Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 24 | 11 - OTTOBRE 2024

Resilienza e sicurezza delle infrastrutture critiche nel contesto italiano ed europeo

di Paola Tessari e Karolina Muti

ABSTRACT

I rischi e le minacce alla resilienza delle infrastrutture critiche (IC) si sono evoluti e comprendono oggi con maggiore frequenza disastri naturali dovuti all'emergenza climatica, ma anche incidenti industriali, attacchi cibernetici e cinetici. Il verificarsi di eventi emergenziali spesso caratterizzati da impatti transfrontalieri e la dimensione non solo nazionale ma anche europea di molte IC, hanno inoltre evidenziato la necessità di una forte cooperazione fra gli Stati membri dell'UE al fine di garantire una gestione condivisa e coordinata a livello europeo. L'adozione della direttiva 2022/2057 sulla resilienza dei soggetti critici (Cer), entrata in vigore il 16 gennaio 2023, ha introdotto novità significative in questo ambito. Il presente studio si sofferma sulla rilevanza delle infrastrutture critiche nel contesto attuale, sulle caratteristiche dell'ecosistema in cui esse operano nell'UE e sulle implicazioni per la loro sicurezza derivanti da eventi come la pandemia Covid-19, l'invasione russa dell'Ucraina o gli investimenti diretti esteri di attori terzi. Lo studio analizza in seguito i nuovi settori considerati dalla direttiva Cer e illustra i suoi principali elementi, considerando anche le sfide in ambito di attuazione. Infine, lo studio si concentra sull'attuazione della direttiva in Italia.

keywords

Sicurezza | *Infrastrutture critiche* | *Unione europea* | *Italia*

Resilienza e sicurezza delle infrastrutture critiche nel contesto italiano ed europeo

di Paola Tessari e Karolina Muti*

ISSN 2280-6164

DOCUMENTI IAI 24 | 11 - OTTOBRE 2024

Executive summary

La compresenza di più tipi di minacce in grado di colpire infrastrutture critiche (IC) con caratteristiche diverse e distribuite in domini differenti pone una sfida rilevante in termini di gestione, controllo, e *decision-making*. Tale sfida riguarda in primis gli Stati membri dell'UE, ma anche gli operatori privati e proprietari delle IC che vengono maggiormente responsabilizzati dall'introduzione di nuove misure. La varietà delle minacce include quelle intenzionali e non intenzionali, condotte da attori statali e non statali, cinetiche e non cinetiche.

In tale contesto si inserisce l'adozione della direttiva 2022/2057 sulla resilienza dei soggetti critici, entrata in vigore il 16 gennaio 2023, conosciuta come direttiva Cer (*Critical Entities Resilience*)[1], che ha introdotto novità significative per rafforzare il ruolo di coordinamento dell'Unione, cercando in particolare di superare l'approccio strettamente settoriale e fornire maggiore supporto agli Stati membri per evitare la frammentazione che ha caratterizzato l'attuazione a livello nazionale della precedente direttiva[2].

La direttiva Cer amplia l'ambito di applicazione rispetto alla precedente direttiva del 2008 e riguarda un totale di 11 settori complessivi: a quelli dell'energia (1) e dei trasporti (2) già oggetto del quadro normativo precedente, si aggiungono

[1] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2557.

[2] Consiglio dell'Unione europea, *Direttiva 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32008L0114.

* Paola Tessari è responsabile di ricerca nel Programma Sicurezza dell'Istituto Affari Internazionali (IAI). Karolina Muti è responsabile di ricerca nei programmi Sicurezza e Difesa dello IAI. Le autrici ringraziano Federica Di Camillo e Alessandro Marrone per i feedback sulle bozze iniziali dello studio e Maria Vittoria Massarin e Mariano Varesano per il supporto nell'editing. Le autrici ringraziano gli interlocutori nelle istituzioni e nell'accademia che hanno gentilmente acconsentito a essere intervistati ai fini di questo studio.

quindi il settore bancario (3), quello delle infrastrutture dei mercati finanziari (4), della salute (5), dell'acqua potabile (6), delle acque reflue (7), delle infrastrutture digitali (8), della pubblica amministrazione (9), dello spazio (10) e della produzione, trasformazione e distribuzione degli alimenti (11). La direttiva Cer, ponendo l'accento sull'importanza della resilienza anche del settore *cyber*, richiede un approccio coordinato con la direttiva 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza, conosciuta come Nis2 (*Network and Information Security*)[3]. La direttiva Cer fornisce una cornice unica e di ampia portata ponendosi come obiettivo il raggiungimento di un livello di "armonizzazione minima" delle normative nazionali, ma allo stesso tempo lascia margine di manovra e autonomia ai singoli Stati membri.

Nel complesso, l'adozione della direttiva Cer amplia e approfondisce la tendenza ad affrontare un crescente numero di aspetti della sicurezza con un approccio comune a livello europeo, compreso il settore delle infrastrutture critiche. Tuttavia, non pregiudica la competenza degli Stati membri e delle rispettive autorità in termini di autonomia amministrativa, né la loro responsabilità di salvaguardare la sicurezza e la difesa nazionale o il potere di salvaguardare altre funzioni essenziali dello Stato, in particolare quelle di sicurezza pubblica, e l'integrità territoriale.

Per quanto riguarda l'approccio coordinato con la direttiva Nis2, la Cer prevede che gli Stati membri identifichino, fra le infrastrutture digitali, quelle che si qualificano come soggetti critici ai sensi della Cer. Le autorità competenti per le due direttive sono inoltre chiamate a cooperare con scambio di informazioni e con l'intento di attuare le misure delle rispettive normative in maniera complementare.

Per come si configura il rapporto con i soggetti critici, quest'ultimi dovrebbero essere sostenuti dagli Stati membri, "compresi quelli che si qualificano come piccole e medie imprese, nel rafforzamento della loro resilienza" evitando "oneri amministrativi eccessivi"[4]. Considerando il contesto italiano, il rischio di un peso burocratico e amministrativo scaricato sui soggetti critici, specialmente quelli "nuovi" e di piccole dimensioni, andrebbe attenzionato fin da subito.

Alcuni di questi soggetti, inoltre, essendo operatori privati che devono stare sul mercato, potrebbero non vedere incentivi a essere classificati come "soggetto critico". Infatti, ciò comporta significative responsabilità a loro carico e maggiori controlli, a fronte di un supporto che dovrebbe essere fornito dalla Commissione e dallo Stato membro ma che, nei termini descritti nella direttiva, non sembra sufficiente a compensare la mole di adempimenti. Al contempo, tuttavia, la direttiva andrebbe vista anche come uno stimolo per aumentare la cultura di sicurezza dei

[3] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva Nis 2)*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2555.

