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 2023 | **n. 10/ 2023** | **novembre 2023**

Infrastrutture Critiche e Geopolitica: un'introduzione alla vulnerabilità globale

Le infrastrutture critiche svolgono un ruolo cruciale nella vita moderna, contribuendo a sostenere il funzionamento dei principali servizi essenziali di una nazione, come l'approvvigionamento idrico ed energetico, i trasporti, le comunicazioni e altro ancora. La loro importanza è ancora più evidente in un contesto geopolitico, poiché queste infrastrutture non sono solo fondamentali per il benessere dei cittadini, ma possono anche influenzare le dinamiche internazionali e le relazioni tra le nazioni. L'interconnessione globale ha reso le infrastrutture critiche più vulnerabili a minacce di vario genere, come attacchi cibernetici, eventi climatici estremi e atti di sabotaggio. Tale vulnerabilità può avere gravi ripercussioni sulla sicurezza nazionale e sulla stabilità economica, portando alla necessità di affrontare il problema della protezione delle infrastrutture critiche a livello globale. Una delle sfide principali in questo contesto è la dipendenza reciproca tra le nazioni. Pensiamo ad esempio alle interconnessioni create dall'infrastruttura energetica globale e la conseguente interdipendenza tra molti Paesi che può essere sfruttata come leva in dispute geopolitiche. Un Paese può minacciare il blocco o l'attacco alle infrastrutture energetiche di un altro Stato come forma di coercizione politica, mettendo in pericolo la fornitura di energia e l'economia dell'altro. Un esempio noto è il taglio dell'approvvigionamento di gas naturale all'Europa da parte della Russia durante la guerra in Ucraina, che ha causato tensioni sia a livello regionale che internazionale, mettendo in evidenza la vulnerabilità della sicurezza energetica di molti Paesi europei. Le minacce cibernetiche rappresentano un'altra importante sfida per le infrastrutture critiche. Gli attacchi informatici possono compromettere il funzionamento di reti di energia, sistemi di trasporto e comunicazioni, creando caos e instabilità. Paesi con forti capacità cibernetiche possono utilizzare queste minacce per sfruttare i punti deboli delle infrastrutture di altre nazioni, mettendo in pericolo la loro sicurezza. Un esempio emblematico di questo tipo di minaccia è rappresentato dall'attacco alla rete elettrica ucraina avvenuto nel 2015. In quell'occasione, un sofisticato attacco informatico (avvenuto tramite l'utilizzo del malware BlackEnergy 3) compromise il sistema di controllo industriale della rete elettrica ucraina, causando blackout in diverse regioni del Paese. Questo episodio ha dimostrato la capacità di attori statali o non statali di utilizzare strumenti di attacco da remoto per compromettere i sistemi informatici delle infrastrutture critiche di una nazione, causando gravi interruzioni dei servizi pubblici e mettendo in pericolo la sicurezza dei cittadini. Per affrontare queste sfide, è essenziale una cooperazione internazionale efficace. Le nazioni devono condividere informazioni, sviluppare protocolli di sicurezza e lavorare insieme per proteggere le infrastrutture critiche globali. L'Unione Europea e le organizzazioni internazionali (come l'ONU e la NATO) hanno un ruolo importante da svolgere nel facilitare questa cooperazione. In particolare, la NATO, a seguito dei recenti avvenimenti internazionali, ha posto maggiore enfasi sul concetto di resilienza, rivolgendo la sua attenzione alla protezione delle infrastrutture critiche. All'interno del contesto internazionale la vulnerabilità delle infrastrutture critiche può essere sfruttata come leva di pressione nelle dispute tra nazioni, pertanto, la protezione di queste infrastrutture è diventata una componente chiave nella strategia di sicurezza internazionale[1]. In ambito nazionale molte aziende

[1] https://formiche.net/2023/10/nato-resilienza-infrastrutture-critiche-peronaci/

