OPINIO JURIS
LAW & POLITICS REVIEW

Le infrastrutture critiche e la sfida della cyberwarfare

Il recente attacco informatico alla Colonial Pipeline ha confermato che lo spazio cibernetico è il fondamentale campo di battaglia e di competizione geopolitica del XXI secolo

A cura di Raimondo Fabbri

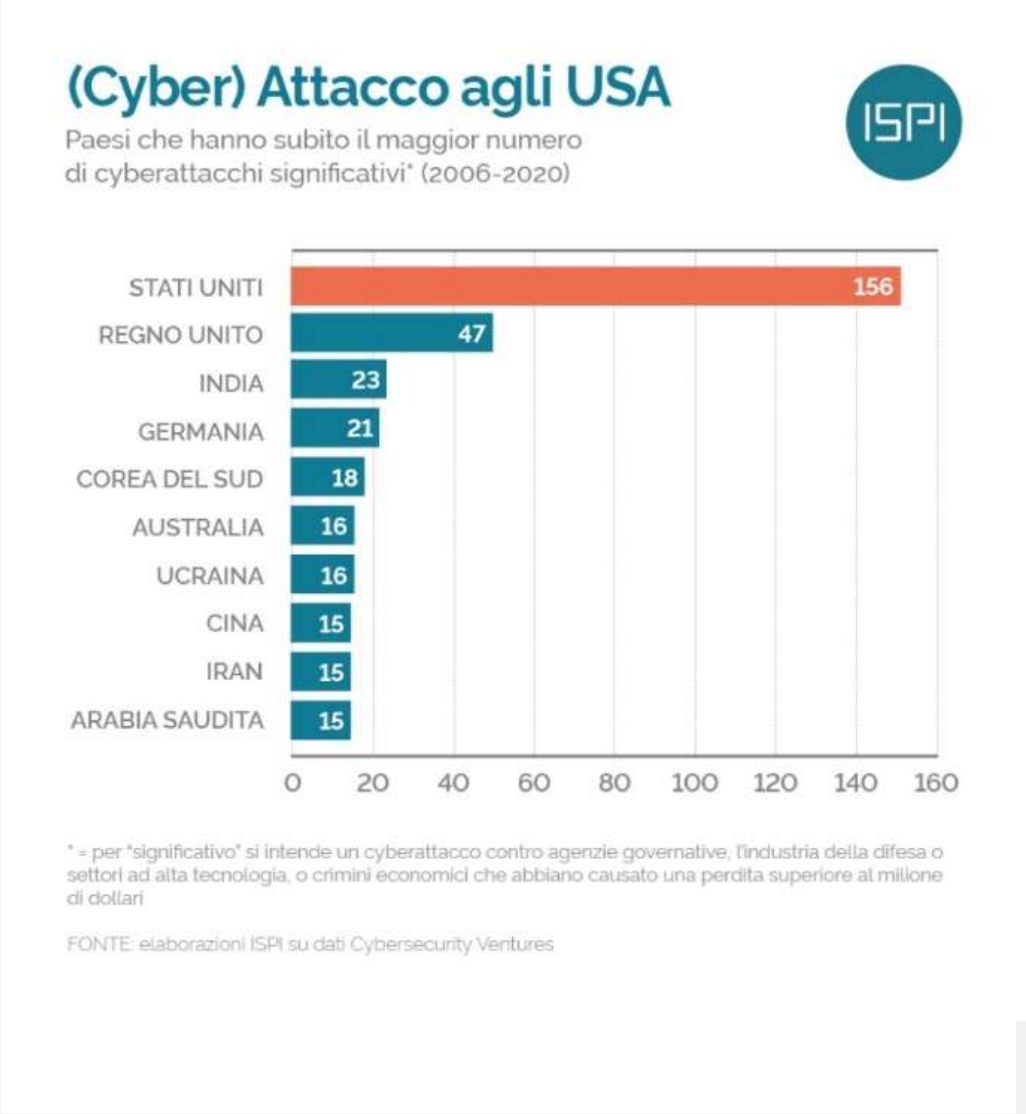
L'attacco alla Colonial Pipeline. L'ultimo di una lunga serie

Venerdì 7 maggio un attacco informatico ha temporaneamente bloccato le operazioni del Colonial Pipeline, il più grande sistema di oleodotti degli Stati Uniti, formato da 8.850 chilometri di condutture di prodotti raffinati, capaci di trasportare oltre 3 milioni di barili di benzina, diesel e carburante per aerei tra la costa del Golfo degli Stati Uniti e l'area del porto di New York.
Si è trattato dell'ultimo di una serie di episodi che negli ultimi anni sono aumentati ed hanno preso di mira una serie di infrastrutture critiche degli Stati Uniti e di altri importanti paesi come dimostrato dai recenti casi di SolarWinds e di quello più pericoloso che ha visto protagonista il sistema idrico della città di Oldsam, cittadina della Florida che il 7 febbraio scorso è stata oggetto di un attacco con il quale gli *hackers*