[4] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., para. 25.

ISSN 2280-6164

soggetti critici e, in tal senso, i costi relativi agli adempimenti normativi previsti andrebbero interpretati come un investimento in sicurezza e non solo come un onere. I costi di incidenti e attacchi infatti spesso sono superiori rispetto a quelli di un'adeguata prevenzione.

Per quel che riguarda l'Italia, attualmente vi sono numerosi atti normativi relativi a specifici settori di infrastruttura critica, ma manca un quadro di riferimento univoco che raccolga tutte le misure nazionali rilevanti per la protezione e resilienza delle IC[5]. In Italia, la responsabilità dell'attuazione della direttiva, che deve avvenire entro il 18 ottobre 2024, è attribuita al Presidente del Consiglio dei ministri, che verrà supportato dall'istituzione di alcuni enti e organi ad hoc: il Punto di contatto unico (Pcu), le Autorità settoriali competenti (Asc), il Comitato interministeriale per la resilienza (Cir) e la Conferenza per la resilienza dei soggetti critici (Crsc). L'accentramento nel Presidente del Consiglio della responsabilità dell'attuazione delle misure di resilienza è un elemento positivo che può garantire il coordinamento a livello orizzontale con le autorità competenti per gli specifici settori, a fronte di misure che ne coinvolgono 11. Nella mappatura e nell'identificazione a livello nazionale dei soggetti sarà importante individuare con attenzione i criteri che permettono di definire un soggetto come "critico", tenendo conto dell'essenzialità dei servizi che fornisce, dei destinatari, nonché della diffusione e dispersione dei vari tipi di IC sul territorio nazionale, attraverso i cinque domini operativi (terrestre, marittimo, aereo, spaziale e cibernetico) e nella dimensione subacquea. Sarà inoltre importante fare attenzione alla complessa catena logistica e di approvvigionamento dietro le IC che comprende spesso sub-componenti, soggetti secondari ma imprescindibili di una catena di approvvigionamento (*supply chain*) che sovente, per alcuni tipi di soggetti critici, è per natura transnazionale.

[5] Patrizia Di Micco e Giulia Pascuzzi, "Resilienza, ecco la chiave per proteggere le infrastrutture critiche", in *Formiche.net*, 27 settembre 2023, https://formiche.net/?p=1580470.

ISSN 2280-6164

Introduzione

Dagli anni 2000 le infrastrutture critiche (IC) hanno ricevuto un'attenzione crescente da parte delle istituzioni europee e degli Stati membri dell'UE.

Il concetto di infrastruttura critica di per sé non è nuovo: sin dall'antichità, in situazioni di conflitto, IC e risorse primarie sono state oggetto di attacchi. I rischi e le minacce alla resilienza delle IC si sono evoluti e comprendono oggi con maggiore frequenza disastri naturali dovuti anche all'emergenza climatica, ma anche incidenti industriali, attacchi cibernetici e cinetici. Basti pensare agli incidenti ai gasdotti Nord Stream 1 e 2 nel settembre 2022[6], e ai danni alle infrastrutture critiche nel contesto dell'invasione russa dell'Ucraina[7] o nel quadro delle azioni degli Houthi nel Mar Rosso[8].

Negli ultimi anni, inoltre, il concetto stesso di infrastruttura critica si è evoluto fino a includere settori e servizi nuovi: ne è testimonianza la pandemia globale da Covid-19 che ha aumentato notevolmente la sensibilità e la consapevolezza verso la centralità di quei settori e servizi che non erano stati considerati in precedenza "critici" e che tuttavia, se interrotti, hanno dato prova di poter mettere in difficoltà intere comunità, rendendo evidente come fattori geostrategici si facciano spazio anche in aree meno attenzionate, come poteva sembrare in un primo momento il settore della Sanità.

La complessità della società contemporanea richiede alla popolazione, ai soggetti privati e alle istituzioni di fare crescente affidamento su un numero sempre maggiore di servizi essenziali, creando una rete di interdipendenze. Questo pone le istituzioni di fronte a una sfida su come assicurare la resilienza di tali servizi e la sicurezza delle infrastrutture, ma anche su come interfacciarsi efficacemente con un numero e una varietà senza precedenti di soggetti privati (operatori o proprietari di servizi e infrastrutture) in questo ambito. La globalizzazione, le dinamiche di interdipendenza economica a essa collegate, e il processo di integrazione europea, richiedono inoltre di uscire dalla tradizionale concezione delle infrastrutture e dei servizi che esse garantiscono come di una materia di azione esclusivamente nazionale.

Si osserva ad esempio in maniera crescente l'utilizzo dei sistemi spaziali per i servizi di geolocalizzazione e posizionamento, di comunicazione, di previsione di eventi meteorologici estremi, come strumento oramai indispensabile anche per

[6] "Nord Stream: danni senza precedenti. Danimarca: 'Atti deliberati. Perdite per 7 giorni'", in *SkyTG24*, 27 settembre 2022, https://tg24.sky.it/mondo/2022/09/27/attacco-nord-stream-gasdotto.

[7] Paola Tessari, "La doppia minaccia nucleare che grava sull'Ucraina", in Alessandro Marrone et al., *La guerra russo-ucraina, la sicurezza dell'Europa e la difesa europea*, Roma, IAI, 2022, https://www.iai.it/it/node/16243.

[8] Daniel Bellamy, "Mar Rosso: petroliera battente bandiera greca in fiamme dopo un attacco degli Houthi", in *Euronews*, 24 agosto 2024, https://it.euronews.com/2024/08/24/mar-rosso-petroliera-battente-bandiera-greca-in-fiamme-dopo-un-attacco-degli-houthi.

ISSN 2280-6164

l'individuo nella sua quotidianità. Lo stesso vale per le infrastrutture cosiddette digitali, del mercato finanziario e bancario, oltre a quelle tradizionalmente e da più tempo individuate come IC da precedenti normative europee, ovvero il settore dei trasporti e quello dell'energia. A questo si aggiungono la sicurezza alimentare (per quel che riguarda tanto l'acqua potabile che la produzione e distribuzione di cibo), il funzionamento della pubblica amministrazione e, come appunto evidenziato dalla pandemia da Covid-19, il settore sanitario.