industriali stanno collaborando per incrementare la sicurezza delle infrastrutture critiche in diversi settori. Un esempio è rappresentato dal Memorandum Of Understanding, sottoscritto da Fincantieri e Leonardo nell'ambito della protezione delle infrastrutture critiche sottomarine, con l'obiettivo di integrare le reciproche competenze e capacità delle due aziende. In particolare, l'accordo ha come obiettivo la realizzazione di una rete di piattaforme e sistemi di sorveglianza, controllo e protezione di infrastrutture critiche e aree marittime subacquee in conformità con gli obiettivi di sicurezza posti sia a livello nazionale che europeo. Nell'ambito di questa collaborazione, sono inclusi la salvaguardia delle reti sottomarine strategiche, la protezione dei cavi e delle dorsali di comunicazione, la creazione di sistemi di allerta per minacce sottomarine, nonché la sicurezza delle operazioni di prospezione, estrazione e sea-mining sul fondale marino[2]. Un'altro settore oggetto di investimenti in ambito di sicurezza, da parte dei soggetti pubblici e privati, è quello cyber. È stato, infatti, avviato un iter per la formazione di una rete di Laboratori Accreditati di Prova (LAP) che innalzeranno il livello di sicurezza delle infrastrutture critiche del nostro Paese. I LAP dovranno valutare la sicurezza di varie tipologie di beni ICT usati dagli Operatori posti all'interno del Perimetro di Sicurezza Nazionale Cibernetica contribuendo così a una maggiore resilienza del Paese[3]. In definitiva, la protezione delle infrastrutture critiche rappresenta una sfida globale che richiede un profondo impegno di collaborazione tra nazioni, organizzazioni internazionali e aziende operanti nei settori critici. In questo contesto, spiccano esempi significativi di collaborazione. A livello sovranazionale, l'Unione Europea e la NATO hanno intensificato la loro collaborazione attraverso la creazione, avvenuta il 16 Marzo 2023, della task force UE-NATO sulla resilienza delle infrastrutture critiche, con il compito di individuare soluzioni per il rafforzamento delle infrastrutture critiche all'interno di quattro settori di importanza trasversale (energia, trasporti, infrastrutture digitali e spazio)[4]. Nel contempo, a livello nazionale, attraverso la costituzione del Perimetro di Sicurezza Nazionale Cibernetica, il nostro Paese, si è posto l'obiettivo di difendere gli asset strategici nazionali dagli attacchi cyber attraverso una costante collaborazione con le aziende operanti all'interno dei settori critici, con il fine di sviluppare piani di sicurezza e investire in tecnologie avanzate per la difesa del nostro Stato. Tale assetto si completa, inoltre, con il ruolo di collegamento che l'Agenzia per la Cybersicurezza Nazionale (ACN) assicura con l'Unione Europea. Infatti, a livello comunitario l'ACN fa parte della rete europea degli CSIRT (Computer Security Incident Response Team) e della rete CyCLONe (Cyber Crisis Liaison Organisation Network), costituita con il compito di rispondere in maniera tempestiva ed efficace ad ogni tipologia di attacco informatico che dovesse colpire o coinvolgere un qualsiasi Paese membro dell'Unione Europea[5]. Tali esempi testimoniano come la protezione delle infrastrutture critiche non può prevedere un approccio unilaterale, ma richiede una sinergia globale per assicurare la resilienza e la sicurezza a livello mondiale.

Marco Raul Massoni Laureato in "Scienze della Politica" presso l'Università degli Studi di Macerata. Ha conseguito un master in Protezione Strategica del Sistema Paese: Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente svolge attività di consulenza in materia di cybersecurity

[2] https://www.industriaitaliana.it/fincantieri-leonardo-infrastrutture-critiche-sottomarine/
[3] https://www.ilsole24ore.com/art/cybersecurity-5-milioni-i-laboratori-prova-che-rendono-piu-sicure-infrastrutture-critiche-AFamYFHB
[4] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564
[5] https://www.acn.gov.it/ACN_Strategia.pdf

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 2024

Il 31 dicembre 2023 scadrà 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 2024".
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.

Il Consiglio Direttivo di AIIC ha deciso una facilitazione per chi si iscriverà come nuovo socio: a partire dal mese di ottobre 2023, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2024.

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.

ATTIVITA' DI EDUCATION

Proseguono le attività di formazione per soci e simpatizzanti per l'anno 2023.

L'accordo con IsacaRoma consente ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

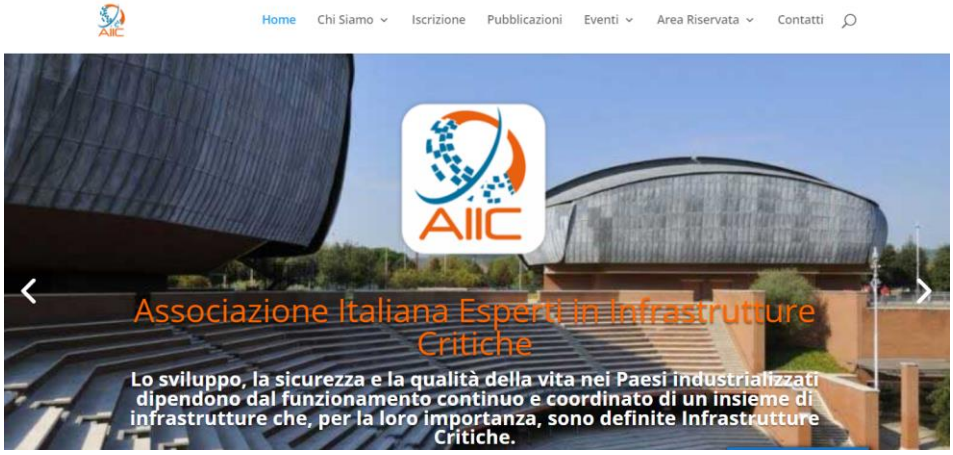
Stiamo valutando le modalità di svolgimento di altri eventi possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, come avrete notato, abbiamo ripreso le visite aziendali presso enti/imprese di rilevanza nazionale.

