Crosetto, 'Intelligenza artificiale priorità del governo'
Va contrastato potenziale uso improprio di clan e terroristi

(ANSA) - ROMA, 06 MAR - "In anni recenti, la crescente presenza e complessità delle minacce informatiche ha fatto sì che il cyberspazio fosse considerato, nel settore della Difesa, un nuovo dominio operativo, al pari dei domini terrestre, marittimo, aereo e spaziale". Così il ministro della Difesa, Guido Crosetto, in una nota letta al CyberSec2024 in corso a Roma. "Di fronte alle insidie, i Paesi più avanzati hanno incrementato gli sforzi per rafforzare le proprie strutture di cybersecurity, le proprie capacità di resilienza. La difesa italiana, da parte sua, sta potenziando la digitalizzazione e aggiornando i suoi modelli operativi per garantire la sicurezza al massimo grado - prosegue - Questo include l'adozione di tecnologie all'avanguardia come l'intelligenza artificiale, i servizi cloud evoluti, le info-strutture spaziali, fino ai nuovi standard di cifratura a protezione delle informazioni. Investire nella formazione di professionalità con specifiche competenze nel settore cyber è, oggi come oggi, essenziale". Crosetto nel messaggio sottolinea che "sono molte le iniziative per attrarre le migliori competenze a supporto dell'ecosistema difesa: tra queste, la realizzazione di una 'riserva cyber' che possa coinvolgere anche professionalità del mondo privato, da attivare in caso di crisi, a supporto delle capacità esprimibili della difesa. L'intelligenza artificiale rappresenta quindi una priorità per il governo italiano, soprattutto per contrastare il potenziale uso improprio da parte di organizzazioni con finalità ostili, tra le quali quelle di matrice terroristica e criminale". "Uno degli obiettivi più complessi - conclude - è quello di trovare un equilibrio tra sicurezza e difesa dei diritti puntando su governance multilaterali e regolamentazioni etiche. A partire dalla collaborazione con l'Unione Europea per l'approvazione dell'Artificial intelligence act: strumento utile a stabilire principi di gestione dell'Ia che assicurino il pieno controllo umano, senza compromettere le opportunità di sviluppo". (ANSA).

Cybersecurity: Fontana, è essenziale per la sicurezza nazionale

(ANSA) - ROMA, 06 MAR - "La cybersecurity è diventata in tempi brevi una componente essenziale della sicurezza nazionale. La capacità di prevenire, contrastare e rispondere agli attacchi informatici è, infatti, parte integrante di tutte le moderne strategie di difesa. La crescente interconnessione digitale del nostro mondo rende, dunque, imperativo comprendere e affrontare le sfide emergenti legate alla sicurezza online. L'intelligenza artificiale, divenuta un catalizzatore di innovazione in molteplici settori, già offre strumenti potenti e sofisticati per migliorare la nostra capacità di difenderci dalle minacce emergenti. Tuttavia, questo traguardo non ci esime dalla responsabilità di affrontare questioni ulteriori che l'impiego dell'intelligenza artificiale porta con sé e che non si erano mai poste prima: questioni che spaziano dalla sicurezza all'etica, dal controllo delle minacce alla libertà d'espressione e informazione, dalla tutela degli interessi pubblici sensibili alla protezione della riservatezza di ciascun individuo. In tale contesto, siamo chiamati a bilanciare progresso tecnologico e responsabilità sociale. Insieme, possiamo plasmare un futuro in cui la tecnologia e la sicurezza interagiscano armoniosamente, promuovendo la prosperità e la stabilità della nostra democrazia". Così il presidente della Camera dei deputati, Lorenzo Fontana, in un messaggio rivolto in occasione del convegno "Cybersec2024" a Roma. (ANSA).

Mantovano, 'Effetti IA saranno anche su sicurezza Paese'
'Rivoluzionerà la nostra vita. Ma ha duplice risvolto'

(ANSA) - ROMA, 06 MAR - L'intelligenza artificiale "rappresenta già oggi - e ancor più lo sarà nei prossimi anni - uno dei fenomeni che maggiormente rivoluzioneranno ogni aspetto della nostra vita e i cui effetti si dispiegheranno, come è inevitabile, anche sulla sicurezza nazionale". A dirlo in una nota letta al CyberSec2024 in corso a Roma è il sottosegretario alla presidenza del Consiglio Alfredo Mantovano. "Il rapido sviluppo e la repentina adozione di tecnologie basate sull'intelligenza artificiale genereranno un

insieme complesso di opportunità e di sfide, le quali necessitano fin da subito di una profonda analisi e di azioni strategiche ben congegnate e pianificate - prosegue - Tuttavia, come accade per la maggior parte delle tecnologie, anche l'intelligenza artificiale può essere esaminata attraverso una duplice lente di osservazione". Se si prendono in considerazione "gli effetti positivi per la nostra sicurezza nazionale - continua Mantovano - l'intelligenza artificiale può elaborare e analizzare rapidamente una grande mole di dati e di informazioni, rilevando, ad esempio, schemi e correlazioni utili a far emergere imminenti minacce alla sicurezza nazionale. Così come può prevedere e coordinare in maniera tempestiva ed efficace le risposte in emergenza, ottimizzando il dispiegamento di risorse. Inoltre, attraverso l'analisi mirata e automatizzata delle comunicazioni e delle transazioni finanziarie, l'intelligenza artificiale può supportare anche i nostri operatori nell'identificazione e nel monitoraggio di individui o gruppi sospettati di terrorismo o appartenenti alla criminalità organizzata". Per quanto riguarda la cybersicurezza, "questa tecnologia può continuare a innalzare le capacità di identificazione e valutazione degli attacchi informatici, contrastandoli in tempo reale e con sempre maggiore efficacia". (ANSA).