Di fronte ad una tale espansione del concetto di infrastruttura critica, la direttiva UE 2022/2557 relativa alla resilienza dei soggetti critici (conosciuta come direttiva Cer - "*Critical Entities Resilience*")[9] fa chiarezza introducendo una distinzione tra *critical entities* (tradotto in italiano con "soggetti critici") e "infrastruttura critica". La Cer, inoltre, sposta l'attenzione dal concetto di "protezione" della IC, come stabilito nel quadro normativo precedente introdotto dalla direttiva 2008/114/CE, al concetto di "resilienza", termine più complesso che ne amplia il focus. L'approccio precedente, incentrato prettamente sulla risposta ad un evento che colpisce un'IC, evolve verso una serie di azioni da mettere in atto prima, durante e dopo eventuali incidenti volte a garantire la continuità del servizio. In ambito UE, con l'approvazione della direttiva Cer, i settori cui si rivolgono le misure di resilienza sono ben 11: un'espansione del campo di attuazione notevole, rispetto ai due settori di energia e trasporti oggetto della direttiva precedente.

Partendo da una riflessione sulla rilevanza delle IC nel contesto attuale, il presente studio mira a evidenziare gli elementi che caratterizzano tale ecosistema, con particolare attenzione alla diversità delle minacce a cui si trovano esposte. Vengono poi analizzate brevemente le implicazioni sulla resilienza delle IC derivate da recenti eventi emergenziali quali la pandemia, da altre crisi di diversa natura quale l'invasione russa dell'Ucraina, e da strumenti di politica estera e commerciale quali gli investimenti diretti all'estero.

A livello europeo, lo studio analizza in profondità la direttiva Cer, con particolare attenzione alle misure innovative introdotte rispetto al quadro normativo della precedente direttiva 2008/114/CE e relative all'individuazione e alla designazione di nuovi settori rilevanti per l'erogazione di servizi essenziali. Segue una spiegazione delle misure di attuazione a livello nazionale, unitamente a una ricerca degli enti che possono avere un valore "critico" sulla base dei più significativi e recenti documenti strategici, istituzionali e normativi di riferimento, e di recenti eventi che hanno avuto come obiettivo le infrastrutture critiche. Tale analisi servirà a tracciare dei suggerimenti di *policy* articolati nel capitolo conclusivo.

[9] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit.

ISSN 2280-6164

1. La rilevanza delle infrastrutture critiche nel contesto attuale

1.1 Le caratteristiche dell'ecosistema di IC nell'UE

Come già evidenziato nell'introduzione, le IC sono esposte a molteplici rischi e minacce, che si possono distinguere a seconda delle loro caratteristiche relative all'obiettivo, all'origine e allo spazio di azione. Con riferimento all'obiettivo, il tipo di attacchi cui sono esposte le IC possono essere suddivisi in attacchi che vanno a colpire l'integrità fisica delle stesse, e quelli rivolti alla dimensione cibernetica (*cyber*). Una seconda suddivisione può essere fatta differenziando tra minacce di tipo cinetico e non-cinetico, poiché permette di considerare anche gli attacchi nello spettro elettromagnetico (ad esempio ai satelliti), oltre a quelli *cyber* nella categoria non-cinetica. Questi ultimi si sono distinti per la loro frequenza negli ultimi anni, colpendo sistematicamente la maggior parte dei tipi di IC considerati nel presente studio, sfruttandone la vulnerabilità diffusa in questo campo, derivante ad esempio da obsolescenza dei sistemi informatici e di protezione, scarsa conoscenza e formazione del personale, mancanza di manutenzione e degli aggiornamenti di sicurezza necessari[10].

Un'ulteriore distinzione è possibile in riferimento all'origine degli attacchi, ovvero che si tratti di azioni intenzionali (mosse da attori statali o non statali, incluse quelle causate dall'uomo, o *insider threat*[11]) oppure di eventi non intenzionali (disastri naturali ed eventi meteorologici estremi, malfunzionamenti, guasti, incidenti industriali). A questi ultimi si sono aggiunti recentemente le minacce e i rischi legati all'emergenza climatica, i cui effetti possono compromettere ad esempio la resistenza dei materiali. Vari tipi di minacce co-esistono e necessitano di contromisure, procedure di protezione e attivazione di catene di comando diverse tra loro, rendendo il quadro di resilienza più complesso.

Va sottolineato, inoltre, il crescente livello di interdipendenza tra diversi tipi di IC che secondo alcuni osservatori può essere fisica, geografica, o logica[12]. L'interdipendenza fisica sussiste quando delle infrastrutture dipendono per il proprio funzionamento da un input materiale, fisico appunto, di un'altra infrastruttura[13]. Un esempio calzante di interdipendenza fisica riguarda il caso della centrale nucleare di Zaporizhzhia e della diga di Kakhovka, il cui danneggiamento

[10] Elio Calcagno et al., "Le minacce cyber ed elettromagnetiche alle infrastrutture spaziali", in *Documenti IAI*, n. 24|07 (luglio 2024), https://www.iai.it/it/node/18696.

[11] Si tratta di azioni malevole, come sabotaggi, furti, danneggiamenti, provocati da un membro del personale che direttamente o indirettamente ha familiarità con una determinata infrastruttura o servizio perché ci lavora.

[12] Georgios Giannopoulos, Bogdan Dorneanu e Olaf Jonkeren, "Risk Assessment Methodology for Critical Infrastructure Protection", in *JRC Scientific and Policy Reports*, 2013, https://publications.jrc.ec.europa.eu/repository/handle/JRC78292.

[13] Steven M. Rinaldi, James P. Peerenboom e Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", in *IEEE Control Systems Magazine*, vol. 21, n. 6 (dicembre 2001), p. 11-25, DOI 10.1109/37.969131.