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 terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

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 nelle 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.



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.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

WORKSHOP SU "GESTIONE DEL RISCHIO NELLA PROSPETTIVA DEI CAMBIAMENTI CLIMATICI" – Roma, 14 novembre 2023, ore 9.30

il Consiglio Direttivo di AIIC è lieto di informarvi che, nell'ambito del processo di formazione e informazione dei propri associati, i soci e i simpatizzanti di AIIC potranno partecipare ad un workshop sponsorizzato da AIIC sul tema

GESTIONE DEL RISCHIO NELLA PROSPETTIVA DEI CAMBIAMENTI CLIMATICI

Martedi' 14 Novembre 2023,
Aula Conferenze, Università di Roma Tre, Via Vito Volterra 62, Roma

Il workshop intende identificare una nuova agenda per la gestione delle Emergenze e di quella del Rischio quotidiano in una prospettiva di cambiamenti climatici che tenderanno ad imporre una

maggiore attenzione nella gestione delle Infrastrutture e degli Asset strategici. La nuova Agenda, introdotta da una serie di iniziative legislative (recepimento della Direttiva Europea 2022/2557 relativa a "Critical Entity Resilience" da parte degli Stati Membri) ma anche quelle nazionali (D.L. Morandi), necessiterà di un utilizzo sempre maggiore di nuovi approcci che hanno necessità di essere integrati nei protocolli di Analisi del Rischio e dispiegate per la gestione delle Emergenze. Il Workshop mira a fornire una visione delle differenti componenti del Rischio nel nostro Paese, sia quelle endemiche che quelle che si aspetta avranno un impatto maggiore nei prossimi decenni alla luce delle nuove sfide legate ai cambiamenti climatici.

Tra i relatori è prevista la partecipazione del dott. Sandro Bologna, componente del Consiglio Direttivo di AIIC e coordinatore del Gruppo di Studio AIIC su "Resilienza delle Infrastrutture Critiche e cambiamenti climatici" che sta terminando i lavori con la pubblicazione di un apposito report.

AGENDA
09:30 *Welcome*
Stefano Panzieri (Università di Roma Tre)
09:40 *Presentazione degli obiettivi del Workshop*
Simona Cavallini (TIEMS Italia e Progress Consulting)
09:50 *L'Evoluzione della Gestione delle Emergenze Nazionali e i Cambiamenti Climatici*
Guido Parisi (già Capo del Corpo Nazionale dei Vigili del Fuoco)
10:10 *Analisi eventi dell'alluvione in Romagna del Maggio 2023*
Massimo Bosi (Comune di Faenza)
10:30 *Cambiamenti Climatici e Resilienza delle Infrastrutture Critiche*
Sandro Bologna (TIEMS Italia e AIIC)
10:50 *Il rischio incendi: nuove prospettive*
Sergio Pirone (TIEMS Italia e Formont)
11:10 *Il rischio idrogeologico degli impianti industriali*
Fabrizio Paolacci (Università di Roma Tre)
11:30 *Osservazione dallo Spazio: interferometria e dati multispettrali per il monitoraggio del territorio e degli asset*
Salvatore Stramondo (Osservatorio Nazionale Terremoti, INGV)
11:50 *I servizi climatici*
Gianmaria Sannino (ENEA, Centro Ricerche Casaccia)
12:10 *Nuovi strumenti per l'Analisi del Rischio e l'Emergency Management*
Maurizio Pollino (ENEA)
12:30 Q&A e Chiusura
Vittorio Rosato (TIEMS Italia e EISAC.it)

La partecipazione all'evento è gratuita, previa registrazione.
Per ulteriori informazioni sul workshop:
info@tiems-ic.it
http://www.tiemsitalianchapter.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

NEWS E AVVENIMENTI

Certificazioni di prodotto ICT, lo stato dell'arte: standard, requisiti e regolamentazioni
Entro la fine del 2024 la catena del valore pensata per la certificazione e la valutazione dei prodotti ICT in ambito di cyber security in Italia dovrà essere operativa. Facciamo il punto della situazione, tra standard e schemi di certificazione in attesa della piena operatività del Cyber Resilience Act.
L'ACN, Agenzia per la Cybersecurity Nazionale, sta proseguendo ad accreditare LAP, Laboratori Accreditati di Prova, per la collaborazione con il CVCN, Centro di Valutazione e Certificazione Nazionale: entro la fine del 2024 la catena del valore pensata per la certificazione e la valutazione dei prodotti ICT in ambito di cyber security in Italia dovrà essere operativa.
Indice degli argomenti