Frattasi (Acn),'intelligenza artificiale può portare benefici
'Attenzione ai rischi. Dati possono essere manipolati'

(ANSA) - ROMA, 06 MAR - "L'intelligenza artificiale è un tema straordinariamente importante, come sappiamo può portare un beneficio immenso alla vita della nostra società: un miglioramento dei nostri sistemi difensivi, un miglioramento della nostra vita associata, può semplificare i processi produttivi, farci risparmiare nei costi dei sistemi produttivi". Così il direttore generale dell''Agenzia per la cybersicurezza nazionale (Acn), il Prefetto Bruno Frattasi, a CyberSec2024 in corso a Roma. "Ma ci sono anche dei rischi associati anche alle ultime forma di intelligenza artificiale che chiamiamo di intelligenza generativa e che si avvicinano al linguaggio umano - prosegue - Il problema dell'intelligenza artificiale applicata ai vari settori diventa immediatamente un problema di sicurezza informatica per quello che riguarda la protezione e la vulnerabilità dei dati e che possono essere oggetto di un intervento esterno di manipolazione che vuol dire correzione del dato per fini non accettabili, che non possono essere accettati secondo i parametri valoriali che ci siamo dati da sempre".

Frattasi (Acn), 'Regolamentazione europea è indispensabile'
'Punto di riferimento ineludibile. Bisogna partire da questo'

(ANSA) - ROMA, 06 MAR - "Il modello europeo regolatorio è indispensabile perché se ci siamo resi conto di avere dei rischi seri non può non conseguire da questo che ci sia una regolamentazione che governi e minimizzi il rischio". Così il direttore generale di Acn, L'Agenzia per la cybersicurezza nazionale, il Prefetto Bruno Frattasi, a CyberSec2024 in corso a Roma. "Non c'è dubbio che il modello regolatorio è un punto di riferimento ineludibile da cui bisogna partire. Vedremo nei prossimi mesi come arriveremo alla conclusione del processo che sta portando all'approvazione di questo provvedimento", conclude. (ANSA).

Frattasi (Acn), 'Lavorare a policy di sicurezza informatica'
'Vogliamo costruire un gruppo permanente strutturato'

(ANSA) - ROMA, 06 MAR - "Vogliamo costruire un gruppo permanente strutturato che lavori alle policy di sicurezza informatica in modo che queste policy siano frutto di condivisione". Così Bruno Frattasi, direttore generale dell'Agenzia per la cybersicurezza nazionale, a margine dell'evento CyberSec2024 presso il Palazzo delle Esposizioni a Roma, sulla proposta dell'Acn riguardo la sicurezza informatica in vista della presidenza italiana del G7. "Lo abbiamo lanciato perché ci sembrava opportuno farlo in vista della presidenza italiana

del G7 e abbiamo già ricevuto dei riscontri positivi dagli altri responsabili delle agenzie e centri di sicurezza cyber. Stiamo costruendo l'agenda dei lavori che a maggio si svolgeranno in Italia insieme agli altri colleghi degli altri sei paesi. Porteremo il frutto del nostro lavoro all'attenzione dei vertici delle varie nazioni e spero che ci ascolteranno". La volontà è "far conoscere alla politica quali sono tutte le questioni che si dispiegano sul campo della sicurezza informatica e dare a loro tutti gli strumenti per governare il rischio digitale", conclude Frattasi. (ANSA).

Gagliano, 'Su intelligenza artificiale unire le forze'
'Se lavoriamo in modo disgiunto non andiamo lontano'

(ANSA) - ROMA, 06 MAR - "Bisogna fare sistema paese, siamo agli albori dell'avvento dell'intelligenza artificiale. È Necessario unire le forze. Da soli non possiamo guidare tale complessità. È necessario che tutti, il mondo industriale, la ricerca, la pubblica amministrazione, le istituzioni, le forze armate siano in grado di collaborare davvero condividendo risorse e progetti". Così il capo del VI reparto informatica cyber e telecomunicazioni dello stato maggiore della Difesa, Giovanni Gagliano, a CyberSec 2024 in corso al Palazzo delle Esposizioni a Roma. "Abbiamo la necessità di sviluppare Ia secondo i bisogni delle nostre istituzioni. Ma se facciamo questo in maniera disgiunta non andiamo lontano, è un mondo molto complesso", aggiunge. (ANSA).

Gagliano, 'l'Ia è stata cambio di paradigma per la difesa'
'Modifica di video e audio può influenzare l'opinione pubblica'

(ANSA) - ROMA, 06 MAR - "L'introduzione dell'intelligenza artificiale è stata una rivoluzione che ha avuto effetti nella nostra società ma è stata anche un cambio di paradigma per la difesa che impiega già strumenti di Ia sia per controllare l'accesso alle reti sia per analizzare la quantità notevole di dati che tutti i giorni vengono trattati". Così il capo del VI reparto informatica cyber e telecomunicazioni dello stato maggiore della Difesa, Giovanni Gagliano, a margine dell'evento CyberSec 2024 in corso al Palazzo delle Esposizioni a Roma.Chi perpetra attacchi "alle nostre reti utilizza oggi algoritmi al posto di cyber warrior veri e propri - prosegue - attacchi che possono essere automaticamente capaci di vedere dove sono le nostre reti e colpirle". Gagliano sottolinea infine che "forse uno degli aspetti più importanti di questi ultimi mesi, di cui stiamo avendo contezza, è il fatto che venga impiegata l'intelligenza artificiale per hackerare la realtà attraverso la modificazione di video e audio. Questo può influenzare le opinioni pubbliche a seconda di quelli che sono gli scopi di chi li impiega". (ANSA).

