine di definire un periodo di supporto, durante il quale verranno forniti obbligatoriamente tutti gli aggiornamenti di sicurezza. Tali obblighi saranno stabiliti per gli operatori economici (produttori, distributori e importatori) in relazione all'introduzione sul mercato di prodotti con elementi digitali, sulla base delle specifiche responsabilità nella catena di approvvigionamento.

[20] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
[21] L'impianto regolamentare prevede sinergie sia con il *Cyber Resilience Act* che con diverse normative settoriali, ad esempio, su trasporti e aviazione.
[22] Negli artt. 1 e 2 della richiesta è fatta esplicita indicazione di tenere anche nella opportuna considerazione il lavoro svolto dall'ETSI in materia.
[23] Attualmente in fase di Proposta. Si veda https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

- Parallelamente ai precedenti, lo *European Chips Act*[24] mira a definire requisiti di cybersicurezza *by-design* per la progettazione di circuiti basati su semiconduttori, fondamentali per l'IA sia per quanto riguarda le architetture di calcolo (ad esempio, le infrastrutture di calcolo ad elevate prestazioni – *high performance computing*, HPC – utilizzate per l'addestramento dei modelli di *machine learning* più complessi), sia per quanto riguarda i sistemi integrati (*embedded*), che hanno a bordo modelli di inferenza basati su IA (ad esempio, alcuni *chip* per il riconoscimento biometrico che rientrano nelle previsioni dei sistemi ad alto rischio individuati dall'*AI Act*).

Globalmente è possibile osservare tre principali approcci esistenti, alla data di scrittura del presente articolo, alla regolazione dell'IA. Se da un lato l'UE, come sopra riportato, ha elaborato proposte specifiche che riflettono una visione precauzionale e orientata ai diritti degli utilizzatori, l'approccio anglosassone (USA e Regno Unito) si distingue per un orientamento che, pur contemperando le preoccupazioni etiche e di sicurezza, eviti vincoli eccessivi che potrebbero ostacolare la crescita dell'economia digitale e l'innovazione tecnologica, anche attraverso l'incoraggiamento della collaborazione pubblico-privata per lo sviluppo di norme e linee guida che forniscano un quadro chiaro in cui l'industria può operare[25]. La Cina ha destinato considerevoli risorse e investimenti nella direzione di diventare leader mondiale nell'IA, ponendo tuttavia, anche in ragione delle specificità politiche, culturali ed economiche, particolare enfasi sulla garanzia che la tecnologia sia allineata con gli obiettivi strategici del paese [28], anche per le finalità di sicurezza nazionale, con un approccio più mirato alla normazione tecnica di tipologie specifiche di IA, come i sistemi di raccomandazione e, più recentemente, per gli algoritmi generativi [29].

Nel mondo e anche in Italia, le grandi aziende tecnologiche manifestano in sempre più occasioni l'intenzione di unire gli sforzi per promuovere proattivamente lo sviluppo responsabile di modelli, sistemi e prodotti di IA, minimizzando i rischi e condividendo informazioni con la società civile e i *policy maker*[26]. In quest'ottica, l'attenzione degli attori governativi italiani è alta nel tentativo di ridurre le barriere allo sviluppo e al raggiungimento di una autonomia tecnologica, anche attraverso il confronto con le aziende nel processo di attuazione della regolamentazione normativa. Un primo esempio di tali sinergie è costituito dalla stesura delle linee guida per lo sviluppo sicuro dell'IA [30], promosse dal *National Cyber Security Centre* (NCSC) del Regno Unito e dalla *Cybersecurity and Infrastructure Agency* (CISA) degli USA e cui hanno aderito 23

[24] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0046.
[25] Un esempio è l'istituzione dell'*Artificial Intelligence Safety Institute* (USAISI) istituito presso il NIST e del relativo consorzio, che prevede la collaborazione di enti pubblici, privati e accademia, per la creazione collaborativa di tecniche e metriche comprovate, scalabili e interoperabili per guidare gli sforzi del governo USA nella promozione, lo sviluppo e l'uso responsabile di un'intelligenza artificiale sicura e affidabile.
[26] Si veda https://openai.com/blog/frontier-model-forum.

Agenzie di 18 Paesi, tra cui l'ACN italiana, e realizzate anche grazie al contributo di diversi soggetti privati.

3.4 Gestione di minacce, incidenti e crisi cibernetiche potenziate dall'IA

Come evidenziato in [31], i recenti sviluppi dell'IA, in particolare sul fronte dell'IA generativa, hanno portato ad un fondamentale cambio di paradigma nelle metodologie necessarie ad assicurare la sicurezza cibernetica. In particolare, tale cambio si sostanzia in alcuni elementi specifici che includono:

- diminuzione dell'efficacia degli aggiornamenti del software, che, con il paradigma tradizionale, sono invece tra le principali misure di difesa da attacchi *cyber*. Infatti, la velocità con cui attacchi basati su IA possono essere realizzati e condotti si scontra con la lentezza che invece attualmente caratterizza le strategie di aggiornamento dei sistemi, determinando una sproporzione in favore degli attacchi;
- necessità di meccanismi di risposta con gradi di automazione maggiore, determinata anch'essa dalla velocità delle nuove tipologie di attacco basate su IA, oltre che dalla elevata scala che tali attacchi possono assumere;
- maggiore vulnerabilità degli esseri umani, che possono essere oggetto di attacchi più sofisticati e mirati a causa dell'impiego di sistemi di IA generativa. Si pensi ad esempio ad e-mail di phishing personalizzate o a messaggi vocali manipolati che riescano a riprodurre fedelmente le voci di amici o colleghi;
- sovranità digitale, ed in particolare la dipendenza dell'UE da modelli di IA generativa sviluppati al di fuori dell'Europa, e con principi etici che possono essere fondamentalmente diversi, così determinando problemi di allineamento culturale.

Pertanto, si rende necessario ridefinire i processi di gestione delle minacce, degli incidenti e delle crisi cibernetiche potenziate dall'IA di modo da includere nuovi insiemi di misure da attuare per proteggersi dalla minaccia, e nuovi processi che ridefiniscano i comportamenti che gli esseri umani devono tenere in scenari di difesa in cui è enormemente cresciuta la complessità delle interazioni tra agenti umani e artificiali.

3.5 Ricerca e innovazione sui sistemi di IA&Cybersicurezza

L'ultimo macro-processo si occupa di gestire le molteplici sfide poste dalle varie connotazioni di IA&Cybersicurezza, oltre che dagli altri macro-processi precedentemente descritti, e che attualmente sono ancora sulla frontiera di ricerca.

A livello europeo, l'ENISA ha pubblicato diversi studi e documenti di indirizzo su temi di cybersicurezza e IA. In particolare, [32] è stato recepito come indirizzo per l'Agenda di Ricerca e Innovazione di ACN. Più recentemente, [5] individua alcuni *gap* di ricerca e innovazione in IA&Cybersicurezza, che includono:

- necessità di *testbed*, per studiare e ottimizzare metodi e tecnologie;

- sviluppo di strumenti di *penetration test* basati su IA e *machine learning* per trovare vulnerabilità e valutare il comportamento degli attaccanti;
- sviluppo di framework standard;
- sviluppo di modelli di training per professionisti che utilizzino scenari realistici;
- istituzione di un osservatorio per l'intelligenza artificiale e le minacce alla cybersicurezza.

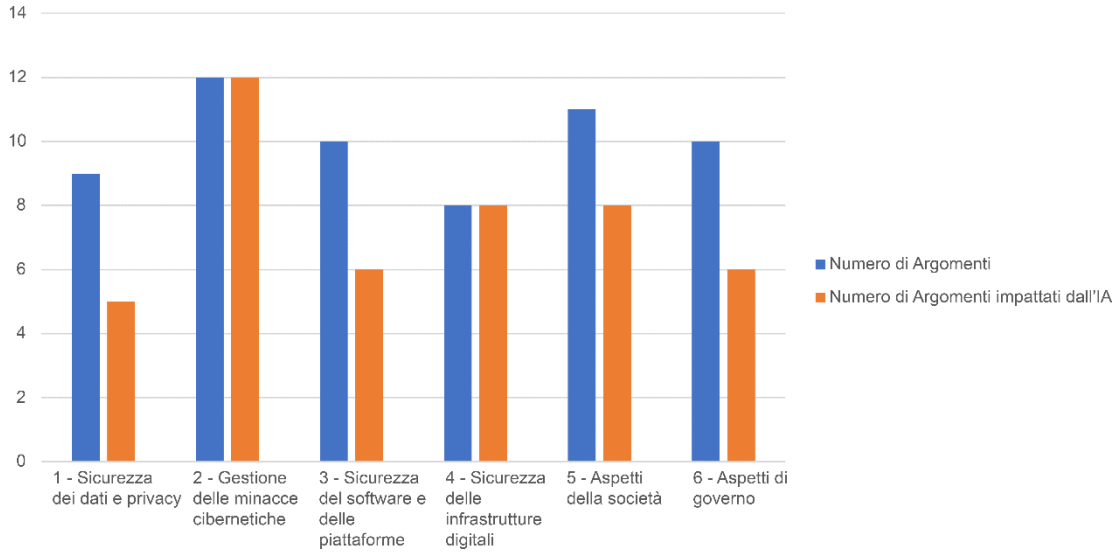
Dal punto di vista dei finanziamenti sui temi relativi all'IA&Cybersicurezza possiamo citare i programmi *Horizon Europe* (in particolare, il Cluster 3 – "*Civil Security for Society*", con 1,6 miliardi di euro) e *Digital Europe*, quest'ultimo con 1,6 miliardi di euro destinati alla cybersecurity e 2 miliardi di euro a Cloud, Data e IA.

A livello nazionale, sono stati già avviati importanti programmi di finanziamento che hanno dato luogo a numerosi investimenti in corso, tra cui citiamo i finanziamenti del Piano Nazionale di Ripresa e Resilienza (PNRR) per la costituzione dei partenariati estesi SERICS – "*SEcurity and RIghts in CyberSpace*" e FAIR – "*Future Artificial Intelligence Research*".

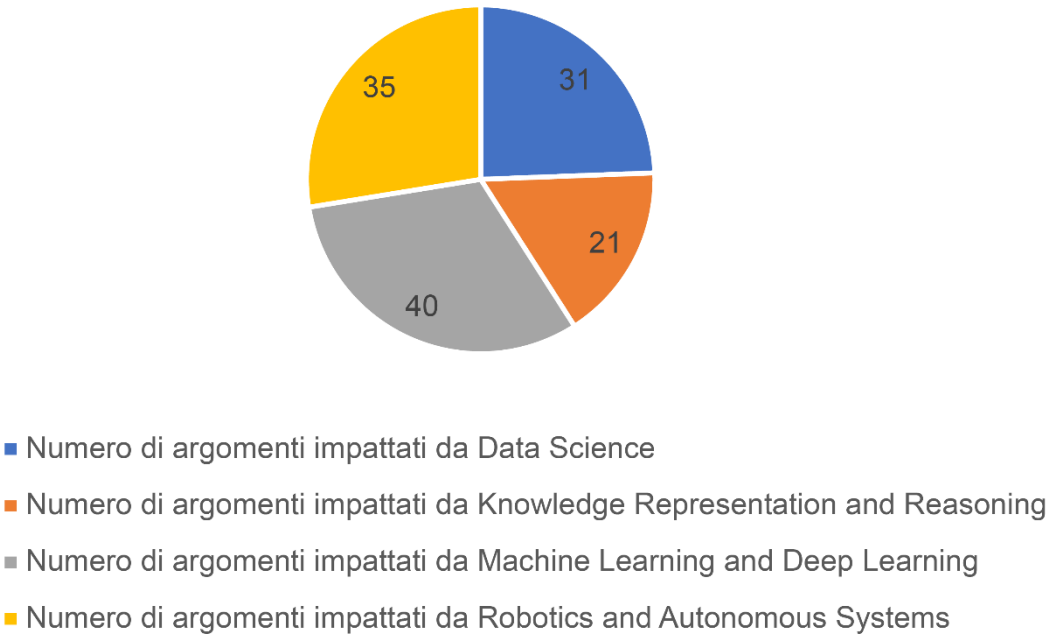
L'ACN, in collaborazione con il Ministero dell'Università e della Ricerca, ha pubblicato un'Agenda di Ricerca e Innovazione per la Cybersicurezza [7] basata su rilevanti riferimenti sia nazionali che internazionali, al fine di promuovere e valorizzare i prodotti di ricerca di cybersicurezza sia in ambito pubblico sia in quello privato. L'Agenda identifica 6 aree nel dominio di conoscenza della cybersicurezza, 18 subaree e 60 argomenti di ricerca prioritari afferenti alle diverse subaree. Individua inoltre un insieme di *Emerging and Disruptive Technology* (EDT) che supportano o vincolano gli argomenti di ricerca dell'Agenda.

L'IA è identificabile come una combinazione di quattro di esse: *data science*, rappresentazione della conoscenza (*knowledge representation and reasoning*), machine learning e deep learning, robotica e sistemi autonomi (*robotics and autonomous systems*) [7].

Come riportato in Figura 5, l'IA in generale ha un forte impatto su tutte le aree individuate dall'Agenda (vedasi grafico in Figura 5a). Inoltre, andando a considerare le singole EDT costituenti l'IA, si può apprezzare come il contributo allo studio degli argomenti prioritari dell'Agenda è sostanzialmente equidistribuito tra di esse, con una lieve predominanza dell'EDT *machine learning and deep learning*. Possiamo, quindi, affermare che ciascuna EDT ha un impatto rilevante sulla ricerca e l'innovazione per la cybersicurezza (vedasi grafico in Figura 5b).



(a) Impatto dell'IA sulle diverse aree di ricerca e innovazione individuate dall'Agenda.



(b) Contributo delle singole EDT costituenti l'IA allo studio degli argomenti dell'Agenda.

Figura 5
Relazioni tra l'IA e gli argomenti di ricerca dell'Agenda.

Focalizzandosi, invece, sulle subaree individuate dall'Agenda, ben 14 su 18 di esse sono direttamente impattate da almeno una delle quattro EDT costituenti l'IA.

In particolare, dalla Figura 6 è possibile apprezzare le 14 subaree in ordine di impatto decrescente, sulla base di quante EDT sono state associate a ciascuna di esse nell'Agenda (vedasi Tabella 3-3 in [7]).

Subarea	Data Science	Knowledge Representation and Reasoning	Machine learning and Deep Learning	Robotics and Autonomous Systems
Attacco e difesa	x	x	x	x
Cyberthreat intelligence	x	x	x	x
Gestione degli incidenti e operazioni di sicurezza	x	x	x	x
Ingegneria della protezione dati	x	x	x	
Trusted information sharing	x	x	x	
Aspetti umani	x		x	x
Aspetti legali	x		x	x
Gestione del rischio	x	x		x
Standardizzazione	x	x	x	
Scienze forensi digitali	x		x	
Sicurezza nello sviluppo e test del software			x	x
Hardware			x	x
Reti			x	x
Sicurezza nei sistemi operativi e tecniche di virtualizzazione				x

Figura 6
Relazione tra le EDT che costituiscono l'IA e le subaree impattate.

Nell'ottica delle tre declinazioni della relazione tra cybersicurezza e IA (vedasi inizio di Sezione 2), osserviamo infine che:

- l'Argomento #2.1.3 – "Messa in sicurezza di algoritmi e modelli di machine learning" è totalmente dedicato agli aspetti di **cybersicurezza dell'IA**;
- l'**IA per la cybersicurezza** e l'**IA per scopi offensivi** sono rilevanti, in particolare, per l'Area #2 – "Gestione delle minacce cibernetiche" che, infatti, è interessata da tali tecniche per il tramite di tutte le subaree ad essa afferenti (#2.1 – "Attacco e difesa", #2.2 – "*Cyberthreat intelligence*", #2.3 – "Gestione degli incidenti e operazioni di sicurezza" e #2.4 – "Scienze forensi digitali").

I filoni principali di finanziamento che anche l'ACN supporterà a livello nazionale italiano includono [9]:

- ricerca e innovazione in ambito IA&Cybersicurezza, con riferimento sia a dottorati di ricerca sia alla crescita delle imprese e all'efficienza ed efficacia dei servizi di difesa *cyber* nazionale;
- promozione di attività di test e sperimentazione per valutare soluzioni di IA, ed in particolare *sandbox*, *cyber range*, ambienti di test per soluzioni di IA cybersicure e per IA a supporto della difesa da minacce cibernetiche.

4 Applicazioni di IA&Cybersicurezza

In questa sezione analizzeremo tre applicazioni esemplificative, ma rappresentative, di IA&Cybersicurezza. Nello specifico, le prime due applicazioni sono esempi di IA a supporto della cybersicurezza, mentre il terzo è di IA per scopi offensivi (cfr. Sezione 2).

4.1 Caso d'uso: IA nella cybersicurezza delle infrastrutture critiche

Le infrastrutture critiche costituiscono sistemi complessi essenziali per il mantenimento delle funzioni vitali della società, dalla salute al benessere economico delle persone, e sono tali che un'interruzione dei servizi da loro offerti comporterebbe un significativo impatto per lo Stato. Per questo motivo, è necessario proteggerle sia dalle minacce provenienti dal mondo fisico, siano esse riconducibili a disastri naturali imprevedibili oppure ad attacchi cinetici dolosi, che dal cyberspazio. Tali minacce possono essere dirette alla singola infrastruttura critica, ma possono anche derivare dalle catene di approvvigionamento [25] dei servizi offerti da un'infrastruttura critica all'altra, determinando diverse dipendenze come raffigurato in Figura 7.

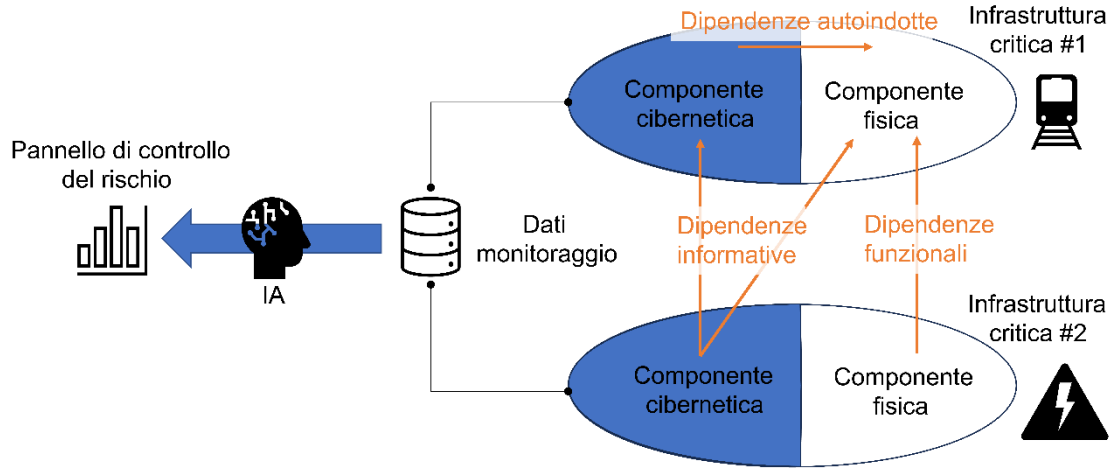


Figura 7

Rappresentazione delle possibili dipendenze tra infrastrutture critiche, per componente (cibernetica o fisica). Lungo le direttrici possono essere veicolati anche attacchi alla catena di approvvigionamento, determinando crisi sistemiche su scala nazionale.

In letteratura esistono metodologie analitiche e strumenti di valutazione e monitoraggio del rischio cibernetico[27], ma considerata la grande mole di dati che si può ottenere dal monitoraggio automatizzato dei sistemi informatici e di rete, potrebbe essere strategico implementare un sistema di IA in grado di aumentare le capacità di prevenzione degli incidenti. Tale sistema dovrebbe effettuare operazioni di *data preparation* sulla grande mole di dati raccolta, implementare algoritmi di machine learning per effettuare inferenza, predizioni, simulazioni di

[27] A titolo d'esempio, [44], [45] e [46].

comportamenti futuri, e restituire i risultati ad un “cruscotto”, ovvero un pannello di controllo che assista i decisori a livello strategico oppure operativo.

4.2 Caso d’uso: IA per operatori SOC

I *security operations center* (SOC) rappresentano i “presidi di difesa cibernetica” di enti pubblici e imprese private. Gli operatori dei SOC si affidano estensivamente a sistemi di monitoraggio delle infrastrutture digitali quali *Security Information and Event Management* (SIEM) e *Security Orchestration, Automation and Response* (SOAR) per collezionare dati ed eventi e correlarli al fine di far emergere comportamenti anomali. L'integrazione all’IA in questi sistemi può fornire un supporto prezioso agli operatori dei SOC per contrastare attacchi informatici in modo più efficiente ed efficace, automatizzando le attività di risposta agli incidenti e coordinando le azioni degli operatori. Una delle principali applicazioni in cui l'IA viene utilizzata nei SOAR è l'automazione delle attività ripetitive e manuali. Ciò include l'esecuzione di azioni di mitigazione automatiche o l'attivazione di contromisure senza richiedere intervento umano, come l'isolamento di sistemi compromessi o la disattivazione di account sospetti. Questo permette agli operatori di concentrarsi su compiti più complessi e strategici, migliorando la produttività complessiva del SOC. Inoltre, i modelli di IA giocano un ruolo essenziale nel rilevamento tempestivo delle minacce e in particolare l’identificazione di pattern e comportamenti sospetti, anche tramite tecniche di *anomaly detection* [33].
Oltre all'analisi e al rilevamento, l'IA contribuisce alla gestione delle fasi di risposta agli incidenti o addirittura di crisi cibernetiche di ampio spettro attraverso la generazione di suggerimenti e raccomandazioni basate sui dati, fornendo agli operatori suggerimenti sulla gravità di un incidente, sulle azioni consigliate e sulle priorità. In quest’ottica, si potrebbe pensare ad un sistema di supporto alle decisioni sotto forma di chatbot realizzato da un motore di IA. Tale strumento consentirebbe di dotare gli operatori di un “*crisis assistant*” in grado di i) fornire rapidi riscontri (stile chatbot, appunto) durante l’evolversi del contesto d’attacco e difesa e ii) anche formulare un piano d’azione per contenere lo specifico incidente, basandosi su uno storico degli incidenti.

4.3 Caso d’uso: IA contro la disinformazione

L’utilizzo malevolo di alcuni sistemi di IA, in particolare quelli basati sui modelli generativi preaddestrati, permette di generare in modo massivo contenuti falsi, come notizie, immagini, audio o video (questi ultimi, anche noti come *deepfake*), che sembrano autentici. Questa possibilità consente di automatizzare (tipicamente a basso costo) attacchi su larga scala quali campagne di spam e phishing e campagne di disinformazione sulle reti sociali.

D’altro canto, è possibile realizzare soluzioni innovative basate su IA anche per il contrasto alla disinformazione, in particolare in risposta alle due dimensioni principali di tale minaccia, la scala e la rapidità di diffusione, agendo a diversi stadi. Il primo di questi è il rilevamento, ovvero l’identificazione di pattern che distinguano le notizie false o artefatte da quelle vere localizzando la falsificazione

sintetica degli elementi manipolati all'interno di foto, video e audio[28]. Inoltre, l'analisi delle reti di interazione sui social media e la verifica automatica della credibilità delle fonti, consentirebbero il tracciamento dell'informazione sospetta, il riconoscimento di *botnet* e la potenziale identificazione degli attori coinvolti. In ultimo è possibile utilizzare agenti intelligenti per implementare meccanismi di *alerting* preventivi e attivare i meccanismi di verifica di cui sopra con una latenza minima rispetto alla velocità di propagazione dei contenuti.