- **Gli schemi di certificazione in Europa**
- **Gli standard per le certificazioni di prodotto**
- **Cyber Resilience Act: un passaggio decisivo**

Gli schemi di certificazione in Europa
Qual è la situazione degli schemi di certificazione in Europa? La Commissione con la DG Connect ha confermato che entro il 2024 dovrà essere emanato il primo schema di certificazione di prodotto per la cyber security in territorio Europeo.
L'ENISA, Agenzia Europea per la sicurezza delle Reti e dell'Informazione, sta preparando un report sullo stato dell'arte delle certificazioni di prodotto in Europa e nel mondo per illustrare l'attuazione del Cyber security Act, promulgato nel 2019.
I prodotti certificati nel 2020 erano circa 840 e sono saliti a circa 1260 nel 2021 per attestarsi sul medesimo valore nel 2022. Complice probabilmente la pandemia, il numero resta alto rispetto agli anni anteriori all'attuale decennio, ma stazionario. (continua…)
https://www.cybersecurity360.it/legal/certificazioni-di-prodotto-ict-lo-stato-dellarte-standard-requisiti-e-regolamentazioni/
Cybersecurity360 *- Luisa Franchina- 10 Ott 2023*

Gestione delle crisi o crisi di gestione? - Gli esperti del settore consigliano, in una situazione di crisi, di non commettere l'errore di sottovalutarla; una crisi, se davvero di crisi si tratta, può rappresentare per un'azienda un'opportunità per migliorare, per imparare dai propri errori, ma può anche rappresentare un pericolo che, se non viene gestito adeguatamente, può ampliarsi e portare alla perdita della credibilità, della reputazione, della fiducia e, non di rado, al fallimento.
Da tempo è invalsa l'abitudine di abusare del termine di crisi. Eventi definibili come emergenze, problemi o incidenti, sono spesso scambiati per crisi, ma a differenza di queste ultime essi sono considerati eventi abituali, risolvibili con i mezzi a disposizione. Può definirsi crisi, invece, una situazione nella quale lo straordinario deborda. Possono causare una crisi: disastri naturali, l'errore umano, un guasto meccanico, una débâcle tecnologica, riorganizzazione o licenziamenti, problemi di comunicazione interna, etc.
L'analisi di tre casi emblematici di crisi
Analizziamo i tre casi più emblematici e paradigmatici, a nostro avviso, degli ultimi 15 anni: l'esplosione della Deepwater Horizon, il naufragio della Costa Concordia, il crollo del Ponte Morandi. (continua)
https://www.snewsonline.com/gestione-delle-crisi-o-crisi-di-gestione/
SNEWS *– Cristhian Re - 15 Settembre 2023*

Valutazione del rischio delle tecnologie critiche: la Commissione UE raccomanda un'azione unitaria

Il 3 ottobre la Commissione Europea ha **adottato** una raccomandazione sui settori tecnologici critici che si inquadra nell'ambito della strategia comunitaria in materia di sicurezza economica.
Un passaggio importante, perché "la tecnologia è attualmente al centro della concorrenza geopolitica e l'UE vuole essere un player economico con una posizione solida che si basi su una valutazione comune dei rischi": così ha **dichiarato** in conferenza stampa Věra Jourová, vicepresidente della Commissione europea per i valori e la trasparenza.
Indice degli argomenti:

Il contesto geopolitico

La natura della misura risiede, infatti, nella *Joint Communication* firmata a giugno da Bruxelles e dall'Alto Rappresentante dell'UE per gli affari esteri e la politica di sicurezza, Josep Borrell, che si fonda su tre pilastri fondamentali:*(Continua…)*
https://www.cybersecurity360.it/cybersecurity-nazionale/valutazione-del-rischio-delle-tecnologie-critiche-la-commissione-ue-raccomanda-unazione-unitaria/
Cybersecurity360 *– Gaia d'Ariano – Luca Marchese – 17 Ott 2023*

Pro-Iranian Hacktivists Set Sights on Israeli Industrial Control Systems

The hacktivists known as SiegedSec identify ICS targets, but there's no evidence of attacks yet.
The hacktivist group SiegedSec has claimed responsibility for a series of attacks against Israeli infrastructure and industrial control systems (ICS), but there is no indication that the listed IP addresses have experienced any attacks.
The hacking group put together a list of what it claims are its Israeli ICS targets, which was recently uncovered by SecurityScorecard's Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team. An image of the list — found via analysis of various dark Web groups — shows a series of IP addresses with the claim "we have unleashed mass attacks on Israeli infrastructure."