Rizzi, 'Adeguare codice di procedura penale al digitale'
Vicecapo della Polizia, 'davanti sfida giuridico ordinamentale'

(ANSA) - ROMA, 06 MAR - "Siamo davanti a una sfida tecnica e giuridico ordinamentale. Sotto quest'ultimo aspetto siamo lontanissimi da una soluzione. Il nostro nuovo codice di procedura penale è nato in epoca analogica, oggi le scie digitale e tutto il mondo cyber in quel codice non ci sono. Nel momento in cui non ci sono, le norme nate con il mondo analogico e dell'imperfezione, della tradizione, vengono tirate e stirate e alla fine si spezzano per potersi adeguare al mondo digitale". Così il vice capo della polizia, Vittorio Rizzi, a CyberSec2024 in corso a Roma. "La vera sfida è adeguare il nostro codice di procedura penale alle scie digitali, poter imparare a riconoscerle, usarle nell'ambito di un processo penale", sottolinea. (ANSA).

Rizzi, 'Confine tra virtuale e digitale sempre più complesso'
'Il primo esiste solo in potenza. Ma lì vittime reali'

(ANSA) - ROMA, 06 MAR - "Se dovessi scegliere una parola per definire il tempo in cui viviamo, la parola giusta è: confine. Siamo abituati a confrontarci con questa parola immaginando i confini territoriali. Ma è anche il confine tra mondo reale e digitale, che non amo chiamare virtuale perché è ciò che non esiste, esiste solo in potenza. E da poliziotto so che nel mondo virtuale si mietono vittime reali, per questo motivo ho imparato a chiamarlo mondo digitale. In questo mondo, questo confine diventa sempre più complesso tra ciò che è vero, verosimile, falso e illusorio". Così il vicecapo della polizia, Vittorio Rizzi, a CyberSec2024 in corso a Roma. (ANSA).

Aceto (Carabinieri), 'Serve modello difesa agile'
'Non sottovalutare il fattore della tecnologia'

(ANSA) - ROMA, 06 MAR - "Serve un modello di difesa snello, agile, scalabile che credo debba essere fondato su tre fattori chiave". Così il capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, Paolo Aceto, a CyberSec2024 in corso a Roma. "Il primo fattore sono le competenze, la formazione continua degli utenti, di specializzazione e anche in termini di consapevolezza. È un fattore determinante per il successo o il fallimento per le scelte su tutti gli altri campi. Il secondo da non sottovalutare è quello delle tecnologie. Sono l'insieme degli asset posti a difesa delle infrastrutture ma è anche il bacino informativo di partenza da cui attingere per selezionare le minacce e individuare le risposte . Il terzo elemento - conclude- è costituito dai processi che devono essere efficienti e consolidati per ridurre al minimo i tempi di risposta alle minacce". (ANSA).

Aceto (Carabinieri), 'L'Ia ha rischi e opportunità'
'Pericolo criminalità cyber riguarda anche i cittadini'

(ANSA) - ROMA, 06 MAR - "Se da un lato esiste la reale preoccupazione che le piattaforme di intelligenza artificiale possano fornire a utenti malevoli nuovi fattori abilitanti in grado di aggirare le tecnologie e i processi di sicurezza esistenti, dall'altro sono in molti a ritenere che siano destinate a imprimere un enorme impulso alla sicurezza". Così il capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, Paolo Aceto, a CyberSec2024 in corso a Roma. "Si tratta di una sfida tecnologica tra rischi e opportunità sotto tanti punti di vista - prosegue - Sfida nella quale assume rischio dirompente il rapido sviluppo dell'intelligenza artificiale generativa. Può creare contenuti digitali inediti che determinano molteplici aspetti nel campo della sicurezza informatica. Tuttavia - sottolinea Aceto - le potenzialità dell'intelligenza generativa assumono rilievo anche sotto l'aspetto del rischio della criminalità cyber. È un rischio che riguarda non solo le nostre istituzioni e aziende ma anche i singoli cittadini sui quali la nostra attenzione e il nostro impegno deve essere al massimo livello". (ANSA).

Benifei, modelli fondativi IA tema difficile nei negoziati Ue
'Abbiamo fatto bene a non cedere alle pressioni di Parigi'

(ANSA) - BRUXELLES, 06 MAR - La regolamentazione dei modelli fondativi di intelligenza artificiale, come GPT-4, alla base del chatbot ChatGPT, "è stato uno dei temi più difficili da sciogliere anche nella sua costruzione complessiva del negoziato finale" sulla legge europea in materia di IA, ma "abbiamo fatto bene a non cedere a determinate pressioni che forse oggi" alla luce della partnership siglata di recente tra Microsoft e Mistral, start up francese campione dell'IA "potrebbero essere lette in un altro modo". Così il

capodelegazione Pd al Parlamento Europeo e relatore dell'AI Act, Brando Benifei, intervenendo al CyberSec2024 in corso a Roma. L'idea che si dovesse avere una "mano leggera" sui modelli più potenti, come chiesto in particolare da Parigi, "non era condivisa nemmeno dal commissario francese Breton che ha tenuto la stessa linea di noi negoziatori parlamentari" ha spiegato l'eurodeputato, rivendicando il risultato finale delle trattative, al netto di "una vicenda di cui magari vorremmo capire meglio tempi e modalità". (ANSA).

