AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

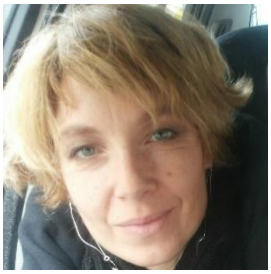
Newsletter

ANNO 2025 **n. 5/ 2025** **maggio 2025**

Cambiamenti del cyber warfare: l'impatto delle AI

La conduzione di operazioni nel dominio cibernetico e, più ampiamente, il cyber warfare rappresenta una minaccia sempre più concreta per la sicurezza nazionale nel contesto geopolitico internazionale.
L'uso dei sistemi di AI in questi contesti non può che complicare ulteriormente il quadro operativo. Facciamo un breve passo indietro per discutere di alcune premesse all'introduzione delle AI nel cyber warfare.
In generale, la contrapposizione bellica (warfare n.d.r.) vede nella dimensione del cyberspazio un ulteriore dominio della conflittualità, come espresso anche dalla Nato nel Summit di Varsavia nel 2016. In sostanza è avvenuto il riconoscimento del dominio cibernetico, come dominio operativo. Da qui il termine cyber warfare.
"*Questo spazio è stato definito come un ambiente virtuale che integra sistemi, reti e dati per supportare le operazioni militari e civili. Tuttavia, la natura in parte immateriale e transnazionale del dominio cibernetico presenta sfide uniche per la governance e la regolamentazione*" (fonte ISSMI 2024).
Durante l'ultimo governo Draghi, nel 2021, l'Italia aveva pubblicato il documento Position Paper dell'Italia sul Diritto internazionale e lo spazio cibernetico, in cui era stata fornita una prima analisi relativamente ad alcuni temi correlati al cyber warfare. Più specificamente il testo trattava la protezione della sovranità nel cyberspazio e le violazioni del principio di non intervento; l'applicazione del diritto della responsabilità internazionale degli Stati alle attività svolte nel cyberspazio; le operazioni informatiche e l'uso della forza; l'applicazione del diritto internazionale dei diritti umani, il ruolo degli stakeholder privati; e la cooperazione internazionale nel cyberspazio. Tenendo conto di tale paper, il tema del cyber warfare ha recentemente stimolato un nuovo studio di "*analisi del quadro normativo internazionale che regola la conduzione delle cyberspace operations dei diversi Stati. Il testo evidenzia:*
- la posizione delle più importanti organizzazioni internazionali circa l'applicabilità del diritto internazionale alla nuova dimensione operativa,
-l'applicazione sia di quanto previsto nella Carta delle Nazioni Unite nell'ambito dello jus ad bellum, sia del Diritto Internazionale Umanitario nell'ipotesi di un conflitto armato,
-l'evoluzione della dottrina NATO per la conduzione di operazioni nel dominio cibernetico, con particolare attenzione alle operazioni offensive,
IL fine ultimo del testo è creare una base di partenza per introdurre una definizione di arma cibernetica ed esplorare la possibilità di definire regole di ingaggio per la conduzione di un'operazione cibernetica" (fonte ISSMI 2024).
Anche se tale studio conclude affermando che "*uno Stato, pur nell'osservanza dell'intero quadro normativo, per restare competitivo nel sistema internazionale, deve necessariamente dotarsi di una capacità di condurre operazioni nel dominio cibernetico, inclusa la competenza per sviluppare e impiegare armi cibernetiche*", la cyber warfare fin qui teorizzata, pur con le incertezze del quadro normativo internazionale, si complica considerevolmente, alla luce dell'introduzione di sistemi di AI, che, sebbene adottati tanto per l'attacco quanto per la difesa, introducono maggiori rischi.
Una prima serie di rischi riguarda l'estensione della superficie di attacco, perché il codice con cui sono realizzate le AI potrebbe contenere vulnerabilità e perché i dati di apprendimento delle AI possono essere a loro volta soggetti ad attacchi che ne alterano e falsano l'apprendimento e quindi il comportamento durante l'uso. Inoltre, in caso di adozione di AI di tipo generativo, il codice stesso eventualmente prodotto dalle AI potrebbe non essere, a sua volta, sicuro. In aggiunta, test sulla sicurezza delle AI hanno evidenziato come in contesti critici o sensibili, le AI ancora non garantiscano piena robustezza e sicurezza e come si comportano