Who Made the List

According to a new report from STRIKE, SiegedSec claims it conducted a series of denial of service (DoS) attacks against a number of ICS devices and other Israeli infrastructure with the support of the pro-Iranian hacktivist group Anonymous Sudan. The purported targets included: global navigational satellite system receivers, building automation and control networks, and Modbus ICS — a communication protocol for communication between industrial electronic devices.
However, a sample of NetFlow data seen by SecurityScorecard does not indicate that the listed IP addresses had experienced volumes of traffic consistent with a DoS attack.
"In the absence of reported disruptions to Israeli infrastructure, the available NetFlow sample appears to support assessments that SiegedSec's attacks were either unsuccessful or have not yet begun in earnest," the report said.
Other researchers' assessments also determined that these attempts were likely to have been unsuccessful, and to conduct a DoS against these targets may be outside the attacker's capability. (continua…)

https://www.darkreading.com/dr-global/pro-iranian-hacktivists-sights-israeli-industrial-control-systems
Dark Reading - *Dan Raywood-October 18, 2023*

Le città sono un "campo di battaglia fondamentale" per contrastare la crisi climatica - Secondo il Climate crisis advisory group, il 59% dei nuclei urbani più popolosi è "ad alto rischio". Necessario "ripensare e reinventare" i centri abitati, rafforzando la resilienza e modernizzando normative edilizie e infrastrutture.
Nel nuovo rapporto "Risk & resilience: the role of cities in tackling the climate crisis", pubblicato il 20 settembre, gli scienziati del Climate crisis advisory group (Ccag), hanno dichiarato che, data la crisi ambientale in atto, "la futura pianificazione urbana deve avere come principio guida la resilienza all'aumento delle temperature".
(continua)
https://www.puntosicuro.it/ambiente-C-94/le-citta-sono-un-campo-di-battaglia-fondamentale-per-contrastare-la-crisi-climatica-AR-23737/
PuntoSicuro – *Redazione, 19/10/2023*

Resilienza delle infrastrutture critiche, così la Nato si prepara alla sfida. Parla Peronaci
Lo sguardo della Nato di fronte alle sfide del futuro intende essere davvero a 360°, estendendosi non solo all'aspetto geografico, ma anche di altri ambiti strategici, a partire dalla protezione delle strutture alla base del benessere e della stabilità delle società, tra cui spiccano le infrastrutture strategiche. Sul tema, Airpress ha intervistato il rappresentante permanente d'Italia presso il Consiglio atlantico, **Marco Peronaci.**
Ambasciatore, spesso si sente parlare di "resilienza" dei sistemi, che devono essere in grado di assorbire gli shock senza venirne travolti. Come declina la Nato questo concetto?
Per comprendere la portata e la rilevanza della "resilienza" in ambito Nato è necessario innanzitutto fare chiarezza sul concetto stesso di resilienza: un termine che da oltre un decennio si è diffuso anche in Italia divenendo parte del linguaggio comune, ma il cui uso ha ampliato sia il ventaglio dei settori in cui la parola è utilizzata, dall'originario ambito tecnologico (la proprietà dei materiali di resistere agli urti senza spezzarsi) alla psicologia, ai settori sociale, economico e politico, sia le sfumature del significato stesso di resilienza, che talvolta ha perso concretezza.
Concretezza e operatività che, invece, sono centrali nel concetto di resilienza per la Nato e per gli Alleati. Radicata nell'articolo 3 del Trattato dell'Atlantico del Nord, ossia dall'istituzione dell'Alleanza Atlantica nel 1948, la resilienza assume una funzione essenziale per l'Alleanza, tanto in tempo di pace come in caso di crisi o di conflitto: ossia, la capacità dei singoli Alleati e collettiva di essere preparati e, ove necessario, resistere, rispondere e riprendersi rapidamente da gravi shock, siano essi causati da disastri naturali, interruzioni delle infrastrutture critiche o attacchi ibridi o armati. *(Continua…)*
https://formiche.net/2023/10/nato-resilienza-infrastrutture-critiche-peronaci/
Formiche.Net *– Marco Battaglia – 23 Ott 2023*

Rockwell's Verve Buy Enlivens Critical Infrastructure Security
The industrial automation giant agrees to buy Verve Industrial Protection, joining in an ICS trend of bringing cybersecurity capabilities in-house to keep up with attackers.
Manufacturers of industrial automation and control systems continue to scoop up industrial cybersecurity firms to provide customers with more protection for their factories and facilities.