ISSN 2280-6164

causato da un attacco missilistico russo a giugno 2023, ha messo a rischio l'approvvigionamento di acqua necessario per il raffreddamento del reattore della centrale[14]. Oppure, l'interruzione del funzionamento di un satellite con funzioni di geolocalizzazione può impattare direttamente sui mezzi di trasporto marittimi, ferroviari e su gomma. Ancora, la rottura di un cavo sottomarino in fibra ottica, oppure un attacco *cyber* alla rete, può implicare mancanza di connessione ad Internet per una vasta gamma di servizi: sanitari (sistemi di prenotazione), finanziari, bancari, digitali, della pubblica amministrazione. Oltre ad una interdipendenza fisica tra tipi di IC, esiste anche una interdipendenza geografica che riguarda tanto le IC situate in prossimità all'interno dello stesso territorio nazionale, quanto una dimensione transfrontaliera (*cross-border*) che interessa sia i paesi membri UE sia quelli extra-UE. Questo aspetto va considerato perché la cornice istituzionale di riferimento influisce sul quadro politico, normativo e procedurale e condiziona la risposta a un'emergenza legata all'IC. Nel marzo 2022 un velivolo a pilotaggio remoto di fabbricazione russa, più comunemente noto come drone, è entrato nello spazio aereo croato e si è schiantato nella periferia della capitale Zagabria. L'incidente avvenne a meno di 40 chilometri dalla centrale nucleare slovena di Krško, stimolando entrambi i paesi a investire in difese aeree.

Infine, l'interdipendenza logica riguarda invece quei casi che non derivano da una interdipendenza geografica o fisica e hanno al centro l'azione e la decisione umane e le norme, regole e attività codificate nei piani riguardanti le infrastrutture[15].

Un ulteriore elemento di vulnerabilità è dato dal fatto che le IC, ampiamente gestite, operate e/o di proprietà di attori privati, possono essere oggetto di interferenze e/o attacchi riconducibili invece ad attori statali che hanno capacità e mezzi significativamente superiori rispetto ai singoli gestori privati dell'infrastruttura. Gli attacchi possono variare in termini di intensità e scopi, andando da un'ingerenza ottenuta attraverso pratiche lecite, come gli investimenti diretti esteri finalizzati ad assicurarsi il controllo di una IC o di una sua parte fondamentale, quale la logistica di uno snodo essenziale come un porto, fino al sabotaggio (caso Nord Stream 2), o addirittura a un attacco militare diretto contro una IC, come nel caso degli attacchi contro le infrastrutture in Ucraina. La linea di demarcazione, sia tra pubblico e privato, sia tra civile e militare, è dunque sempre più sfumata, e questo mette sotto pressione le istituzioni competenti che sono chiamate a investire tempo e risorse in un adeguato coordinamento di un ventaglio di attori sempre più ampio e diversificato, fuori dall'approccio per "silos" settoriali e locali che impedisce di vedere gli effetti a cascata e l'impatto intersettoriale (*cross-sectoral*) delle potenziali interruzioni.

[14] "Ucraina: colpita la diga di Kakhovka, paura per la centrale di Zaporizhzhia", in *Euronews*, 6 giugno 2023, https://it.euronews.com/2023/06/06/ucraina-colpita-la-diga-di-kakhovka-concordano-russi-e-ucraini-evacuati-i-residenti.

[15] David J. Yu et al., "Logical Interdependencies in Infrastructure: What Are They, How to Identify Them, and What Do They Mean for Infrastructure Risk Analysis?", in *Risk Analysis*, 1 agosto 2024, https://doi.org/10.1111/risa.16555.

ISSN 2280-6164

Guardando al contesto dell'UE, attualmente le minacce alle IC sono rimaste sotto la soglia del conflitto armato, in quella "zona grigia" che rende più semplice l'offesa e più difficile l'attribuzione – zona cui si ricorre per convenienza a minacce e tattiche di tipo ibrido[16]. Si tratta di una differenza fondamentale rispetto a scenari di guerra come quello ucraino, in cui le IC (energetiche, di telecomunicazioni, trasporti, etc.) sono sistematicamente obiettivo di attacchi militari russi, parte integrante di una più ampia strategia volta a piegare la resistenza della popolazione ucraina.

La compresenza di più tipi di minacce in parallelo (intenzionali e non, da parte di attori statali e non statali, cinetiche e non cinetiche), capaci di colpire IC di natura e caratteristiche diverse distribuite in domini e dimensioni differenti, pongono una sfida rilevante in termini di gestione, controllo e capacità di *decision-making*. Tale sfida riguarda in primis gli Stati membri UE inclusa l'Italia, ma anche agli operatori privati e proprietari delle IC che vengono maggiormente responsabilizzati. Si pensi a quanto diverse possono essere la protezione e la risposta di fronte a un evento che danneggia la rete di distribuzione idrica di un'intera regione italiana, rispetto a quella di un satellite in orbita che viene colpito da un detrito spaziale o manomesso da un braccio robotico di un satellite nemico, oppure alla tranciatura o perforazione di un gasdotto che garantisce gli approvvigionamenti energetici del paese.

A questo si aggiunge in maniera diffusa la dislocazione, anche decentrata, delle varie infrastrutture critiche sul territorio nazionale (e in alcuni casi oltre), attraverso domini operativi e dimensioni come quella subacquea. Si pensi ai processi necessari per proteggere i giacimenti di risorse energetiche al di fuori dalle acque territoriali italiane, ai satelliti in orbita, o ai cavi sottomarini attraverso i quali viaggiano dati.

Un ulteriore aspetto di cui non si tiene sufficientemente conto riguarda la distribuzione dei settori di IC da proteggere e di cui garantire la resilienza attraverso tutti i cinque domini operativi, oltre che nella dimensione subacquea. L'allargamento dei settori di IC menzionati dalla direttiva Cer dai due tradizionali a 11, rende la protezione, sia fisica che cyber, ancor più complessa. Questa caratteristica interessa meno i soggetti critici e/o gli operatori della IC che sono focalizzati sul loro settore specifico, ma è molto importante per gli Stati membri e per i loro apparati nazionali di sicurezza e difesa, dalle Forze armate all'intelligence.

Facendo una mappatura dei settori di IC[17], si può osservare come sia il settore bancario e quello delle infrastrutture dei mercati finanziari, così come quello della pubblica amministrazione, coinvolgono i domini terrestre e cyber, oltre la dimensione subacquea. Il settore della salute coinvolge i domini terrestre, cyber e

[16] Henrik Praks, "Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage", in *Hybrid CoE Working Papers*, n. 32 (maggio 2024), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage.

[17] Si veda la Tabella 1.

ISSN 2280-6164

quello aereo. I settori dell'acqua potabile e delle acque reflue interessano i domini marittimo e terrestre, mentre il secondo anche la dimensione subacquea. Le infrastrutture digitali sono connesse trasversalmente a tutti i domini a eccezione di quello marittimo, oltre che alla dimensione subacquea. Il settore dei trasporti e quello della produzione, distribuzione e trasformazione degli alimenti condividono la presenza nei domini terrestre, aereo e marittimo, mentre il primo dei due settori riguarda anche il dominio cyber. Il segmento di terra delle infrastrutture spaziali che rientra negli 11 settori, oltre al dominio spaziale coinvolge anche quello cyber e naturalmente quello terrestre. Il settore dell'energia invece riguarda i domini terrestre e marittimo e la dimensione subacquea.