Polizia Postale, 'a gennaio 1008 casi di sicurezza cibernetica'
Direttore, '66 attacchi critici'

(ANSA) - ROMA, 06 MAR - "Il trend di gennaio 2024 conferma quello dello scorso anno: 1008 casi di sicurezza cibernetica solo a gennaio scorso. Sono quindi 12, 13mila casi l'anno. Fino a pochi anni fa eravamo nell'ordine di qualche centinaia di casi annui. Oggi siamo davanti a una significativa esplosione di criminalità informatica specializzata e iper strutturata". Questi i dati illustrati dal direttore del Servizio Polizia Postale e delle Comunicazioni, Ivano Gabrielli, a CyberSec2024 in corso a Roma.Sono stati poi "66 i cyber attacchi critici. Gli eventi riguardano soprattutto le infrastrutture più sensibili che erogano servizi essenziali", e quindi contro Pa e aziende.

Gabrielli, 'Cybercrime comincia a mettere a rischio economia'
'C'è bisogno di implementare un framework internazionale'

(ANSA) - ROMA, 06 MAR - Il costo globale della criminalità informatica raggiungerà i 10.5 trilioni di dollari entro il 2025, "è una stima fatta nell'ultima assemblea generale dell'Interpol. Il Cybercrime è stato messo al primo posto da un punto di vista delle emergenze. Comincia a essere una realtà criminale sfruttata da gruppi criminali che cominciano a mettere a rischio la moderna economia. Potremmo trovarci a parlare del cybercrime come nuova forma di criminalità organizzata altamente redditizia e quindi appetito dalla criminalità organizzata. Stiamo parlando di un fenomeno mondiale". Così il direttore del Servizio Polizia Postale e delle Comunicazioni, Ivano Gabrielli, a CyberSec2024 in corso a Roma. Per contrastarlo "C'è bisogno di implementare un framework internazionale che faccia condividere a tutti gli stati un framework di norme penali e procedurali che velocizzi e permetta lo sviluppo rapido dell'attività investigativa", conclude. (ANSA).

Perego, 'fornire linee guida etiche a sviluppatori Ia'
'Trasformazione che richiederà flessibilità istituzionale'

(ANSA) - ROMA, 06 MAR - "È fondamentale fornire agli sviluppatori delle linee guida etiche così da assicurarsi fin dall'inizio che gli algoritmi si attengano ai nostri codici morali. Questa è la ragione per cui sia gli Stati Uniti sia l'Unione Europea si sono dotati di linee guida nel campo dell'etica per lo sviluppo dell'uso dell'intelligenza artificiale. Questa trasformazione richiederà creatività individuale, agilità organizzativa, flessibilità istituzionale e sostegno politico ed economico". Così il sottosegretario di Stato al ministero della Difesa, Matteo Perego di Cremnago, al CyberSec2024 in corso a Roma. "Più che identificare chi vincerà questa sfida possiamo identificare facilmente chi la perderà: i paesi lontani da questo modello e che si stanno allontanando - prosegue - Mantenere, quindi, i cervelli in sinergia con le aziende di settore e gestire correttamente gli investimenti legati alla difesa e mantenere la sovranità nel settore tecnologico è al momento l'unica soluzione possibile". (ANSA).

Cybersecurity: Casu (Pd), servono maggiori investimenti

(ANSA) - ROMA, 06 MAR - "A pagina 12 della strategia nazionale di Cybersicurezza è scritto chiaramente che per proteggerci nel nuovo mondo sempre più digitale serve destinare a questo l'1,2% degli investimenti pubblici lordi, guardando i dati del 2022 almeno 1,8 miliardi l'anno. Visto che il Governo Meloni non ha cambiato questo impegno, adesso ha il compito di rispettarlo a partire dal prossimo Documento di Economia e Finanza. Non è un costo in più, ma un investimento indispensabile e non più rinviabile". Così il deputato democratico, Andrea Casu, intervenendo all'evento CyberSec2024 in corso a Roma. "Grazie a un ordine del giorno che abbiamo presentato dall'opposizione, approvato dalla Camera in occasione della legge di delegazione europea, anche i dati di Comuni e province possono essere protetti con i massimi livelli di cybersicurezza previsti dalla direttiva Nis 2, ma adesso per farlo servono risorse concrete. E anche le piccole e medie imprese - aggiunge - non possono essere lasciate sole nel fronteggiare una minaccia crescente che ci sta trasformando nel paese di Bengodi dei cybercriminali: se In Italia gli attacchi crescono oltre 7 volte più velocemente che nel resto del mondo è perché non stiamo alzando la guardia della difesa come dovremmo e come stanno facendo gli altri". "L'evento di oggi - conclude - è importante perché richiama l'attenzione di un punto centrale ma troppo spesso sottovalutato dell'agenda politica: la regolamentazione è importante ma le regole da sole non bastano servono anche gli strumenti e una politica industriale italiana ed europea che sostenga un cambiamento di sistema non più rinviabile". (ANSA).

