Dai blackout «iberici» alle smart-city: la Difesa italiana indica la tecnologia ZeroSurface®.

9 maggio 2025

Il fatto e le interpretazioni

Come ormai tutti sappiamo, il 28 aprile 2025 la Penisola Iberica – Spagna, Portogallo e per pochi minuti anche una manciata di linee francesi di confine – ha visto spegnersi semafori, treni e centrali di telecomunicazioni nel giro di secondi. *Red Eléctrica* e *REN* hanno parlato di "distacco di generazione a cascata". Madrid e Lisbona hanno insistito sul fatto che **non si sia trattato di un attacco informatico**, benché il tribunale dell'*Audiencia Nacional* e un *panel* speciale di ENISA/ACER stiano comunque scavando nell'ipotesi di un sabotaggio *cyber*. Il risultato, per ora, è una mezza verità ufficiale: «niente hacker», **accompagnata però da un'inchiesta per reati di terrorismo digitale**…

Oltre la nebbia

Ignorando per qualche minuto la nebbia delle indagini possiamo trarre, in ogni caso, una lezione limpida, a prescindere dalla "verità" che poi ci verrà comunicata: affidarsi a **dorsali monolitiche** – elettriche o digitali che siano – significa lasciare al destino (o a un nemico) un gigantesco set di… *tessere del domino* già in equilibrio precario. Quando ne cade una, **l'effetto valanga si propaga in modo automatico e veloce**. In alcuni commenti, all'indomani dell'evento, si è parlato di "iperconnessione delicata": il *blackout* iberico infatti non ha soltanto "spento le luci" ma ha paralizzato *big data center*, linee AVE, aeroporti, comunicazioni cellulari, la rete internet, ha messo in gravissima difficoltà i centri sanitari…

Insomma trasporti, sanità, logistica (fra le tante pensiamo a quella alimentare, per esempio), mercati finanziari, comunicazioni: **tutti i sistemi critici europei condividono lo stesso vizio di forma**. E in uno scenario di conflitto (argomento mai tanto sensibile) l'esercizio diventa quasi banale: non servono missili, **basta colpire il nodo giusto** – fisico o digitale – perché i servizi civili collassino insieme alla fiducia pubblica e alla tenuta stessa di un territorio.

Prevenire è meglio che…

Pensando a un simile scenario, pare allora particolarmente lungimirante quanto lo **Stato Maggiore della Difesa** ha presentato alla Cecchignola dal 2 al 4 aprile scorsi, e cioè la prima "Live Demo" di uno **Smart Military Camp**, progetto che ha **terminato la fase esecutiva** e si avvia alla gara d'assegnazione che si terrà a settembre: un piccolo villaggio di tende, *shelter* e sensori, alimentato da fotovoltaico, biocarburanti e batterie, capace di restare autonomo per giorni senza agganciarsi a reti civili. Presente all'evento, **il Capo di SMD, generale Luciano Portolano**, ha definito l'autosufficienza energetica "cardine della strategia operativa", mentre il **Segretariato Generale della Difesa** e l'AIAD presentavano pannelli, mini-reti e sistemi di purificazione acqua già pensati per eserciti e Protezione Civile.

Venendo alla parte che ci interessa molto da vicino, **e che ci chiama a un'importante responsabilità**, è l'inserimento, fra le specifiche di progetto, della tecnologia **ZeroSurface®** per lo scudo *cyber*. Diversamente dalle architetture *Zero Trust* nate per l'IT aziendale – firewall, segmentazioni, VPN, *auditing* continuo, con tutto il carico di complessità ed energia che comportano – **ZeroSurface® riduce la superficie d'attacco a zero** prima ancora di difenderla. Finché l'utente (uomo o macchina) non presenta la sua *iceKey (processo che avviene sempre in modalità asimmetrica)*, l'apparato OT **non esiste sulla rete**: niente IP pubblici, niente porte di servizio, niente *ping* o *scanning*, quindi nessuna necessità di separare forzatamente la micro-rete (il cosiddetto *islanding* difensivo) per timore di intrusione. Se un guasto fisico impone davvero l'isola, la base sa farlo; **ma non è obbligata** a spezzare le connessioni "per prudenza" – una differenza cruciale quando servono telediagnosi o supporto remoto in piena emergenza.