meglio in applicazioni in domini ben limitati come ad esempio nei casi di test nei quali si conosce bene il tipo di attaccante e le sue tecniche.
Una seconda serie di rischi riguarda i temi di attribuzione che, con l'uso delle AI, potrebbe diventare ancora più inestricabile. Recentemente Giorgio Mulè, Vicepresidente della Camera dei deputati in proposito ha osservato che: "le tecnologie di AI non sono controllabili come si vorrebbe e la mancanza di certezza sulla attribuzione renda globale l'impunità" aggiungendo anche l'ulteriore rischio di essere "in ritardo sul fronte AI, soprattutto del tipo usato per scopi di disinformazione e per le conseguenze a carattere cognitivo" sottintendendo difficoltà nella difesa da queste dinamiche di cognitive warfare.
Tutto ciò significa che l'adozione delle tecnologie di AI, da parte degli avversari digitali, aggrava un panorama già complicato dalle difficoltà proprie della cyber warfare che sono legate alla capacità di stabilire una violazione che abbia carattere di ostilità, confermare un'attribuzione e quantificare con precisione l'impatto, a livello di singolo Stato; questo perché le AI conferiscono le ulteriori complessità legate alla velocità d'azione ed alla estensione della portata di attacco (globalizzazione della minaccia).
Ovviamente anche le capacità dei difensori possono beneficiare di sistemi sofisticati di AI per le azioni di deception, detection e difesa, ma in generale "*si passa dalla contrapposizione strategico/militare fra Stati con mezzi digitali (definizione di Cyberwarfare) alla Algorithmic Warfare o dal cosiddetto Hyper Warfare, ovvero il confronto generato fra sistemi di algoritmi su fronti opposti, che si contrappongono in frazioni di secondo*" (Fonte Fabio Rugge vice rappresentante permanente presso il consiglio atlantico).
Nel panorama geopolitico di stati che si fronteggiano nel Cyberspazio, non sono da dimenticare i paesi emergenti che vengono dotati di tecnologie digitali, (quindi anche di sistemi di AI n.d.r.), per le quali non sono pronti, poiché è in queste "*cyber periferie digitali, i cyber ghetti che si annidano problemi e minacce*" come sostiene Emanuele Galtieri Ceo di C4gate.
Ma se il controllo delle ingerenze digitali resta primario, non è detto che azioni di cyber diplomacy, ovvero i tentativi di dialogo e di coordinamento internazionale al fine di prevenire i conflitti, ridurre le minacce e rafforzare le relazioni internazionali nel cyberspazio, (possano rappresentare la risposta all'impatto dell'AI nelle politiche internazionali ed alla conseguente e accresciuta competitività che ne deriva. In effetti nonostante tutta la tecnologia disponibile e le AI che possono supportare l'individuo, il sistema delle decisioni dovrebbe restare nel dominio umano per le decisioni sulla protezione di infrastrutture critiche civili e ancora di più in quelle militari. Sono quindi le diverse Forze Armate, insieme ad altri soggetti istituzionali, che necessitano di formazione specialistica e investimenti per prepararsi agli scenari di adozione delle AI per il potenziamento delle loro attività operative.



Alessia Valentini

Consulente di Cybersecurity, Advisor e Giornalista. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2025

Il 31 dicembre 2024 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2025".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Ricordiamo agli associati che non hanno ancora rinnovato la quota: il socio rimane iscritto nel libro soci per tre mesi ma perde il diritto di partecipare alla vita sociale e il diritto di voto e viene cancellato dalle mailing list di distribuzione soci. Scaduti i tre mesi il socio decade per morosità e deve effettuare di nuovo l'iscrizione pagando anche la relativa quota una tantum.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nella veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

Pubblicate le preziose linee guida sulla sicurezza dei trasporti ferroviari - Con decreto 4 marzo 2025 il Ministero dei Trasporti ha dato indicazioni cogenti e accurate afferenti allo sviluppo di un programma di valutazione e miglioramento della sicurezza dei trasporti ferroviari sia pubblici che privati. Eccone una breve sintesi.
L'autore ha apprezzato il documento in questione, soprattutto perché esso può costituire una preziosa guida anche per molti altri security manager, operanti in altri settori, che devono affrontare in modo globale il problema della sicurezza dei trasporti, non solo ferroviari. Evidentemente, i trasporti ferroviari hanno delle peculiarità, che devono essere analizzate in maniera specifica, ma la filosofia generale del documento è sicuramente applicabile anche in altri contesti. Ecco il motivo per cui si raccomanda caldamente ad ogni security manager di esaminare attentamente questo documento.
Il documento prende in esame tutti gli aspetti critici della gestione ferroviaria, suddivisi in 14 paragrafi. Dopo l'illustrazione dei principi generali, si passano ad analizzare in particolare i requisiti specifici afferenti alle gallerie, sia di nuova realizzazione, sia quelle già operative. È ben noto come una galleria ferroviaria rappresenti un punto estremamente critico dell'intera rete, e possono essere presenti criticità significative, che richiedono interventi correttivi urgenti, in caso di emergenze. Ecco perché il documento impone al gestore della rete di predisporre uno schema di piano di emergenza e soccorso, applicabile a tutte le gallerie, il cui sviluppo sia superiore a 1000 m; il documento deve essere portato a conoscenza delle strutture locali, ad esempio il prefetto e la protezione civile, in modo che le strutture potenzialmente coinvolte possano essere tempestivamente coinvolte.
(continua…)
https://www.puntosicuro.it/security-C-125/pubblicate-le-preziose-linee-guida-sulla-sicurezza-dei-trasporti-ferroviari-AR-25304/
Punto Sicuro - *Adalberto Biasiotti - 24/04/2025*