This week, Rockwell Automation agreed to acquire Verve Industrial Protection, a cybersecurity software and services firm, which will become part of Rockwell's Lifecycle Services division. The acquisition follows the July commitment by Honeywell to buy SCADAfence, an operational technology and IoT security firm, as a way to acquire asset discovery and threat detection capabilities. And just last week, technology firm Siemens announced an all-in-one testing suite for industrial networks — partnering with Tenable on the initial testing tools, but committing to including more third parties in the future.
The large manufacturers are trying to catch up with attackers and fix their cybersecurity shortcomings, says Katell Thielemann, distinguished vice president analyst at business intelligence firm Gartner.
"OEMs are on a bit of a redemption journey," she says. "Their end-user clients are starting to be vocal about buying multimillion-dollar assets that contain vulnerabilities and misconfigurations, and then having to pay million-dollar support services contracts that allow fixes downstream." (continua…)
https://www.darkreading.com/ics-ot/rockwell-verve-buy-critical-infrastructure-security
Dark Reading *-Robert Lemos- October 26, 2023*

Perché l'accusa della Sec contro Solarwinds per il maxi cyber-attacco è una svolta
Per la Consob americana la società ha frodato gli investitori sopravvalutando i suoi standard di sicurezza e sottovalutando i rischi. Nel mirino anche il chief information security officer
La Sec (Securities and Exchange Commission), cioè la Consob americana, ha accusato di frode SolarWinds e un suo alto dirigente alla luce del grande attacco informatico che ha colpito la società di software alla fine del 2020.L'attacco ha preso il nome della società: per tutti è l'attacco a SolarWinds visto Orion, il software di gestione delle reti aziendali prodotto dalla società texana e compromesso tramite *backdoor* probabilmente nella primavera del 2020, è stato il principale punto d'ingresso degli hacker. Si trattato, dunque, di un attacco alla *supply-chain*, che ha interessato molti dipartimenti del governo degli Stati Uniti e diverse multinazionali causando grosse perdite economiche e danni politici che hanno richiesto mesi per essere individuati e quantificati.
Meno di sei mesi dopo l'attacco, gli Stati Uniti hanno accusato la Russia dell'attacco. Gli indizi puntano verso Cozy Bear (APT29), collettivo legato all'intelligence russa. Ma, oltre alle responsabilità dell'attacco, ci sono quelle di chi avrebbe dovuto prevenirlo e non l'ha fatto.
A distanza di quasi tre anni dall'inizio dell'attacco, la Sec ha accusato SolarWinds e il suo *chief information security officer* (Ciso), **Timothy Brown**, "per frode e carenze di controllo interno in relazione a presunti rischi e vulnerabilità di cybersicurezza noti". Almeno dall'offerta pubblica iniziale dell'ottobre 2018 fino al dicembre 2020, quando l'attacco è divenuto di dominio pubblico, SolarWinds e Brown "hanno frodato gli investitori sopravvalutando le pratiche di sicurezza informatica di SolarWinds e sottovalutando o non rivelando i rischi noti", si legge nella nota diffusa dalla Sec. E ancora: "Nei documenti depositati presso la Sec durante questo periodo, SolarWinds avrebbe ingannato gli investitori divulgando solo rischi generici e ipotetici in un momento in cui l'azienda e Brown erano a conoscenza di carenze specifiche nelle pratiche di sicurezza informatica di SolarWinds e dei rischi sempre più elevati che l'azienda doveva affrontare nello stesso periodo".
La decisione contiene "un messaggio agli operatori del settore", ha dichiarato **Gurbir S. Grewal**, direttore della divisione della Sec per l'applicazione delle norme: "Implementate controlli solidi adeguati ai vostri ambienti di rischio e parlate con gli investitori delle preoccupazioni note". (continua)
https://formiche.net/2023/10/accusa-sec-contro-solarwinds-maxi-cyber-attacco/
Formiche- *Gabriele Carrer - 31/10/2023 -*

L'intelligenza artificiale e la guerra tra Israele e Hamas: Tra disinformazione e questioni lavorative - L'Intelligenza Artificiale, nel contesto del conflitto Israele-Hamas, ha ridefinito la guerra di informazioni, mescolando realtà e disinformazione e sollevando questioni sulla libertà di espressione nel mondo del lavoro.
Negli ultimi tempi, l'uso dell'Intelligenza Artificiale (IA) nella diffusione di disinformazione legata ai conflitti globali è diventato un argomento di rilievo.
La recente guerra tra Israele e Hamas non ha fatto eccezione, ma la natura dell'IA in questo contesto potrebbe sorprendere molti, anche in relazione alla relazione alla guerra tra Russia e Ucraina.
Un recente articolo pubblicato da *WIRED* ha affrontato l'impatto dell'IA generativa nella diffusione della disinformazione relativa al conflitto. Sebbene molti temessero che questa guerra sarebbe stata la prima a essere inondata di false immagini generate da macchine, in realtà, l'effetto dell'IA è stato molto più sottile.
(continua)
https://www.ingenio-web.it/articoli/l-intelligenza-artificiale-e-la-guerra-tra-israele-e-hamas-tra-disinformazione-e-questioni-lavorative/
Ingenio - *Andrea Dari, 31.10.2023*