ZeroSurface
ZeroSurface
une
une
une

…dover curare tutto il resto

La stessa logica, com'è intuibile, può uscire dal perimetro militare. Una *smart-city*, per esempio, che voglia essere davvero intelligente non può permettersi di funzionare come un castello

medievale, chiudendo il ponte levatoio ogni volta che circola un nuovo nemico. Deve rimanere aperta a scambi di dati, energia e servizi, **ma rendere irraggiungibili** – quindi **inattaccabili** – le sue arterie vitali: centrali di teleriscaldamento, colonnine di ricarica, semafori, cartelle cliniche e-chi-più-ne-ha-più-ne-metta. Portare il paradigma **ZeroSurface®** nelle reti urbane significa reinventare la sicurezza come "assenza di bersaglio", non come aggiunta di strati difensivi sempre più costosi.

Se poi sei anche lungimirante è il massimo

E c'è di più. Ricorderete il nostro post di pochi giorni fa sulla **partnership Italia-Albania** per la prima **Comunità Energetica Transfrontaliera**, sempre con protezione ZeroSurface® (qui la nostra intervista rilasciata alla TV albanese), un progetto che può mettere in rete basi logistiche, piccole industrie e comuni rurali sui due versanti dell'Adriatico, senza lasciare la minima fessura ai pirati informatici. Ebbene, a seguito del blackout iberico, il **World Economic Forum** indica come **"cura obbligatoria"** proprio la **cooperazione internazionale e la cybersicurezza nativa** prima di far correre elettroni e dati oltre confine, in altre parole auspicando l'attraversamento dei confini con comunità energetiche **antifragili** (usando il meraviglioso neologismo di *Taleb*) e invisibili agli aggressori.

Conclusione

Non parliamo dunque di un esercizio di stile ma di qualcosa già realizzato e funzionante che concretizza un modo assai serio di evitare che un'interruzione "a domino" prenda in ostaggio mezza Europa. Il *blackout* di aprile ci ricorda che l'energia – e con lei tutti gli altri asset strategici – vive di interdipendenze che possono diventare trappole. Il progetto italiano dei **Smart Military Camps**, con un **guscio digitale a "superficie zero"** sulla parte energetica, mostra una via d'uscita: distribuire la produzione e, soprattutto, **far sparire il bersaglio**. Se riusciamo a farlo in un campo militare, possiamo farlo anche nei quartieri dove viviamo, e trasformare quindi la prossima "città connessa" da bersaglio perfetto a **rete irraggiungibile e invisibile**, capace di restare accesa – e connessa – senza legare la propria sopravvivenza alle grandi tessere del domino.

Fonti:

https://www.difesa.it/smd/casmd/eventi/difesa-capo-stato-maggiore-difesa-allo-smart-military-camp/68352.html

https://www.weforum.org/stories/2025/05/spain-might-not-cyberattack-blackout-power-outage-electric-grids-vulnerable/

https://www.carbonbrief.org/qa-what-we-do-and-do-not-know-about-the-blackout-in-spain-and-portugal/

https://www.acer.europa.eu/news/expert-panel-investigate-blackout-portugal-and-spain

https://www.reuters.com/world/europe/large-parts-spain-portugal-hit-by-power-outage-2025-04-28/

https://www.ilmessaggero.it/italia/smart_military_camp_difesa_futuro_caserma_cecchignola_roma-8759314.html

https://www.theguardian.com/world/2025/apr/29/spain-portugal-returning-normal-experts-cause-blackout
https://www.difesa.it/smd/avvenimenti/smart-military-camps/smart-military-camps/67946.html

---