5 Conclusioni e sviluppi futuri

L'intelligenza artificiale e la cybersicurezza sono due aree che, come discusso, si intersecano su molteplici fronti. La cybersicurezza dei sistemi basati su IA e il potenziale utilizzo di questi sistemi a scopi offensivi sono tra le sfide più attuali e critiche dell'IA. D'altro canto, l'utilizzo di IA a supporto della cybersicurezza è certamente una grande opportunità per rendere automatiche, veloci e scalabili le strategie di risposta agli attacchi *cyber*, rendendo i sistemi di IA per la difesa un investimento da prevedere in maniera prioritaria.

In questo articolo, a partire da un insieme di macro-processi di governo dell'IA&Cybersicurezza, abbiamo identificato attori, ruoli e oggetti che contribuiscono a garantire la cybersicurezza dell'ecosistema dell'IA. Dopo avere dettagliato i macro-processi, abbiamo illustrato altresì alcune applicazioni che mostrano scenari reali di IA&Cybersicurezza.

Gli aspetti di valutazione del rischio, presentati nella Sezione 3.1, hanno una complessità intrinseca elevata e sono un importante esempio di come molte metodologie siano ancora sulla frontiera della ricerca. Come riportato nella roadmap 2022-2030 del progetto europeo *flagship* per l'IA TAILOR (*Trustworthy Artificial Intelligence through Learning, Optimization and Reasoning*) [34], bisogna consolidare le attività di ricerca in corso, rendere solide le teorie fondamentali e le linee guida metodologiche che non sono ancora comunemente utilizzate né nel mondo industriale né in quello accademico.

Tra i programmi di sviluppo e potenziamento sul fronte della ricerca e della innovazione in IA&Cybersicurezza descritti nella Sezione 3.5, evidenziamo l'importanza di avere un'adeguata capacità di calcolo nazionale per sfruttare pienamente i sistemi di IA sia a fini economici sia a fini sociali (cfr. rapporto dell'OECD [35]). Le crescenti esigenze di elaborazione dei sistemi di intelligenza artificiale creano una maggiore domanda di software, hardware e relativa infrastruttura, insieme alla forza lavoro qualificata necessaria per utilizzarli. Si pensi ad esempio che le capacità computazionali necessarie per fare training dei moderni sistemi di apprendimento automatico si è moltiplicata per centinaia di migliaia di volte dal 2012 [36]. Dal punto di vista della cybersecurity, la difesa da minacce *cyber*, anche nell'ottica di sviluppo di sistemi di IA "*counter-AI*", comporta la necessità di poter (i) utilizzare infrastrutture ad elevate prestazioni di

[28] Ad esempio, tramite reti neurali generative (*Generative Adversarial Network*, GAN) [43].

calcolo, quali ad esempio infrastrutture HPC [29], (ii) dotarsi di processi che permettano di sfruttare efficacemente tali infrastrutture, ad esempio facendo sì che aspetti di formazione, legali, di accesso e di ricerca siano definiti in un framework di governance che li contempli e li integri e (iii) assicurarne la resilienza, soprattutto in termini di autonomia strategica e sicurezza.

Per essere pronti a fronteggiare le sfide dell'IA&Cybersicurezza è necessario dotarsi di un'organizzazione strutturata e pianificare attività di governo dedicate. In questa direzione, il CISA degli Stati Uniti ha definito una "*Roadmap for AI*" [37] che, tra le varie linee di azione, identifica la collaborazione con gli attori del governo federale per avere una condivisione di intenti e azioni sul fronte IA&Cybersicurezza. L'ecosistema italiano di cybersicurezza può analogamente cominciare a strutturarsi e a dotarsi delle capacità necessarie a raccogliere le importanti sfide dell'IA&Cybersicurezza e a far sì che anche il nostro Paese possa beneficiare delle enormi potenzialità dell'intelligenza artificiale.

Bibliografia

[1] Università di Stanford, «AI Index 2023,» 2023. [Online]. Available: https://aiindex.stanford.edu/.

[2] National Science and Technology Council, «National artificial intelligence research and development strategic plan - 2023 update,» 2023. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

[3] White House Office of Science and Technology Policy, «Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People,» 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[4] Commissione Europea, «L'intelligenza artificiale per l'Europa,» 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0237&from=IT.

[5] ENISA, «Artificial Intelligence and Cybersecurity Research,» 2023. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research.

[6] Governo italiano, «Programma strategico - Intelligenza artificiale 2022-2024,» 2021. [Online]. Available: https://assets.innovazione.gov.it/1637937177-programma-strategico-iaweb-2.pdf.

[7] ACN, «Agenda di Ricerca e Innovazione per la Cybersicurezza 2023-2026,» 2023. [Online]. Available: https://www.acn.gov.it/documents/agenda/it/ACN_ResearchInnovationAgenda.pdf.

[29] ACN, in collaborazione con il consorzio CINECA, si sta dotando di tali infrastrutture, da mettere a disposizione del Paese sia per scopi industriali che di ricerca.

[8] S. Samoili, M. Lopez Cobo, E. Gomez Gutierrez, G. De Prato, F. Martinez-Plumed e B. Delipetrev, «AI Watch. Defining Artificial Intelligence,» 2020. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC118163.
[9] ACN, «Strategia Nazionale di Cybersicurezza 2022-2026,» 2022. [Online]. Available: https://www.acn.gov.it/ACN_Strategia.pdf.
[10] «DECRETO-LEGGE 14 giugno 2021, n. 82,» [Online]. Available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82.
[11] NIST, «Artificial Intelligence Risk Management Framework (AI RMF 1.0),» 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[12] NIST, «Crosswalk - An illustration of how NIST AI RMF trustworthiness characteristics relate to the OECD Recommendation on AI, Proposed EU AI Act, Executive Order 13960, and Blueprint for an AI Bill of Rights,» 2023. [Online]. Available: https://www.nist.gov/system/files/documents/2023/01/26/crosswalk_AI_RMF_1_0_OECD_EO_AIA_BoR.pdf.
[13] ENISA, «Multilayer Framework for Good Cybersecurity Practices for AI,» 2023. [Online]. Available: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai.
[14] N. Carlini, M. Jagielsky, C. A. Choquette-Choo, D. Paleka, W. Pearce, H. Anderson, A. Terzis, K. Thomas e F. Tramèr, «Poisoning Web-Scale Training Datasets is Practical,» 2023. [Online]. Available: https://arxiv.org/pdf/2302.10149.pdf.
[15] M. Fang, X. Cao, J. Jia e N. Gong, «Local Model Poisoning Attacks to Byzantine-Robust Federated Learning,» in 29th USENIX Security Symposium, 2020.
[16] T. Gu, B. Dolan-Gavitt e S. Garg, «BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain,» 2019. [Online]. Available: https://arxiv.org/pdf/1708.06733.pdf.
[17] B. Chen, W. Carvalho, N. Baracaldo, H. Ludwig, B. Edwards, T. Lee, I. Molloy e B. Srivastava, «Detecting Backdoor Attacks on Deep Neural Networks by Activation Clustering,» 2018. [Online]. Available: https://arxiv.org/pdf/1811.03728.pdf.
[18] A. Vassilev, A. Oprea, A. Fordyce e H. Anderson, «Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artifcial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023,» 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf.
[19] I. Shumailov, Y. Zhao, D. Bates, N. Papernot, M. R e R. Anderson, «Sponge Examples: Energy-Latency Attacks on Neural Networks,» in IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021.
[20] OECD, «Recommendation of the Council on Artificial Intelligence,» 2019. [Online]. Available: https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf.

[21] L. Taylor e G. Nitschke, «Improving Deep Learning with Generic Data Augmentation,» in IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 2018.
[22] L. Truong, C. Jones, B. Hutchinson, A. August, B. Praggastis, R. Jasper, N. Nichols e A. Tuor, «Systematic Evaluation of Backdoor Data Poisoning Attacks on Image Classifiers,» in IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA, 2020.
[23] S. Udeshi, S. Peng, G. Woo, L. Loh, L. Rawshan e S. Chattopadhyay, «Model Agnostic Defence Against Backdoor Attacks in Machine Learning,» IEEE Transactions on Reliability, vol. 71, n. 2, pp. 880-895, 2022.
[24] B. Wang, Y. Yao, S. Shan, H. Li, B. Viswanath, H. Zheng e B. Y. Zhao, «Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks,» in IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019.
[25] R. Baldoni, «Managing the cyber risk in a multipolar world,» International Journal of Critical Infrastructure Protection, vol. 39, n. 100578, pp. 1-3, 2023.
[26] ENISA, «Cybersecurity of AI and standardization,» 2023. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation.
[27] Commissione Europea, «COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation and the,» 2023. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en.
[28] EU Parliament, «China's ambitions in artificial intelligence,» 2021. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA(2021)696206_EN.pdf.
[29] H. Roberts, M. Ziosi, C. Osborne, L. Saouma, A. Belias, M. Buchser, A. Casovan, C. Kerry, J. Meltzer, S. Mohit e M. E. Ouimette, «A Comparative Framework for AI Regulatory Policy,» 2023. [Online]. Available: https://ceimia.org/wp-content/uploads/2023/05/a-comparative-framework-for-ai-regulatory-policy.pdf.
[30] NCSC, CISA, et al.,, «Guidelines for secure AI system development,» 2023. [Online]. Available: https://www.acn.gov.it/documents/Guidelines-for-secure-AI-system-development.pdf.
[31] H. Janssen, «Generative AI: Security paradigm shift,» ENISA AI Cybersecurity Conference, 2023. [Online]. Available: https://www.enisa.europa.eu/events/2023-enisa-ai-cybersecurity-conference/huub-jansen-presentation-enisa-conference-rdi.pdf/view.
[32] ENISA, «Cybersecurity Research Directions for the EU's Digital Strategic Autonomy,» 2021. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy.

[33] A. B. Nassif, M. A. Talib, Q. Nasir e F. M. Dakalbab, «Machine Learning for Anomaly Detection: A Systematic Review,» IEEE Access, vol. 9, pp. 78658-78700, 2021.
[34] TAILOR, «Strategic Research & Innovation Roadmap of Trustworthy AI - The Scientific Foundations of Trustworthy AI in Europe for the Years 2022-2030,» [Online]. Available: https://tailor-network.eu/wp-content/uploads/2022/07/TAILOR-Roadmap-Full-Version-1.pdf.
[35] OECD, «A blueprint for building national compute capacity for artificial intelligence,» OECD Digital Economy Papers, 2023. [Online]. Available: https://www.oecd-ilibrary.org/docserver/876367e3-en.pdf?expires=1690191390&id=id&accname=guest&checksum=94EADBB2EF8203FEC9F16765ADD8494A.
[36] J. Sevilla, L. Heim, A. Ho, T. Besiroglu, M. Hobbhahn e P. Villalobos, «Compute Trends Across Three Eras of Machine Learning,» in International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022, 2022.
[37] CISA, «CISA Roadmap for Artificial Intelligence,» 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf.
[38] OECD, «Tools for trustworthy AI: A framework to compare implementation tools for trustweorthy AI systems,» OECD Digital Economy Papers, 2021. [Online]. Available: https://www.oecd-ilibrary.org/docserver/008232ec-en.pdf?expires=1690207133&id=id&accname=guest&checksum=2F0E59A18DFD2464AECFA73CE8F89567.
[39] ISO/IEC, «Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making,» ISO/IEC TR 24027, 2021.
[40] ISO/IEC, «Information security management systems,» ISO/IEC 27001, 2022.
[41] NIST, «Security and Privacy Controls for Information Systems and Organizations,» NIST SP 800-53, 2020.
[42] ISO/IEC, «Information technology — Security techniques — Privacy framework,» ISO/IEC 29100:2011, 2011.
[43] M. F. Mridha, A. J. Keya, M. A. Hamid, M. M. Monowar e M. S. Rahma, «A Comprehensive Review on Fake News Detection With Deep Learning,» IEEE Access, vol. 9, pp. 156151-156170, 2021.
[44] A. P. Henriques de Gusmão, M. M. Silva, T. Poleto, T. L. Camara e Silva e A. P. Cabral Seixas Costa, «Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory,» International Journal of Information Management, vol. 43, pp. 248-260, 2018.
[45] M.-E. Paté-Cornell, M. Kuypers, M. Marshall e P. Keller, «Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies,» Risk Analysis, vol. 38, n. 2, pp. 226-241, 2018.
[46] C. Foglietta e S. Panzieri, «Resilience in Critical Infrastructures: The Role of Modelling and Simulation,» in Issues on Risk Analysis for Critical Infrastructure Protection, IntechOpen, 2020.

[47] OWASP, «OWASP Top 10 for LLM,» 2023. [Online]. Available: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_0.pdf.

BIOGRAFIE

Luca Nicoletti. Luca Nicoletti si è laureato in Fisica presso l'Università degli Studi di Roma "La Sapienza" nel 1996. Dopo aver svolto il servizio militare come Ufficiale di Marina, dal 1997 opera nel campo informatico, interessandosi fin dall'inizio ai sistemi distribuiti e alle tecnologie Web. Tra il 1998 e il 2000 ha lavorato su Sistemi di Controllo di Gestione per importanti aziende italiane nei settori delle Telecomunicazioni e dell'Energia. Tra il 2000 e il 2013 lavora in Consip, prima nell'area "Architetture Tecnologiche" e poi nell'area "Soluzioni di Sistema". Nel 2013 si trasferisce in Sogei S.p.A. nell'area "Architetture Tecnologiche e Servizi" dove è responsabile del gruppo *Technological Demand Management*. Dal 2007 al 2018 ha aderito a progetti server FP7/H2020, in qualità di esperto tecnico o technical leader. Dal 2019 ha lavorato presso la Presidenza del Consiglio dei Ministri, e dal 2021 è passato all'Agenzia per la Cybersicurezza Nazionale, dove ricopre il ruolo di Capo del Servizio Programmi industriali, tecnologici, di ricerca e formazione. I suoi principali campi di interesse sono le Architetture *Service Oriented*, la virtualizzazione di sistemi e applicazioni, il Cloud Computing, i sistemi di gestione di Identity & Access, argomenti sui quali ha scritto articoli ed è stato chiamato a tenere seminari.

E-mail: l.nicoletti@acn.gov.it

Monica Scannapieco. Monica Scannapieco è attualmente a capo della Divisione "Programmi di Ricerca e Awareness" dell'Agenzia per la Cybersicurezza Nazionale (ACN). In precedenza, ha lavorato presso l'Istituto Nazionale di Statistica italiano per più di 15 anni, con ruoli di direzione e coordinamento di strutture organizzative in ambito ricerca e sviluppo e IT. Ha fatto parte di diversi comitati, tra cui l'*executive board* dell'UNECE (*United Nations Economic Commission for Europe*) sulla modernizzazione delle statistiche ufficiali e comitati di Eurostat su temi legati all'innovazione. Ha collaborato con diversi organismi nazionali, europei ed internazionali, tra cui la Presidenza del Consiglio dei Ministri italiana, la Commissione Europea, la FAO e la Banca Mondiale. Ha conseguito la Laurea in Ingegneria Informatica con lode e un Ph.D. in Ingegneria Informatica presso SAPIENZA Università di Roma. È autrice di articoli e libri scientifici su varie tematiche di *data management* e *data science;* in particolare, i suoi principali campi di interesse sono qualità dei dati, integrazione dei dati, gestione di Big Data e sicurezza dei dati.

E-mail: m.scannapieco@acn.gov.it

Mara Sorella. Consigliere presso l'Agenzia per la Cybersicurezza Nazionale dal 2021. In precedenza, a partire dal 2020 ha ricoperto il ruolo di Funzionario superiore presso la Presidenza del Consiglio dei Ministri. Ha conseguito il titolo di Dottore di ricerca in Ingegneria Informatica presso Sapienza Università di Roma nel 2018. Durante il dottorato ha svolto diverse collaborazioni di ricerca, tra cui un tirocinio presso il *Big Data Experience Lab* di *Adobe Research* (USA) e ha lavorato su importanti progetti europei del programma H2020 in ambito *data mining*, *machine learning e cybersecurity*. Ha inoltre svolto attività di ricerca post-dottorato presso il Centro di Ricerca in *Cyber Intelligence and Information Security (CIS)* di Sapienza Università di Roma, nonché incarichi di docenza a contratto presso diversi atenei. I suoi principali ambiti di interesse sono il progetto di algoritmi di *data mining* in contesti distribuiti*, streaming* e *online*, e la modellazione delle minacce *(threat modeling*) in ambito cybersecurity.

E-mail: m.sorella@acn.gov.it

Marco Centenaro. Esperto presso l'Agenzia per la Cybersicurezza Nazionale dal 2022, ha conseguito il titolo di Dottore di ricerca in Scienza e Tecnologia dell'Informazione (specializzazione telecomunicazioni) dall'Università degli Studi di Padova nel 2018. In passato, ha lavorato come assegnista di ricerca post-dottorato presso le Università di Padova e Aalborg (Danimarca), *expert researcher* alla Fondazione Bruno Kessler di Trento e *system engineering manager* presso Athonet S.r.l. (oggi HPE). I suoi principali campi di interesse vertono sui sistemi di telecomunicazione radiomobile e sull'*Internet of things* (IoT).

E-mail: m.centenaro@acn.gov.it

IL FATTORE UMANO E LA REGOLAZIONE DELLA CYBERSECURITY

Federica Camisa, Andrea Simoncini[1]

Sommario

Viviamo ormai da tempo in una realtà digitalizzata e costellata da molteplici attività dipendenti da sistemi tecnologici interconnessi. Una vera e propria transizione cibernetica, dunque, che da un lato offre prospettive di avanzamento e progresso, ma dall'altro espone gli utilizzatori a inedite minacce che permeano la sfera della sicurezza digitale e dei diritti fondamentali. La regolazione della cybersicurezza diviene elemento imprescindibile per mitigare l'incremento degli attacchi informatici potenzialmente dannosi per le infrastrutture e per i dati ivi contenuti. Per le stesse finalità e nonostante l'elevato tecnicismo che caratterizza la "sfera digitale", parimenti determinante risulta il fattore umano, ovvero il ruolo assunto dagli stessi utilizzatori.

Abstract

We live in a digitalised reality, where many activities depend on interconnected technological systems. A real cyber transition that offers the prospect of evolution and progress, but also exposes users to unprecedented threats in the field of digital security and fundamental rights. Therefore, cybersecurity regulation is imperative for containing potentially damaging cyber-attacks on infrastructures. For these same purposes, it is equally critical to consider the role that users play (i.e. the human factor).

Keywords: cyber attacks – cybersecurity – regulation – fundamental rights – human factor

1. Introduzione

Basta guardarsi intorno per realizzare che viviamo immersi in ambienti costantemente "connessi e intelligenti". Moltissime delle attività che svolgiamo, sia come singoli, sia come imprese o come pubbliche amministrazioni, dipendono sempre più da sistemi tecnologici tra loro interconnessi.

Con la rivoluzione cibernetica [1] e l'avanzamento delle nuove tecnologie digitali, è possibile realizzare in rete numerose e significative attività (accedere al Servizio

[1] Sebbene l'articolo sia il frutto di un lavoro comune, il paragrafo 1 è di Andrea Simoncini mentre i paragrafi 2, 3, 4 e 5 sono di Federica Camisa.

sanitario regionale, gestire il settore delle comunicazioni elettroniche, dell'energia, dei trasporti, ecc.).

Come tutte le innovazioni della tecnica, questi strumenti costituiscono contemporaneamente, da un lato, opportunità senza precedenti per il progresso e lo sviluppo della conoscenza, per il miglioramento culturale, sanitario ed economico; tuttavia, dall'altro lato, rappresentano un rischio e una potenziale minaccia, poiché attraverso essi possono realizzarsi inedite violazioni dei diritti [2].

Vivere in una realtà iperconnessa *(onlife* [3]*)* espone la società a una serie di nuove sfide legate al concetto di *sicurezza*, nonché a nuovi rischi di cui spesso non si ha percezione, né consapevolezza [4]. Si considerino, per esempio, le forme di sorveglianza di massa esercitabili mediante l'utilizzo delle tecnologie [5], come le c.d. tecniche di "profilazione" e i sistemi di videosorveglianza [6].
Oltre alle consuete dimensioni della sicurezza che attengono alla vita della persona – come il mantenimento dell'ordine pubblico, la sicurezza sul lavoro o la circolazione stradale – si affiancano, dunque, tutte le implicazioni suscitate dall'avvento del digitale, tra cui spicca la necessità di salvaguardare l'ambiente "virtuale" [7].

Nell'incessante progresso tecnologico, infatti, la rete e i servizi ivi offerti, divengono sempre più frequentemente bersaglio di attacchi informatici *(cyber attacks)*, i quali non solo possono causare malfunzionamenti e interruzioni dei servizi, ma possono altresì provocare preoccupanti fughe di dati personali. In questa prospettiva, emerge una stretta correlazione tra la salvaguardia delle infrastrutture e la tutela delle informazioni, richiamando in modo ineludibile la normativa relativa alla protezione dei dati personali, con particolare riferimento, a livello europeo, il *General Data Protection Regulation* (GDPR) [8].

Considerato il contesto in cui viviamo, caratterizzato da una crescente condivisione di dati personali e da sempre più frequenti violazioni della *cybersecurity*, l'Unione Europea, con il GDPR, ha manifestato un deciso impegno nella salvaguardia della privacy[2], o meglio, della protezione dei dati personali [9] e della sicurezza degli stessi [10]. La connessione tra il GDPR e la cybersicurezza richiede l'adozione di misure concrete volte all'implementazione di dispositivi sicuri e in grado di difendersi da possibili attacchi che potrebbero compromettere la riservatezza, integrità e disponibilità dei dati personali in essi contenuti [11]. In

[2] Il concetto di privacy affonda le sue radici in epoche piuttosto recenti. Una sua prima elaborazione giuridica può essere identificata solo verso la fine del diciannovesimo secolo. ® nel 1890, in occasione della pubblicazione dell'articolo *The Right to* Privacy di due giuristi statunitensi (D. Warren e L. D. Brandeis), che il concetto di privacy è riconosciuto come "il diritto ad essere lasciato solo". Da allora si osserva l'insorgere di una dimensione sociale della privacy. È risaputo come, a causa dell'incessante sviluppo tecnologico, la questione della tutela della sfera privata di ciascun individuo abbia assunto connotazioni completamente inedite, mettendo in crisi gli antichi schemi.
In altre parole, il diritto alla privacy ha subito un'evoluzione dalla sua concezione iniziale come diritto di essere lasciati soli al diritto di esercitare un controllo sulle informazioni riguardanti la sfera personale.

questo quadro emerge con chiarezza la necessità di mantenere un costante equilibrio tra le esigenze di protezione dati e di sicurezza, poiché sono due aspetti che, come abbiamo già detto, risultano strettamente interconnessi e reciprocamente dipendenti [12].
Posto che la sicurezza della rete diviene un elemento cardine che deve essere garantito nel mondo digitale [13], prima di interrogarci su come prevenire e reagire alle aggressioni perpetrate sul *web*, occorre chiarire cosa si intende con l'espressione «sicurezza»? Chi sono i soggetti che devono garantirla e in che modo è auspicabile farlo? Perché è importante discutere di un «diritto costituzionale ibrido» [14][3]?