ISSN 2531-6931

hanno tentato di avvelenare l'acqua pubblica.
Questi uniti ai numerosi tentativi di intrusione nelle industrie della difesa oppure in quelle dei settori ad alta tecnologia, hanno dimostrato quanto la dimensione informatica sia divenuta di fatto il nuovo spazio operativo favorito dall'assenza di regole, in cui soggetti criminali privati o che agiscono come *longa manus* di apparati statali, mirano a paralizzare il nemico senza dover sparare un colpo [1] .
In questo senso le tecniche offensive cibernetiche tramite un sistema di computer piuttosto che attraverso la Rete, possono essere sfruttate al fine di ottenere informazioni, di interrompere, degradare o distruggere gli *endpoint* informatici e le infrastrutture di rete, contribuendo in questo modo a definire il cosiddetto terrorismo informatico come un attacco che utilizzando la tecnologia informatica può paralizzare o disattivare le reti fisiche ed elettroniche di una nazione, provocano la perdita di servizi critici come l'elettricità, i sistemi di emergenza, il servizio telefonico, i servizi bancari, Internet con l'obiettivo non solo di dare un colpo all'economia di un Paese, ma anche di amplificare gli effetti di un tradizionale attacco terroristico fisico, ingenerando confusione e panico nella popolazione[2]

[1] VISANI P., Storia della guerra nel XX secolo, Oaks editrice, Milano 2020 pp.202-203
[2] VIGNERI F., Fenomenologia del terrorismo: dall'11 settembre al cyberterrorismo, Opinio Juris, 03/06/2018 url: https://www.opiniojuris.it/fenomenologia-del-terrorismo/.



Infrastrutture sempre più critiche

Per tali ragioni il sistema delle infrastrutture critiche, ovverosia l'insieme di quei sistemi, risorse, processi, la cui distruzione, interruzione o anche parziale o momentanea indisponibilità, porterebbero all'indebolimento dell'efficienza e del normale funzionamento di uno Stato, si sono trasformati negli obiettivi sensibili da presidiare e proteggere al fine di garantire continuità all'erogazione dei servizi essenziali e all'operatività degli impianti. La pandemia ha senza dubbio complicato e reso più delicata la gestione di un quadro siffatto come peraltro hanno rilevato i servizi di intelligence italiani a

ISSN 2531-6931

proposito delle attività ostili perpetrate per mezzo del dominio cibernetico a danno degli assetti informatici rilevanti per la sicurezza nazionale, registrando in tal senso un generale incremento delle aggressioni (+20%) e confermando il preponderante ricorso a tecniche di *SQL Injection* per violare le infrastrutture informatiche delle vittime ed acquisirne il controllo remoto [3] . L'impegno finalizzato alla protezione delle infrastrutture critiche per Bruxelles vale oltre 38 milioni di euro, stanziati attraverso Horizon2020 proprio per affrontare le minacce cyber e fisiche. Tra i cinque progetti si alcuni si segnalano per l'entità degli stanziamenti: *Safety4Rails* dedicato alla sicurezza cibernetica e fisica delle linee di trasporto su rotaia, metro e ferrovie, con un budget complessivo pari a 9,6 milioni di euro, che vede tra i 29 partecipanti sei realtà italiane come Leonardo, Rina Consulting, Stam, Rete Ferroviaria Italiana, Comune di Milano e Alpha Cyber; *S4allCities* cui è stato destinato un budget di 9,7 milioni per realizzare un sistema di protezione delle città intelligenti[4]. Le minacce ibride alle reti iperconnesse sono i nuovi strumenti di offesa, utilizzabili in modo coordinato da entità statali o non statali per raggiungere determinati obiettivi, rimanendo però sempre al di sotto della soglia di una guerra ufficialmente dichiarata seppur rientrando pienamente nella strategia che intende sfruttare i punti deboli del bersaglio per ostacolarne i processi decisionali. Ecco perché anche questa è diventata una materia che ha assunto una dimensione europea[5].