Countries Begin NATO's Locked Shields Cyber-Defense Exercise
The 15th annual event helps countries test and develop defenses against current and emerging cyber threats, including disinformation, quantum computing, and AI.

Countries face increasingly sophisticated attacks and cyber threats that require evolving strategies to keep pace. Coordination among countries is also key. However, it can be difficult to test preparedness on the large scale required.

Nearly 4,000 cyber experts from 41 nations are taking part in this week's 15th annual Locked Shields live cyber-exercise event hosted by NATO's Corporative Cyber Defence Centre of Excellence (CCDCOE). The three-day event (May 6 to May 9) tests the cyber readiness on the country level, with attack simulations against critical systems and infrastructures, like gas, telecommunication, and energy. The focus on critical infrastructure is particularly important, as attackers ramp up their efforts to target systems in the water and wastewater sector.

Locked Shields officially kicked off on May 6 with multinational teams working to defend against cyber crises.

Dubbed the world's biggest live-fire cyber exercise, Locked Shields extends beyond attacks to measure how prepared the countries are to deal with disinformation, political pressure, communication challenges, and legal dilemmas that stem from cyber threats. The countries are organized into 17 multinational blue teams to defend two fictional islands located in the Atlantic Ocean. While some countries sent their teams to Tallin, Estonia, where the event is taking place, others, such as Japan, are joining remotely.

To mimic the high stakes and intense pressure of a real-life scenario, Locked Shields features more than 8,000 virtual systems under attack. The simulation combines cyberattacks, disinformation, and infrastructure crises, according to NATO CCDCOE. The cyber defense exercise also brings challenges related to quantum computing and AI. The teams are tasked with maintaining services and networks while countering the threats, as well as coordinating effective strategic communications and making decisions under significant time pressure. The goal is to mirror the complex dynamics of what a real-world cyber crisis would look like.

"This is where nations train for tomorrow's crises," NATO CCDCOE stated. (continua…)

https://www.darkreading.com/cybersecurity-operations/countries-nato-locked-shields-cyber-defense-exercise

***DARKREADING** - Arielle Waldman - May 7, 2025*

'Lemon Sandstorm' Underscores Risks to Middle East Infrastructure

The Iranian state-backed group targeted the operational technology of a critical national infrastructure (CNI) network and persisted in its network for years, but ultimately failed.

An Iran state-backed threat group targeted a critical national infrastructure (CNI) provider in a rival Middle Eastern nation and spread malicious software deep into its network over the past two years but ultimately failed to compromise their desired target: the operational technology (OT) network.

The compromise started at least two years ago, when the attackers used stolen VPN credentials to gain access to the organization's network, according to a May 1 report published by cybersecurity firm Fortinet, which helped with the remediation process that began late last year. Within a week, the attacker had installed Web shells on two external-facing Microsoft Exchange servers and then updated those backdoors to improve their ability to remain undetected.

In the following 20 months, the attackers added more functionality, installed additional components to aid persistence, and deployed five custom attack tools. The threat actors, which appear to be part of

an Iran-linked group dubbed "Lemon Sandstorm," did not seem focused on compromising data, says John Simmons, regional lead for Fortinet's FortiGuard Incident Response team.
"The threat actor did not carry out significant data exfiltration, which suggests they were primarily interested in maintaining long-term access to the OT environment," he says. "We believe the implication is that they may [have been] positioning themselves to carry out a future destructive attack against this CNI." (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/lemon-sandstorm-risks-middle-east-infrastructure
DARKREADING - *Robert Lemos - May 8, 2025*