Negli anni, la riflessione su queste domande ha assunto la consistenza di una vera e propria disciplina, quella della *cybersecurity* [15], intesa come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[4].

È opportuno ora contestualizzare e delineare i confini entro cui sarà sviluppato il contributo per fornire sin dal principio una panoramica generale dei temi che saranno trattati.

Nei successivi paragrafi verrà approfondito il concetto di cybersicurezza e segnalata la sua centralità nelle dinamiche quotidiane. Un *focus* particolare sarà riservato all'esame di un caso paradigmatico: l'attacco informatico alla Regione Lazio. In tale occasione, verranno spiegate brevemente le dinamiche di tale aggressione per poi evidenziare le implicazioni e le conseguenze in termini di sicurezza delle infrastrutture e protezione dei dati personali.

Saranno poi dedicati alcuni paragrafi a una rapida analisi del quadro normativo, partendo inizialmente dalla legislazione vigente a livello europeo; per poi successivamente soffermarsi sul piano nazionale.

Una specifica riflessione sarà riservata al ruolo assunto dal fattore umano nel campo della sicurezza informatica al fine di comprendere come le dinamiche comportamentali e decisionali di ciascun utente possano incidere sulle vulnerabilità di un sistema informatico e possano, finanche, determinare il successo di un attacco informatico.

In conclusione sarà offerta una sintesi delle principali argomentazioni avanzate nel contributo, proponendo considerazioni critiche e sollecitazioni riguardo alla necessità di adottare un approccio che favorisca una maggiore pedagogia digitale e promuova buone pratiche nel cyberspazio.

[3] Con il termine «diritto costituzionale ibrido» l'autore, Andrea Simoncini, esprime la necessità di dover recepire i valori del diritto costituzionale sin nella fase di progettazione degli strumenti informatici.
[4] In questi termini si esprime l'art. Art. 2, punto 1) del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013.

2. La (cyber)sicurezza come esigenza quotidiana. Il caso dell'attacco informatico alla Regione Lazio

Come abbiamo visto, la capillare diffusione delle tecnologie e il loro sempre crescente impiego nelle più disparate attività quotidiane, nell'ambito di una società dell'informazione, incrementano il rischio di essere esposti, anche indirettamente, a nuove minacce che hanno come bersaglio le strutture informatiche.

I dati che emergono dal rapporto Clusit 2023 rilevano nel periodo dal 2018 al 2022 una crescita preoccupante degli attacchi informatici a livello globale pari al 60%[5]. Queste forme di attacchi, i c.d. *cyber attacks*[6], sono realizzati da soggetti malintenzionati che, attraverso azioni illegali compiute sovente nel c.d. *dark* web [16][7], sfruttano malignamente le vulnerabilità dei sistemi informatici con l'obiettivo di arrecare danni, causare l'interruzione di servizi, rubare i dati o chiedere riscatti (*ransomware*).

Un esempio di attacco informatico è quello che nell'agosto 2021, in piena emergenza pandemica da Covid-19, ha visto coinvolta la Regione Lazio.

L'aggressione cibernetica è stata perpetrata ai danni del centro di elaborazione dati (CED) e ha avuto una particolare risonanza soprattutto perché ha colpito anche le piattaforme adibite alla prenotazione dei vaccini contro il Covid-19. Seppure vi siano differenti ricostruzioni della vicenda, il dato certo è che sia stato utilizzato un *malware,* in particolare un *ransomware,* ossia un programma informatico dannoso che infetta il dispositivo e impedisce l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto per rimuovere tale limitazione.

Nel caso di specie, il *ransomware* avrebbe colpito un dispositivo, connesso al *server* di erogazione dei servizi di gestione e organizzazione delle attività di interesse regionale, di un dipendente che lavorava in *smartworking*. Questo attacco avrebbe causato una interruzione dei servizi del sistema sanitario regionale.

Le conseguenze spesso gravi derivanti da queste tipologie di attacchi informatici – che frequentemente si manifestano sotto forma di danni alle infrastrutture e di fughe di dati – confermano la rilevanza della disciplina sulla *cybersecurity* e, non

[5] Per un'analisi più approfondita è possibile consultare il report al seguente indirizzo: https://clusit.it/wp-content/uploads/area_stampa/2023/Anteprima_Rapporto_Clusit_2023.pdf (ultimo accesso novembre 2023).

[6] Si veda la definizione fornita dall'Enciclopedia Treccani https://www.treccani.it/vocabolario/cyberattacco_%28Neologismi%29/#:~:text=s.%20m.%20Attacco%20terroristico%20condotto%20con%20mezzi%20tecnologici%2C%20attraverso%20Internet (ultimo accesso novembre 2023).

[7] L'autore, Stefano Pietropaoli, per *dark web* intende quello spazio in cui «è possibile mettere in vendita le proprie prestazioni di qualsiasi natura esse siano, insieme ad altri oggetti e, purtroppo, persone». Questo termine, aggiunge l'autore, «va tenuto distinto dal deep web che pur non essendo indicizzato è perfettamente lecito».

limitandosi a colpire una singola entità o un singolo Stato membro ma diffondendosi in pochi minuti tra organizzazioni, settori e diversi Stati membri, è indispensabile la previsione di misure di prevenzione e contrasto che tengano in considerazione la dimensione transfrontaliera particolarmente marcata della materia.

Dinanzi all'evidenza di situazioni sociali in cui l'uso di determinati strumenti può recare danno alla vita o al patrimonio dei consociati, la reazione è stata quella, da un lato, di moltiplicare gli sforzi nella ricerca scientifica per aggiornare e migliorare i sistemi tecnici, in modo da "immunizzarli" il più possibile da questi attacchi malevoli o dall'uso criminoso che se ne può fare. Dall'altro lato, la risposta delle organizzazioni sociali e politiche è stata quella di proporre norme volte a vietare o disincentivare l'impiego illecito dei dispositivi tecnologici.

Nel paragrafo che segue proporremo una sintesi della disciplina normativa in materia di *cybersecurity,* dapprima a livello europeo e poi a livello nazionale [17], per infine soffermarci sul ruolo assunto in queste vicende da quello che definiamo il "fattore umano".

3. La reazione del legislatore

La preminente necessità di individuare una normativa specifica in materia di *cybersecurity* è stata chiara sin dalle fasi iniziali dello sviluppo della rete *internet*, quando si è compreso che gli attacchi informatici avrebbero inevitabilmente impattato sulle informazioni, sui dati e sui servizi offerti, determinando conseguentemente effetti diretti e, potenzialmente, di portata catastrofica sul tessuto sociale e sulle libertà sancite a livello costituzionale. La sicurezza informatica diviene dunque un fattore essenziale oltre che per la corretta operatività ed efficienza delle infrastrutture pubbliche e private, anche per garantire un sicuro esercizio dei diritti fondamentali [18], compresi i diritti alla riservatezza e alla protezione dei dati personali nonché la libertà di espressione e di informazione.

La natura globale delle minacce cibernetiche richiede una cooperazione internazionale e un'armonizzazione delle norme e delle pratiche di sicurezza informatica tra i Paesi. In questa prospettiva, il legislatore e le istituzioni pubbliche hanno reagito alla impellente esigenza di contrastare l'uso distorto e criminoso delle tecniche offerte dalla tecnologia, attraverso l'introduzione di disposizioni normative e regolamentazioni che mirano ad assicurare un ambiente digitale sicuro.

L'Unione europea, pioniera in questo ambito, si è occupata di analizzare approfonditamente le vulnerabilità, le minacce e il rischio associato agli *asset* informatici, al fine di salvaguardarli da potenziali attacchi suscettibili di cagionare danni di notevole entità [19].

La legislazione nazionale degli Stati membri in materia di *cybersecurity* è stata adottata seguendo l'impulso del legislatore eurounitario. E infatti, al quadro normativo europeo delineato nel corso degli anni, si sono affiancate le disposizioni dei legislatori nazionali [20].

3.1. L'ordinamento UE

L'Unione europea, come precedentemente affermato, ha posto le fondamenta normative della *cybersecurity*, le cui previsioni costituiscono oggi il cuore della strategia eurounitaria in tale ambito.

Nonostante le prime regolamentazioni sulla sicurezza informatica risalgano agli anni '90, il primo intervento che ha portato all'istituzione di un'apposita agenzia, l'*European Union Agency for Cybersecurity* (ENISA), è avvenuto nel 2004[8], in risposta alla necessità di riunire in capo ad un unico attore la responsabilità di contribuire alla politica informatica dell'UE, di migliorare l'affidabilità dei prodotti e dei servizi, nonché di delineare una strategia di sicurezza comune tra gli Stati membri. Nel corso del tempo, si è assistito a un progressivo consolidamento del ruolo riconosciuto all'ENISA accompagnato da un notevole accrescimento delle sue competenze[9].

Tra le iniziative di maggiore rilevanza figura la Direttiva NIS (*Network And Information Security*)[10], adottata nel 2016 e attuata in Italia solamente nel 2018, che rappresenta il primo esempio di normativa "orizzontale" e, quindi, il primo tentativo di armonizzazione dei livelli di sicurezza dei sistemi informatici [21]. Sostanzialmente gli scopi perseguiti sono quelli di migliorare le capacità *cyber* degli Stati membri, rafforzare la cooperazione e promuovere una cultura di prevenzione degli incidenti e di gestione del rischio.

Con lo strumento giuridico della direttiva, l'Unione ha voluto garantire, mediante la previsione di obblighi di risultato che stabiliscono standard minimi, un livello omogeneo di sicurezza delle infrastrutture sull'intero territorio europeo. In particolare, la Direttiva NIS ha identificato, attraverso una classificazione, i soggetti destinatari della disciplina. Questi ultimi si articolano in due categorie specifiche: gli "operatori economici di servizi essenziali" (art. 5) e i "fornitori di servizi digitali" (FSD), ciascuno dei quali è soggetto a precisi obblighi volti all'implementazione di adeguate misure tecniche e organizzative adeguate, atte a prevenire gli incidenti informatici (art. 14 e ss.).

L'indiscussa rilevanza strategica della disciplina sulla *cybersecurity*, insieme alla crescente necessità di incrementare i livelli di sicurezza e di delineare un quadro armonizzato atto a coordinare le iniziative in questo contesto, hanno stimolato il legislatore europeo a intervenire, nel 2019, mediante lo strumento giuridico del regolamento, per assicurare la diretta applicabilità delle disposizioni su tutto il

[8] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione e che attribuisce alla stessa il compito di contribuire ad assicurare un elevato livello di sicurezza delle reti nonché a promuovere una cultura in materia a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno.

[9] Il ruolo dell'ENISA è stato rafforzato prima con il Regolamento (UE) n. 526/2013, poi con il Regolamento UE 2019/881 (c.d. Cybersecurity Act).

[10] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

territorio europeo. L'entrata in vigore dell'EU Cybersecurity Act (o Cyber Act)[11] ha non solo definito una cornice normativa europea più coincisa rispetto al passato, ma ha altresì prefissato l'ambizioso obiettivo di instaurare un mercato unico digitale più sicuro attraverso l'introduzione di un sistema europeo di certificazione dei prodotti e dei servizi. In questa prospettiva, il Cyber Act ha rafforzato il ruolo dell'ENISA, conferendole la funzione fondamentale di coordinamento attivo al fine di garantire un elevato e omogeneo livello di sicurezza informatica all'interno dell'Unione Europea.

La declinazione di principi comuni e di regole di policy sulla *cybersecurity* per favorire una risposta comune alle crisi determinate da diversi livelli di *cyber* resilienza tra gli Stati membri, ha trovato un primo vero momento di concretizzazione all'interno della Direttiva NIS 2 [12] e della proposta di Regolamento Cyber Resilience Act (CRA) [22], dalle quali emerge un approccio maggiormente proattivo rispetto al passato. Nel dicembre 2020 la Commissione europea ha proposto la NIS 2 [23], entrata in vigore a gennaio 2023, che mira a sostituire la precedente NIS del 2016, ritenuta ormai non più adeguata alle crescenti e mutevoli minacce cibernetiche. Con questa nuova disciplina è stato operato un ampliamento dell'ambito di applicazione degli obblighi e degli *standard* di sicurezza informatica, ora estesi a una porzione più ampia dell'economia, al fine di fornire una copertura completa dei settori e dei servizi ritenuti di vitale importanza per le principali attività sociali ed economiche nel mercato interno. Questa nuova Direttiva, orientata alla creazione di un quadro normativo più nitido rispetto al passato e alla promozione di una definizione più efficace degli aspetti operativi, assegna, mediante un approccio *top down* e di *hard rule*, specifici obblighi di gestione e segnalazione dei rischi di cybersicurezza (artt. da 17 a 23) e obblighi in materia di condivisione delle informazioni (artt. 26 e 27) a tutti gli operatori del settore. I soggetti destinatari di tali obblighi sono distinti tra "soggetti essenziali" e "soggetti importanti", a seconda del settore in cui esercitano la propria attività. A titolo esemplificativo, i primi sono coloro che nei settori dell'energia, trasporti, bancario e sanitario (ecc.)[13], mentre i secondi sono coloro che operano nei settori dei servizi postali, gestione rifiuti, fabbricazione, produzione e distribuzione (ecc.)[14]. La *ratio* di tale

[11] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 («Regolamento sulla cibersicurezza»), che disciplina e rafforza il ruolo dell'ENISA riconoscendole la funzione fondamentale di coordinamento attivo al fine di garantire un elevato e omogeneo livello di sicurezza informatica all'interno dell'Unione. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019R0881 (ultimo accesso novembre 2023).

[12] Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555 (ultimo accesso novembre 2023).

[13] Allegato I della Proposta di Direttiva NIS 2.

[14] Allegato II della Proposta di Direttiva NIS 2.

categorizzazione risiede nell'intenzione di evitare di sottoporre indifferentemente tutti gli operatori all'interno di un unico quadro di obblighi e doveri, proponendo invece un regime differenziato[15] che tenga conto del rischio che certi settori, proprio in virtù dell'attività svolta, potrebbero subire conseguenze più gravi in caso di violazioni della sicurezza. È proprio da questo ragionamento che nasce l'approccio di una regolazione del rischio.

La Direttiva NIS 2 manifesta chiaramente una duplice volontà del legislatore che, da un lato, interviene con una disciplina più chiara e uniforme identificando esplicitamente gli obblighi applicabili a tutti i destinatari e, dall'altro, riserva loro una sfera di autonomia. In particolare, gli operatori del settore beneficeranno del vantaggio di poter individuare, sulla base delle loro attività svolte e della conoscenza dei rischi ad esse connessi, gli ambiti prioritari su cui intervenire per colmare le lacune di sicurezza e ridurre le vulnerabilità a cui rimarrebbero altrimenti esposti. Questo processo li indurrà a adottare misure tecniche proporzionate e adeguate, nonché ad assumere una maggiore responsabilità in considerazione del regime di vigilanza a cui sono assoggettati e delle corrispondenti misure sanzionatorie.

Al fine di salvaguardare i consumatori e le imprese anche da prodotti digitali caratterizzati da livelli di sicurezza inadeguati e insufficienti, la Commissione europea, come già anticipato, ha fatto nuovamente ricorso allo strumento del Regolamento presentando il 15 settembre 2022, il Cyber Resilience Act (c.d. CRA)[16]. Con questa proposta, il legislatore europeo ha delineato un quadro dettagliato di obblighi e requisiti orizzontali di cybersicurezza, ai quali i soggetti destinatari, ossia i produttori e i fornitori, sono tenuti a adeguarsi a seconda dei prodotti con elementi digitali che intendono introdurre nel mercato interno[17].

---

[15] Per ciò che concerne invece l'approccio regolamentare e, quindi, la scelta concreta delle misure di mitigazione del rischio – che la Direttiva NIS 2 lascia in mano ai soggetti regolati (modello *bottom-up* e *co-regulation*) – si distingue la previsione di intervenire *ex ante* ed *ex post* per i soggetti essenziali e, unicamente, *ex post* per i soggetti importanti. Conseguentemente sono previsti due differenti sistemi di supervisione da parte delle Autorità competenti, da un lato, uno più stringente e proattivo mentre, dall'altro lato, uno più leggero e reattivo. Ad esempio, la classificazione dei soggetti è significativa al fine di prescrivere quando debba intervenire la scelta, da parte dei soggetti regolati, in ordine alle misure da applicare – se in via preventiva o se in via successiva – e, inoltre, al fine di assoggettare i destinatari ad un regime di vigilanza più o meno stringente a seconda dell'attività svolta.

[16] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 (ultimo accesso novembre 2023).

[17] Infatti, a differenza della Direttiva NIS 2, il CRA fissa regole orizzontali, direttamente applicabili agli Stati membri, sull'immissione e sull'utilizzo di sistemi e prodotti con elementi digitali nel mercato dell'Unione. Ciò avviene mediante un approccio proporzionato basato sul rischio che prevede, similmente a quanto previsto dalla NIS 2, requisiti essenziali di sicurezza informatica che i prodotti digitali devono possedere (Allegato I, sez. 1), requisiti di gestione della vulnerabilità che i produttori devono rispettare (Allegato I, sez. II) e informazioni e istruzioni minime che devono essere fornite agli utenti con riferimento ai prodotti immessi sul mercato (Allegato II).
L'oggetto della regolazione nel CRA, a differenza della NIS 2 (che individua regole e requisiti facendo riferimento ai settori in cui gli operatori svolgono le proprie attività), riguarda nello specifico i "prodotti

La distinzione degli obblighi e dei requisiti operata a monte dal legislatore, prende atto non solo della categoria generale dei settori in cui agiscono i destinatari, quanto piuttosto della specificità dei prodotti con elementi digitali introdotti nel mercato. Questo approccio mira a creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri sin dalle fasi iniziali del ciclo di vita del prodotto. In ragione di questo principio (della *security by design*) è richiesto agli operatori del settore di agire in modo preventivo (*ex ante*), eliminando, sin dalle prima fasi di progettazione e produzione dei prodotti con elementi digitali, le vulnerabilità e i pericoli ad essi associati.

La scelta della fonte regolamentare sottostà alla volontà politica di istituire nuove regole uniformi a livello europeo, finalizzate ad aumentare il grado di fiducia tra gli utenti e promuovere l'attrattiva dei prodotti con elementi digitali provenienti dall'UE. Questo approccio implica un potenziamento del principio di proporzionalità delle misure tecniche, poiché gli operatori del settore saranno tenuti a implementare, in base al livello di rischio associato ai loro prodotti e già individuato dalla normativa, misure tecniche proporzionate e adeguate. Ciò determinerà altresì un ampliamento del principio di *accountability* degli operatori, i quali, nel conformarsi ai requisiti stabiliti dal legislatore, assumeranno la responsabilità del proprio operato.

Anche i sistemi informatici aziendali si trovano in una crescente condizione di vulnerabilità nei confronti di possibili attacchi informatici. Per tale ragione, il 14 dicembre 2022, il Parlamento europeo ha approvato un ulteriore Regolamento, denominato Digital Operational Resilience Act (c.d. DORA)[18] che definisce un *framework* comune di resilienza operativa digitale per tutti gli operatori del settore finanziario vincolandoli al rispetto di una serie di requisiti di sicurezza informatica.

Sulla base di tali fondamenta, si è sviluppata successivamente la legislazione nazionale in materia di cybersicurezza.

---

con elementi digitali" che l'art. 3 definisce come "qualsiasi prodotto che preveda almeno una componente digitale e che, anche solo potenzialmente, si connetta a Internet". In particolare, l'Allegato III effettuata una classificazione dei c.d. "critical products with digital elements" sulla base di due classi di rischio: quelli definiti a rischio moderato che rientrano nella "Class I" (password, software di condivisione, sistemi non rientranti nell'alto rischio) e quelli definiti a rischio elevato che rientrano nella "Class II" (cripto processori, chiavi pubbliche, certificatori, mobile devices).
A seconda dei prodotti coinvolti nelle attività dei produttori, fornitori e distributori, essi devono rispettare obblighi e doveri diversificati: meno stringenti nel caso di prodotti a rischio moderato, poiché gli operatori sono assoggettati ad un regime di autocertificazione vincolata al rispetto di standard di trasparenza finalizzata a garantire la conformità di tali prodotti alle regole di sicurezza; più stringenti nel caso di prodotti a rischio elevato che, per essere immessi nel mercato, devono rispettare una serie di requisiti obbligatori orizzontali per garantire una maggiore affidabilità nonché seguire le procedure di valutazione della conformità affidate, diversamente dall'altra categoria, ad un ente esterno. Invece, per i prodotti digitali classificati come sistemi di IA, previsti dall'art. 15 dell'AI ACT, l'art. 8 del CRA prevede una presunzione di conformità ai requisiti di sicurezza informatica e, dunque, sono prodotti esentati dal rispetto dei requisiti sopra descritti.

[18] Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 (ultimo accesso novembre 2023).

3.2. L'ordinamento nazionale

L'Italia, sulla base del quadro normativo previsto dall'Unione europea, si è dotata di una cospicua normativa volta a disciplinare il settore della cybersicurezza.

In evidente ritardo rispetto agli altri Paesi, nel 2013 è stata formulata una prima architettura della sicurezza cibernetica nazionale mediante il DPCM del 24 gennaio 2013 (c.d. Decreto Monti)[19]. Il DPCM ha delineato «l'architettura istituzionale deputata alla sicurezza nazionale […] con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale» assegnando a questo scopo compiti spesso strettamente complementari a vari attori istituzionali (Presidente del Consiglio dei ministri, Comitato Interministeriale per la Sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza, Nucleo per la Sicurezza Cibernetica) rendendo perciò indispensabile l'instaurarsi di numerose interazioni reciproche tra gli stessi.

Il panorama normativo nazionale ha poi subito modifiche nel 2017 con l'emanazione di un nuovo DPCM (c.d. Decreto Gentiloni)[20], che ha delineato i nuovi assetti organizzativi dell'architettura nazionale di *cybersecurity* e ha introdotto una Strategia nazionale in materia mediante l'adozione del nuovo Piano Nazionale[21], che aggiorna i provvedimenti del dicembre 2013.

Per il primo intervento di rango primario, invece, si è dovuto attendere il 2018, con l'emanazione del d.lgs. 65/2018 (c.d. d.lgs. NIS)[22]. Con questo atto l'Italia, in recepimento della Direttiva NIS, ha rafforzato il proprio quadro normativo in materia di *cybersecurity* attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica, oltre l'adozione di una Strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei ministri[23].

---

[19] Decreto del Presidente del Consiglio dei ministri, 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, attraverso il quale è stata delineata una prima architettura della materia fondata su due distinti documenti: il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg (ultimo accesso novembre 2023).

[20] Decreto del Presidente del Consiglio dei ministri, 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. Consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg (ultimo accesso novembre 2023).

[21] È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'adozione del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica. Consultabile al seguente indirizzo: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf (ultimo accesso novembre 2023).

[22] Convertito con modificazioni dalla legge 4 agosto 2021, n. 109.

[23] Questa Strategia è orientata alla definizione di misure che riguardano la preparazione, risposta e recupero dei servizi a seguito di incidenti informatici. Essa comprende la formulazione di un piano di valutazione dei rischi informatici e l'implementazione di programmi volti a fornire formazione e sensibilizzazione nel campo della sicurezza informatica. Parallelamente, è previsto un piano complessivo di valutazione dei rischi che include anche l'ambito della ricerca e dello sviluppo nel contesto della cybersicurezza.