Tabella 1 | La distribuzione dei settori menzionati dalla Cer e la loro relazione con i cinque domini operativi (aereo, terrestre, marittimo, spaziale e cyber) e nella dimensione subacquea

	Spaziale	Aereo	Terrestre	Marittimo	Subacqueo	Cyber
Settore bancario			X		X	X
Infrastrutture dei mercati finanziari			X		X	X
Salute		X[(a)]	X			X
Acqua potabile			X	X[(b)]		
Acque reflue			X	X	X[(c)]	
Infrastrutture digitali	X	X	X		X[(d)]	X
Enti della pubblica amministrazione			X		X	X
Produzione, trasformazione e distribuzione di alimenti		X	X	X		
Spazio	X		X			X
Energia			X	X	X	
Trasporti		X	X	X		X

Note: Va precisato che l'ambito di applicazione della Cer riguarda solo il segmento di terra (le infrastrutture di terra) e non il segmento spazio (che riguarda i satelliti in orbita) dei sistemi spaziali. Tuttavia, al fine di mostrare integralmente i collegamenti tra i settori di infrastrutture in tutti i domini operativi, la tabella fa riferimento al dominio spaziale considerando quindi anche il segmento spaziale.
(a) Per il trasporto rapido di pazienti, organi per trapianti e forniture mediche urgenti vengono utilizzati elicotteri e aerei.
(b) In alcune regioni o isole l'acqua potabile viene trasportata via mare, o l'acqua del mare viene depurata per essere bevuta.
(c) Esistono tubature subacquee per trasporto o smaltimento.
(d) Esistono cavi sottomarini e cavi transoceanici.

Il caso CrowdStrike, accaduto a luglio 2024, ha colpito vari settori di infrastrutture in tre domini diversi e mostra bene gli effetti a cascata dovuti alle dipendenze e

ISSN 2280-6164

interdipendenze[18]. Il malfunzionamento che ha interessato il software CrowdStrike al momento dell'aggiornamento di sicurezza ha generato interruzioni e disagi nei settori del trasporto aereo, della salute (sistemi informatici degli ospedali e servizi di emergenza), bancario e finanziario e dell'alimentazione (cinque degli undici settori affrontati dalla Cer), in maniera trasversale attraverso i domini terrestre, aereo e cyber.

Un fattore collegato alla natura decentralizzata e alla presenza in tutti i domini dei settori coinvolti riguarda la complessità delle catene di approvvigionamento (*supply chain*) che garantiscono il funzionamento delle infrastrutture e dei servizi e che sono difficili da mappare e controllare, essendo spesso di natura globale/internazionale. A livello europeo si è iniziato a parlare quindi di regionalizzazione delle *supply chain* nelle aree considerate critiche al fine di renderle meno vulnerabili rispetto alle interruzioni e per garantire la sicurezza degli approvvigionamenti.

1.2 Le implicazioni della pandemia Covid-19

La pandemia da Covid-19, che ha portato i sistemi sanitari pubblici quasi al collasso, la conseguente necessità crescente di mascherine e dei respiratori/dispositivi di ventilazione, la successiva corsa della comunità scientifica alla produzione di un vaccino, oltre che l'attuazione di misure emergenziali eccezionali e senza precedenti su scala nazionale come le zone rosse, hanno reso evidente in maniera più diffusa quanto il settore sanitario sia vulnerabile e cruciale e, quando messo sotto pressione, quanto possa limitare il funzionamento della società. Il caso italiano nella crisi da Covid-19 permette di notare almeno due ulteriori fattori che possono essere validi per altri settori fornitori di servizi essenziali oltre quello della salute.

Il primo riguarda una maggiore attenzione alle *supply chain* e alle scorte di determinati beni. L'Italia, in quanto primo Paese europeo colpito dall'ondata proveniente dalla Cina a fine 2019, nella prima fase della pandemia ha ricevuto assistenza e materiali sanitari da paesi europei, ma anche extra-UE come Cina e Russia, a riprova della vulnerabilità complessiva del sistema-Paese in quel momento storico[19]. Si parlò in quel contesto di "*mask diplomacy*", per indicare come le mascherine fossero diventate uno strumento di azione politica internazionale da parte dei fornitori[20]. Nel caso della Russia sembrò che l'aereo militare atterrato a Pratica di Mare per la consegna di respiratori e mascherine avesse altri obiettivi, come ad esempio la raccolta di informazioni e intelligence. Il personale russo

[18] Lily Hay Newman, Matt Burgess e Andy Greenberg, "Come il bug di Crowdstrike ha mandato in tilt i computer di mezzo mondo", in *Wired*, 22 luglio 2024, https://www.wired.it/article/crowdstrike-microsoft-guasto-come-e-successo.

[19] Si veda Francesca Ghiretti, "China, Italy and COVID-19: Benevolent Support or Strategic Surge?", in *IAI Commentaries*, n. 20|14 (marzo 2020)2022, https://www.iai.it/it/node/11436.

[20] Brian Wong, "China's Mask Diplomacy", in *The Diplomat*, 25 marzo 2020, https://thediplomat.com/2020/03/chinas-mask-diplomacy; e Sarantis Michalopoulos, "How Effective Is China's 'Mask Diplomacy' in Europe?", in *Euractiv*, 26 marzo 2020, https://www.euractiv.com/?p=1447230.

ISSN 2280-6164

arrivato in Italia in quell'occasione era non solo civile e medico, ma in parte significativa militare, a fronte di un volume di materiali sanitari consegnati considerato limitato. Il personale avrebbe inoltre chiesto di sanificare degli uffici pubblici oltre agli ospedali[21]. L'episodio mostra come determinate vulnerabilità infrastrutturali e di *supply chain* possano potenzialmente mettere a rischio la sicurezza nazionale. Con la crisi pandemica si inizia infatti a porre attenzione non solo alle infrastrutture – seguendo l'esempio del Covid, gli ospedali – ma anche alla catena logistica e di approvvigionamenti operante intorno alle infrastrutture e garante del loro funzionamento.