Telefoni usa e getta per chi va negli Usa, l'Ue affronta il tema dello spionaggio
Secondo il Financial Times l'Ue vorrebbe che i propri emissari in viaggio negli Usa utilizzassero telefoni usa e getta. La parziale smentita di Bruxelles non smorza i reali timori di spionaggio e conferma che le precauzioni sono d'obbligo
Un articolo dal titolo "L'Ue fornisce **telefoni usa e getta** al personale diretto negli Stati Uniti per timore di **spionaggio**" pubblicato **sul Financial Times** il14 aprile ha sollevato una polemica che apre le porte a riflessioni la cui portata va ben oltre il rapporto tra Bruxelles e Washington e va anche al di là delle logiche dello **spionaggio commerciale** e industriale.
L'idea in sé può sembrare balzana e persino **macchiata da una sorta di isterismo** dettato dal timore irrazionale e incontrollato. Se si esamina la questione facendo anche ricorso a politiche e decisioni recenti, emerge un quadro prudenziale che subordina la paura alla necessità.
Indice degli argomenti
- Telefoni usa e getta, spionaggio e tensioni: cosa dice l'articolo del Financial Times
- Il confine labile tra isteria e precauzione

Telefoni usa e getta, spionaggio e tensioni: cosa dice l'articolo del Financial Times
Riassumiamo l'articolo del Financial Times (coperto da paywall) al fine di estrapolarne l'essenziale.
L'Ue avrebbe deciso (condizionale d'obbligo) di dotare di telefoni usa e getta i propri emissari in viaggio negli Stati Uniti. Questo per lenire i rischi di spionaggio perché, come si legge nell'articolo, le **strategie di sorveglianza elettronica** attuate da Washington sono sempre più affilate.
Tuttavia, credere che questa misura sia originata soltanto da una diffidenza dell'Ue nei confronti degli Usa è fuorviante. Rientra, infatti, nei canoni di **una postura cautelativa** che per l'Ue va assunta a prescindere, così come ha sottolineato un portavoce dell'Unione che ha solo parzialmente smentito la notizia, ridimensionando a mera raccomandazione e non a un obbligo l'uso di dispositivi da distruggere al rientro da ogni missione. (continua….)
https://www.cybersecurity360.it/news/telefoni-usa-getta-spionaggio-usa/
CYBERSECURITY360 - *Giuditta Mosca - 8 mag 2025*

Surfshark study probes data hunger of web browsers
Findings reveal Chrome has a huge appetite, 'collecting 20 different data types across numerous categories.'
A new survey by VPN provider Surfshark has found that Chrome collects the most information from users' phones, while "TOR stands out as the most privacy-centric browser by collecting no data at all."

The two were among 10 that researchers analyzed, after using AppMagic, a market intelligence tool, to select the most popular browser apps on Apple phones in the US in 2025, they said in a post outlining their findings.
The researchers noted, "Chrome is the most data-hungry, collecting 20 different data types across numerous categories. These include contact info, financial details, location, browsing history, search history, user content, identifiers, usage data, diagnostics, and other types of data. Chrome is the only browser that collects financial information, such as payment methods, card numbers, or bank account details."
It is also, they stated, the only browser that collects a list of contacts from the user's phone, address book, or social graph.
The researchers said that the remaining browsers each only collect an average of six data types, with Bing having the second-largest appetite, collecting 12 data types. Apple's Safari browser collects eight.
Other findings revealed that:

- 40% of the analyzed browsers apps collect users' locations. Safari, Chrome and Opera "collect coarse location, which refers to a user's or device's location with less precision than exact latitude and longitude. Bing is the only app that collects precise location data." The report pointed out that 60% of the apps don't collect any location information, suggesting that it is not necessary for a browser app to collect user location in order to function. "This raises concerns about why some browsers collect this data and how it is used," the researchers wrote. (continua…)

https://www.computerworld.com/article/3982319/surfshark-study-probes-data-hunger-of-web-browsers.html
COMPUTERWORLD - Paul Barker - *May 9, 2025*

Google to pay Texas $1.4 billion in data privacy settlement
KEY POINTS

- Google agreed to pay nearly $1.4 billion to the state of Texas to settle allegations of violating the data privacy rights of the state's residents, Texas Attorney General Ken Paxton said.
- Paxton sued Google in 2022 for allegedly unlawfully tracking and collecting the private data of users.
- The attorney general in July 2024 obtained a $1.4 billion settlement for Texas from Meta to resolve claims of unauthorized use of biometric data belonging to Facebook and Instagram users.

Google agreed to pay nearly $1.4 billion to the state of Texas to settle allegations of violating the data privacy rights of state residents, Texas Attorney General Ken Paxton said Friday.
Paxton sued Google in 2022 for allegedly unlawfully tracking and collecting users' private data.
The attorney general said the settlement, which covers allegations in two separate lawsuits against the search engine and app giant, dwarfed all past settlements by other states with Google for similar data privacy violations.
Google's settlement comes nearly 10 months after Paxton obtained a $1.4 billion settlement for Texas from Meta, the parent company of Facebook and Instagram, to resolve claims of unauthorized use of biometric data by users of those popular social media platforms.
"In Texas, Big Tech is not above the law," Paxton said in a statement on Friday.
"For years, Google secretly tracked people's movements, private searches, and even their voiceprints and facial geometry through their products and services. I fought back and won," said Paxton.