Al d.lgs. NIS ha fatto seguito il d.l. 21 settembre 2019, n. 105[24] che ha definito il Perimetro di sicurezza nazionale cibernetica [24] al fine di garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi informatici delle amministrazioni pubbliche nonché degli enti e degli operatori sia pubblici che privati.

Sul piano del diritto, pertanto, si riscontra una continua evoluzione della cornice normativa, a cui si aggiungono il d.l. 14 giugno 2021, n. 82[25] e alcuni specifici commi della l. n. 197/2022[26].

Il d.l. 14 giugno 2021, n. 82 mira a rafforzare le misure a tutela della sicurezza mediante l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), il Comitato interministeriale per la cybersicurezza (CIC) e il Nucleo per la cybersicurezza, al quale è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri in materia di prevenzione di eventuali crisi o attacchi *cyber.* L'ACN assume la responsabilità di tutelare la sicurezza nazionale, inclusa quella nello spazio cibernetico, e dispone di funzioni di coordinamento tra le altre Autorità competenti nel settore e di predisposizione della Strategia nazionale di cybersicurezza. Al CIC sono attribuite funzioni di sorveglianza sull'attuazione della suddetta Strategia e di supporto alle politiche della Presidenza del Consiglio dei ministri nell'ambito del Perimetro di sicurezza. Infine, al Nucleo per la cybersicurezza è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri nella prevenzione di eventuali crisi o attacchi *cyber.*
I commi da 899 a 902 della legge n. 197/2022 danno attuazione alla Strategia nazionale di cybersicurezza, formalmente adottata mediante DPCM in data 17 maggio 2022, e rendono effettivo il relativo piano di implementazione istituendo nel bilancio del Ministero dell'Economia e delle Finanze specifici Fondi.

Nella prospettiva di garantire infrastrutture tecnologiche adeguate alle sfide emergenti dalla digitalizzazione, la cybersicurezza assume un ruolo fondamentale anche all'interno del Piano Nazionale di Ripresa e Resilienza (PNRR)[27], specie nella Missione 1 incentrata sulla "Digitalizzazione, innovazione, competitività, cultura e turismo"[28]. La *cybersecurity*, infatti, costituisce, di fatto, la

[24] Convertito con modificazioni dalla legge 18 novembre 2019, n. 133.
[25] Convertito con modificazioni dalla legge 4 agosto 2021, n. 109. Il testo della legge è consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/SG (ultimo accesso novembre 2023).
[26] Legge 29 dicembre 2022, n. 197, Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025, commi da 899 a 902. Al fine di implementare la Strategia nazionale di cybersicurezza, formalmente adottata mediante decreto del Presidente del Consiglio dei ministri in data 17 maggio 2022, e per concretizzare il relativo piano di implementazione, sono stati istituiti nel bilancio specifici Fondi.
[27] Trasmesso alla Commissione europea il 30 aprile 2021.
[28] Le iniziative in corso e quelle attuate comprendono l'investimento specifico sulla cibersicurezza (M1C1), la M1C1-5 per l'istituzione dell'Agenzia per la cybersicurezza nazionale e l'adozione del relativo regolamento (MITD).
Le attuali iniziative e quelle già attutate comprendono un investimento specifico in cybersecurity (M1C1, investimento 1.5). Inoltre, sono in corso di attuazione interventi quali la transizione verso l'ambiente cloud, l'integrazione di servizi digitali come pagoPA, le attività rivolte alla cibersicurezza e quelle volte allo sviluppo delle competenze digitali (M1C1, investimenti 1.1, 1.2, 1.7).

prima delle sei missioni delineate nel PNRR e ad essa sono pertanto destinate ingenti risorse finanziarie. Per il perseguimento degli obiettivi di digitalizzazione, il PNRR destina un importo pari a 40,29 miliardi di euro, corrispondenti a circa il 21,05% dell'importo totale del Piano. In particolare, nella sezione "Digitalizzazione, innovazione e sicurezza nella PA", è previsto un investimento specifico dedicato alla cybersicurezza pari a 623 milioni di euro, con cui viene sottolineata la necessità di incrementare le capacità *cyber* nazionali anzitutto attraverso la piena attuazione della disciplina in materia di Perimetro di sicurezza nazionale cibernetica. Questi finanziamenti sono indirizzati a quattro aree di intervento: al rafforzamento delle capacità di prevenzione dagli attacchi informatici e della gestione degli allarmi, allo sviluppo di più avanzate capacità tecniche di valutazione per un'erogazione dei servizi sempre più sicura, nonché all'aumento del personale dedicato alla prevenzione e all'indagine del crimine informatico.
Dal quadro normativo nazionale richiamato, emerge una progressiva tendenza dell'ordinamento italiano verso un approccio sempre più incisivo in materia di cybersicurezza, in linea con la cornice eurounitaria.

Data la complessità intrinseca del panorama offerto dalla *cybersecurity* si rivela essenziale, in punto di attuazione che i legislatori – prima europeo e poi nazionale – intervengano attraverso forme di regolazione efficaci ma soprattutto flessibili, in grado cioè di adattarsi ai rapidi progressi tecnologici. Tuttavia, la continua proliferazione di norme rischia di generare un quadro normativo intricato e variegato che, oltre a non facilitare una lettura unitaria degli obblighi e dei doveri, determina una disparità di livelli di cyber-resilienza tra gli Stati membri.

In tale scenario, l'elaborazione della Strategia europea dovrebbe favorire e promuovere, nel tentativo di stabilire principi e regole comuni e condivise, un maggior coordinamento tra gli Stati membri e garantire così un funzionamento più efficiente del mercato attraverso la creazione di un *framework* di cybersicurezza coerente e uniforme.

4. Il ruolo del fattore umano

In conclusione occorrerà ricondurre l'attenzione al "fattore umano".

Non vi sarà mai un sistema tecnico così perfetto o una regolazione talmente efficace da poter sostituire la responsabilità umana nell'uso della tecnologia.

Invero, nel settore della *cybersecurity* alla centralità assunta dalla tecnologia deve necessariamente affiancarsi il ruolo del fattore umano. Occorre ricordare, infatti, che la questione della sicurezza informatica coinvolge anzitutto i comportamenti delle persone e, di conseguenza, richiede un adeguato livello di conoscenza e di consapevolezza che dovrebbe caratterizzare l'agire umano nel mondo digitale. Il primo elemento che ci espone a un possibile uso criminale delle tecnologie è proprio rappresentato dall'ignoranza spesso impieghiamo questi strumenti. La diffusa consuetudine nell'utilizzo dei sistemi informatici, infatti, non implica automaticamente la conoscenza dei rischi e delle vulnerabilità ad essi associati [25]. È proprio in ragione di questa scarsa consapevolezza dei rischi e della

conseguente fragilità nelle difese che l'utente finale rappresenta un appetibile punto di accesso per gli attacchi informatici. L'attacco alla Regione Lazio che abbiamo esaminato costituisce un esempio che mette in luce in maniera inequivocabile come i comportamenti umani rivestano un ruolo cruciale nel determinare l'esito di un'aggressione, specialmente laddove siano impiegate tecniche di *phishing* per inoculare *malwares* nei sistemi informatici. Dal caso appena citato emerge chiaramente che gli elementi che possono compromettere la sicurezza informatica di un sistema sono, da un lato, gli stessi strumenti informatici, i quali possono manifestare vulnerabilità connesse alla loro infrastruttura o al loro funzionamento, e, dall'altro, l'errato o inconsapevole uso umano di tali strumenti.

Il fattore umano spesso rappresenta addirittura l'elemento determinante del successo dell'attacco informatico. A titolo esemplificativo, si possono considerare i risultati emersi dallo studio condotto nel quadro del progetto europeo Dogana [26][29]. Questi dati indicano che solo nel 3% dei casi il successo degli attacchi informatici può essere attribuito a vulnerabilità di natura tecnica, mentre nel restante 97%, l'esito positivo non è tanto correlato a falle nei sistemi informatici, quanto piuttosto alla fragilità e all'ingenuità delle persone (*social engineering*[30]). Il motivo per cui gli utenti risultano spesso bersagli o mezzi attraverso i quali sferrare gli attacchi informatici può essere attribuito alla facilità con cui possono essere ingannati e indotti a compiere azioni che, in modo inconsapevole, agevolano il successo dell'aggressione. Questo rischio sarebbe notevolmente ridotto se ciascun fruitore sviluppasse una maggiore consapevolezza e una più acuta percezione delle minacce che quotidianamente è possibile incontrare in rete.

Alcune buone pratiche attraverso le quali potremmo contribuire personalmente alla sicurezza dei nostri dati e alla tutela del nostro supporto informatico potrebbero essere, per citarne alcune: l'impiego di procedure di autenticazione robuste, l'implementazione di codici di accesso complessi, la configurazione di parametri di autorizzazione restrittivi, l'adozione di un sistema di *backup* e l'installazione di *antivirus* e *firewall*.

La mancata adozione di precauzioni elementari può essere imputata alla combinazione di diversi fattori, fra i quali spicca l'insufficiente educazione digitale, ossia l'assenza di adeguate competenze digitali di base. Per mitigare l'incidenza del fattore umano sui rischi associati alla *cybersecurity* è quindi essenziale investire nella alfabetizzazione digitale e nella formazione delle persone. Per raggiungere tale obiettivo è indispensabile sottolineare e riconoscere che il dominio della sicurezza informatica non può essere esclusivamente ancorato

[29] L'autore, Pier Luca Montessoro, a pp. 791-794, durante l'analisi del ruolo fattore umano nella *cybersecurity*, cita lo studio svolto nell'ambito del progetto Dogana.
[30] Basti pensi agli attacchi realizzati attraverso la tecnica del *phishing* e al fenomeno crescente detto *man-in-the-mail*, trattasi di una sofisticata manovra di attacco informatico in cui un individuo si insinua fraudolentemente nei trasferimenti di dati tra due parti, acquisendo, in modo clandestino, le informazioni tra le due parti al fine di accedere a informazioni riservate della vittima.

all'ambito tecnico, vale a dire ai vincoli normativi, ma richiede altresì un'indispensabile assunzione di consapevolezza proattiva in merito ai rischi connessi all'uso degli strumenti informatici. Questa epifania non deve limitarsi alla mera adozione di pratiche elementari di precauzione digitale e buone consuetudini di sicurezza informatica, ma deve estendersi anche all'allocazione di risorse verso programmi e iniziative finalizzate a promuovere una maggiore sensibilizzazione verso la cybersicurezza e a fornire agli utenti una formazione adeguata su come affrontare le minacce riscontrabili online.

5. Conclusione: rispetto delle regole e maggiore pedagogia digitale

L'esponenziale utilizzo di strumenti informatici, l'incessante evoluzione digitale, la crescente interconnessione e l'innegabile aumento degli attacchi cibernetici hanno rappresentato e rappresentano il cuore del dibattito in materia di *cybersecurity*.

Come è stato osservato la regolazione di questo settore e la necessità di affrontare l'incidenza del fattore umano sono questioni complesse e sfidanti. Da un lato perché la natura mutevole della tecnologia richiede una regolazione flessibile e adattabile; dall'altro perché, nonostante la predisposizione di regole e i continui progressi tecnologici, le azioni umane spesso continuano a compromettere la sicurezza delle infrastrutture. Il dato su questo punto è, per certi versi, sconfortante. Secondo l'indice DESI (*Digital Economy and Society Index*)[31] del 2022, basato sui dati dell'anno 2021, l'Italia, con riferimento alle competenze digitali di base, si colloca al 25° posto su 27 Stati membri dell'UE.
Parallelamente alla necessità di un impianto normativo robusto diventa, dunque, indispensabile l'elaborazione di programmi di educazione e formazione digitale, poiché altrimenti nessuna regola, per quanto rigorosa, potrà mai garantire la sicurezza se gli utenti non raggiungono un sufficiente grado di consapevolezza delle minacce informatiche.

Bibliografia

[1] Wiener, N. (1948). Cybernetics or Control and Communication in the Animal and the Machine. Cambridge.

Simoncini, A. (2019). "L'algoritmo incostituzionale: intelligenza artificiale il futuro della libertà", in BioLawJournal, 1, pp. 63 ss.; Frosini, V. (1968). Cibernetica e diritto. Edizioni di Comunità.

[31] Il Digital Economy and Society Index è uno strumento utilizzato dall'Unione Europea per valutare e confrontare il grado di digitalizzazione dei paesi membri in vari settori, tra cui l'educazione digitale. Questo indice considera diversi parametri, tra cui la connettività, le competenze digitali, l'uso di internet e servizi pubblici digitali. Il testo del 2022 è consultabile al seguente indirizzo: https://digital-strategy.ec.europa.eu/it/policies/desi (ultimo accesso novembre 2023).

[2] Micklitz, H.W., Pollicino, O., Reichman, A., Simoncini, A., Sartor, G., De Gregorio, G. (2021). Constitutional Challenges in the Algorithmic Society. Cambridge University Press.

[3] Floridi, L. (2015). The onlife Manifesto: Being Human in a Hyperconnected Era. Springer.

[4] Simoncini, A. (2021). "L'uso delle tecnologie nella pandemia e le nuove diseguaglianze", in Violante, L. e Pajano, A. Biopolitica, pandemia e democrazia. Rule of law nella società digitale. Il Mulino, pp. 225 ss.

[5] Resta, G. (2015). "La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE", in Diritto dell'informazione e dell'informatica, 4-5, pp. 697 ss.

Ziccardi, G. (2015). Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica. Giuffrè.

Rodotà, S. (1982). "Tecnologie dell'informazione e frontiere del sistema socio-politico", in Pol. dir., pp. 28 ss.

Rodotà, S. (1973). Elaboratori elettronici e controllo sociale, Il Mulino.

[6] Ziccardi, G.; Perri, P. (2019). Tecnologia e diritto (vol. III). Sorveglianza, segreto, controllo, cybersecurity, crimini informatici, cyberterrorismo, guerra dell'informazione, odio online. Giuffrè.

Ziccardi, G. (2015) Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica. Raffaello Cortina.

[7] De Vergottini, G. (2019). "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normatizzata", in Rivista AIC, 4, pp. 65 ss.

[8] Finocchiaro, G. (2012). Privacy e protezione dei dati personali. Zanichelli.

Busia, G.; Liguori, L.; Pollicino, O. (2016). Le nuove frontiere della privacy nella tecnologia digitale. Aracne.

Zeno-Zencovich, V. (2018). "Data protection in the Internet", in Annuario di diritto comparato e di studi legislativi, pp. 431 ss.

[9] Brandeis, L.; Warren, S. (1890). "The Right to Privacy", in Harvard Law Review, pp. 193 ss.

Rodotà, S. (1973). Elaboratori elettronici e controllo sociale, Bologna, pp. 78 ss.

Rodotà, S. (1982). "Tecnologie dell'informazione e frontiere del sistema socio-politico", in Pol. dir., pp. 28 ss.

[10] Porcedda, M.G. (2023). Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, Oxford.

[11] Maurino, M. (2023). "Cybersecurity, sicurezza nazionale e trattamento dei dati personali", in Ursi, R., La sicurezza nel cyberspazio, Franco Angeli, pp. 169 ss.

[12] Orofino, M. (2022). "Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione", in MediaLaws, 2, pp. 82 ss.

Brighi, R. (2021). “Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati”, in Casadei, T.; Pietropaoli, S., Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, CEDAM, pp. 135 ss.

[13] Busia, G. (2020). “Cybersecurity: una sfida per tutti”, in A. Contaldo, D. Mula, Pisa, Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche, pp. IX-XVI.

[14] Simoncini, A. (2019). “L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà”, in BioLawJournal, pp. 87 ss.

[15] Bruno, B. (2020). “La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell’Unione Europea”, in Federalismi.it, 14, pp. 11 ss.

[16] Pietropaoli, S. (2022). Informatica criminale. Diritto e sicurezza nell’era digitale. Giappichelli.

[17] Longo, E.; (in corso di pubblicazione). “La sicurezza nel ciberspazio. La disciplina della cybersecurity nell’Unione europea e in Italia”.

Cassano, G.; Iaselli, M.; Spangher, G.; (2022). “Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo”, in Dir. internet, 4, pp. 637 ss.

Renzi, A. (2021). “La sicurezza cibernetica: lo stato dell’arte”, in Giorn. di dir. amm., 4, pp. 538 ss.

[18] De Gregorio, G.; Dunn, P.; (2022) “The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age”, in Common Market Law Review, pp. 473 ss.

[19] Maglio, M. (2017), “Cybersecurity e dati personali”, in Maglio, M.; Polini, M.; Tilli, N.; Manuale di diritto alla protezione dei dati personali, pp. 719 ss.

[20] Cencetti, C. (2014). “Cybersecurity: Unione europea e Italia. Prospettive a confronto”. Edizioni Nuova Cultura.

Contaldo, A.; Peluso, F. (2018). “Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS”. Pacini Editore.

[21] Salandri, L.; Contaldo, A. (2016) “La nuova disciplina giuridica cd. “orizzontale” della cybersicurezza per le infrastrutture in un’ottica di sviluppo dei sistemi”, in Rivista amministrativa della Repubblica Italiana, 11-12, pp. 567 ss.

[22] Chiara, P.G. (2023). “Il “Cyber Resilience Act”: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali”, in Riv. it. inf. dir., 1, pp. 143 ss.

[23] Bavetta, F. (2023). “Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo”, in MediaLaws. Rivista di diritto dei media, 3, pp. 405 ss.

[24] Poletti, S. (2023). “La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica”, in MediaLaw, Rivista di diritto dei media, 2, pp. 398 ss.

Mele, S. (2020). “Il Perimetro di Sicurezza Nazionale Cibernetica”, in Diritto di internet, 1, pp. 15 ss.

[25] Montessoro, P. L. (2019). “Cybersecurity: conoscenza e consapevolezza come prerequisiti per l’amministrazione digitale”, in Istituzioni del federalismo, 3, pp. 783 ss.

BIOGRAFIE

Andrea Simoncini è professore ordinario di Diritto costituzionale presso l’Università degli Studi di Firenze dove ha ricoperto anche il ruolo di Direttore del Dipartimento di Scienze giuridiche. I suoi principali interessi di ricerca spaziano dai temi legati al diritto costituzionale italiano ed europeo alle fonti del diritto, al rapporto tra tecnologia e diritti costituzionali, al diritto ambientale, i diritti sociali e le relazioni tra il diritto naturale e il diritto positivo. È membro del comitato scientifico della Fondazione Security and Rights in the Cyberspace (SERICS) nonché Principal Investigator del progetto Law and regulation for a better-safe Cyberspace (CYBERIGHTS).

E-mail: andrea.simoncini@unifi.it

Federica Camisa è dottoranda di ricerca in Diritto pubblico presso l’Università degli Studi di Firenze e abilitata all’esercizio della professione forense. Ha frequentato il Seminario di Studi e Ricerche Parlamentari “Silvano Tosi” a seguito del quale ha svolto uno *stage* presso la Presidenza del Consiglio dei ministri. Le sue ricerche sono principalmente rivolte all’analisi del rapporto tra diritto e nuove tecnologie ed è attualmente impegnata nello studio delle interconnessioni tra ambiente e tecnologia. Si interessa inoltre di cybersecurity, privacy e Metaverso.

E-mail: federica.camisa@unifi.it

Formazione in cybersicurezza: sfide e opportunità

Paolo Atzeni, Bernardo Palazzi

Sommario

L'articolo affronta la carenza a livello nazionale ed europeo di professionisti qualificati in cybersicurezza sia da un punto di vista quantitativo che qualitativo, con particolare enfasi sulla necessità di attrarre più studenti e ridurre il divario di genere.

I principali temi trattati nell'articolo includono la necessità di integrare conoscenze tecniche e organizzative in cybersicurezza, il ruolo delle certificazioni professionali e la formazione continua nel contesto lavorativo. Si sottolinea, inoltre, l'importanza di un approccio "cybersecurity by design" e la formazione mirata per diverse figure professionali. Viene discussa la distinzione tra formazione formale, non formale e informale, e vengono esplorati i contesti specifici dell'istruzione scolastica e universitaria, compresi i programmi di Master e i percorsi di dottorato.

L'articolo si conclude evidenziando l'importanza di una collaborazione tra università, industria e settore pubblico per sviluppare un ecosistema di formazione in cybersicurezza per rispondere in modo efficace alle esigenze di un mercato del lavoro in rapida evoluzione.

Abstract

This article addresses the Italian and European shortage of qualified cybersecurity professionals from a quantitative and qualitative perspective, emphasizing the need to attract more students and reduce the gender gap.

Key themes discussed in the article include the necessity of integrating technical and organizational knowledge in cybersecurity, the role of professional certifications, and ongoing training in the work context. The article highlights the importance of a "cybersecurity by design" approach and of targeted training for different professional figures. It discusses the distinction between formal, non-formal, and informal education and explores specific contexts of school and university education, including Master's programs and doctoral pathways.

The article concludes by emphasizing the importance of collaboration between universities, industry, and the public sector to develop a cybersecurity training ecosystem to effectively meet the needs of a rapidly evolving job market.

Keywords: Cybersecurity, cyber-skills, academic programs, continuing education

1. Introduzione

Il tema della limitata disponibilità di risorse umane qualificate nel contesto della cybersicurezza è indiscutibile, come spesso succede nelle aree di recente costituzione e con rapida evoluzione. Una recentissima Comunicazione[1] della Commissione Europea (al Parlamento e al Consiglio Europeo), che ha affrontato l'argomento, proponendo alcune iniziative di coordinamento, ha indicato (sulla base di fonti autorevoli[2]) una carenza di professionisti quantificata in diverse centinaia di migliaia, rispetto a una forza lavoro di circa un milione di unità, e ha anche ribadito un significativo divario di genere. Un rapporto di ENISA, l'agenzia europea per la cybersecurity,[3] oltre a citare numeri diversi ma comunque grandi, sottolinea due facce del problema, l'una di natura quantitativa e l'altra qualitativa: da una parte una carenza di competenze ("skill shortage"), cioè la disponibilità di persone qualificate in numero significativamente inferiore rispetto alle esigenze del mercato del lavoro, e dall'altra un divario di competenze ("skill gap"), cioè la presenza di persone che, impiegate nel settore o apparentemente disponibili sul mercato, non hanno competenze adeguate alle effettive esigenze di posizioni ricoperte o da ricoprire.

Per quanto riguarda l'Italia, non sono noti studi specifici relativi al settore della cybersicurezza, ma sono disponibili analisi che riguardano l'intero settore informatico, per il quale recenti documenti[4] hanno rilevato la carenza di competenze della forza lavoro nel settore, sia dal punto di vista operativo (le cosiddette competenze digitali di base), sia dal punto di vista specialistico, confrontate con le significative richieste, non soddisfatte, da parte del mercato del lavoro.