Cavi sottomarini, reti stradali e di trasporto come soggetti vulnerabili

Lo sviluppo delle tecnologie legate all'Internet of Things se per un verso ha aumentato il numero di oggetti fisici connessi, per l'altro ha esteso i rischi di infiltrazione dei perimetri aziendali. Pur riconoscendo

[3] Il rapporto dell'anno 2020 curato dal Sistema di informazione per la sicurezza della Repubblica è disponibile al seguente url: https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html

[4] PIOPPI S., Più (cyber) sicurezza per le infrastrutture critiche. Ecco i progetti di Bruxelles, Formiche.net, 15/06/2020 url: https://formiche.net/2020/06/cyber-sicurezza-infrastrutture-europa/

[5] VIGNERI F., Il ruolo dell'intelligence tra vecchie e nuove sfide, in Opinio Juris n.5/2021, p.114

a simili innovazioni un ruolo sempre più centrale nei piani di sviluppo della mobilità integrata collettiva, in particolare delle grandi aree metropolitane, così come nello sfruttamento più efficace ed efficiente delle infrastrutture critiche, tipo il settore dei trasporti, non si può non sottovalutare l'aspetto cruciale della sicurezza informatica. Basti pensare al trasporto aereo, fortemente interconnesso ed alla continua ricerca di maggiore efficienza grazie ai servizi cloud che consentono il contenimento dei costi ed il miglioramento dell'esperienza di volo. Ebbene questi investimenti in Information Tecnology, hanno tuttavia un aspetto critico: se non sistematicamente monitorarti e basati su una cyber security preventiva possono prestare il fianco ad attacchi, anche con finalità terroristiche, che possono comportare non soltanto il furto di informazioni confidenziali e riservate, ma anche il blocco dei servizi essenziali e di mobilità collettiva come potrebbe avvenire per le cosiddette *smart road*, strade intelligenti che prevedendo maggiori connessioni in grado di renderle più sicure, permettendogli di dialogare con gli utenti a bordo dei veicoli fornendogli in tempo reale informazioni su traffico, incidenti, condizioni meteo, le renderanno obiettivi sensibili di eventuali azioni di sabotaggio.
Non potrà sfuggire agli attacchi informatici neanche il settore dei trasporti marittimi. Le minacce cyber per le navi e le loro merci sono anzi uno dei rischi emergenti e destinati, potenzialmente, a un impatto maggiore perché l'industria marittima ed i porti dipendono e dipenderanno in misura crescente da sistemi digitali interconnessi. Per non parlare del dedalo dei cavi sottomarini che si snoda proprio lungo le principali rotte commerciali navali. Arterie nelle quali viaggia la quasi totalità del traffico internet globale e che rappresentano la spina dorsale dell'economia globalizzata.
Le connessioni planetarie facendo affidamento su queste infrastrutture per la loro efficienza e la loro convenienza economica sono meno costose dei satelliti ed hanno un'elevata capacità in termini di terabytes, divenendo nello stesso tempo il centro nevralgico dei dati, delle transazioni economiche, delle comunicazioni e dello scambio di informazioni. Tutto ciò le rende naturalmente vulnerabili tanto agli incidenti casuali quanto e soprattutto agli attacchi pianificati che danneggiandole potrebbero causare l'interruzione del flusso di dati

ISSN 2531-6931

essenziali sia per le operazioni finanziarie che per le comunicazioni militari, soprattutto in momenti di crisi e di conflitto[6].

Attacchi informatici, la nuova normalità

Gli episodi richiamati all'inizio hanno acclarato che gli attacchi informatici non rappresenteranno degli sporadici eventi, quanto piuttosto un fattore di normalità che potrà essere contrastato solamente sviluppando notevoli capacità di resilienza cibernetica per le infrastrutture critiche, la cui compromissione potrebbe pregiudicare funzioni vitali per lo Stato. Una simile necessità di sicurezza sarà vieppiù cruciale non solamente per la protezione delle aziende e delle reti fisiche e digitali, ma anche per la collocazione dell'Italia nel contesto geopolitico europeo e internazionale, dato l'attivismo dimostrato in questo spazio dall'Unione Europea a cui il nostro paese sta adeguando il proprio quadro normativo ricomprendendo la sicurezza informatica nel più strategico obiettivo della tutela della sicurezza nazionale[7].

[6] SPOSINI A., PATRIARCA M.., La geografia del cyberspazio Cavi sottomarini, Data Center e Cloud Service Provider: tra connettivita' e competizione, Domino - Geopolitical Brief, n.18-febbraio 2021, url: https://www.geopolitica.info/geopolitical-brief-18-la-geografia-del-cyberspazio/

[7] LO PRETE D., Cybersecurity in Italia: verso un approccio strutturale per la resilienza delle infrastrutture critiche, Geopolitica.info, 12/04/2021 url: https://www.geopolitica.info/cybersecurity-in-italia-verso-un-approccio-strutturale-per-la-resilienza-delle-infrastrutture-critiche/