"This $1.375 billion settlement is a major win for Texans' privacy and tells companies that they will pay for abusing our trust."
Google spokesman Jose Castaneda said the company did not admit any wrongdoing or liability in the settlement. The deal covers allegations related to the Chrome browser's incognito setting, disclosures related to location history on the Google Maps app, and biometric claims related to Google Photo. (continua…)
https://www.cnbc.com/2025/05/09/google-texas-data-privacy-settlement-paxton.html
CNBC - *Dan Mangan - MAY 9 2025*

La Spagna al buio: un campanello d'allarme per il sistema elettrico europeo? - Il blackout che ha interessato la penisola iberica il 28 aprile 2025 costituisce il primo incidente significativo su un sistema elettrico alimentato in prevalenza da fonti energetiche rinnovabili (qualche commentatore, con buona semplificazione, lo ha definito "il primo blackout dell'era green").
Analisi complete, che consentiranno una dettagliata ricostruzione dell'evento, sono in corso da parte di varie entità: prima tra tutte, l'organizzazione dei TSO elettrici europei (ENTSO-e), che ha impostato un percorso di indagine destinato a durare qualche mese.
Nel frattempo, passato qualche giorno dall'incidente, è possibile tratteggiare una ricostruzione plausibile: quella che proponiamo in questo articolo è basata su dati di monitoraggio in tempo reale (come i portali dati di Red Eléctrica de España -REE – e la piattaforma di trasparenza di ENTSO-e), nonché su registrazioni di apparecchiature sperimentali legate al progetto di ricerca MedFasee coordinato da INESC P&D Brasil cui partecipa il Politecnico di Milano, Dipartimento di Energia.
Nell'articolo, a partire da una panoramica tecnica dettagliata della rete spagnola, inclusa la sua struttura, il mix di generazione, le interconnessioni transfrontaliere, ci si concentra sui fattori che influenzano la stabilità della rete. Si riporta poi una possibile sequenza degli eventi accaduti il 28 aprile 2025. Si propone infine qualche parallelo tra il fenomeno del 28 Aprile 2025 in Spagna e l'analogo incidente accaduto in Italia il 28 Settembre del 2003, per poi dettagliare alcune misure specifiche messe in atto nel nostro Paese.
Si tracciano infine alcune conclusioni, senza dubbio provvisorie, e alcune prospettive future, anche alla luce della profonda mutazione che sta interessando i sistemi elettrici ed energetici di tutto il pianeta.
Indice dei contenuti
Parco di generazione del sistema spagnolo
Interconnessioni con i sistemi confinanti
Fattori che influenzano la stabilità della rete
Stato del sistema la mattina del 28 aprile
Le oscillazioni inter-area
Una possibile ricostruzione dell'incidente
Analisi dei fenomeni chiave
Analogie con il blackout in Italia del 28 settembre 2003
I generatori e la stabilità di rete
Conclusioni
(continua…)
https://www.rinnovabili.it/energia/infrastrutture/blackout-spagna-campanello-allarme-sistema-elettrico-europeo/
RINNOVABILI.IT - *A. Berizzi, M. Delfanti - 9 Maggio 2025*

Adattamento ai cambiamenti climatici: come migliorare il comfort estivo negli stabilimenti industriali - L'aumento delle ondate di calore impone nuove strategie progettuali per il comfort estivo negli edifici industriali. Un caso studio reale mostra come simulazione dinamica, analisi microclimatiche e interventi passivi possano ridurre fino a 9°C la temperatura interna, migliorando efficienza e vivibilità. In un contesto segnato dal riscaldamento globale, garantire il comfort estivo negli edifici industriali diventa una priorità. Attraverso un caso studio reale, analizziamo criticità e soluzioni per affrontare le nuove sfide climatiche, con un focus sull'adattamento passivo e sulla simulazione dinamica.

Adattarsi al cambiamento climatico è diventato urgente

La crisi climatica non è più un'ipotesi futura: è una realtà che incide già oggi sulle nostre città, i nostri edifici e la nostra salute. In Italia, che rientra a pieno titolo nell'"hotspot" climatico del Mediterraneo, le ondate di calore sono sempre più frequenti, lunghe e intense. In questo contesto, la resilienza edilizia – intesa come capacità di adattarsi alle nuove condizioni ambientali – è un tema centrale per progettisti, ingegneri e decisori.