ANSA/ Al CyberSec2024 rischi e opportunità dell'IA

Al via la due giorni al Palazzo delle Esposizioni a Roma

ROMA

(ANSA) - ROMA, 06 MAR - I rischi e le opportunità dell'intelligenza artificiale, le sfide della cybersecurity e il cybercrime, dalla difesa alla sanità. Sono i temi che CyberSec2024 ha messo al centro della sua terza edizione e lo ha fatto "nell'era dell'Ai", anche sottotitolo all'evento. A partire dalla Difesa, come è stato ricordato più volte nei panel della prima giornata al Palazzo delle Esposizioni di Roma, si sta potenziando la digitalizzazione. "Questo include l'adozione di tecnologie all'avanguardia come l'intelligenza artificiale, i servizi cloud evoluti, le info-strutture spaziali, fino ai nuovi standard di cifratura a protezione delle informazioni", ha infatti sottolineato il ministro della Difesa, Guido Crosetto, in un messaggio letto all'inizio della prima giornata di CyberSec2024. L'Ia rappresenta, quindi, "una priorità per il governo italiano", si legge ancora nella lettera, "soprattutto per contrastare il potenziale uso improprio da parte di organizzazioni con finalità ostili". Parlando proprio di Cybercrime il direttore del Servizio Polizia Postale, Ivano Gabrielli, ha ricordato come questo sia sempre più "una realtà criminale sfruttata da gruppi criminali che cominciano a mettere a rischio la moderna economia". Soltanto a gennaio si sono contati "1008 casi di sicurezza cibernetica" e "66 cyber attacchi critici". Pericolo e futuro, rischi e opportunità. Le due facce dell'intelligenza artificiale sono state quindi illustrate nel corso di tutti i panel. Come ha infatti sottolineato il direttore generale dell'Agenzia per la cybersicurezza nazionale (Acn), Bruno Frattasi, l'Ia "può portare un beneficio immenso alla vita della nostra società". Ma "ci sono dei rischi associati anche alle ultime forme di intelligenza generativa". Questo diventa un problema di sicurezza informatica per "la protezione e la vulnerabilità dei dati che possono essere oggetto di un intervento esterno di manipolazione". È un rischio che riguarda "non solo le nostre istituzioni e aziende ma anche i singoli cittadini", ha poi ribadito il capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, Paolo Aceto. Per il capo del VI reparto informatica cyber e telecomunicazioni dello stato maggiore della Difesa, Giovanni Gagliano, sull'intelligenza artificiale "è necessario quindi unire le forze. Da soli non possiamo guidare tale complessità". E proprio per riuscire a gestire questi nuovi fenomeni e il mondo cyber, la sfida che suggerisce il vicecapo della polizia Vittorio Rizzi è di "adeguare il nostro codice di procedura penale alle scie digitali, poter imparare a

riconoscerle, usarle nell'ambito di un processo penale". Questo perché le norme nate con il mondo analogico "vengono tirate e stirate e alla fine si spezzano per potersi adeguare al mondo digitale". (ANSA).

Al via la giornata conclusiva di Cybersec2024
Direttore Garofalo, 'è un tema che dipende dalla geopolitica'

(ANSA) - ROMA, 07 MAR - "Secondo noi la cybersicurezza non è solo una questione tecnologica ma dipende fortemente dal contesto geopolitico e ci troviamo in un contesto geopolitico caratterizzato da conflitti e da guerre ibride che vanno dall'Ucraina al Medio Oriente al mar Rosso". Così il direttore di Cybersecurity Italia, Luigi Garofalo, in apertura della seconda e ultima giornata della terza edizione di CyberSec2024, nella Serra del Palazzo delle Esposizioni, a Roma. La prima parte della mattinata sarà dedicata alla cooperazione internazionale in tema di cybersicurezza. (ANSA).

Cirielli, IA e cybersecurity, far squadra in istituzioni globali
Tecnologie 'amplificano la possibilità di minacce'

(ANSA) - ROMA, 07 MAR - Le tecnologie legate all'attacco alla cybersicurezza e quelle dell'intelligenza artificiale "ampliano a dismisura la possibilità di minacce, che non sono sono quelle normalmente simmetriche legate alla minaccia militare, ma anche tutte quelle asimmetriche, soprattutto di tipo economico, che riguarda le aziende": lo ha detto il viceministro degli Esteri Edmondo Cirielli intervenendo all'evento Cybersec24 in corso a Roma, dedicato proprio alla sicurezza informatica nell'era dell'intelligenza artificiale. Per Cirielli, "la difesa dei nostri interessi, tecnologici ed economici, rappresenta un elemento centrale della nostra politica globale" e dal momento che "con i nostri alleati dell'Unione Europea, del G7, della Nato condividiamo in maniera profonda dei valori di democrazia e dello stato di diritto, in queste istituzioni bisogna cercare di fare ancora più squadra. Non è sempre facile. Sappiamo che spesso abbiamo divergenze di vedute con i nostri alleati. Spesso qualche alleato è più spregiudicato, magari il primo che ci fa concorrenza anche subito dal punto di vista tecnologico ed economico. Però dobbiamo avere l'intelligenza la capacità di avere uno sguardo globale". (ANSA).