Un secondo fattore riguarda invece la potenziale compresenza di minacce di tipo diverso, da affrontare contemporaneamente, parte di certe strategie ibride che mirano a mettere sotto pressione le istituzioni pubbliche e la popolazione agendo su più fronti in parallelo. Torna utile nuovamente l'esempio della pandemia, per cui nella seconda fase dedicata alle vaccinazioni, superato il periodo prettamente emergenziale, un attacco *cyber* mise fuori uso il sistema informatico responsabile per le prenotazioni delle vaccinazioni dell'intera Regione Lazio, generando così una concatenazione di vulnerabilità nel settore sanitario.

1.3 Le implicazioni della guerra in Ucraina

I fattori sopra descritti sono visibili in un'altra crisi che ha scosso l'Europa, ovvero l'invasione russa dell'Ucraina, con l'importante distinzione che, nel caso della pandemia, si stava affrontando globalmente una minaccia di tipo non convenzionale Cbrn (minacce chimiche, biologiche, radiologiche e nucleari) – in particolare biologica – non intenzionale e non statuale. Nel caso della guerra russo-ucraina, questi fattori sono presenti in un contesto di attacco intenzionale, con componenti sia convenzionali che non[22], da parte di un attore statale – la Federazione Russa – contro un altro Stato. La sistematicità degli attacchi russi alle infrastrutture critiche civili ucraine[23] ne fanno una vera e propria strategia di guerra, volta a piegare la resistenza della popolazione. Prendere di mira la popolazione civile e le infrastrutture che essa utilizza è una strategia che la Russia aveva adottato già in Siria, dal 2015.

La persistenza con la quale Mosca ha colpito infrastrutture critiche civili in Ucraina ha alzato il livello di consapevolezza su questo punto a livello euro-atlantico. Di conseguenza, nelle capitali europee e in seno all'Alleanza atlantica si discute di come prioritizzare le infrastrutture da proteggere in caso di attacco russo. Inoltre, la Nato e l'UE hanno riconosciuto, attraverso la Dichiarazione congiunta del

[21] "Perché si parla della missione russa a Bergamo del marzo del 2020" in *Il Post*, 23 marzo 2022, https://www.ilpost.it/2022/03/23/missione-russa-bergamo-2020.

[22] Alessandro Marrone (a cura di), *Russia-Ukraine War's Strategic Implications*, Roma, IAI, 2024, https://www.iai.it/it/node/18118.

[23] Simon Aebi, Andrin Hauri e Jurgena Kamberaj, "Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication", in *CSS Risk and Resilience Reports*, marzo 2024, https://doi.org/10.3929/ethz-b-000662463.

ISSN 2280-6164

2023, che la resilienza delle infrastrutture critiche è un'area in cui approfondire la cooperazione[24], creando un'apposita Task Force dedicata alla resilienza delle IC. La Task Force ha pubblicato il suo primo *Final Assessment Report* a giugno 2023[25]. Il rapporto indica sfide e raccomandazioni e considera in particolare i settori energetico, spaziale, dei trasporti e digitale come trasversali e fondamentali, in quanto fornitori di servizi che sono necessari per il funzionamento di altri settori di IC. Nel rapporto si sottolinea come i collegamenti tra settori di IC e il grado di interdipendenza tra questi andrebbe compreso meglio e si raccomanda una sistematica e coordinata valutazione delle minacce alle IC da parte di entrambe le organizzazioni. La Task Force consiglia inoltre l'inclusione della resilienza delle IC nelle esercitazioni future e lo svolgimento di "scenario-based" tra gli staff della NATO e dell'UE per comprendere meglio gli effetti a cascata e le interdipendenze, oltre che promuovere lo scambio di *best practices* tra gli attori civili e militari.

1.4 Gli investimenti diretti esteri

La rilevanza e il ruolo strategico delle IC nel contesto internazionale, anche come oggetto di forme sempre più svariate di ingerenza, sono emersi negli scorsi anni in riferimento agli investimenti diretti esteri (Ide) in infrastrutture critiche come strumento di espansione da parte di alcuni Stati della propria influenza nei paesi europei. Seppure gli Ide rappresentino principalmente un mezzo di crescita economica e di sviluppo tecnologico, la questione diventa più complessa quando questi sono destinati all'acquisto o al controllo di IC. Uno dei paesi che più si è distinto nel contesto europeo per l'uso di Ide come strumento sistematico di politica estera, industriale e commerciale è la Cina[26]. Quest'ultima ha intrapreso azioni volte ad espandere la sua presenza in alcuni punti chiave o colli di bottiglia, in primis i porti, funzionali anche al progetto complessivo della Belt and Road Initiative – nota in Italia anche come Nuova via della seta[27]. Questo piano ha interessato in particolare alcuni importanti porti europei: in alcuni di questi, soggetti sotto controllo diretto o indiretto di Pechino detengono attualmente la maggioranza relativa o assoluta delle azioni della società proprietaria dell'infrastruttura critica, come nei casi del porto del Pireo in Grecia o nel porto belga di Antwerpen-Zeebrugge. In Italia, Cosco, una società per azioni controllata dallo Stato cinese che opera nel settore della logistica marittima, controlla il 40 per cento del porto di Vado Ligure. Alcuni dei porti in cui Pechino ha fortemente investito sono importanti *hub* logistici[28]

[24] UE e Nato, *Dichiarazione congiunta sulla cooperazione UE-NATO*, 10 gennaio 2023, https://www.consilium.europa.eu/it/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023.

[25] EU-NATO Task Force on the Resilience of Critical Infrastructure, *Final Assessment Report*, 29 giugno 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564.

[26] Paola Tessari e Karolina Muti, "Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations", in *European Parliament Studies*, luglio 2021, https://doi.org/10.2861/179721.

[27] Hu Luo, "La Belt and Road Initiative e lo sviluppo di China COSCO Shipping nel Mediterraneo", in *OrizzonteCina*, vol. 9, n. 1 (gennaio-marzo 2018), p. 14-17, https://www.twai.it/?p=3426.

[28] Parlamento europeo e Consiglio dell'UE, *Regolamento (UE) 2019/452 del 19 marzo 2019 che*

ISSN 2280-6164

con una valenza persino militare, poiché vengono utilizzati per far arrivare le forze armate americane in Europa. È questo il caso dei porti di Gdynia in Polonia, Rotterdam nei Paesi Bassi e Antwerpen-Zeebrugge.