Cosa si intende per "hotspot climatico"?

Un "hotspot" climatico è una area del pianeta dove gli effetti del cambiamento climatico si fanno sentire più velocemente e in modo più marcato rispetto alla media, causando impatti più forti su popolazione ed ecosistemi. Le cause possono essere di tipo fisico-geografiche o umane.

(continua….)

https://www.ingenio-web.it/articoli/adattamento-ai-cambiamenti-climatici-come-migliorare-il-comfort-estivo-negli-stabilimenti-industriali

Ingenio - *Isaac Scaramella - 09.05.2025*

Compliance Ospedaliera: Guida Operativa per la Conformità Normativa, Gestionale e Clinica - Negli ultimi anni, la compliance in ambito sanitario è diventata un elemento cruciale per garantire non solo la qualità delle cure, ma anche la sostenibilità e la trasparenza delle strutture ospedaliere. In un contesto normativo sempre più articolato, caratterizzato da regolamenti europei, leggi nazionali e linee guida tecniche, ogni ospedale è chiamato a rispondere a precisi obblighi di legge e standards operativi. L'inosservanza può portare non solo a sanzioni, ma anche a gravi conseguenze reputazionali e cliniche. Questo articolo propone un'analisi sistematica degli ambiti principali di conformità richieste a un ospedale moderno, utilizzando una checklist strutturata come strumento operativo, per valutare il livello di adeguamento normativo. Ogni area – dalla sicurezza sanitaria alla privacy dei dati, dalla sostenibilità ambientale alla governance interna – rappresenta un tassello fondamentale nella costruzione di un sistema ospedaliero sicuro, efficiente e conforme. *(continua…)*

https://www.snewsonline.com/saccone-compliance-ospedaliera-guida-operativa-conformita-normativa-gestionale-clinica/

SNews *- Umberto Saccone - 9 Maggio 2025*

Come individuare email pericolose - Alcuni indizi che possono aiutare ad individuare messaggi di posta elettronica, di sospetta provenienza.

È noto come un gran numero di frodi informatiche viene portato a termine inviando un messaggio di posta elettronica al destinatario, che non effettua appropriati accertamenti e risponde a quanto

richiesto. Ecco perché può essere opportuna una esemplificazione di alcuni indirizzi di posta elettronica, che potrebbero meritare approfondimenti, prima di gestire il messaggio stesso.
Il numero straordinariamente elevato di messaggi di posta elettronica, di origine fraudolenta, richiede quindi un'opera di sensibilizzazione su tutti i collaboratori e dipendenti, per metterli in grado di effettuare una prima valutazione dell'origine del messaggio, che spesso può incorporare indizi, che un occhio attento può evidenziare. Ecco alcuni esempi.

ARossiBPER@gmail.com

Le banche utilizzano sempre degli indirizzi di posta elettronica, in cui il suffisso non è generalistico, come nel caso presente. Un indirizzo corretto dovrebbe essere del tipo……@bper.it

Help@paypay-server.com

In questo caso l'indirizzo di posta elettronica assomiglia molto a quello di un sito di pagamento, ma un'attenta lettura mette in evidenza come il nome del sito non sia correttamente scritto.

Direzione_bancaria@yahoo.com

Anche dall'esame di questo indirizzo di posta elettronica si può capire come un ufficio dirigenziale di una banca non si appoggi a generici indirizzi di posta elettronica, ma ad indirizzi specifici, direttamente riferibili alla banca stessa.

Penali@agentrate.it

In questo caso la seconda parte dell'indirizzo di posta elettronica non corrisponde a quello effettivo della agenzia delle entrate, che è raggiungibile solo mediante accesso a specifici portali, presenti nel sito www.agenziaentrate.gov.it

improvedsecurity@rnicrosoft.com

Questo indirizzo di posta elettronica è particolarmente ingannevole perché, se il destinatario non lo osserva attentamente, potrebbe non rendersi conto che la **m** di **microsoft** è in realtà composta da due lettere: **r** ed **n**

https://www.puntosicuro.it/sicurezza-informatica-C-90/come-individuare-email-pericolose-AR-25346

Punto Sicuro – *Adalberto Biasiotti, 12/05/2025*

Vulnerabilità dei data center di AI: anche Stargate a rischio di spionaggio cinese

La vulnerabilità deriva da diversi fattori, tra cui la dipendenza da componenti critici prodotti in Cina. E la sicurezza nei laboratori di AI è spesso sacrificata sull'altare della rapidità di sviluppo. Ecco i rischi cyber dei data center di AI, esposti allo spionaggio cinese, a partire dal progetto Stargate

Un report di **Gladstone AI** avverte che i **data center statunitensi** per l'**intelligenza artificiale** potrebbero essere **vulnerabili** allo **spionaggio cinese**, mettendo a rischio sicurezza nazionale e investimenti.