L'Agenzia per la Cybersicurezza Nazionale (ACN), nella Strategia Nazionale di Cybersicurezza,[5] ha individuato la formazione e la promozione della cultura della

---

[1] "Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')" https://ec.europa.eu/newsroom/dae/redirection/document/95048 COM(2023) 207 final, 10/04/2023

[2] (ISC)² in https://www.isc2.org/research e European Cyber Security Organisation (ECSO), come affermato nella Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final

[3] Si veda il documento seguente e in particolare la discussione (e le note) alle pagine 5 e 6: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport

[4] Il più significativo, per quanto riguarda il "capitale umano," è il rapporto della Commissione Europea noto come DESI 2022 (Digital Economy and Society Index) https://ec.europa.eu/newsroom/dae/redirection/document/88751 riorganizzato nel 2023 nell'ambito del rapporto sul Decennio Digitale https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts
Altri documenti, fra cui un recente rapporto pubblicato da Anitec-Assinform, segnalano la dimensione delle richieste da parte del mercato del lavoro: https://www.anitec-assinform.it/kdocs/2064212/positioning_paper_competenze_15112022.pdf

[5] La Strategia Nazionale è stata predisposta dall'ACN e adottata dal Presidente del Consiglio nel maggio 2022. Essa è costituita dal documento strategico, da un piano di implementazione e da un manuale operativo: https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza

sicurezza cibernetica (insieme alla cooperazione internazionale) come fattore abilitante per il perseguimento degli obiettivi fondamentali di protezione degli asset strategici nazionali, di risposta alle minacce, agli incidenti e alle crisi cyber nazionali, e di sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività. L'esigenza fondamentale, correlata agli obiettivi di protezione, risposta e sviluppo, viene sintetizzata nel modo seguente: "stimolare la creazione di una solida forza lavoro nazionale, [...] in possesso delle capacità e delle competenze necessarie per essere applicate a beneficio delle imprese e delle amministrazioni italiane, con riferimento alle tecnologie informatiche in generale e a quelle relative alla sicurezza cibernetica in particolare."

Dalle considerazioni precedenti emerge la necessità di promuovere il settore della cybersicurezza, per fare crescere le dimensioni della forza lavoro competente. Un recente documento del progetto REWIRE[6] suggerisce una serie di azioni al riguardo:

- attrarre potenziali studenti, promuovendo la cybersicurezza come possibile area lavorativa ed enfatizzando le relative opportunità;
- operare per la riduzione del divario di genere, aumentando quindi l'insieme dei potenziali candidati;
- fornire a tutti gli interessati informazioni affidabili e aggiornate;
- far interagire fra loro le parti interessate: studenti, istituzioni formative, datori di lavoro pubblici e privati.

La promozione delle attività richiede una comprensione degli obiettivi da perseguire, delle conoscenze e competenze che risultano necessarie e dei percorsi formativi che possono essere sviluppati. Questo articolo approfondisce le diverse problematiche della formazione nel settore della cybersicurezza, con un approccio che cerca di essere il più possibile articolato, perché è necessario fare riferimento a livelli diversi in termini di profondità e specificità delle tematiche e di contesti nei quali la formazione stessa si svolge, quali la scuola, l'università e il mondo del lavoro.
Il resto di questo articolo è organizzato nel modo seguente. Nel paragrafo 2 viene sviluppata una riflessione su quali debbano essere i grandi temi rilevanti per la formazione in cybersicurezza, argomentando da una parte sulla compresenza di tematiche tecniche di natura soprattutto informatica e di tematiche organizzative e normative. Dall'altra sulla necessità di considerare gli aspetti trasversali che correlano la cybersicurezza con le varie aree professionali e applicative. Nel paragrafo 3 indichiamo, con una breve analisi, le fonti principali di riferimento per i contenuti dei percorsi di formazione. Nel paragrafo 4 discutiamo ad alto livello i differenti contesti di formazione: formale, non formale e informale. Poi nel paragrafo 5 illustriamo i percorsi formali, in ambito scolastico e universitario; nel paragrafo 6 discutiamo le problematiche relative ai percorsi che si svolgono nel

[6] The project Cybersecurity Skills Alliance – A New Vision for Europe, https://rewireproject.eu/deliverables

contesto del mondo lavorativo, in fase di ingresso o in itinere. Infine, nel paragrafo 7 concludiamo le nostre riflessioni.

2. Cybersicurezza, informatica e aspetti trasversali

In questo paragrafo ragioniamo brevemente su quali siano le tematiche da prendere in considerazione ai fini di una discussione sulla formazione in cybersicurezza. In effetti, i confini delle aree di interesse non sono semplici da definire, per vari motivi.

Prima di tutto, vale la pena ricordare che il campo stesso della cybersicurezza è in continua e rapida evoluzione, e quindi qualunque riflessione sui contenuti deve essere formulata con la consapevolezza che potrebbe essere in breve tempo sottoposta a revisione.

Più in generale, è importante osservare che la cybersicurezza ha diverse anime. Da una parte essa presenta aspetti tecnologici, che sono strettamente correlati alle metodologie e alle tecnologie informatiche e, di conseguenza, non possono essere affrontati senza un'adeguata base di conoscenze e competenze appunto nel settore informatico. In effetti, la maggior parte delle tematiche tecnologiche di cybersicurezza possono essere considerate come parte dell'informatica, o comunque hanno l'informatica come prerequisito. Al tempo stesso, la cybersicurezza comprende aspetti di natura organizzativa, amministrativa o di conformità a norme e regolamenti o a politiche aziendali, che sono solo indirettamente legati a problematiche tecnologiche. Infatti, con l'aumentare della pervasività degli strumenti digitali e con il loro utilizzo anche in settori strettamente regolamentati, questi aspetti stanno diventando sempre più importanti. Le due anime, pur diverse come caratteristiche fondamentali, sono complementari e non separate: si può senz'altro dire che gli esperti tecnologici di cybersicurezza debbono comunque avere competenze normative e organizzative e, al tempo stesso, gli esperti di politiche della sicurezza possono non essere esperti dal punto di vista tecnologico, ma debbono certamente avere le competenze per poter interagire con gli esperti tecnologici. In altre parole, pur in presenza delle due anime sopra citate, ogni esperto di cybersicurezza deve avere competenze di ciascuno dei due tipi: non esiste un esperto puramente tecnologico né un esperto solo di politiche della sicurezza.

La trasversalità e l'importanza dell'interazione fra specialisti con competenze diverse sono rilevanti anche da un altro punto di vista. I sistemi informatici vengono di solito realizzati per rispondere alle esigenze di specifici domini applicativi e quindi molto spesso è necessario che gli specialisti informatici interagiscano con quelli del dominio applicativo e siano in grado di comprenderne le esigenze, mentre gli specialisti del dominio applicativo (di solito i committenti dei sistemi) debbono essere in grado di comprendere i benefici che possono derivare dai sistemi informatici. Analogamente, la cybersicurezza è un'esigenza per tutte le organizzazioni, in ogni dominio applicativo, e anche qui si pone la necessità di interazione fra specialisti e non specialisti. In particolare, viene spesso enfatizzata la necessità di applicare un approccio denominato

"cybersecurity by design" (cybersicurezza fin dalla fase di progettazione), che mira a considerare la sicurezza come requisito fondamentale fin dalla genesi di ogni sistema, piuttosto che come misura aggiuntiva. Questo concetto si basa sull'idea che prevenire le vulnerabilità e proteggere gli asset dell'organizzazione sin dall'inizio sia molto più efficace e meno costoso rispetto alla gestione dei problemi di sicurezza dopo che un sistema è stato già implementato. Quindi, la riflessione sulla formazione deve riguardare non solo lo stretto rapporto che esiste fra la cybersicurezza e le tecnologie di base, soprattutto informatiche, ma anche e soprattutto le modalità secondo cui la formazione in cybersicurezza si rivolge a soggetti che, con responsabilità di livello diverso, da quello operativo a quello dirigenziale, non hanno comunque le tecnologie come oggetto principale delle attività e competenze. E' importante sottolineare che, a livello manageriale, la cybersicurezza va considerata un tema cruciale, perché si tratta di un aspetto che, pur potendo essere delegato nella pratica operativa, rimane sostanzialmente (e anche giuridicamente) nella responsabilità della dirigenza; si usa infatti spesso l'affermazione "la cybersicurezza non è delegabile." Questo è anche dovuto all'introduzione di specifiche prescrizioni normative e regolamentari in molti contesti, sia pubblici sia privati.

Vale la pena aggiungere poi che la trasversalità ha, sia nel contesto della cybersicurezza sia in quello più ampio delle tecnologie informatiche, un livello operativo, connesso ad attività di routine. Nel caso dell'informatica si parla spesso delle cosiddette "competenze digitali di base," relative all'accesso a Internet, all'utilizzo di servizi digitali della pubblica amministrazione, oppure bancari o di commercio elettronico, o di posta elettronica o di strumenti di produttività individuale. Nel caso della cybersicurezza, questo livello fa riferimento alla consapevolezza ("awareness") e all'uso sicuro delle tecnologie, per motivi lavorativi o personali. Infatti, il termine "cyber hygiene" sta diventando sempre più comune per indicare le misure basilari che ogni utente di sistemi digitali dovrebbe conoscere e seguire. La metafora con il mondo sanitario, semplificata dall'utilizzo del termine "igiene", aiuta a comunicare che il mondo digitale presenta rischi che possono essere mitigati con semplici misure preventive, simili al lavaggio delle mani nel mondo reale. Un esempio è l'importanza di effettuare regolarmente gli aggiornamenti di sicurezza forniti dai produttori del software.

Le correlazioni sopra citate, in particolare quella tecnica ma anche quella legata alle competenze operative, fanno sì che la promozione iniziale delle discipline, fra i giovani, soprattutto nella scuola in termini di orientamento, possa essere svolta in forma coordinata e parallela, coprendo entrambe, magari con una prevalenza dell'una o dell'altra a seconda dei casi. Nel prosieguo dell'articolo faremo solo qualche accenno alle problematiche relative alla consapevolezza, concentrandoci sugli aspetti specialistici e di governo.

Concludiamo segnalando che le tematiche di cybersicurezza presentano specificità riconducibili a due dimensioni principali. Da una parte, vi sono quelle relative ai singoli paesi, in particolare per via delle normative e delle prassi. Dall'altra, la varietà dei settori applicativi interessati dalla cybersicurezza richiede attenzioni mirate ai vari casi, si pensi ad esempio al settore finanziario o a quello

delle infrastrutture critiche. Per evidenti ragioni di spazio, nel prosieguo di questo articolo non entreremo nel dettaglio né riguardo agli aspetti locali né riguardo alle specificità dei domini applicativi.

3. Conoscenze, competenze e contenuti di formazione: possibile quadro di riferimento

L'analisi delle competenze e delle relative esigenze formative nell'ambito della cybersicurezza risulta particolarmente complessa poiché esistono numerosi ruoli e figure professionali nei diversi contesti lavorativi, che sono eterogenei tra di loro e rapidamente variabili nel tempo.

Le aree di interesse per la cybersicurezza sono molteplici e trasversali a praticamente tutti i settori legati alla digitalizzazione. Da diversi anni sono in corso proposte e progetti di analisi e catalogazione delle aree da parte di varie organizzazioni a livello europeo e internazionale e numerosi progetti, che presentano punti di vista diversi, enfatizzando da una parte i contenuti e dall'altra gli obiettivi formativi e i conseguenti ruoli professionali. I criteri di classificazione e i confini delle aree stesse sono diversi nei vari contesti e in questo articolo non abbiamo l'ambizione né di fornire nuove definizioni né di adottarne una rispetto alle altre. Riteniamo però importante indicare e presentare brevemente alcune fonti.

Il *Cyber Security Body Of Knowledge (CyBOK)* è un catalogo sviluppato dal National Cyber Security Center (NCSC) del Regno Unito, disponibile liberamente e considerato fra i più completi in ambito cybersicurezza. Copre una vasta gamma di argomenti, dalle fondamenta teoriche agli aspetti tecnici e normativi. Il CyBOK fornisce un quadro approfondito per la formazione e lo sviluppo di professionisti della sicurezza informatica.

Le *ACM/IEEE Cybersecurity Curricular Guidelines CSEC 2017* sono state sviluppate da un gruppo di lavoro congiunto della ACM (Association for Computing Machinery) e della IEEE (Institute of Electrical and Electronics Engineers) allo scopo di fornire un quadro per la progettazione di programmi di studio di corsi di livello post secondario e aiutano a definire le competenze essenziali che gli studenti dovrebbero acquisire per le professioni disponibili in questo settore.

Il *NIST National Initiative for Cybersecurity Education (NICE) Framework* descrive le competenze, le conoscenze e le abilità necessarie per svolgere le diverse funzioni all'interno del settore della sicurezza informatica. È stato sviluppato dal National Institute of Standards and Technology (NIST) degli Stati Uniti ed è ampiamente utilizzato da organizzazioni pubbliche, private e accademiche. Esso prevede l'identificazione delle diverse figure professionali (work role) attraverso l'utilizzo di tre differenti parametri: il primo riguarda le conoscenze (knowledge), ovvero gli argomenti che devono essere noti; il secondo riguarda le capacità (skills), ovvero gli argomenti che devono essere padroneggiati per poter effettuare azioni pratiche; e il terzo riguarda le abilità (abilities), ovvero le azioni necessarie che devono essere implementate per la messa in sicurezza dell'organizzazione. I differenti ruoli professionali sono definiti come

un'aggregazione di KSA (conoscenze, capacità e abilità), che sono parametri molto specifici e quindi numerosi. Questo approccio, sebbene comporti una notevole complessità di gestione, permette un'estrema flessibilità ed è utile per catturare l'eterogeneità dei lavori e delle funzionalità utilizzate dalle diverse organizzazioni per gestire la cybersicurezza. Inoltre, il NICE Framework aiuta a creare un linguaggio comune per la cybersecurity, che facilita la comunicazione tra le diverse parti interessate.

ENISA, la già citata Agenzia europea, ha sviluppato lo *European Cyber Security Framework (ECSF),* un quadro di riferimento per le competenze in materia di sicurezza. Esso identifica e dettaglia 12 profili professionali, ritenuti rilevanti in ambito europeo.

REWIRE, un progetto finanziato dal programma ERASMUS+ della Commissione Europea, mira a costruire (entro la conclusione prevista per il 2024) un quadro per il settore della sicurezza informatica e una strategia europea concreta per le competenze in materia di cybersicurezza. Il progetto riunisce una vasta gamma di stakeholder, tra cui aziende, università, enti pubblici e privati, per sviluppare raccomandazioni e soluzioni sostenibili. I risultati del progetto contribuiranno a colmare il divario di competenze tra le esigenze dell'industria e l'offerta formativa disponibile e a promuovere la cooperazione tra gli stakeholder interessati.

In generale, la maggior parte delle fonti indicate ha redatto dei cataloghi che elencano in modo più o meno dettagliato gli argomenti chiave per la formazione in questo settore per facilitare l'individuazione delle competenze necessarie per le diverse attività lavorative. Tanto i cataloghi quanto i profili professionali e i percorsi di studio, ove descritti, sono diversi nelle varie proposte. Questo conferma la dinamicità del settore e fa presagire che possa manifestarsi in futuro lo sviluppo di nuove tematiche, come ad esempio quelle legate a prospettive etiche o ambientali. In ogni caso, ciascuna delle varie fonti, sia pure con bilanciamento diverso, tiene conto del fatto che la formazione in cybersicurezza deve comprendere sia aspetti tecnologici, sia aspetti organizzativi o di conformità regolamentare/normativa.

La ricchezza delle tematiche e la dinamicità del settore suggeriscono la definizione di percorsi formativi diversi, con obiettivi specifici, ciascuno dei quali può essere efficace, purché progettato in modo coerente con gli obiettivi stessi, ma al tempo stesso flessibile e modificabile anche nel breve o medio termine.

4. Contesti della formazione e articolazione dei percorsi

Questo paragrafo discute brevemente come le conoscenze e competenze discusse nel paragrafo precedente possono essere acquisite. Si usa spesso al riguardo il termine “processo di apprendimento” e si sottolinea che l’apprendimento stesso può svolgersi secondo percorsi, modalità e tempi molto diversificati. Può essere utile, allo scopo, richiamare la terminologia utilizzata in

vari documenti, ad esempio quelli dell'UNESCO[7] o del Cedefop (Centro Europeo per lo sviluppo della Formazione Professionale),[8] che distingue i contesti di apprendimento in tre categorie: formali, non formali e informali.

Per il contesto formale e quello non formale si parla di solito di *education*, termine che possiamo tradurre in italiano con "istruzione e formazione," perché ciascuna delle due parole descrive solo parzialmente una realtà che è in effetti molto articolata. Nel prosieguo utilizzeremo spesso i due termini in modo intercambiabile, preferendo "istruzione", per fare riferimento soprattutto all'ambito scolastico e "formazione" per l'ambito professionale e lavorativo. Per l'ambito universitario, useremo indifferentemente i due termini, con l'aggiunta dell'aggettivo "superiore" o "universitaria."

L'istruzione formale è strutturata e attuata da istituzioni pubbliche o enti privati riconosciuti. I programmi di istruzione formale portano all'acquisizione di qualifiche pure riconosciute.[9] Una componente molto significativa dell'istruzione formale è quella cosiddetta "iniziale", che avviene in modo continuativo e di solito a tempo pieno, prima del primo ingresso nel mondo del lavoro. Fanno parte dell'istruzione formale anche le iniziative di formazione per gli adulti, a tempo pieno o parziale, permanenti o ricorrenti, nel caso in cui siano finalizzate al conseguimento di qualifiche riconosciute da autorità pubbliche. L'istruzione formale è di solito "istituzionalizzata", cioè gestita da organizzazioni (come le scuole, le università e altri istituti di formazione) che offrono in modo strutturato un'interazione fra docenti e discenti (e anche fra i discenti). Secondo le definizioni, in particolare dell'UNESCO, la formazione svolta nel mondo del lavoro viene considerata istruzione formale se porta a qualifiche riconosciute, come nei casi precedenti.

L'istruzione non formale, come quella formale, è anch'essa strutturata, organizzata e "intenzionale" (cioè pianificata con obiettivi formativi da un soggetto gestore e responsabile). La differenza principale rispetto all'istruzione formale è nel fatto che ad essa non sono associate qualifiche formalmente riconosciute. L'istruzione non formale è quindi da considerare complementare a quella formale e può essere particolarmente efficace in un contesto di formazione permanente, anche con percorsi brevi e diluiti nel tempo. Al tempo stesso, è possibile che percorsi non formali contribuiscano, a seguito di opportune valutazioni, all'ottenimento di qualifiche formali. Molto spesso, l'istruzione non formale viene svolta nel mondo lavorativo, per iniziativa del lavoratore o del datore di lavoro,

[7] International Standard Classification of Education ISCED 2011: http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[8] Terminology of European education and training policy - A selection of 100 key terms https://www.cedefop.europa.eu/files/4064_en.pdf

[9] Il riconoscimento dei titoli può corrispondere al valore legale, come in Italia e molti paesi europei, oppure a forme di accreditamento, come nel Regno Unito o negli Stati Uniti d'America. La questione presenta profili articolati. Per una discussione, risalente ad alcuni anni fa ma, nella sostanza, ancora valida, si può consultare un dossier del Senato della Repubblica: https://www.senato.it/documenti/repository/dossier/studi/2011/Dossier_280.pdf

oppure nell'ambito di iniziative a contrasto della disoccupazione, spesso con il supporto di soggetti pubblici.

Citiamo anche il terzo ambito di apprendimento, quello informale, anche se poi non lo approfondiremo ulteriormente nel prosieguo dell'articolo. L'apprendimento informale si realizza nello svolgimento delle attività quotidiane, nel contesto lavorativo, familiare e del tempo libero. Viene anche associato al termine "learning by doing" ("imparare facendo", cioè con l'esperienza). Alcuni, ad esempio i documenti UNESCO, prevedono che l'apprendimento informale sia intenzionale, distinguendolo così da quello incidentale o casuale, che si realizza come risultato secondario di attività che non sono di per sé legate alla formazione. Spesso, però, anche queste attività vengono ricomprese nel contesto dell'apprendimento informale.

In ogni caso, poiché l'apprendimento informale deriva da attività che non sono organizzate o strutturate, non approfondiamo ulteriormente l'argomento, pur segnalando che l'apprendimento delle conoscenze e competenze relative alla cybersicurezza può essere in parte acquisito anche con l'esperienza, che può quindi talvolta parzialmente sostituire la partecipazione a iniziative formali o non formali.

A conclusione di questa sezione, prima di illustrare come le due sezioni successive approfondiscono rispettivamente l'istruzione formale e quella non formale, svolgiamo alcune riflessioni, relative alla cybersicurezza ma che valgono anche per altre aree.

La formazione ha certamente componenti e percorsi diversificati. Ogni persona segue una propria formazione iniziale, che può arrivare senza soluzione di continuità temporale fino ad un alto livello accademico (laurea magistrale o dottorato) e, in casi, che possiamo definire estremi, ma molto diffusi, la continuità si presenta anche dal punto di vista delle tematiche, negli studi e per proseguire poi anche nel contesto lavorativo, con una professione strettamente correlata alla qualificazione ottenuta. Stesso discorso può valere per percorsi di formazione più brevi, dalla qualifica professionale alla laurea di primo livello, passando per il diploma di scuola secondaria superiore e quello ITS. In molti altri casi, oggi come in passato, il percorso è più articolato, perché la formazione prosegue dopo l'ingresso nel mondo del lavoro, e questo può avvenire con continuità oppure in tempi successivi, e può avvenire con istruzione formale oppure informale. Inoltre, i temi di questa ulteriore formazione possono essere più o meno correlati con quelli della formazione iniziale.

Le osservazioni appena svolte sono valide con riferimento a molte aree accademiche, scientifiche e professionali, soprattutto per quelle giovani o in rapida evoluzione, come è il caso della cybersicurezza. In effetti, le richieste del mondo del lavoro nel settore qui trattato non sono facilmente soddisfatte dai percorsi di formazione iniziali, semplicemente perché tali percorsi sono tuttora in fase di assestamento e perché l'esigenza lavorativa non era così evidente quando coloro che completano gli studi in questo momento hanno effettuato le loro scelte. Inoltre, insieme agli specialisti effettivamente necessari in alcune situazioni, molti

contesti lavorativi richiedono anche persone con buona formazione generale, a vari livelli, scolastico o universitario, in grado di affrontare argomenti nuovi, specifici, che possono richiedere competenze acquisibili attraverso percorsi mirati. Per queste ragioni, nel settore della cybersicurezza, oltre ai percorsi formali, troviamo molte iniziative non formali che possono servire a completare la formazione o che possono essere utilizzate con l'obiettivo di far entrare nel campo della cybersicurezza persone formate in altri settori. È anche importante ricordare che, nell'ottica di una formazione permanente e ricorrente, i vari percorsi, formali e non formali, possono essere svolti anche con significativa soluzione di continuità e anche in combinazione con apprendimento informale.

Quindi, i prossimi due paragrafi sono dedicatl rispettivamente ai percorsi di apprendimento formale (e quindi ai contesti degli ITS e universitario, con un accenno alla formazione professionale formale) e non formale (soprattutto nel contesto lavorativo). I primi, come detto, si concretizzano prevalentemente come percorsi di formazione iniziale, mentre i secondi contribuiscono soprattutto alla formazione permanente e ricorrente.

5. Formazione scolastica e universitaria

Trattiamo in questo articolo soprattutto la formazione iniziale successiva al completamento della scuola secondaria superiore, ma premettiamo alcuni brevi spunti relativi a percorsi precedenti o più brevi.

Con riferimento alla cybersicurezza, non ci sono percorsi specifici nell'ambito della scuola primaria e secondaria che approfondiscano l'argomento, però è importante sottolineare che ci sono iniziative che possono avvicinare i ragazzi quantomeno al tema della sicurezza come utente, all'uso corretto e rispettoso degli strumenti informatici e alla mitigazione del cybercrime e alla prevenzione del cyberbullismo. Queste iniziative non rientrano nelle tematiche di interesse di questo articolo, ma è importante citarle perché, vista la complessità del problema, anche queste azioni possono dare un contributo importante alla prevenzione dei rischi e alla riduzione delle conseguenze degli attacchi e possono contribuire ad avvicinare i giovani alle tematiche più specifiche.