Antartide, via alla nuova missione italiana - 130 scienziati e tecnici per 31 progetti che riguardano scienze dell'atmosfera, storia del clima, biologia, geologia, oceanografia e astronomia. Coordinano il Cnr e l'Enea.
Le basi in Antartide sono un luogo d'elezione per i film di fantascienza fin dai tempi del cinema bianco e nero. Ma per riprendere un vecchio slogan pubblicitario, "noi siamo scienza e non fantascienza", e la trentanovesima spedizione scientifica italiana nel continente più a Sud parte con 130 fra ricercatori e tecnici impegnati in 31 progetti nei settori delle scienze dell'atmosfera, storia del clima, biologia, geologia, oceanografia e astronomia. Per citare un esempio, le attività di carotaggio del ghiaccio forniranno dati sull'evoluzione delle temperature e sulla composizione dell'atmosfera, tornando indietro nel tempo di 1 milione e mezzo di anni. Le attività di ricerca si svolgeranno nelle due basi "Zucchelli" (al livello del mare sul promontorio di Baia Terra Nova) e "Concordia" (a 3mila metri di altezza e 1.200 chilometri dalla costa), oltre che a bordo della nave rompighiaccio Laura Bassi. Le missioni italiane in Antartide, finanziate dal Ministero dell'Università e della Ricerca nell'ambito del Programma Nazionale di Ricerche in Antartide, sono gestite dal Cnr per il coordinamento scientifico, dall'ENEA per la pianificazione e l'organizzazione logistica delle attività e dall'Istituto Nazionale di Oceanografia e di Geofisica Sperimentale per la gestione tecnica e scientifica della rompighiaccio Laura Bassi. Le Forze Armate partecipano alla spedizione con 16 esperti militari di Esercito, Marina, Aeronautica e Arma dei Carabinieri**.**
https://www.lastampa.it/scienza/2023/10/31/news/antartide_via_alla_nuova_missione_italiana-13822466/
La Stampa *– Luigi Grassia - 31 Ottobre 2023*

L'intelligenza artificiale (IA) sta trasformando la cyber security - L'intelligenza artificiale sta trasformando decisamente la cyber security; si utilizzano algoritmi di apprendimento automatico in grado di rilevare e rispondere in tempo reale sia alle minacce note sia a quelle sconosciute. Sarà migliorata la collaborazione uomo-macchina: tra IA ed esperti. L'IA potrà individuare le potenziali minacce, libererà tempo degli analisti per valutarle e intervenire. I sistemi di intelligenza artificiale

saranno uno strumento fondamentale per la formazione di un maggior numero di professionisti della cybersicurezza e li aiuterà a lavorare con migliori risultati.
https: www.ilsole24ore.com/art/come-l-intelligenza-artificiale-sta-rivoluzionando-cyber-security-AFcI7VSB
24 Ore Professionale *– Alessandro Longo – 1° Novembre 2023*

Ukraine braced for attacks on its power grid as winter draws in
Ukraine is rushing to bolster its energy infrastructure ahead of winter as a renewed Russian aerial campaign starts to home in on the country's power stations, seeking to leave its people in the dark and cold. Over the summer Russia largely targeted Ukraine's seaports and grain-exporting infrastructure. But in recent weeks missile and drone strikes have again started to focus on energy infrastructure, as they did last year when they caused blackouts for days.
This time around Kyiv is confident it is better prepared.
At a critical electricity grid substation in northern Ukraine, a wall of concrete blocks has been erected to protect transformers. Gabions, or cylinder cages filled with rocks or sand, can be seen surrounding another nearby substation, the location of which cannot be revealed due to wartime security rules. "We call it passive protection," Ukraine's prime minister Denys Shmyhal told the Financial Times. He said the country was "much more prepared" after testing and improving its fortifications during Russia's missile strikes last winter. The defences were still "not 100 per cent effective", Shmyhal said. But they worked "in 80 to 90 per cent of cases", especially against drones that veer off course or whose debris falls on to critical infrastructure after being intercepted. Last winter Russia fired more than 1,200 missile and drone strikes on Ukraine's power stations, "destroying more than 40 per cent of our electricity infrastructure, including generation and power grid", Shmyhal said. "We repaired most of this damage." *(Continua…)*
https://www.ft.com/content/aea600e6-2c19-42ab-ad13-5c6507c00579
Financial Times *- Roman Olearchyk – 2 Nov 2023*

Regole su intelligenza artificiale, ecco le differenze tra Ue e Usa
Come per molti altri aspetti dell'economia digitale, anche sull'intelligenza artificiale Europa e Stati Uniti adottano approcci sostanzialmente diversi. Differenze e analogie tra l'AI Act Ue e l'executive order Usa in merito a ricerca e sviluppo, privacy, tutela del copyright
Mentre in Europa proseguono i negoziati del trilogo per chiudere la partita sul **regolamento AI Act** prima della fine della legislatura, emergono alcune novità a livello internazionale, **l'ordine esecutivo firmato dal Presidente Joe Biden** delinea la posizione politica e strategica degli Stati Uniti sulla creazione, diffusione e utilizzo dei modelli di **intelligenza artificiale**.
Esaminiamo e mettiamo a confronto i due approcci allo sviluppo dell'intelligenza artificiale.
Indice degli argomenti