La vulnerabilità deriva da diversi fattori, tra cui la **dipendenza da componenti critici prodotti in Cina**. Inoltre, la **sicurezza nei laboratori di AI** è carente, spesso **sacrificata in nome della rapidità di sviluppo** e alcuni modelli avanzati hanno già mostrato capacità di "evasione" dai sistemi di contenimento.

Indice degli argomenti

- Serve un cambio di paradigma

I data center di AI nel mirino dello spionaggio cinese

Nel contesto dell'attuale corsa globale allo sviluppo dell'intelligenza artificiale (AI), laboratori privati negli Stati Uniti sarebbero sul punto di sviluppare una **superintelligenza artificiale.** Ma un rapporto dei ricercatori di **Gladstone AI** ha sollevato dubbi riguardo alla **sicurezza dei data center** statunitensi. Secondo lo studio, tutte le strutture dedicate all'IA negli Usa, comprese quelle di nuova generazione come **Stargate**, sarebbero vulnerabili a operazioni di **spionaggio da parte della Cina**, mettendo a rischio la sicurezza nazionale.

Progetto Stargate

Il progetto **Stargate**, annunciato dal presidente **Donald Trump** a gennaio, è una joint venture tra **OpenAI, SoftBank, Oracle e MGX**, e prevede un investimento di **500 miliardi di dollari nei prossimi quattro anni** per costruire infrastrutture dedicate all'IA. Grandi **data center** sul suolo statunitense, contenenti migliaia di chip informatici avanzati, necessari per addestrare nuovi sistemi di intelligenza artificiale.

La **prima fase del progetto** è già in corso ad Abilene, **Texas**. Nonostante il progetto abbia suscitato **critiche** riguardo alla sua fattibilità finanziaria e alla concentrazione di potere nelle mani di poche grandi aziende tecnologiche, Trump ha espresso il suo sostegno all'iniziativa, definendola una questione di **competitività nazionale** contro il concorrente cinese. (continua…)

https://www.cybersecurity360.it/cybersecurity-nazionale/vulnerabilita-dei-data-center-di-ai-anche-stargate-a-rischio-di-spionaggio-cinese/?utm_campaign=cybersec_nl_20250514&utm_source=cybersec_nl_20250514&utm_medium=email&sfdcid=0030O00002LXHlXQAX

CYBERSECURITY360 - *Luisa Franchina, Ginevra Detti - Pubblicato il 13 mag 2025*

Chips Act: perché l'UE rischia di fallire l'obiettivo 2030

La strategia UE per l'autonomia nei semiconduttori mostra progressi limitati. Secondo la Corte dei conti, l'obiettivo del 20% della produzione mondiale entro il 2030 è irraggiungibile senza correzioni strategiche significative e investimenti più coordinati

Si sta consolidando, a livello europeo, la consapevolezza dell'importanza di un'**autonomia tecnologica nel settore della microelettronica**, cruciale per garantire la resilienza e la competitività dell'Unione nel contesto globale.

L'obiettivo, fissato dalla Commissione come parte del Decennio digitale, è di conseguire il 20% della produzione mondiale di microprocessori entro il 2030, ma un recente report della Corte dei conti europea avverte che **tale traguardo è ormai difficile da raggiungere senza un aggiustamento strategico sostanziale.**