Altra iniziativa particolarmente rilevante nel mondo scolastico è quella delle competizioni di cybersicurezza, su cui non ci soffermiamo, perché sono approfondite in un altro articolo di questo numero della rivista.[10]

Un argomento molto importante che qui possiamo però trattare solo brevemente, perché non centrale, è quello dell'informatica nella scuola. Accenniamo solo a due aspetti. Da una parte, esistono in Italia da diversi decenni percorsi di informatica negli istituti tecnici industriali e in quelli commerciali, nonché alcune

[10] G. Ferraro, S. Montegiove, P. Prinetto. The Big Game: giocando si impara la cybersicurezza.

sperimentazioni nei licei scientifici. Sono iniziative molto importanti, ma coprono comunque una frazione relativamente piccola degli studenti.[11]

Sempre con riferimento alle scuole secondarie superiori, vi sono poi alcuni indirizzi che prevedono alcune ore di informatica, comunque molto poche, solitamente due, in una scuola, il liceo scientifico delle scienze applicate, che raccoglie una frazione pure limitata di studenti.[12] Questi dati, pur schematici e forse parziali, segnalano che la diffusione dell'approfondimento dell'informatica nella scuola è ancora limitata e andrebbe certamente promossa e incrementata, sia per avvicinare i giovani a carriere nel settore informatico in generale e in quello della cybersicurezza in particolare, sia perché l'informatica oggi è pervasiva e, come detto nelle sezioni precedenti, è importante per tutti avere conoscenze di base, culturali e non solo strumentali. Al riguardo, è interessante segnalare che alcuni paesi, ad esempio il Regno Unito, hanno recentemente avviato iniziative in questa direzione.[13]

Nel resto di questo paragrafo discuteremo i percorsi di formazione di interesse per la cybersicurezza successivi alla scuola secondaria del secondo grado e tratteremo quindi degli ITS e dei vari percorsi universitari.

5.1 Istituti Tecnologici Superiori (ITS Academy)

Il sistema ITS costituisce il segmento di formazione terziaria non universitaria sviluppato in forte collaborazione con il mondo produttivo. Esso è ispirato almeno in parte alle esperienze di altri paesi, che hanno molte iniziative che si collocano ad un livello intermedio fra la scuola secondaria e l'università e con molti studenti che conseguono il titolo. Come noto, le statistiche internazionali indicano per l'Italia un numero di laureati molto inferiore a quello degli altri paesi, ma in effetti la vera differenza non è tanto al livello di laurea né tantomeno di laurea magistrale, ma è legata alla dimensione limitata del segmento non universitario. Per quanto ovviamente le esperienze dei vari paesi siano diverse, notiamo che, ad esempio, la Germania, ha il sistema delle *Fachhochschulen,* che risalgono ad almeno cinquanta anni fa e hanno un numero di studenti pari a circa la metà di quelli universitari.
Il sistema degli ITS è stato definito negli anni 2006-2008[14] e riformato e sistematizzato con la legge 99/2022, che li ha denominati Istituti Tecnologici

[11] Secondo i dati pubblicati dal Ministero dell'Istruzione e del Merito, per l'anno scolastico 2021-22, https://dati.istruzione.it/opendata/opendata/catalogo/elements1/leaf/?datasetId=DS0070ALUSECGRADOINDSTA, su oltre 460 mila studenti iscritti al quinto anno delle scuole secondarie di secondo grado, circa 17mila risultavano iscritti ad un percorso tecnico tecnologico di informatica e circa 11.500 ad un percorso tecnico economico di sistemi informativi aziendali, rispettivamente quindi 3,5% e il 2,5% del totale.
[12] Nei dati sopra citati, si tratta di quasi 34mila studenti, pari a poco più del 7% degli studenti del quinto anno.
[13] Impact Report 2018-2022, National Center for Computing Education, https://static.teachcomputing.org/NCCE-Impact-report-2022.pdf
[14] La legge 631/2006, art.1 comma 361 ha disposto la riorganizzazione del sistema dell'istruzione e formazione tecnica superiore. Poi, la legge 40/2007, art. 13, comma 2, ha introdotto il termine ITS

Superiori (introducendo anche la forma breve ITS Academy) e ne ha confermato il ruolo come strumento di promozione dell'occupazione nei settori innovativi. La promozione degli ITS è anche parte degli obiettivi del Piano Nazionale di Ripresa e Resilienza, che prevede anche significativi finanziamenti, finalizzati all'incremento del numero degli ITS, e dei relativi frequentanti, con un raddoppio di frequentanti e diplomati. Ad oggi, il numero degli studenti è inferiore a 20 mila, quindi una frazione molto piccola del numero di giovani impegnati nella formazione terziaria (le università hanno attualmente oltre 1 milione 700 mila studenti, di cui circa 400 mila nelle aree tecnico scientifiche, che sono di interesse per gli ITS).

Il sistema ITS può essere molto importante per il settore della cybersicurezza, perché numerose realtà, aziende e amministrazioni, possono reclutare giovani con un titolo di studio intermedio, acquisito in tempi più brevi, con percorsi mirati e, auspicabilmente, vista la natura pratica e il coinvolgimento delle aziende, con tassi di ritardo e abbandono molto inferiori rispetto a quelli universitari. Nell'ultimo anno, sono stati effettivamente attivati diversi nuovi corsi ITS in cybersicurezza.

5.2 Formazione universitaria

Come noto, la formazione universitaria, in Italia, come in molti altri paesi, si articola su vari livelli. I principali, normati a livello nazionale, talvolta indicati come "primo, secondo e terzo ciclo", sono quelli relativi rispettivamente a laurea, laurea magistrale e dottorato di ricerca. Esistono poi altri tipi di corsi, definiti con grande autonomia dagli atenei, i più importanti dei quali, ai fini del presente documento, sono quelli di master universitario.

Discutiamo brevemente i vari livelli, cominciando da quelli quantitativamente più significativi: laurea e laurea magistrale.

5.2.1 Corsi di laurea e laurea magistrale

I corsi di laurea hanno l'obiettivo di assicurare allo studente una formazione solida, finalizzata tanto all'inserimento nel mondo lavorativo quanto alla prosecuzione degli studi.

I corsi di laurea magistrale hanno l'obiettivo di fornire una formazione avanzata e, salvo casi specifici che non interessano, hanno durata biennale e prevedono il possesso di una laurea per l'ammissione.

Si usa spesso il termine "corso di studio" per indicare genericamente un corso di laurea o di laurea magistrale. I singoli corsi di studio sono definiti in autonomia dalle università, anche nel nome, con riferimento alle classi di corsi di studio, che sono invece definite, a livello nazionale, nel nome, negli obiettivi generali e nei contenuti qualificanti. Nel processo di progettazione dei corsi di studio le università sono tenute a consultare le organizzazioni rappresentative del settore

con riferimento ad alcune delle iniziative previste dalla L.631/2006. Infine, il DPCM del 25/01/2008 ha specificato le caratteristiche degli ITS come istituzioni e alcune caratteristiche dei relativi percorsi, nonché ha definito le aree tecnologiche di interesse.

con particolare riferimento alla valutazione dei fabbisogni formativi e degli sbocchi professionali.
In termini quantitativi, è forse utile segnalare che i numeri dei titoli di studio conseguiti al primo e al secondo livello sono paragonabili: gli ultimi dati disponibili[15] indicano 208 mila laureati, 162 mila laureati magistrali. Si può notare che, in Italia (a differenza di quanto accade in altri paesi), la maggior parte degli studenti considera la laurea solo un passo intermedio verso la laurea magistrale. E si tratta spesso di corsi di studio strettamente correlati, in quanto, nel sistema italiano, l'articolazione in livelli viene recepita molto lentamente e la maggior parte degli studenti opta per un percorso in "filiera", con una magistrale strettamente correlata alla triennale.
I corsi di laurea e di laurea magistrale svolgono un ruolo essenziale nella formazione dei giovani, con contenuti e risultati che debbono contemperare una prospettiva formativa a lungo termine (in quanto nella maggior parte dei casi il percorso universitario viene seguito una volta nella vita, in età abbastanza giovane, quindi come "formazione iniziale") con obiettivi specifici volti a favorire l'inserimento nel mondo del lavoro. In effetti, è prassi comune caratterizzare le competenze complessive dei singoli con riferimento alla laurea o laurea magistrale conseguita.

Nel contesto della cybersicurezza, per quanto riguarda gli obiettivi e i contenuti, possono essere considerate varie coordinate. Una prima è quella legata alla cybersicurezza stessa: ci possono essere corsi focalizzati sulla cybersicurezza e corsi che hanno alcuni contenuti di cybersicurezza, nonché quelli intermedi, che includono significativi contenuti di cybersicurezza, insieme ad altri. Una seconda coordinata è quella relativa all'informatica (o ad altra disciplina tecnologica): la cybersicurezza può essere approfondita dal punto di vista tecnico informatico oppure da altri, ad esempio organizzativo o giuridico.

Tralasciando i corsi di studio che contengono al più elementi di consapevolezza sul tema della cybersicurezza e anche i corsi di studio che prevedono solo uno o due corsi di insegnamento sul tema, emergono alcune categorie interessanti, quali le seguenti (come in molti contesti, si possono presentare situazioni di confine, ma non è necessario approfondire questo aspetto):

- corsi di studio in cybersicurezza dal punto di vista informatico;
- corsi focalizzati sulle discipline informatiche, con un significativo contenuto di cybersicurezza (corsi in informatica o ingegneria informatica con un "indirizzo" in cybersicurezza);
- corsi di natura multidisciplinare, non strettamente tecnologica, con un significativo contenuto di cybersicurezza.

Entrando nella realtà degli Atenei italiani, pur senza fare riferimento diretto ai singoli corsi di studio, si nota che i corsi di laurea (cioè quelli di primo livello) sono molto pochi in ciascuna delle tre categorie. Probabilmente ciò accade perché si

[15] Anno accademico 2021/22, sito del Ministero http://ustat.miur.it/dati/didattica/italia/atenei

ritiene che la focalizzazione possa essere eccessiva e che sia non semplice ricondurre gli obiettivi della cybersicurezza a quelli delle classi di laurea esistenti, che sono relativamente poche e abbastanza ampie. In effetti, le poche esperienze esistenti per il primo livello sono nelle classi L-31 (Scienze e tecnologie informatiche) e L-8 (Ingegneria dell'Informazione), che hanno un respiro molto ampio e obiettivi formativi che comunque richiedono insegnamenti di molte discipline e anche molti insegnamenti in discipline informatiche diverse da quelle strettamente legate alla cybersicurezza (e spesso prerequisito per queste ultime).

Più ampie sono le esperienze (e le possibilità) a livello di laurea magistrale, per vari motivi. Da una parte, il percorso di laurea magistrale è di soli due anni, e una parte significativa del secondo anno è dedicata alla tesi e quindi è relativamente più semplice avere la disponibilità di un corpo docente sufficientemente ampio per coprire gli insegnamenti. Dall'altra, è possibile prevedere requisiti di ingresso che includano competenze informatiche tali da permettere una significativa concentrazione sulla cybersicurezza. Inoltre, fra le classi previste a livello magistrale, c'è la LM-66 (Sicurezza informatica) dedicata a corsi di studio effettivamente mirati. In ogni caso, molti atenei prevedono corsi offerti nelle classi informatiche, LM-32 (Ingegneria informatica) e LM-18 (Informatica), con ampi contenuti di cybersicurezza, che permettono di offrire un indirizzo (con almeno cinque o sei insegnamenti) dedicato ad essa. Per quanto riguarda i corsi di natura multidisciplinare, è interessante segnalare la classe LM-91 (Tecniche e metodi per la società dell'informazione) che permette di offrire percorsi che coniugano contenuti tecnologici (in particolare sono qui rilevanti quelli di cybersicurezza, oltre a quelli informatici) con contenuti di altre discipline (ad esempio giuridiche, umanistiche o economico-organizzative). L'offerta degli atenei in queste classi è abbastanza ampia, e copre le tre categorie sopra citate (corsi tecnologici mirati alla cybersicurezza, corsi informatici con contenuti di cybersicurezza e corsi multidisciplinari non tecnici con contenuti di cybersicurezza).

In molti paesi, in particolare in Francia, Regno Unito e USA, le agenzie nazionali di cybersicurezza hanno sviluppato iniziative volte a "certificare" i corsi di studio nel settore, con un approccio complementare rispetto all'accreditamento dei corsi stessi. In sostanza, l'attività di certificazione prende in esame (su proposta degli Atenei) corsi di studio che siano istituiti o accreditati secondo le prassi locali e ne valuta la pertinenza rispetto alla tematica specifica della cybersicurezza, prendendo in esame obiettivi, contenuti, corpo docente e altre risorse, nonché i risultati, inclusi la soddisfazione dei laureati e il loro inserimento nel mondo del lavoro. Queste iniziative sono motivate dal fatto che tanto gli Atenei quanto le istituzioni (ministeri o simili) che vigilano sull'offerta formativa non sempre hanno le competenze tecniche specifiche per apprezzare le iniziative in settori emergenti e di rapida evoluzione come quello della cybersicurezza e quindi l'intervento di un soggetto terzo, competente in materia, può fornire un contributo interessante alla conferma della validità e dell'appropriatezza dei corsi di studio.

5.2.2 Corsi di dottorato di ricerca

Il dottorato di ricerca è stato introdotto in Italia negli anni '80 (mentre in molti altri paesi esiste da molto tempo) con lo scopo di formazione alla ricerca, soprattutto accademica, e ha successivamente ampliato il proprio spettro con l'attenzione anche alle amministrazioni pubbliche e al mondo produttivo. I numeri del dottorato sono molto più piccoli rispetto a quelli dei corsi di studio: secondo i più recenti dati sopra citati, si hanno meno di 8 mila dottori di ricerca all'anno, rispetto ai 162 mila laureati magistrali. Va però osservato che, negli ultimi anni, sono stati emanati provvedimenti, con appositi finanziamenti, volti a incrementare il numero degli studenti di dottorato e quindi il numero di dottori di ricerca. L'ammissione ai corsi di dottorato richiede il possesso di una laurea magistrale e il superamento di un concorso per l'accesso. La durata è di almeno tre anni. Il dottorando deve elaborare una tesi originale di ricerca.

Le attività di dottorato nel settore della cybersicurezza si svolgono tanto in corsi esplicitamente mirati alla cybersicurezza, quanto in contesti più ampi, motivati questi ultimi dal fatto che spesso il numero di posti (e borse) di dottorato disponibili presso un ateneo è limitato e quindi, per giustificare un corso di dottorato è necessario fare riferimento ad un insieme ampio di discipline. I corsi di dottorato interamente dedicati alla cybersicurezza sono certamente interessanti e vanno incoraggiati e sostenuti, ma sono realizzabili solo da parte di sedi accademiche grandi (e comunque spesso consorziate) oppure nell'ambito dei corsi di dottorato di interesse nazionali, attivati secondo la normativa più recente.[16]

D'altra parte, l'aspetto più importante, che caratterizza il titolo di dottorato conseguito da uno studente è la tematica della tesi e quindi ha senso parlare di tesi di dottorato in cybersicurezza piuttosto che di corsi di dottorato in cybersicurezza. Le tesi di dottorato relative a temi di cybersicurezza, se di natura tecnologica, sono sviluppate nell'ambito di corsi di dottorato nei settori dell'informatica o dell'ingegneria informatica (o di aree più ampie che includono tali settori) oltre che ovviamente nei corsi di dottorato in cybersicurezza. Questi ultimi sono, nelle prime sperimentazioni, in particolare a livello nazionale, di ampio respiro, con riferimento tanto a discipline tecnologiche quanto ad altre discipline, quali quelle giuridiche o economico organizzative.

5.2.3 Corsi di master universitario

Nel contesto della formazione universitaria, oltre ai tre cicli fondamentali descritti in precedenza, esiste un altro tipo di iniziative interessanti, meno formalizzate a livello nazionale e quindi più flessibili. Secondo la normativa,[17] le università possono attivare *corsi di perfezionamento scientifico e di alta formazione permanente e ricorrente, successivi al conseguimento della laurea o della laurea magistrale, alla conclusione dei quali sono rilasciati i master universitari di primo e di secondo livello*. Nella terminologia ormai diffusa, si usa per queste iniziative

[16] DM 226/2021, art.11
[17] DM 270/2004, art.3 comma 9.

il termine “corso di master”. I due livelli si distinguono sulla base del requisito di ammissione: i master di secondo livello permettono l’accesso solo ai laureati magistrali, mentre quelli di primo livello anche ai laureati triennali.

Un master universitario ha di solito fra le 400 e le 600 ore di lezione e un impegno complessivo dello studente stimato in almeno 1500 ore. È importante notare che, nella pratica corrente, il termine “master” (senza l’aggettivo “universitario”) viene utilizzato anche da soggetti diversi dalle università per indicare iniziative di formazione di vario tipo, anche molto più brevi: Nel seguito, si farà riferimento solo ai master universitari e, spesso, per non appesantire il testo si userà semplicemente il termine “master”.
I corsi di master universitario sono dedicati a tematiche specifiche, anche con approccio multidisciplinare, e vedono spesso il coinvolgimento di soggetti esterni, in particolare provenienti dal mondo produttivo e da quello delle professioni. Nel contesto della cybersicurezza, essi possono risultare utili come strumento per la specializzazione o la formazione ricorrente, ad esempio per offrire:

- approfondimenti mirati a laureati con specializzazione nell’informatica, ma senza competenze sui temi specifici della cybersicurezza;
- l’opportunità di maturare competenze in cybersicurezza a laureati con una certa anzianità, che non abbiano avuto la possibilità, nel corso dei loro studi, di affrontare queste discipline, a quel tempo non ancora mature;
- l’opportunità di acquisire competenze multidisciplinari, ad esempio, elementi di competenze tecnologiche per laureati in discipline giuridiche o economico-manageriali oppure elementi di competenze giuridiche e manageriali per laureati in discipline tecnico-scientifiche.

I corsi di master hanno molti iscritti (circa 70 mila nell’ultima rilevazione già citata), che conseguono quasi tutti il titolo. In effetti, questi corsi hanno caratteristiche molto diversificate, perché gestiti in completa autonomia dagli atenei, senza alcun processo di accreditamento o valutazione della qualità da parte di soggetti esterni. In particolare, si presenta una grande variabilità nelle valutazioni del profitto, che vanno da esami analoghi a quelli universitari, con verifiche puntuali e accurate, fino all’altro estremo di richiedere solo la presenza e la redazione di un lavoro finale (“tesina”).

6. Formazione e aggiornamento nel contesto professionale

In questo paragrafo discutiamo le problematiche relative alle iniziative di formazione non formale, solitamente nel contesto del mondo del lavoro o in preparazione all’ingresso in tale mondo. In questo caso l’attenzione è spesso più focalizzata di quanto non accada per la formazione universitaria, che, pur includendo, insieme agli aspetti metodologici, anche quelli applicativi, non può tenere conto delle specifiche esigenze dei numerosi contesti professionali che, come già detto, dipendono anche dal dominio applicativo.

La formazione professionale dovrà quindi essere strutturata in modo da rispondere alle esigenze specifiche delle organizzazioni tenendo in considerazione sia i fattori strutturali sia i fattori contingenti e dovrà essere prevista come formazione permanente basata su un'attenta analisi dei rischi che potenzialmente potrebbereo bloccare il funzionamento previsto, in modo da permettere l'individuazione di misure di sicurezza preventiva con l'obiettivo di mitigare gli effetti delle più probabili minacce cyber.

In ciascun contesto lavorativo, il primo passo nella creazione di una strategia di formazione professionale in cybersicurezza è l'identificazione delle competenze di base richieste. Queste competenze includono la conoscenza dei principi di sicurezza informatica, la comprensione dei possibili rischi a seguito di attacchi cyber, procedura da intraprendere per effettuare segnalazioni di possibili anomalie. Questo tipo di formazione di base è generalmente utile a larghe porzioni di personale e per questo è spesso prevista, o almeno dovrebbe esserlo, come componente della formazione aziendale comune.

Una volta identificate le competenze di base, il percorso di formazione dovrebbe essere strutturato in modo da essere concentrato sulle caratteristiche specifiche dell'organizzazione e della posizione lavorativa. In questo caso un riferimento importante è costituito dalla conformità normativa, che può essere un utile punto di partenza sia per l'implementazione delle misure minime di sicurezza, sia per eventuali adempimenti specifici, come il regolamento europeo per la privacy (GDPR) nel caso del trattamento di dati personali o come codici di autoregolamentazione come ad esempio in ambito bancario.

Il percorso di formazione deve essere flessibile e tenere conto tanto delle conoscenze e competenze possedute quanto di quelle richieste per la specifica posizione, nonché di quelle potenzialmente interessanti per la crescita professionale. La flessibilità, con opportuni gradi di ampiezza e profondità, è rilevante anche perché, nel settore della cybersicurezza, come e forse più che in altri, si presentano spesso iniziative di "reskilling", che possono essere indirizzate a personale con background eterogeneo e in aree diverse dalla cybersicurezza. Questo può essere utile all'inizio della carriera o anche in fasi successive.

Le esigenze sopra citate portano alla necessità di prevedere iniziative di formazione articolate e modulari, con corsi di diversa durata a seconda delle esigenze. Sono diffusi anche moduli molto brevi su aspetti puntuali della cybersicurezza che permettono l'acquisizione di competenze che vengono definite "micro certificazioni". Questo tipo di formazione, anche se presenta ovvi limiti stante l'esiguo numero di ore a disposizione, sta diventando sempre più comune con l'obiettivo di soddisfare le numerose esigenze di questo settore.

Prendendo spunto dal recente documento statunitense intitolato "National Cyber Workforce and Education Strategy", emerge chiaramente la necessità di trasformare l'istruzione nel campo della Cyber Security mediante la creazione di un vero e proprio "ecosistema". Non è realistico affidarsi esclusivamente agli sforzi degli insegnanti; occorre, piuttosto, sviluppare autentici ecosistemi locali che agevolino la creazione e il mantenimento di percorsi formativi attentamente

progettati con la partecipazione attiva e il supporto di aziende e organizzazioni pubbliche e private presenti sul territorio. Ciò consentirà di comprendere i rischi specifici legati alle principali categorie di prodotti presenti e le relative misure di sicurezza necessarie.

L'obiettivo primario è instaurare un ciclo virtuoso che favorisca lo scambio tra i percorsi formativi e le specifiche esigenze lavorative del territorio. Nel contesto della cybersicurezza orientata al paradigma della security by design, escludendo una formazione di base comune a tutte le attività produttive, è indispensabile tenere conto delle specificità dei diversi contesti lavorativi. Ad esempio, si pensi alle normative sulla privacy che regolamentano un ospedale, in contrasto con le esigenze operative di un broker finanziario che deve eseguire le proprie operazioni con affidabilità e continuità, evitando ritardi e interruzioni.