L'executive order Usa a confronto con l'AI Act

Tutto questo mentre a Washington il Presidente Biden rendeva noto l'**Executive Order** sull'Intelligenza Artificiale.
La prima cosa che vale la pena di analizzare e comprendere è **il diverso approccio tra USA ed Europa sul tema.**
La proposta di legge sull'IA in discussione in Europa adotta un approccio basato sul rischio, ma definisce le applicazioni IA ad alto rischio in modo più ristretto.
Al contrario, l'**approccio statunitense adotta un approccio più completo**, che comprende una gamma più ampia di applicazioni di intelligenza artificiale, ma manca di un'attenzione specifica all'alto rischio presente nella proposta dell'UE.
L'aspetto legislativo
Per quanto attiene all'aspetto legislativo l'UE segue un approccio orientato alla conformità, che prevede una valutazione di conformità obbligatoria e un processo di approvazione per l'IA ad alto rischio. In particolare, impone restrizioni rigorose su alcuni usi dell'intelligenza artificiale, come la classificazione sociale e il riconoscimento facciale.
Nell'Executive Order USA si fa affidamento principalmente sulla collaborazione volontaria con le autorità governative, unita all'enfasi sullo sviluppo di standard di sicurezza dell'IA. L'obiettivo è garantire la sicurezza, la protezione e l'affidabilità dei sistemi di intelligenza artificiale senza divieti specifici su applicazioni come la classificazione sociale o il riconoscimento facciale (continua…).
https://www.agendadigitale.eu/mercati-digitali/tutela-dei-diritti-dai-rischi-dellai-approcci-ue-e-usa-a-confronto/
Agenda Digitale- *Enzo Mazza- 3 nov 2023*

Rafforzamento della cooperazione europea sull'intelligenza artificiale: una visione condivisa
L'intelligenza artificiale sta emergendo come una tecnologia trasformativa con profonde implicazioni in vari settori. Roma, Parigi e Berlino hanno quindi avviato una collaborazione trilaterale per rafforzare il ruolo dell'Europa nello sviluppo, nella regolamentazione e nella competitività industriale dell'IA. In un **significativo segno di unità e visione condivisa**, i Ministri delle tre maggiori economie dell'UE, Italia, Germania e Francia, si sono recentemente riuniti a Roma per intensificare la loro **cooperazione nel campo degli affari digitali e dell'intelligenza artificiale (IA)**.
Questa **collaborazione trilaterale**, nota come triangolo Roma-Parigi-Berlino, sottolinea l'impegno a **rafforzare il ruolo dell'Europa nello sviluppo, nella regolamentazione e nella competitività industriale dell'IA**.
L'incontro, tenutosi sotto la nuova formula trilaterale, ha enfatizzato il **ruolo cruciale dell'IA nella duplice transizione verso un futuro digitale e verde**.
Ecco i principali punti salienti dei loro sforzi collaborativi, l'importanza dell'IA nel contesto globale e l'imperativo di una governance innovativa e responsabile dell'intelligenza artificiale.
Indice degli argomenti

- **Panorama globale dell'IA: un'epoca trasformativa**
- **Guidare l'iniziativa: l'impegno di Francia, Germania e Italia**
- **Priorità dell'IA nella politica industriale europea**
- **Materiali grezzi critici e future collaborazioni**
- **Guardando avanti: il percorso dell'Europa nella governance dell'IA**

Panorama globale dell'IA: un'epoca trasformativa
Negli ultimi anni, l'IA è emersa come una tecnologia trasformativa con profonde implicazioni in vari settori. I paesi del G7 hanno **recentemente pubblicato** il loro **Codice Internazionale di Condotta per i sistemi avanzati di IA**, evidenziando l'urgenza di stabilire linee guida

Inoltre, il Presidente degli Stati Uniti Joe Biden ha firmato un decreto per rafforzare il controllo governativo sul settore dell'IA, sottolineando l'importanza globale della regolamentazione e dello sviluppo dell'IA. (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/rafforzamento-della-cooperazione-europea-sullintelligenza-artificiale-una-visione-condivisa/
Cybersecurity360 - *Tommaso Maria Ruocco- 03 Nov 2023*

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

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	Nella sezione "Newsletter"del sito

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

http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.

Comitato di Redazione

Alberto Traballesi
Glauco Bertocchi
Silvano Bari
Gianluca Cipriani
Andrea Agostino Fumagalli

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.