I risultati ottenuti da parte cinese non sono stati univoci. Se da un lato, con la sua presenza, la Cina ha aumentato gradualmente la sua capillarità nei porti europei, dall'altro varie acquisizioni non sono andate a buon fine e/o sono state bloccate dal Paese dove si colloca l'infrastruttura[29]. L'UE, dal canto suo, ha introdotto dal 2019 il Regolamento (UE) 2019/452 che istituisce un quadro per il controllo degli investimenti diretti esteri nell'Unione europea[30], un meccanismo che prevede la possibilità di fare uno screening degli investimenti esteri nelle infrastrutture, tecnologie e attività economiche europee. La maggior parte delle segnalazioni raccolte tramite questo meccanismo ha riguardato attività manifatturiere nei settori dell'energia, dell'aerospazio e difesa, della salute, cybersicurezza, delle comunicazioni e dei trasporti. Alla luce del rapido peggioramento del contesto di sicurezza e delle ingerenze multilivello anche nella sicurezza economica dei paesi membri UE, è in corso una revisione del meccanismo per renderlo più efficace[31]. Il Parlamento europeo ha inoltre chiesto alla Commissione di elaborare entro la fine del 2024 una Strategia portuale europea globale (*Comprehensive European Port Strategy*), richiamando l'attenzione sugli aspetti di sicurezza e dipendenza economica da paesi terzi dei porti europei[32].

2. La dimensione europea: la direttiva 2022/2557 relativa alla resilienza dei soggetti critici

Gli elementi illustrati nella sezione precedente rendono evidente come determinate IC forniscano servizi essenziali per il funzionamento delle società, servizi che sono tradizionalmente di competenza nazionale. Ugualmente, la gestione degli incidenti che li coinvolgono e le azioni volte a garantirne il ripristino sono responsabilità che non rientrano storicamente nella regolamentazione dell'UE ma sono competenze nazionali. Tuttavia, come illustrato nella prima parte dello studio, la frequenza sempre maggiore di eventi emergenziali spesso caratterizzati da impatti transfrontalieri, e la natura stessa delle IC con dimensione non solo nazionale ma europea, ha evidenziato la necessità di una forte cooperazione fra gli Stati membri al fine di garantire una gestione condivisa e coordinata a livello europeo.

istituisce un quadro per il controllo degli investimenti diretti esteri nell'Unione, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32019R0452.

[29] Intervista, aprile 2021.

[30] EUR-Lex, "Quadro per il controllo degli investimenti esteri diretti", in *Summaries of EU Legislation*, aggiornato al 7 gennaio 2022, https://eur-lex.europa.eu/it/legal-content/summary/screening-framework-for-foreign-direct-investments.html.

[31] Commissione europea, *EU Foreign Direct Investment Screening – 2024 Revision*, Publications Office of the European Union, aggiornato al 24 gennaio 2024, https://doi.org/10.2781/130838.

[32] Parlamento europeo, *Risoluzione del 17 gennaio 2024 "Costruire una strategia portuale europea globale"* (2023/2059(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0025_IT.html.

ISSN 2280-6164

Secondo uno studio pubblicato nel 2021 dal centro di ricerca Netherlands Organization for Applied Research, dal 2004 al 2018 si sono verificati in Europa oltre 3.000 eventi che hanno coinvolto infrastrutture critiche e hanno causato un'interruzione nell'erogazione di servizi essenziali[33]. I settori maggiormente colpiti nel periodo analizzato sono quello dell'energia (42,8 per cento degli incidenti oggetto dello studio), seguito dai trasporti (22,3 per cento) e dalle telecomunicazioni (14,6 per cento). Con riferimento alla natura degli incidenti, la stragrande maggioranza degli eventi è stata di tipo accidentale (circa il 65 per cento) e, in parte molto minore, intenzionale (circa l'8 per cento)[34]. Analizzando più dettagliatamente i dati relativi agli episodi di origine accidentale, si evidenzia come nel 25 per cento dei casi l'interruzione dell'erogazione dei servizi sia stata causata dall'effetto "a cascata", ovvero dall'impatto derivato da eventi originati in altre infrastrutture.

Negli anni 2000 si sono inoltre verificati gli attacchi terroristici alla metropolitana di Madrid nel 2004 e ai trasporti pubblici di Londra nel 2005. Di fronte alla presenza concreta della minaccia terroristica sul territorio dell'UE, rivolta a spazi pubblici di altissima frequentazione e parte di servizi essenziali, si è avuto un forte impulso verso l'avvio di iniziative sovranazionali con l'intento di mettere in atto un programma completo e coordinato per la protezione delle infrastrutture critiche a livello europeo. Proprio a seguito dei suddetti eventi di Madrid, la Commissione europea ha adottato diverse iniziative politiche, la prima delle quali è stata la comunicazione del 2004 sulla protezione delle infrastrutture critiche nella lotta contro il terrorismo[35]. A questa si sono succedute altre azioni finalizzate a un maggiore coordinamento e supervisione UE a protezione delle IC presenti sul suo territorio, con una particolare attenzione alla dimensione europea in cui esse operano e alla possibilità, in caso di malfunzionamenti, di impatti su più Stati membri. Fra le suddette iniziative, va ricordata la sopracitata direttiva 2008/114/CE relativa alla definizione delle caratteristiche per l'individuazione di infrastrutture critiche europee e per la loro protezione[36].

La direttiva del 2008 era caratterizzata da un ambito di applicazione limitato ai settori dell'energia e dei trasporti, insieme ai loro sottosettori: elemento che è stato poi alla base di un processo di revisione della normativa stessa e che ha portato all'adozione della direttiva Cer, oggetto di questo studio. Quest'ultima ha introdotto

[33] Eric Luiijf e Marieke Klaver, "Analysis and Lessons Identified on Critical Infrastructures and Dependencies from an Empirical Data Set", in *International Journal of Critical Infrastructure Protection*, vol. 35 (dicembre 2021), articolo 100471, p. 5, DOI 10.1016/j.ijcip.2021.100471.

[34] Per altri eventi la causa non è nota.

[35] Commissione europea, *La protezione delle infrastrutture critiche nella lotta contro il terrorismo* (COM/2004/702), 20 ottobre 2004, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52004DC0702.

[36] La direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee sarà abrogata e sostituita dalla più recente direttiva 2022/2557 relativa alla resilienza dei soggetti critici, oggetto di questo studio.