Nel settore della formazione professionale in cybersicurezza un elemento fondamentale è rappresentato dalle certificazioni professionali. Queste certificazioni, disponendo di un catalogo capillare, si pensi che un sito indipendente ne ha catalogate diverse centinaia,[18] permettono di dimostrare le competenze acquisite in ambiti specifici, grazie a esami comuni disponibili a livello globale. In generale le certificazioni sono create come argomenti e settore di applicazioni sia direttamente dalle società produttrici (vendor specific) di dispositivi hardware o software, sia da organizzazioni indipendenti (vendor neutral) che affrontano le problematiche di cybersicurezza senza riferirsi a specifiche soluzioni commerciali. I certificati sono rilasciati tipicamente da un ente di certificazione accreditato e terzo rispetto al produttore dei contenuti, che garantisce che l'esame si sia svolto in modalità idonea alla verifica delle competenze richieste. I certificati hanno spesso una validità temporale di qualche anno e si richiedono attività di formazione professionali, quali partecipazione a conferenze, seminari o corsi per permetterne il mantenimento. Molte certificazioni prevedono la necessità di superare diversi esami intermedi per essere ottenute, arrivando anche a creare percorsi gerarchici di formazione. In ambito commerciale sta diventando sempre più comune che alcuni vendor richiedano ad aziende partner un numero minimo di dipendenti certificati a diversi livelli per permettere la possibilità di diventare rivenditori e accedere a speciali condizioni di acquisto.

Le certificazioni hanno avuto sicuramente il merito di avere svolto un ruolo pionieristico nella formazione in cybersicurezza e di aver agevolato il mercato del lavoro grazie alla possibilità di legare le offerte di specifiche posizioni al possesso di determinate certificazioni. I forti interessi commerciali legati alle certificazioni hanno a volte comportato un'eccessiva compressione dei tempi di formazione, cercando di utilizzare questi titoli come sostitutivi invece che complementari a quanto previsto nella formazione formale. Ciò ha creato una classe di professionisti che tendono a concentrarsi su dettagli della cybersicurezza e

[18] Security Certification Roadmap - https://pauljerimy.com/security-certification-roadmap/

perdono di vista il quadro di insieme del sistema da proteggere, lasciando la possibilità a numerosi attacchi.

7 Conclusioni

Il quadro delle esigenze e delle opportunità che abbiamo discusso è chiaramente molto articolato e molte direzioni sono da considerare prioritarie. Certamente, il mondo del lavoro presenta richieste pressanti, non facili da soddisfare e per giunta urgenti. Pertanto, la coordinata temporale dovrà essere presa come principale direzione di indirizzo.

Una via privilegiata è certamente costituita dalla formazione formale con la crescita di nuovi curricula dedicati alla cybersicurezza appositamente disegnati. Questa strada richiede, in particolare in ambito universitario, un lungo periodo di tempo, spesso diversi anni, prima di manifestare la sua efficacia e produrre risultati concreti. Tuttavia, benché la via appena indicata rappresenti un percorso necessario, vi sono altre direzioni che meritano attenzione immediata, con l'obiettivo di produrre risultati a breve.

Una via promettente è la crescita di programmi di Master Universitari in Cybersicurezza, che permetterebbero in pochissimi anni di espandere in modo significativo alcune competenze cyber nel mondo del lavoro. Infatti, sebbene possano non avere un impatto significativo a medio-lungo termine, questi programmi possono fornire un terreno fertile per la sperimentazione verso nuovi percorsi formativi come nuovi corsi di laurea magistrale specifici o indirizzi dedicati alla cybersicurezza. Inoltre, è sicuramente importante promuovere l'attivazione di insegnamenti specifici nel settore, che possono poi favorire l'attivazione di nuovi indirizzi e poi magari nuovi corsi di studio (L o LM). Un'altra opportunità che non abbiamo ancora citato è la possibile offerta di insegnamenti come "corsi singoli", cui persone esterne all'università, magari già laureate, possono iscriversi per arricchire le proprie competenze.

Fra le iniziative di istruzione formale che abbiamo citato, gli ITS costituiscono una realtà che può produrre risultati in tempi relativamente brevi e ha grandi spazi di crescita, in cui gli studenti possono acquisire competenze più operative, direttamente applicabili nel mondo del lavoro ed eventualmente poi procedere anche a livello universitario. Non vanno però in questo contesto trascurati gli investimenti, visto che la crescita desiderata è quantitativamente molto significativa.

Le iniziative nel contesto del mondo del lavoro, sia privato sia pubblico, possono fornire opportunità di upskilling e reskilling. Oltre a quelle realizzate direttamente da aziende o altri enti preposti, se ne potrebbero promuovere in collaborazione con le università o gli ITS.

Le certificazioni professionali, associate a corsi spesso di breve o brevissima durata, rappresentano attualmente un'importante risorsa per colmare il divario tra la domanda e l'offerta di professionisti in cybersicurezza. Questo approccio risulta

di grande utilità per acquisire competenze fortemente specialistiche, ma sarebbe probabilmente più efficace se avvenisse per professionisti aventi già una formazione formale, anche in settori diversi da quello informatico.

Relativamente a tutti i contesti, il miglioramento e l'ampliamento dei percorsi formativi hanno come prerequisito la crescita delle competenze del corpo docente. Per l'università ciò è possibile solo attraverso un aumento del numero dei dottori di ricerca, negli altri settori è necessario un aumento dei laureati e, più a breve termine, è necessaria una formazione di docenti già attivi, vuoi nel mondo della scuola vuoi in quello del lavoro. A breve termine, tanto nella scuola quanto nell'università il problema può essere gestito anche tramite il coinvolgimento di docenti che insegnano materie vicine. Negli ITS, la possibilità di avvalersi in modo consistente di insegnanti esterni che si siano formati tramite significative esperienze professionali, rappresenta forse l'unica possibilità per reperire docenti in tempi rapidi.

BIOGRAFIE

Paolo Atzeni è Direttore per lo sviluppo di capacità e competenze presso l'Agenzia per la Cybersicurezza Nazionale. È in aspettativa dall'Università Roma Tre, dove è professore dal 1992 ed è stato Prorettore alla Didattica e Direttore del Dipartimento di Ingegneria. Ha ricevuto la laurea in Ingegneria Elettronica presso l'Università di Roma "La Sapienza" nel 1980. In passato ha lavorato presso lo IASI-CNR di Roma, e le università di Napoli e La Sapienza di Roma. Ha pubblicato numerosi articoli su vari argomenti nel campo delle basi di dati, tra cui teoria relazionale, modelli concettuali, basi di dati e Web, gestione di modelli e metamodelli. È stato Vicepresidente del VLDB Endowment e Presidente dell'Associazione EDBT nonché Presidente del GII, l'Associazione dei Professori di Ingegneria Informatica in Italia.

E-mail: p.atzeni@acn.gov.it

Bernardo Palazzi è consigliere per lo sviluppo di capacità e competenze presso l'ACN. Precedentemente in Istat ha ricoperto per primo il ruolo di Responsabile Protezione Dati personali e ha progettato le misure di sicurezza dell'ultimo censimento generale della popolazione. Inoltre, collabora da più di 15 anni con la Brown University negli USA, dove dirige nell'ambito della cybersecurity un Master of Science e tiene due corsi.

L'ingegner Palazzi ha pubblicato diversi articoli scientifici sulla sicurezza informatica ed è inventore di un brevetto internazionale sulla sicurezza dei database. Inoltre, è stato socio fondatore e CTO di una startup su sicurezza dei dati nel cloud, basata sul suo brevetto.

Ha conseguito il dottorato di ricerca in Ingegneria Informatica presso l'Università "Roma Tre".

E-mail: b.palazzi@acn.gov.it

The Big Game: giocando si impara la cybersicurezza

Gaspare Ferraro, Sonia Montegiove, Paolo Prinetto

Sommario

L'articolo presenta "The Big Game", una iniziativa gratuita di formazione e gioco sui temi della cybersicurezza, della consapevolezza digitale e dell'uso sicuro della Rete e dei social network, rivolta ai giovani, realizzata dal Cybersecurity National Lab del CINI (Consorzio Interuniversitario Nazionale per l'Informatica), con il patrocinio dell'Agenzia per la Cybersicurezza Nazionale - ACN. Oltre 30mila i ragazzi e le ragazze coinvolti finora, grazie anche alla costituzione di una rete di scuole, che supportano queste attività accompagnando studenti e studentesse nei diversi programmi organizzati.

Abstract

The paper presents "The Big Game", a free training and gaming initiative on cybersecurity, digital awareness, and safe use of the Net and social networks, aimed at young people, carried out by the Cybersecurity National Lab of CINI (National Interuniversity Consortium for Informatics), under the sponsorship of the National Cybersecurity Agency - ACN. More than 30 thousand students have been involved so far, thanks also to the development of a network of high schools, which support these activities by accompanying their students in the different organized programs.

Keywords: Cybersecurity; Training; Digital Awareness; Gamification; Gender gap; CTF competitions; Skill shortage; School

1. Introduzione

L'Italia si colloca al 25° posto su 27 paesi dell'UE per capitale umano secondo l'indice DESI 2022, ovvero l'indice che traccia i progressi compiuti negli Stati membri dell'UE nel digitale. Solo il 46% delle persone, infatti, possiede perlomeno competenze digitali di base, un dato al di sotto della media UE pari al 54%. Un problema molto sentito da anni nel nostro Paese e in Europa, tanto da portare la Commissione europea a fissare l'obiettivo dell'80% di adulti con competenze digitali di base entro il 2030 e a riaffermare che "tutti gli europei hanno bisogno di digital skill per studiare, lavorare, comunicare, accedere ai servizi pubblici online e trovare informazioni affidabili".

Un percorso non banale quello che porta all'acquisizione da parte dei cittadini delle competenze e conoscenze necessarie a muoversi in modo consapevole e sicuro in un mondo ogni giorno più digitalizzato e connesso.

Se è vero che la sicurezza informatica assume un ruolo sempre più centrale e di primo piano per lo sviluppo dei Paesi, è vero che non c'è adeguata disponibilità della forza lavoro richiesta. Solo per citare qualche numero, secondo l'Unione Europea, nel 2022, "la carenza di professionisti della sicurezza informatica nell'UE variava tra 260.000 e 500.000, mentre il fabbisogno di forza lavoro della sicurezza informatica dell'UE era stimato a 883.000 professionisti. Inoltre, le donne rappresentano solo il 20% dei laureati in cybersicurezza e il 19% degli specialisti in tecnologie dell'informazione e della comunicazione".

2. Quali le azioni a supporto dello sviluppo di competenze cyber in Europa e in Italia?

A livello europeo, la Strategia di sicurezza informatica dell'Unione europea[1] fissa, tra gli altri, l'obiettivo di promuovere la consapevolezza, lo sviluppo delle competenze e le opportunità di carriera nella sicurezza informatica. Questi obiettivi sono stati ulteriormente sviluppati nell'ambito della Cybersecurity Skills Academy[2], di recente costituzione. L'Accademia, che rientra nell'ambito delle iniziative organizzate dalla UE per l'anno europeo delle competenze 2023[3], è progettata per mettere insieme iniziative pubbliche e private, volte a promuovere le competenze in materia di sicurezza informatica a livello europeo e nazionale, con l'obiettivo di aumentare la forza lavoro europea in ambito cyber e migliorare le competenze dei professionisti della sicurezza informatica e renderli visibili su una piattaforma online.

Nel nostro Paese, a supporto della Strategia europea c'è la Strategia nazionale italiana per la sicurezza informatica 2022-26[4], che tra le sue 82 misure a rendere il Paese più sicuro e resiliente prevede anche azioni specifiche in termini di sensibilizzazione di tutti i cittadini e le cittadine.

3. Come il gioco supporta l'acquisizione di digital skill: l'esperienza di The Big Game

Il Cybersecurity National Lab[5] del CINI (Consorzio Interuniversitario Nazionale per l'Informatica, composto da oltre 50 Università italiane)[6], con il patrocinio dell'Agenzia per la Cybersicurezza Nazionale ACN, ha dato vita a una iniziativa gratuita di formazione e gioco sui temi della consapevolezza digitale e dell'uso sicuro della Rete e dei social network, rivolta ai giovani, chiamata "The Big Game".

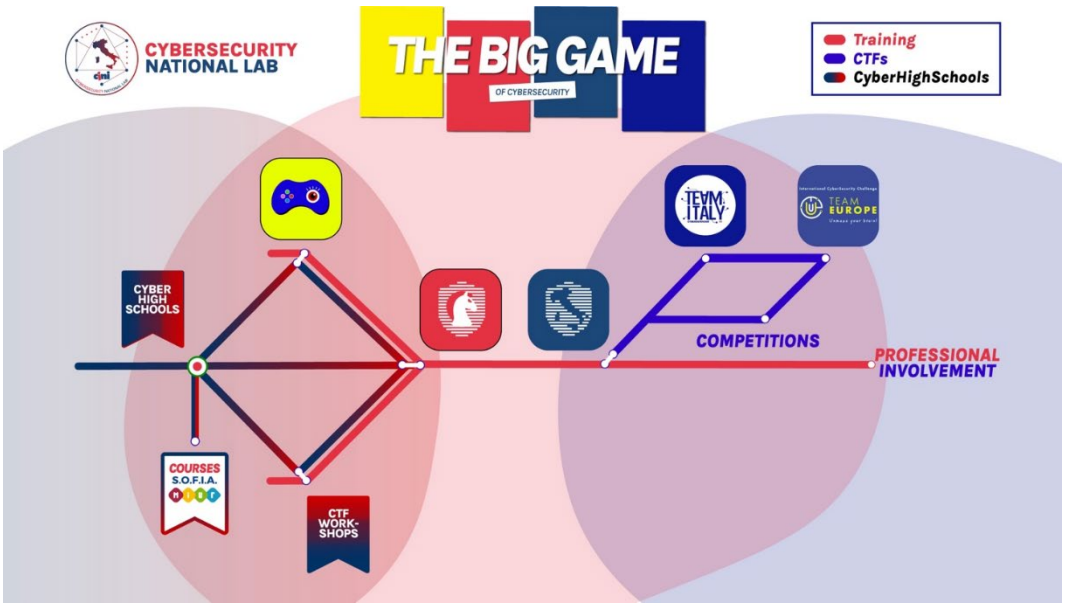
1 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
2 https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy
3 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-year-skills-2023_en
4 https://www.acn.gov.it/strategia-nazionale-cybersicurezza
5 https://cybersecnatlab.it
6 https://www.consorzio-cini.it

Oltre 30mila sono stati i ragazzi e le ragazze coinvolti finora, grazie anche alla costituzione di una rete di scuole, CyberHighSchools, che supportano queste attività accompagnando studenti e studentesse nei diversi percorsi organizzati. The Big Game si inserisce all'interno della misura 65 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026: "Favorire l'organizzazione di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, che tengano in debita considerazione principi di bilanciamento di genere, mirate all'individuazione di giovani talenti anche al fine di propiziarne l'ulteriore formazione e l'inserimento nel mondo del lavoro. Ciò, anche al fine di promuovere iniziative volte a colmare il "confidence gap" delle studentesse nei confronti di carriere in ambiti scientifici e tecnologici."

Il grande gioco della sicurezza informatica rientra tra le azioni che il Cybersecurity National Lab - organizzato come una rete di 65 nodi interconnessi, dislocati nelle principali Università italiane, Enti di ricerca e Accademie militari – introduce per favorire la costituzione di un ecosistema nazionale italiano di cybersicurezza.

4. Le anime di The Big Game: CyberChallenge.IT, OliCyber.IT e CyberTrials

Il gioco, partendo da una prima esperienza con CyberChallenge.IT, si è arricchito negli anni di altre iniziative rivolte a target differenti, come OliCyber.IT e CyberTrials, che andiamo a vedere più nel dettaglio.



5. CyberChallenge.IT

CyberChallenge.IT[7] è il primo programma italiano di formazione e training in cybersicurezza per studenti delle scuole superiori, laureandi e laureati (16-24

7 https://cyberchallenge.it

anni) che mira a ridurre l'odierna carenza di forza lavoro informatica in Italia, identificando, attraendo, reclutando e collocando la prossima generazione di professionisti della cybersicurezza, mettendo così a disposizione del Paese le loro competenze.

In particolare, il programma mira a creare e far crescere la comunità dei cyberdefender stimolando l'interesse per le aree STEM e principalmente per l'informatica e l'ingegneria informatica; individuando i giovani talenti informatici, contribuendo così alla loro crescita professionale; affrontando le sfide multidisciplinari del mondo reale in diversi settori della sicurezza informatica, compresi gli aspetti etici e legali; condividendo opportunità di occupazione professionale offerte dagli sponsor e dalle parti interessate pubbliche e private del programma.

Ogni edizione si svolge ogni anno da gennaio a luglio in oltre 40 sedi, tra università, centri regionali e accademie militari, sparse in tutto il territorio italiano. Le 7 edizioni del programma hanno registrato finora 25.170 studenti iscritti e 3.474 partecipanti al percorso di formazione. Una panoramica delle varie edizioni è nella Tabella 1, mentre le statistiche dettagliate per le varie edizioni sono disponibili tramite il sito web del programma[8]. Vale la pena sottolineare che l'attuazione del programma è stata resa possibile grazie alla peculiarità nazionale del Cybersecurity National Lab: nessuna università italiana, anche tra le più grandi, avrebbe avuto la capacità di realizzarlo in proprio raggiungendone gli attuali livelli di coinvolgimento.

Anno	Sedi	Scuole	Studenti partecipanti								
			Registrati							Ammessi	
			Totale	Genere		Provenienza					
				M	F	Scuole		Università			
			#	#	#	#	%	#	%	#	%
2017	1	-	683	603	80	57	8.34	626	91.65	26	3.80
2018	8	-	1866	1698	168	583	31.24	1283	68.87	160	8.57
2019	18	19	3203	2830	373	1341	41.86	1862	58.13	360	11.23
2020	28	114	4452	3848	604	1960	44.02	2492	55.97	560	12.57
2021	33	184	4902	4258	644	2255	46.00	2647	54.00	671	13.68
2022	34	316	5344	4635	661	2461	46.06	2883	53.94	754	14.10
2023	43	503	4720	4153	567	2066	43.77	2654	56.23	944	20

Tabella 1

Dal 2021 CyberChallenge.IT è riconosciuto dal MIUR come "Progetto per la Valorizzazione delle Eccellenze" [9] ; di conseguenza, il Ministero assegna annualmente agli studenti delle scuole superiori primi classificati numerosi premi

8 https://cyberchallenge.it/stats

9 Ex Art. 4 del DL No. 262 del 29 dic 2007

e riconoscimenti. Inoltre, molte università italiane riconoscono crediti secondo il Sistema Europeo di Accumulo e Trasferimento dei Crediti (ECTS)[10] ai partecipanti al programma CyberChallenge.IT.

Lo stesso Ministero ha contribuito alla realizzazione delle ultime due edizioni nell'ambito di un Accordo quadro tra il MIUR e il CINI.

6. Come si svolge CyberChallenge.IT?

Ogni edizione del programma prevede 4 fasi principali: test di ammissione e formazione delle squadre locali, percorso di addestramento, gara locale e gara nazionale. I partecipanti vengono selezionati attraverso una sequenza di test on-line, finalizzati rispettivamente a una selezione iniziale e alla composizione delle squadre locali. Una volta ammessi, i partecipanti vengono raggruppati in gruppi di formazione di 20 persone ciascuno (più 5 riserve) e ogni gruppo viene formato in uno dei Nodi di formazione del programma.

In particolare, il processo di selezione si articola in due fasi, tra cui un pre-test e una prova di programmazione.

Gli studenti iscritti possono formarsi in preparazione alla prova di ammissione sfruttando una piattaforma software personalizzata sviluppata internamente. Su questa piattaforma gli studenti possono affrontare i quiz proposti e sottoporre le proprie soluzioni ai problemi di programmazione per ottenere una valutazione automatica. Il punteggio acquisito tiene conto sia della correttezza delle soluzioni sia dei tempi di risoluzione.

Il percorso formativo mira a fornire le basi metodologiche e pratiche necessarie per analizzare debolezze, vulnerabilità e possibili attacchi, individuando le soluzioni più idonee a prevenirli, nei diversi ambiti della cybersicurezza. Nello specifico, gli argomenti trattati sono raggruppati in otto aree tematiche (Introduzione alla Cybersicurezza, Crittografia, Sicurezza Hardware, Sicurezza Software, Sicurezza delle Reti, Sicurezza Web, Attacco-Difesa, Etica & Soft Skill), a loro volta composte da un totale di 24 moduli. In genere, ogni modulo viene svolto nell'arco temporale di una settimana e comprende 6 ore di attività sorvegliate (2 di lezioni e 4 di attività pratiche). Queste sono organizzate per guidare gli studenti, passo dopo passo, nella risoluzione di sfide di tipo Capture the Flag (CTF) di crescente complessità. Non si presume alcuna conoscenza precedente in materia di sicurezza informatica. Le attività didattiche e formative sono programmate localmente in fasce orarie compatibili con le attività scolastiche e universitarie dei partecipanti, includendo, in alcuni casi, il venerdì pomeriggio o il sabato mattina. Il programma di formazione completo dura 12 settimane e l'insieme dei moduli da coprire in ciascun Nodo di formazione è liberamente selezionato a livello locale.

Il percorso formativo si conclude con due gare, organizzate rispettivamente a livello di Nodo formativo locale e a livello nazionale. La prima è una competizione

10 https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/european-credit-transfer-and-accumulation-system

CTF in stile Jeopardy gestita centralmente e giocata contemporaneamente da tutti i partecipanti di tutti i Nodi. La seconda, ovvero il campionato nazionale in Cybersicurezza, è una competizione CTF in stile Attacco-Difesa, alla quale partecipano squadre composte da 6 membri ciascuna, uno per Nodo, e organizzata ogni anno in una sede specifica.

7. OliCyber.IT, le olimpiadi italiane di cybersicurezza

Nel 2020 ci siamo resi conto che su 2.035 studenti delle scuole superiori inizialmente iscritti al programma CyberChallenge.IT, solo 156 erano stati ammessi al programma di formazione, avendo superato tutta la fase di ammissione. L'alto tasso di fallimento era dovuto in primis al fatto di dover competere con studenti universitari, laureandi e laureati, che ovviamente avevano background e competenze differenti. Così, si è deciso di dare vita a un nuovo programma di formazione e gioco rivolto solo agli studenti delle scuole superiori: OliCyber.IT[11], le Olimpiadi italiane di cybersicurezza.

Il gioco è aperto a tutti gli studenti degli Istituti superiori di secondo grado, con l'obiettivo di favorirne e incentivarne l'avvicinamento alle sfide della sicurezza informatica. In particolare, OliCyber.IT mira a creare e a far crescere la comunità dei cyberdefender investendo sui giovani e puntando a stimolarne l'interesse verso le materie tecnico scientifiche e, in particolare, verso l'informatica e la sicurezza informatica. Il programma mira, inoltre, a identificare i giovani talenti, contribuendo al loro orientamento e alla loro formazione professionale, anche condividendo le opportunità offerte dai vari percorsi formativi su tematiche di cybersicurezza.

Il programma Olicyber.IT si avvale dell'esperienza e degli strumenti messi a punto nell'ambito del programma CyberChallenge.IT, al quale, come abbiamo visto, è possibile accedere al compimento del sedicesimo anno di età. Da questo punto di vista, le Olimpiadi Italiane di Cybersicurezza si pongono come programma "propedeutico" a CyberChallenge.IT, che ne è visto come il naturale complemento a valle.

OliCyber.IT è riconosciuto dal Ministero dell'Istruzione come Percorso per le Competenze Trasversali e per l'Orientamento (PCTO)[12] e, dal 2021, in modo dal tutto analogo a quanto avviene per CyberChallenge.IT, lo stesso Ministero lo ha riconosciuto come "Progetto per la valorizzazione delle eccellenze".