Cirielli, sulle tecnologie l'Italia mette al centro l'uomo
Viceministro, usare nostra capacità diplomatica per governarle

(ANSA) - ROMA, 07 MAR - L'interesse principale dell'Occidente e dell'Italia è regolare e governare a livello internazionale la cybersicurezza e l'intelligenza artificiale, "perché andranno avanti, non sono cose che si possono arrestare": lo ha detto il viceministro degli Esteri Edmondo Cirielli intervenendo a Cybersec24. "L'importante è riuscire a governarli secondo la nostra visione - ha osservato il viceministro - E la nostra visione è mettere l'uomo sempre al centro, mettere i diritti umani sempre al centro, i diritti dei cittadini e la democrazia, cioè i valori fondanti del nostro modo di vivere. E per farlo dobbiamo sederci al tavolo con gli altri. Gli altri probabilmente sono interessati ad altri aspetti. Ecco perché è fondamentale trovare un punto di intesa che ci consenta di far passare dei principi di regolamentazione del fenomeno". "Il tema - ha detto Cirielli - verrà affrontato in moltissime delle riunioni dei sette grandi organizzate dalla presidenza italiana del G7. Molti dei nostri ministeri stanno cercando di lavorare in tal senso. La Farnesina proietta la nostra azione diplomatica nei forum multinazionali, sia quelli dei paesi alleati, ma anche in quelli di confronto, oltre che chiaramente quello centrale delle Nazioni Unite per lavorare secondo la visione italiana". Grazie alla spiccata capacità diplomatica dell'Italia, ha concluso, "la Farnesina deve parlare dialogare, stringere alleanze e giocare un ruolo di mediazione sul piano internazionale. Lo stato deve mettere a regime le risorse anche con gli alleati, ma capire che deve intervenire più massicciamente investendo soprattutto nella tecnologia. Il

tema della cybersecurity, e ancor più dell'intelligenza artificiale, è l'elemento centrale che caratterizzerà il futuro del nostro pianeta, per cui è qualcosa su cui dobbiamo concentrarci". (ANSA).

Cirielli, 'dossieraggio? Non mi sorprende'
'Spero accessi avvenuti secondo la legge. Altrimenti mi tutelo'

(ANSA) - ROMA, 07 MAR - "Non conosco i fatti, ho soltanto letto da giornali che ci sarebbero stati degli accessi abusivi per spiarmi, la cosa non mi sorprende né mi amareggia più di tanto, in Italia il binomio di una certa parte della magistratura collegato alla spregiudicatezza di alcuni giornalisti usando i meccanismi illegali del potere statale per spiare le persone, quindi senza giornalismo d'inchiesta, mi ha già toccato in passato. Il tema bisogna vedere se è vero, io voglio sperare che questi accessi siano avvenuti nel rispetto delle norme, non voglio credere sia accaduto altrimenti. Se così non fosse mi tutelerò non solo come parte civile ma anche chiedendo accesso agli atti perché voglio capire bene chi è il mandante di eventuali comportamenti illeciti". Così il viceministro degli Esteri, Edmondo Cirielli, sulla vicenda nota come "dossieraggio" a margine dell'evento CyberSec2024 al Palazzo delle Esposizioni a Roma. (ANSA).

Cirielli, 'tema dell'Ia in uso militare esiste'
'Uso della scienza all'avanguardia nelle relazioni pacifiche'

(ANSA) - ROMA, 07 MAR - "La tecnologia da tempo pervade soprattutto gli schieramenti militari dell'Alleanza atlantica che usa l'impegno militare come deterrenza per un mondo di pace. Sappiamo bene che la Russia, e in genere le organizzazioni terroristiche collegate a essa e ad altri partner mondiali autoritari, usano la tecnologia per controllare i propri popoli, la usano per le guerre asimmetriche, per spionaggio economico e tecnologico, quindi il tema esiste e nelle guerre viene messo ampiamente in campo". Così il viceministro degli Esteri, Edmondo Cirielli, a margine dell'evento CyberSec2024 presso il Palazzo delle Esposizioni a Roma, risponde ai giornalisti che gli chiedono se l'Ia verrà usata in azioni militari in corso come Aspides. "La scienza non è mai malvagia o buona è l'uso che ne fa l'uomo, e da questo punto di vista l'Italia, è all'avanguardia nelle relazioni pacifiche quindi lavoriamo perché in questa vicenda che rappresenta l'umanità giochi un ruolo importante la carta delle Nazioni Unite, il sistema dei valori che mette al centro l'umo, la dignità umana , la democrazia, le relazioni pacifiche. È importante quindi che questo tema del futuro si discuta tra tutte le nazioni per cercare un sistema che lo regolarizzi secondo il diritto internazionale", aggiunge. (ANSA).

Ue, impegno senza precedenti nella sicurezza informatica
Alonso, 'quadro geopolitico ha creato maggiore consapevolezza'

(ANSA) - BRUXELLES, 07 MAR - "Negli ultimi cinque anni siamo stati più attivi nel campo della sicurezza informatica a livello di Unione europea che in tutta la storia dell'Ue. Un motivo molto importante che ci ha spinto a essere così attivi, è stato il panorama delle minacce" che vanno dai comportamenti irresponsabili degli Stati nel cyberspazio alla criminalità informatica all'hacktivismo politicamente motivato, "quel che è cambiato è la situazione geopolitica" con la guerra di aggressione della Russia in Ucraina e il conflitto in Medio Oriente, e "anche se l'impatto nel dominio informatico dell'Ue è stato limitato, ciò ha creato un livello di consapevolezza e di vigilanza sulla sicurezza informatica che prima non esisteva". Così Lorena Boix Alonso, Direttore per la società digitale, l'innovazione e la sicurezza informatica alla DG Connect della Commissione europea, intervenendo al CyberSec2024 in corso a Roma. "In ambito legislativo, cosa piuttosto

eccezionale, nella cybersecurity, siamo passati ora dalla protezione delle infrastrutture critiche alla protezione della catena di approvvigionamento e persino a legiferare il modo in cui gestiamo la capacità operativa" ha aggiunto Alonso, ricordando l'accordo politico raggiunto ieri dalle istituzioni Ue sul Cyber Solidarity Act, che mira a costruire una risposta collettiva dell'Ue più resiliente contro le minacce informatiche. (ANSA).