Indice degli argomenti

I tre pilastri del Chips Act 2030: risultati e limiti

Nel corso del 2025, la Commissione ha aggiornato **lo stato di avanzamento del Chips Act**, descrivendo i risultati conseguiti nelle tre linee di intervento previste.
Nel primo pilastro, dedicato alla ricerca e all'innovazione, la maggior parte del budget è già stata impegnata per sostenere lo sviluppo di piattaforme di progettazione e linee pilota.
Nel secondo pilastro, orientato allo stimolo della capacità produttiva, sono stati approvati provvedimenti di aiuto di Stato per impianti "first-of-a-kind" e l'IPCEI ha mobilitato significativi investimenti pubblici e privati.
Il terzo pilastro, focalizzato sul coordinamento della catena di approvvigionamento, ha visto l'attivazione del European Semiconductor Board per monitorare rischi e identificare attori strategici.
Il problema degli investimenti insufficienti
Nonostante questo avanzamento, la capacità produttiva dell'Unione resta inferiore alle aspettative: proiezioni di mercato indicano che, senza misure correttive, la quota UE non supererà l'11,7% dei microprocessori globali nel 2030, ben al di sotto del 20 % prefissato. A testimonianza di quanto la Commissione abbia supportato il settore, nei primi 1,5 anni di applicazione sono stati raccolti circa 43 miliardi di euro, di cui solo 4,5 miliardi direttamente dal bilancio comunitario; la restante parte proviene principalmente da fondi nazionali.
Le criticità strutturali delle politiche nazionali
Dalla magistratura contabile dell'Unione emerge un richiamo alla **necessità di rafforzare la coerenza strategica tra gli interventi.** Il report della Corte dei conti sottolinea che l'attuale configurazione del programma non ha ancora innescato flussi di investimento sufficienti per colmare il divario con i leader globali e che, **senza una strategia più mirata, l'UE rischia di non riuscire a garantire la propria autonomia tecnologica nel settore microelettronico.**
Le ragioni principali di questo ritardo risiedono nella fra**mmentazione delle risorse tra i vari Stati membri** e nella complessità dei processi autorizzativi per i progetti di nuova generazione. A livello nazionale, ogni Paese ha implementato proprie misure di sostegno, talvolta sovrapponendosi alle iniziative europee, senza creare un quadro finanziario unitario. L'approvazione delle domande di finanziamento per gli impianti IPF e OEF, sebbene già avviata, procede a rilento a causa dell'intenso coordinamento tecnico e giuridico richiesto. (continua…)
https://www.agendadigitale.eu/mercati-digitali/chips-act-perche-lue-rischia-di-fallire-lobiettivo-del-2030/
AGENDADIGITALE - *Tommaso Diddi, Luisa Franchina - 13 mag 2025*

World's first CPU-level ransomware can "bypass every freaking traditional technology we have out there" — new firmware-based attacks could usher in new era of unavoidable ransomware
A cybersecurity expert has created a proof of concept for CPU ransomware.
Rapid7's Chrstiaan Beek has written proof-of-concept code for ransomware that can attack your CPU, and warns of future threats that could lock your drive until a ransom is paid. This attack would circumvent most traditional forms of ransomware detection.
In an interview with The Register, Beek, who is Rapid7's senior director of threat analytics, revealed that an AMD Zen chip bug gave him the idea that a highly skilled attacker could in theory "allow those intruders to load unapproved microcode into the processors, breaking encryption at the hardware level and modifying CPU behavior at will."
Google's Security Team has previously identified a security vulnerability in AMD's Zen 1 to Zen 4 CPUs that allows users to load unsigned microcode patches. It later emerged that AMD Zen 5 CPUs are also affected by the vulnerability. Thankfully, the issue can be fixed with new microcode, just like a previous Raptor Lake instability. However, Beek saw his opportunity. "Coming from a background in

firmware security, I was like, woah, I think I can write some CPU ransomware," and that's exactly what he did.
According to the report, Beek has indeed written proof-of-concept code for ransomware that can hide in a CPU. Reassuringly, he promises they won't release it.
As per the report, Beek reckons this type of exploit could lead to a worst case scenario: "Ransomware at the CPU level, microcode alteration, and if you are in the CPU or the firmware, you will bypass every freaking traditional technology we have out there."
Beek also referenced leaked comments from the Conti ransomware gang, which surfaced in 2022. In a presentation given at RSAC, he highlighted chat logs from the group. "I am working on a PoC where the ransomware installs itself inside UEFI, so even after reinstalling Windows, the encryption stays," reads one. Another noted that with modified UEFI firmware, "we can trigger encryption before the OS even loads. No AV can detect this."
The upshot? "Imagine we control the BIOS and load our own bootloader that locks the drive until the ransom is paid," a hacker hypothesized.
Beek warns that if bad actors were working on these exploits a few years ago, "you can bet some of them will get smart enough at some point and start creating this stuff." (continua…)
https://www.tomshardware.com/pc-components/cpus/worlds-first-cpu-level-ransomware-can-bypass-every-freaking-traditional-technology-we-have-out-there-new-firmware-based-attacks-could-usher-in-new-era-of-unavoidable-ransomware?utm_term=BE399376-883B-4F0A-B0F5-0EF281E9D4C0&lrh=9b8172938b69372afc2de4d1954e1c5a313105adf4497971eee4ea4dbc37c72a&utm_campaign=79B375AA-AA0B-4881-99A1-64F0F9BDBE17&utm_medium=email&utm_content=94E45F82-205E-4F7D-937F-E9EBEAFADE5F&utm_source=SmartBrief
TOMSHARDWARE Stephen Warwick - ***May 14, 2025***

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Glauco Bertocchi Silvano Bari *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.