8. Come si svolge OliCyber.IT?

Le varie fasi di ciascuna edizione del programma possono essere così riassunte:

1. L'adesione (gratuita) al programma CyberHighSchools da parte degli istituti superiori di secondo grado;
2. L'iscrizione (gratuita) al programma da parte degli studenti interessati;

11 https://olicyber.it/

12 https://www.miur.gov.it/-/linee-guida-dei-percorsi-per-le-competenze-trasversali-e-per-l-orientamento

3. Una fase di selezione scolastica per tutti gli iscritti, svolta contemporaneamente online, e finalizzata a selezionare i migliori studenti di ogni istituto federato;
4. Una seconda fase di selezione territoriale, a cui prendono parte gli ammessi dalla prima selezione, finalizzata a selezionare i migliori 100 partecipanti alla competizione finale nazionale;
5. La competizione finale nazionale in presenza: l'Olimpiade Italiana di Cybersicurezza, seguita, il giorno successivo, da una cerimonia di premiazione nazionale, cui partecipano personaggi di rilevo del mondo cyber e rappresentanti delle istituzioni italiane.

Uno dei problemi principali riscontrati nelle prime edizioni delle Olimpiadi Italiane di Cybersicurezza è stato quello del "gap" di conoscenze teoriche richieste tra le diverse fasi del programma. Se, infatti, superare la selezione scolastica richiede solo una buona capacità logica e qualche conoscenza scolastica di base, la fase territoriale, in formato CTF, richiede conoscenze tecniche e pratica in cybersicurezza che possono essere acquisite solo attraverso formazione e addestramento specifico per questa tipologia di eventi.

Questo fenomeno, se in alcuni casi è stato affrontato dai ragazzi più competitivi come una sfida da superare e una nuova opportunità per mettersi alla prova, ha purtroppo rappresentato un motivo di "abbandono" per la maggior parte dei ragazzi che, superata la fase precedente, riscontravano grandi difficoltà nella risoluzione degli esercizi proposti in questa fase.

Per questa ragione, a partire dalla edizione 2023, il problema è stato affrontato e risolto creando un numero maggiore di attività e di possibilità di crescita per i partecipanti nelle fasi iniziali del progetto. Un primo significativo passo in questa direzione è stato rappresentato dalla creazione del portale training.olicyber.it[13] che, tramite videolezioni ed esercitazioni, rende disponibili ai ragazzi gli strumenti per proseguire nelle fasi successive. Un ulteriore passo è stata la creazione di una serie di eventi, denominati "Training camp", per permettere ai ragazzi di conoscere questo mondo grazie al tutoraggio da parte di partecipanti più esperti che hanno vissuto un'analoga esperienza in passato. L'obiettivo principale è portare i ragazzi, al termine del camp, ad avere gli strumenti e le conoscenze necessarie per affrontare la fase di selezione territoriale.

Queste attività hanno preso forte ispirazione dagli stage locali e nazionali delle Olimpiadi della Matematica e di Informatica, che, negli anni, hanno dimostrato come le attività di training intensivo da parte di ex-partecipanti e organizzatori, svolte in presenza anche a livello locale o regionale, siano essenziali per far crescere il progetto.

Quanti hanno superato con successo la selezione scolastica vengono informati della possibilità di partecipare ai camp sulla base di un criterio "first-come first-

13 https://training.olicyber.it

served" e del consenso da parte dal docente di riferimento della scuola, che ne giustificherà anche, di conseguenza, l'assenza dalle lezioni scolastiche.

Ciascuna edizione del camp ha previsto 40 ore di formazione riconoscibili come PCTO e suddivise tra: strumenti di lavoro e metodologia, giornate di allenamento dedicate a scripting in python, network security, web security, software security e crittografia, alternati tra incontri teorici e di laboratorio e simulazioni di una competizione.

Tutti i materiali didattici utilizzati nei camp sono resi fruibili a tutti i tramite i canali ufficiali del progetto.

9. CyberTrials

CyberTrials nasce dall'esigenza di abbattere il divario di genere che era evidente sia in CyberChallenge.IT che in OliCyber.IT dove, nonostante gli sforzi e nonostante un trend che mostrava un numero crescente di ragazze partecipanti, erano però ancora troppo poche le ragazze che riuscivano a superare la selezione e arrivare alla fase finale o accedere a CyberChallenge.IT. Il problema del divario di genere, peraltro, è particolarmente sentito anche a livello europeo in ambito ICT, visto che soltanto una persona su 6 professionisti IT è di genere femminile. Per affrontare il problema nel modo più efficace, il Laboratorio ha deciso di organizzare CyberTrials[14], un programma di formazione e gioco aperto alle sole ragazze degli istituti superiori di secondo grado che non richiedesse competenze in ingresso.

Il programma copre diverse aree della sicurezza informatica, consentendo alle partecipanti di acquisire una comprensione generale di alcuni aspetti tecnici della disciplina. La particolarità di CyberTrials è che alle lezioni frontali si associa un gioco di ruolo in cui le ragazze, a piccole squadre, sono chiamate a risolvere delle sfide basate su quanto ascoltato a lezione. Ancora una volta, si ricorre alla gamification, ovvero all'uso di elementi di gioco, come punti, badge e classifiche, in contesti non di gioco per coinvolgere e motivare le partecipanti.

CyberTrials è un programma riconosciuto nell'ambito dell'iniziativa Repubblica Digitale, iniziativa strategica nazionale coordinata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, che ha l'obiettivo di ridurre il divario digitale e promuovere l'educazione sulle tecnologie del futuro, supportando il processo di sviluppo del Paese.

L'iniziativa è inoltre inserita come buona pratica nella pubblicazione "Superamento del divario digitale di genere nell'ambito delle competenze digitali", curata dal gruppo di lavoro costituito da rappresentanti della società civile (tra i quali il Cybersecurity National Lab), dal Dipartimento per la Trasformazione Digitale e dal Dipartimento per le Pari Opportunità della Presidenza del Consiglio dei Ministri.

10. Come si svolge CyberTrials?

14 https://www.CyberTrials.it/

Così come per OliCyber.IT, al programma possono accedere gratuitamente tutte le ragazze delle scuole superiori che hanno aderito alla rete CyberHighSchools. Il programma consente di acquisire competenze tecniche di base e una comprensione generale di alcuni aspetti della sicurezza informatica, tra cui reti, Web, Open Source Intelligence (OSINT), modellazione delle minacce, ingegneria sociale, informatica forense, crittografia e steganografia. Queste competenze sono integrate da competenze trasversali, tra cui capacità di autogestione, aspetti legali ed etici, capacità di team building e comunicazione digitale.

Tutti questi argomenti sono presentati settimanalmente, in moduli di 2 ore. Gli argomenti teorici sono integrati con una formazione teorica e pratica, basata su una competizione CTF continua svolta durante l'intero processo di formazione. In particolare, ogni settimana vengono rilasciate 3 nuove sfide proprio al termine del modulo presentato. Una particolarità di CyberTrials è quella di basarsi su uno storytelling continuo, dove tutte le sfide presentate sono integrate con la storia principale attraverso riferimenti, descrizioni, suggerimenti e materiali aggiuntivi.
Le ragazze giocano a squadre composte da un massimo di cinque persone scelte in modo casuale, al fine di favorire la relazione tra studentesse che non si conoscono e per evitare la composizione di squadre sbilanciate in termini di competenze. L'esperienza di questi primi due anni ha dimostrato che la scelta casuale delle componenti delle squadre si rivela vincente perché a ragazze tecnicamente più esperte si affiancano spesso ragazze con scarse conoscenze e competenze in ingresso, che possono così trovare un aiuto nelle compagne di gioco.

La prima edizione di CyberTrials ha fatto registrare un numero molto elevato di partecipanti (quasi 400) che è più che raddoppiato nella seconda edizione del 2023 con quasi 1.000 partecipanti.

11. Fuori gara, dentro The Big Game: gli HighSchools CTF Workshops

A partire dal 2023, per diffondere in modo sempre più capillare le varie attività del programma The Big Game, il Cybersecurity National Lab ha dato vita a una serie di workshop organizzati in varie regioni d'Italia, denominati HighSchools CTF Workshop. Organizzati nell'ambito del programma CyberHighSchools, sono eventi pratici di introduzione alla cybersicurezza, rivolti a studenti e professori delle scuole superiori di secondo grado di ogni indirizzo e interessati ad approfondire i concetti basilari della cybersicurezza.

Durante ciascuna edizione vengono affrontati, con un approccio pratico, i concetti fondamentali introduttivi relativi alla OSINT, alla web security, alla network security, alla computer forensics e alla crittografia, tramite la presentazione di strumenti e numerosi esercizi su casi pratici.

Ciascuna edizione del workshop prevede tre diversi momenti:

- Durante la sessione della mattina, alcuni seminari pratici introducono le tematiche base della sicurezza informatica, con la presentazione sia dei concetti base sia dei principali strumenti da utilizzare;

- Al fine di comprendere meglio le tematiche affrontante, la sessione del pomeriggio prevede una competizione informatica al computer, nello stile delle competizioni Capture The Flag (CTF): i partecipanti, suddivisi in squadre da 4-6 persone (composte da studenti e dai loro professori), gareggiano in una competizione con sfide pratiche inerenti agli argomenti della mattinata;
- Al termine della competizione, le migliori squadre sono premiate nella cerimonia finale di chiusura.

Quasi mille studentesse e studenti delle superiori sono stati coinvolti con i workshop del 2023 che si sono svolti in diversi momenti dell'anno nelle città di Bari, Pisa, Verona, Perugia e Udine, grazie al coinvolgimento e alla collaborazione delle Università locali già partecipanti ai programmi di formazione del Cybersecurity National Lab, come CyberChallenge.IT, le Olimpiadi Italiane di Cybersicurezza, CyberTrials e con i membri del TeamItaly, la Nazionale Italiana di Cyberdefender. Preziosa la collaborazione, rispettivamente a Pisa, Verona, Perugia e Udine, dell'Università di Pisa, della Fondazione Edulife, dell'ITTS A. Volta di Perugia e dell'Università di Udine.

12. Il grande gioco delle scuole: CyberHighSchools

Il programma CyberHighSchools[15] nasce con l'intento di attivare una rete tra le Istituti superiori di secondo grado, con l'obiettivo di creare un livello intermedio di formazione e interazione con gli studenti, favorendo, contestualmente, la crescita di una comunità di professori sempre più consapevoli delle tematiche relative alla cybersicurezza e interessati ai programmi del Cybersecurity National Lab.

Aderendo gratuitamente al programma, l'Istituto entra a far parte di una rete di scuole "federate" con il Laboratorio ed è automaticamente considerato come partecipante a tutte le attività del programma The Big Game. A oggi le scuole superiori italiane federate sono oltre 500.

Tra gli aspetti più rilevanti per le insegnanti e gli insegnanti di una scuola federata, ci sono:

- la possibilità di accedere gratuitamente a un ampio e approfondito materiale didattico, predisposto e sistematicamente rivisto da esperti del Cybersecurity National Lab;
- la partecipazione gratuita a corsi mirati di introduzione e/o approfondimento su tematiche di cybersicurezza;
- la possibilità di ricevere, al termine dei percorsi di formazione, sia attestati di partecipazione rilasciati dal Cybersecurity National Lab, sia degli Open Badge[16], fruibili tramite la piattaforma Bestr[17] di CINECA;
- l'accesso a una community di insegnanti, cui sarà offerta l'opportunità di condividere esperienze e proporre iniziative sia tramite forum dedicati, sia attraverso incontri periodici;

15 https://cyberhighschools.it
16 https://openbadges.org
17 https://bestr.it

- la possibilità di monitorare l'andamento dei propri studenti all'interno dei programmi CyberChallenge.IT, OliCyber.IT e CyberTrials.

Le scuole che aderiscono alla rete CyberHighSchools hanno la possibilità di formare i propri docenti in modo gratuito attraverso 2 corsi di formazione disponibili sulla piattaforma S.O.F.I.A.[18] del Ministero dell'Istruzione: introduzione alla Cybersicurezza - Corso di formazione base per docenti delle scuole secondarie di II grado (iniziativa formativa ID. 80532) e introduzione alla Cybersicurezza - Corso di formazione avanzato per docenti delle scuole secondarie di II grado (Iniziativa formativa ID. 80176).

Il Corso Base mira a far crescere la sensibilizzazione verso le problematiche di cybersicurezza nei vari aspetti della vita quotidiana, attraverso un opportuno mix di lezioni e di tutoraggi, fruibili in modalità remota. Il corso è tenuto da docenti universitari e specialisti del settore, afferenti al Cybersecurity National Lab, e prevede 28 ore complessive di impegno, di cui 20 di lezione (4 erogate on-line, tramite la piattaforma Zoom e 16 fruibili da remoto in modalità e-learning asincrono, tramite lezioni videoregistrate) e 8 ore di tutoraggio on-line da parte dei docenti che hanno registrato le lezioni.

Il Corso Avanzato mira ad approfondire tematiche avanzate di sicurezza informatica legate a Crittografia, Web security, Network security, Software security, Hardware security, attraverso un opportuno mix di lezioni e di esercitazioni pratiche, tutte fruibili in remoto e su piattaforme ufficiali del Laboratorio. Il corso, gratuito, è tenuto da collaboratori esperti del Laboratorio e ha una durata complessiva di 32 ore, di cui 16 di lezione, in modalità e-learning, tramite lezioni video-registrate e 16 di tutoraggio on-line.
Sono stati sinora oltre 1.500 i professori che hanno partecipato alle 19 edizioni dei corsi (8 di quello base e 11 di quello avanzato).

13. The Big Game come vivaio della nazionale degli hacker etici

TeamItaly – la Nazionale Italiana di CyberDefender – è la squadra nazionale che ha il compito e la responsabilità di rappresentare il Paese nelle più importanti competizioni internazionali relative a vari settori della cybersicurezza, tra cui l'annuale European Cyber Security Challenge (ECSC) organizzata dalla European Union Agency for Cybersecurity (ENISA).

A partire dal 2018, il Nucleo di Sicurezza Cibernetica (NSC) della Repubblica Italiana ha affidato al Cybersecurity National Lab il compito di organizzare e gestire le attività di TeamItaly e di curarne, tra l'altro, la partecipazione alle competizioni internazionali del settore.

A livello pratico, il Lab provvede alla selezione del gruppo di "preparatori", composto dall'allenatore (coach) Mario Polino (PoliMi), dal Team Manager (referente tecnico organizzativo) Gaspare Ferraro (Cybersecurity National Lab) e da uno staff di esperti. Questi hanno il compito e la responsabilità di selezionare

18 https://sofia.istruzione.it

annualmente (“convocare”) 20 tra i migliori partecipanti di tutte le edizioni dei programmi di addestramento organizzati dal Cybersecurity National Lab. I partecipanti vengono selezionati, al termine delle edizioni annuali dei programmi CyberChallenge.IT e OliCyber.IT, in base ai risultati ottenuti sia durante i percorsi di training sia nelle varie competizioni, con l’obiettivo di ricercare i migliori talenti delle diverse branche della cybersicurezza. In particolare, seguendo i criteri di ECSC, la Nazionale è formata da 10 membri della categoria Junior, tra i 14 e i 19 anni, e da 10 membri della categoria Senior, dai 21 ai 25 anni.

Per potersi preparare e misurare al meglio con le varie tipologia di sfide proposte nelle varie competizioni internazionali cui partecipa, il team viene coinvolto in un percorso di addestramento intensivo (“ritiro”) che si svolge annualmente in presenza, per un’intera settimana.

Il ritiro si allinea alle strategie nazionali di cybersicurezza, promuovendo le competenze cibernetiche come patrimonio per il sistema Paese e sottoponendo i convocati a un percorso formativo d’eccellenza, unico in Europa, con la prospettiva di incrementarne ulteriormente le già elevate capacità difensive e offensive a livello sia individuale sia, soprattutto, come squadra. Proprio con questo fine, i membri della Nazionale vengono formati sull’acquisizione di competenze specifiche in numerosi ambiti, tra i quali crittografia, sicurezza web, analisi forense di computer e dispositivi mobili e sicurezza dell’hardware. Inoltre, durante il ritiro, ciascuno dei componenti della squadra sviluppa la capacità di esporre temi complessi in modo comprensibile a un pubblico di non specialisti. È parte integrante dell’addestramento anche un percorso di Team Building, specificamente progettato per l’iniziativa.

A livello europeo ENISA, la European Union Agency for Cybersecurity fa da volano e, facendo tesoro delle esperienze delle singole nazioni, organizza ogni anno la European Cyber Security Challenge (ECSC) con lo scopo di favorire lo scambio di conoscenza e talenti su tutta Europa. La competizione è aperta a tutti i paesi europei. Ogni nazione che si iscrive all’evento partecipa con una squadra composta da 10 giocatori di un’età compresa tra i 14 e i 25 anni.
Tra gli obiettivi dell’ECSC vi è quello di porre la cybersicurezza a servizio dell’umanità, per promuovere la pace, preservare la democrazia, la dignità e la libertà di pensiero, stimolando la collaborazione tra i giocatori dei paesi partecipanti alla gara e l’importanza della trasparenza e dell’osservanza delle regole per tutte le fasi della competizione.

L’Italia ha partecipato, con TeamItaly, per la prima volta a ECSC nel 2017 conquistando il terzo posto. Nel 2018 ha ottenuto la sesta posizione, mentre nell’edizione del 2019 ha conquistato il secondo posto. L’edizione 2020 non si è svolta a causa del Covid19. L’edizione 2021 della competizione si è svolta a Praga dal 28 settembre al 1° ottobre 2021 e il TeamItaly ha conquistato il terzo posto. L’edizione 2023 si è svolta a Hamar in Norvegia dal 24 al 27 ottobre e la prossima sarà in Italia, a Torino, dal 7 all’11 ottobre del 2024.

Oltre a organizzare l'ECSC, ENISA gestisce anche il Team Europe[19], un gruppo di giovani talenti appassionati di sicurezza informatica e che rappresentano l'Europa nell'International Cybersecurity Challenge. Composto da persone con background e competenze diverse, Team Europe si impegna a far progredire le conoscenze e le competenze in materia di sicurezza informatica, nonché a promuovere la collaborazione internazionale per affrontare le minacce informatiche emergenti. Attraverso la loro partecipazione a questa competizione globale, Team Europe mette in mostra il meglio dei talenti europei della sicurezza informatica e contribuisce a plasmare il futuro della sicurezza informatica.
Gli ultimi 2 anni di attività di Team Europe hanno visto il coinvolgimento di 2 giocatori italiani provenienti da TeamItaly in entrambe le edizioni, mentre, dalla sua costituzione, il coach di TeamItaly è Mario Polino, uno dei 5 allenatori della squadra europea.

14. Persone e infrastrutture a supporto di The Big Game

Il programma – completamente gratuito per tutti i partecipanti e realizzato anche grazie alle sponsorizzazioni sia delle università partecipanti sia di importanti realtà industriali – si avvale della collaborazione non solo di professori e ricercatori esperti nei vari ambiti della cybersicurezza provenienti dalle università coinvolte, ma anche membri dei migliori team italiani Capture-the-Flag, partecipanti alle vecchie edizioni di CyberChallenge.IT, e dei componenti della Nazionale Italiana Cyberdefender TeamItaly.
Per le diverse attività organizzate nell'ambito di The Big Game si usano infrastrutture informatiche avanzate, interamente sviluppate, gestite e costantemente aggiornate internamente dal Cybersecurity National Lab. Il livello di qualità delle infrastrutture è elevato in termini di sicurezza, affidabilità, scalabilità e soluzioni di implementazione, come dimostrato anche dal fatto che queste sono state scelte, a livello internazionale, per le gare di attacco-difesa tra le squadre rappresentanti i vari continenti che si sono svolte nel 2022 ad Atene e nel 2023 a San Diego in California.

Anche i materiali didattici e le sfide utilizzate nelle diverse competizioni sono elaborati internamente al Laboratorio, aggiornati e inseriti nei percorsi formativi rivolti a studenti, studentesse e docenti. Inoltre, per supportare adeguatamente la formazione sulla sicurezza di rete e hardware, è stato implementato un CyberRange ibrido, denominato PAIDEUSIS, fisicamente situato a Lucca, presso la sede di IMT, attraverso il quale i partecipanti possono utilizzare, da remoto, infrastrutture fisiche condivise per il training su tematiche specifiche, quali la sicurezza dell'Hardware e delle Reti.

15. The Big Game: i prossimi passi

Tra le "promesse" del Cybersecurity National Lab per i prossimi mesi, vi è senza dubbio quella di voler coinvolgere un numero crescente di giovani, con

19 https://teameurope.site

particolare riferimento alle ragazze che dovranno sempre più essere presenti alle competizioni di CyberChallenge.IT e OliCyber.IT.

Oltre a questo, tra i sogni nel cassetto c'è quello di rendere "The Big Game" un modello di riferimento per la sensibilizzazione, la formazione e l'addestramento sui temi della cybersicurezza. Un modello che possa diventare scalabile, da proporre ad altri target di popolazione come, per esempio, le persone con diversa abilità o a rischio di emarginazione sociale (carcerati, NEET, disoccupati per esempio).

Il gioco ha dimostrato negli anni e continua a dimostrare come sia tangibile l'impatto in termini di acquisizione di competenze e capacità di "difesa" delle persone, utili a rafforzare la sicurezza informatica di imprese, Pubblica Amministrazione e istituzioni, ovvero dell'intero sistema Paese che potrebbe così contare sulle persone oltre che su tecnologie e processi utili a difendere il proprio perimetro.

BIOGRAFIE

Gaspare Ferraro. Responsabile tecnico del CINI *Cybersecurity National Lab*, è coordinatore di CyberChallenge.IT e delle Olimpiadi Italiane di Cybersicurezza, programmi gratuiti di formazione e competizioni in cybersicurezza che annualmente coinvolgono più di 10.000 studenti e studentesse dai 14 ai 24 anni. Team Manager del TeamItaly, la Nazionale Italiana di Cyberdefender, è Technical Chair nell'Executive Committee di ECSC per ENISA, la European Union Agency for Cybersecurity.

E-mail: gaspare.ferraro@cybersecnatlab.it

Sonia Montegiove. Giornalista, informatica, formatrice, è coordinatrice di CyberTrials, programma gratuito di formazione e gaming per studentesse delle scuole superiori di II grado organizzato dal *Cybersecurity National Lab* del CINI (Consorzio Interuniversitario Nazionale per l'Informatica). È autrice di due libri sull'uso consapevole delle tecnologie digitali: "Gnomeide, salvate le mamme e i papà" e "Gnomeide2, manuale di sopravvivenza ai social network". Ultimo libro, scritto con Chiara Lalli, "Mai dati", storia di una inchiesta giornalistica che rimarca l'importanza dell'apertura dei dati.

E-mail: sonia.montegiove@cybersecnatlab.it

Paolo Prinetto. Professore ordinario di "Sistemi di Elaborazione delle Informazioni" presso il Politecnico di Torino e presso IMT – Scuola Alti Studi Lucca. Direttore del CINI *Cybersecurity National Lab* e coordinatore della filiera di formazione e addestramento *The Big Game*. Membro del Comitato Scientifico del *Centre National de la Recherche Scientifique* (CNRS) francese. Attività di ricerca principalmente rivolte alla sicurezza dell'hardware e alla progettazione e al collaudo di sistemi digitali.
E-mail: paolo.prinetto@cybersecnatlab.it