Esperta Usa cybersec, 'Collaborare per affrontare minacce'
'Privati e governi devono lavorare insieme.Ia tempesta perfetta'

(ANSA) - ROMA, 07 MAR - "Ora che abbiamo raggiunto questa nuova frontiera, penso che la lezione che dobbiamo imparare in questo momento è che il settore privato e i governi devono lavorare insieme per affrontare le minacce del cyberspazio. Abbiamo bisogno di capacità per affrontarle". A dirlo nel corso del suo intervento è la direttrice del Cyber Threat Intelligence Integration Center & the IC Cyber Executive,Office of the Director of National Intelligence, Laura Galante, al CyberSec2024 in corso a Roma. Con l'intelligenza artificiale, sottolinea, "stiamo assistendo alla tempesta perfetta". E, quindi, "dobbiamo usare il vantaggio che abbiamo in questo momento per costruire le nostre difese". (ANSA).

Butti, 'governo presenterà provvedimento su Ia'
'Ci basiamo su peculiarità nazionale, aspetti tecnici a Europa'

(ANSA) - ROMA, 07 MAR - "Il governo ha già predisposto, ed è in discussione alle Camere, un disegno di legge sulla cybersecurity. E sta predisponendo un provvedimento interamente dedicato all'intelligenza artificiale che credo passerà in Consiglio dei ministri entro due o tre settimane al massimo. Noi ci apprestiamo a partecipare alla ministeriale di Trento il 15 marzo relativamente all'intelligenza artificiale e alla digitalizzazione della pubblica amministrazione, con le idee molto chiare sull'IA. Il provvedimento che sarà presentato dalla presidente Meloni a breve raccoglie le indicazioni dell'Ia Act, gli aspetti tecnici li lasciamo all'Europa, noi dobbiamo condire questo provvedimento basandoci sulla peculiarità nazionale", così il sottosegretario alla presidenza del Consiglio con delega all'innovazione tecnologica, Alessio Butti, a margine dell'evento CyberSec2024 in corso al Palazzo delle Esposizioni a Roma. "Oggi c'è una consapevolezza, diversamente da quanto accadeva in passato, cioè che cybersecurity e Ia sono strettamente connessi, anche perché l'implementazione di queste due tecnologie è importantissima sia sotto l'aspetto economico, e quindi dello sviluppo economico, che del welfare per quanto riguarda la preoccupazione sull'occupazione del futuro", conclude. (ANSA).

Butti, 'martedì evento d'ascolto con imprese Ai'
'Rilasciata la strategia.In attesa di valutazioni della premier'

(ANSA) - ROMA, 07 MAR - "Grande attenzione per il G7. Lo stiamo facendo portando al G7 anche iniziative proposte dalla piccola e media, e non solo, impresa. Non è un caso che martedì, a Roma, io abbia organizzato con il presidente del Consiglio un evento importantissimo di ascolto. Perché la strategia dell'intelligenza artificiale è stata rilasciata ed è ora in attesa delle valutazioni politiche del presidente del consiglio. Quella di martedì sarà una fase importante d'ascolto, ci saranno tutte le imprese che fanno Ai". Così il sottosegretario alla Presidenza del Consiglio con delega all'innovazione tecnologica, Alessio Butti, al CyberSec2024 in corso a Roma. "Uno dei nostri obiettivi - prosegue - è quello di dedicare a questo Paese una politica industriale in materia di Ai e, se possibile, anche in tema di telecomunicazione perché

evidentemente a oggi non c'è. È una sfida che stiamo affrontando con dovizia di particolari ma anche con intelligenza". (ANSA).

Butti, 'nel 2025 traguardo 150 progetti Ai già avviati da PA'
'Nel 2026 arriveranno a 400. Si parla di visione'

(ANSA) - ROMA, 07 MAR - "Per il 2025 il traguardo da raggiungere è di almeno 150 progetti di intelligenza artificiale che sono stati già avviati dalla pubblica amministrazione e che arriveranno nel 2026 a 400. Abbiamo sfide interessanti da cogliere e da vincere". Così il sottosegretario alla presidenza del Consiglio con delega all'innovazione tecnologica, Alessio Butti, al CyberSec2024 in corso a Roma. "Si parla di visione. Penso che in questi 14 mesi il governo abbia dato una visione abbastanza chiara di quelli che sono i nostri obiettivi, non solo sulla digitalizzazione della pubblica amministrazione ma anche sulla implementazione dell'intelligenza artificiale nella pubblica amministrazione e una particolare attenzione e cura nei confronti della cybersecurity che è fondamentale", conclude. (ANSA).

Panzeri (Esa), nel 2024 prodotti e infrastrutture per 7 miliardi
'Commissione europea fornisce il 20% del budget per Agenzia''

(ANSA) - ROMA, 07 MAR - "Nel 2024 l'Esa dovrà sviluppare prodotti e infrastrutture spaziali per un totale di 7 miliardi di euro. Sono soldi che vengono da investimenti da parte degli stati membri e anche della Commissione europea che fornisce mediamente il 20% del budget a disposizione dell'agenzia. Vuol dire che la commissione crede nelle nostre attività. Noi abbiamo il dovere di proteggere questi investimenti. Proprio per questo nel 2024, tra qualche mese, saranno operative due infrastrutture che hanno lo scopo di andare a proteggere gli investimenti degli stati membri, della Commissione e di altri attori dello spazio, e i servizi che queste infrastrutture riescono a fornire". Così il Senior system security engineer dell'Agenzia spaziale europea (Esa), Massimo Panzeri, a CyberSec2024 in corso a Roma. (ANSA).

Chessa (Asi),'Attivati per sviluppare processi cybersecurity'
'L'agenzia sta investendo per la formazione del personale'

(ANSA) - ROMA, 07 MAR - "Asi si è attivata per sviluppare dei processi standard di cybersecurity e linee guida specifiche per le missioni spaziali. Sta rafforzando la sicurezza dei propri assetti e dei sistemi da lanciare proponendo lo sviluppo di sistemi sicuri e di sicurezza a vari livelli, provando a ridurre le minacce e le vulnerabilità dei potenziali rischi di attacco. Stiamo realizzando anche uno strumento che servirà ad agevolarci in questa attività", così il responsabile della Direzione Sicurezza dell'Agenzia Spaziale Italiana, Lorenzo Chessa, al CyberSec2024, in corso a Roma. Inoltre, "stiamo cercando di valorizzare la formazione del nostro personale. Stiamo investendo molto soldi, sia fondi nazionali sia del Pnrr, per fare attività che saranno attente all'aspetto della sicurezza e della cybersicurezza", conclude. (ANSA).

Urso, 'l'Ia elemento chiave per sviluppo dell'economia'
'Lavoriamo a provvedimento per nuove tecnologie'

(ANSA) - ROMA, 07 MAR - "L'intelligenza artificiale è un elemento chiave per lo sviluppo dell'economia e del tessuto produttivo. Grazie alla sua capacità di apprendere, adattarsi e migliorare continuamente, l'Ia può rivoluzionare i processi industriali a un livello mai visto prima, prospettando un incremento dell'efficienza e dell'innovazione. I dati indicano una crescita esponenziale del mercato italiano dell'Ia che raggiunge +52%

nel 2023, dopo che già nel 2022 aveva registrato un +32% rispetto all'anno precedente. Sei grandi imprese italiane su dieci hanno già avviato un progetto di Intelligenza Artificiale, almeno a livello di sperimentazione". Così il ministro delle Imprese e del Made in Italy, Adolfo Urso, in una lettera inviata a CyberSec2024 in corso al Palazzo delle Esposizioni a Roma."È importante creare le condizioni per uno sviluppo equo e armonico che coinvolga anche le Pmi - prosegue - È per questo che stiamo lavorando a un provvedimento collegato alla Finanziaria che vada nella direzione dello sviluppo delle nuove tecnologie come fattori abilitanti per lo sviluppo del tessuto produttivo, valorizzando la ricerca e lo sviluppo". Per quanto riguarda la proposta di regolamento europeo Ia Act, Urso sottolinea che "avrà un impatto importante sia per le aziende che producono sistemi e servizi di la che per quelle che le utilizzano". Al G7 con presidenza italiana, "il proposito è focalizzarsi sulla profonda accelerazione che negli ultimi anni si è registrata sul tema dell'integrazione di tali tecnologie nella società e nel tessuto produttivo. Ciò al fine di far convergere le politiche industriali dei paesi G7", aggiunge. Quest' evento "sarà preceduto da una Conferenza dei portatori di interesse, sotto la direzione di Confindustria, in partenariato con le associazioni industriali degli altri paesi del G7". (ANSA).

Urso, 'l'Ia elemento chiave per sviluppo economia' (2)

(ANSA) - ROMA, 07 MAR - "Nella Ministeriale Industria, l'Italia si farà portatrice di tre filoni di discussione: ci confronteremo sulle potenzialità dell'applicazione dell'IA e delle tecnologie emergenti al tessuto industriale, sull'importanza di garantire sicurezza e resilienza delle catene di approvvigionamento e delle reti di connettività (terrestri e non terrestri) e sulla necessità di promuovere e sostenere lo sviluppo digitale sostenibile e inclusivo a livello globale, con un focus sull'Africa, in linea con il Piano Mattei", si legge ancora nella lettera a CyberSec2024. Sui benefici che l'Ai che porterà al settore produttivo, questi "sono strettamente connessi alla cybersicurezza: l'integrazione tra Intelligenza Artificiale e cyber security è diventata essenziale nel settore in continua evoluzione". Il loro connubio "è essenziale per migliorare la protezione contro attacchi informatici e violazioni dei dati, il rilevamento e della risposta alle minacce, la dipendenza dall'intervento umano, i tempi di ripristino più dopo una violazione". Per il ministro "non si devono tuttavia sottovalutare i rischi derivanti dalle minacce in continua evoluzione. L'intelligenza artificiale può essere sfruttata dagli hacker con il duplice obiettivo di aumentare il numero di attacchi e di migliorare la qualità degli stessi e allo stesso tempo, l'Ai generativa può aiutare tecnici informatici malintenzionati nella creazione di nuovi codici malevoli e virus". Per ridurre i rischi "occorrerà adeguare le misure di sicurezza alle potenzialità dell'Ai e parallelamente dovrà essere fatto ogni sforzo per superare la significativa carenza di professionisti qualificati nel campo dell'Ai e della cybersicurezza". E sui corsi del MIMit, "quest'anno sono in programma sette seminari in tema di cybersicurezza di cui tre specificamente dedicati all'interazione tra Cybersecurity e Intelligenza artificiale - conclude Urso - Sarà anche necessario che governi e imprese investano nella ricerca e nello sviluppo. Anche in questo campo il MIMit finanzia numerosi Poli Europei di Innovazione Digitale (Edi) e centri di competenza ad alta specializzazione nei settori dell'Al e della Cybersecurity". (ANSA).