ISSN 2280-6164

novità significative che mirano a rafforzare il ruolo di coordinamento dell'Unione nella protezione delle infrastrutture critiche, cercando in particolare di superare l'approccio strettamente settoriale e di fornire maggiore supporto agli Stati membri per evitare la frammentazione che ha caratterizzato l'attuazione da parte degli Stati membri della precedente direttiva a livello nazionale. L'ampliamento dell'ambito di applicazione riguarda un totale di nove settori inclusi nella Cer. A quelli dell'energia (1) e dei trasporti (2), si aggiungono quindi il settore bancario (3), quello delle infrastrutture dei mercati finanziari (4), della salute (5), dell'acqua potabile (6), delle acque reflue (7), delle infrastrutture digitali (8), della pubblica amministrazione (9), dello spazio (10) e della produzione, trasformazione e distribuzione degli alimenti (11), per un totale di 11 settori[37]. Questi ultimi verranno brevemente analizzati di seguito sulla base di un raggruppamento tematico.

2.1 Energia

Come ricordato, il settore energetico e quello dei trasporti sono le due categorie nell'ambito di applicazione della precedente direttiva del 2008. Gli Stati membri e gli operatori in questo settore possono vantare quindi maggiore esperienza nell'adeguarsi alle nuove norme[38]. La nuova direttiva include i sottosettori dell'energia elettrica, del petrolio, del gas, dell'idrogeno, del teleriscaldamento e teleraffreddamento[39] – gli ultimi tre aggiuntivi rispetto alla precedente direttiva. L'ambito di applicazione riguarda dunque una vasta rete di produttori, di gestori dei sistemi di distribuzione e/o di trasmissione, del mercato elettrico, di oleodotti, di impianti di produzione, raffinazione e/o trattamento, nonché di fornitori di servizi di stoccaggio. Concretamente, può comprendere quindi sia infrastrutture energetiche *onshore* che *offshore* distribuite nei domini terrestre e marittimo e nella dimensione subacquea.

L'attenzione verso i rischi a cui sono esposte queste infrastrutture è significativamente aumentata a seguito dell'episodio di sabotaggio che ha determinato l'esplosione del gasdotto Nord Stream 2 nel Mar Baltico a settembre 2022 e dell'incidente dall'incerta intenzionalità che a ottobre 2023 ha coinvolto il gasdotto Baltic Connector nel Mare del Nord[40]. In quest'ultimo caso, secondo il rapporto delle autorità finlandesi, il gasdotto sarebbe stato tranciato da una nave cinese. Si tratta di episodi che dimostrano come le infrastrutture critiche energetiche siano oggi esposte a minacce ibride, come azioni di sabotaggio intenzionale, oltre che ad azioni non intenzionali, sia provocate dall'uomo che da eventi naturali. È il caso dei cambiamenti climatici che rappresentano una sfida per diversi tipi di

[37] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit.

[38] Intervista, 8 luglio 2024.

[39] Il teleriscaldamento è una forma di riscaldamento che prevede la distribuzione di acqua calda tramite tubazioni coibentate. Attraverso un principio simile, il teleraffreddamento distribuisce acqua attraverso una rete di tubazioni a circuito chiuso.

[40] Andrius Sytas e Anne Kauranen, "Three Baltic Pipe and Cable Incidents 'Are Related', Estonia Says", in *Reuters*, 27 ottobre 2023, https://www.reuters.com/world/europe/three-baltic-pipe-cable-incidents-are-related-estonia-says-2023-10-27.

ISSN 2280-6164

infrastrutture energetiche in termini, ad esempio, di resistenza dei materiali per via dell'aumento delle temperature. Fenomeni di "*space weather*" come le tempeste solari possono invece causare interruzioni di servizi sulla rete elettrica[41].

2.2 Trasporti

Il settore dei trasporti è l'altra categoria già considerata dalla precedente normativa e comprende il trasporto aereo, ferroviario, per vie d'acqua, su strada e quello pubblico. Come in altri casi, questo include una vasta rete di imprese, vettori, gestori (ad esempio organi di gestione dei porti), operatori (ad esempio del controllo e della gestione del traffico aereo). Come accennato in precedenza, gli attacchi terroristici del 2004-2005 a Madrid e Londra hanno costituito uno stimolo per l'UE nello sviluppare un approccio più sistemico di lotta al terrorismo in Europa, con l'istituzione della figura del coordinatore antiterrorismo e di una strategia antiterrorismo dell'UE[42]. Tale approccio si è concretizzato anche attraverso il finanziamento di progetti volti a garantire maggiore protezione delle IC quali le metropolitane e le reti ferroviarie, oltre che degli spazi pubblici, nell'ambito di programmi come quelli del Fondo per la sicurezza interna (*Internal Security Fund*) della Direzione generale Affari interni[43], di Horizon2020 e di Horizon Europe, attraverso lo sviluppo di metodologie e tecnologie innovative e di una spinta ad un maggiore scambio di informazioni tra i gli addetti ai lavori di vari Stati membri, il mondo della ricerca, delle imprese, delle istituzioni e degli operatori[44].

Diversamente da altre categorie di IC, gestite e frequentate fisicamente per lo più dagli operatori e addetti ai lavori, le infrastrutture del settore trasporti sono caratterizzate da spazi pubblici che devono rimanere aperti, facilmente accessibili e disponibili al pubblico. Questo li rende degli obiettivi particolarmente vulnerabili per attacchi di vario tipo (compresi quelli *cyber*) e rappresenta una sfida complessa per la loro resilienza e la sicurezza degli utenti. Nel caso delle infrastrutture più frequentate, si presentano inoltre altri fenomeni potenzialmente rischiosi e che sono legati al comportamento della folla, come nei momenti di spostamento disordinato di un numero elevato di persone, soprattutto in situazioni di panico a seguito di un attacco o di un incidente, con il rischio di schiacciamento e asfissia.

Inoltre, come riportato nel precedente capitolo, la categoria dei trasporti è stata oggetto di Ide operati da imprese e società direttamente o indirettamente riconducibili ad attori statali che ad oggi rappresentano una sfida per la sicurezza dell'UE, quali la Cina. Nel contesto italiano, i casi più noti riguardano il porto di

[41] Sito dello Space Weather Prediction Center: *Electric Power Transmission*, https://www.swpc.noaa.gov/impacts/electric-power-transmission.

[42] Sito del Consiglio dell'UE: *La risposta dell'UE al terrorismo*, aggiornato al 21 marzo 2024, https://www.consilium.europa.eu/it/policies/fight-against-terrorism.

[43] Commissione europea-Direzione generale degli Affari interni, *Internal Security Fund (2021-2027)*, 27 agosto 2024, https://home-affairs.ec.europa.eu/node/6905_en.

[44] Si veda ad esempio il progetto EUProtect: https://www.euprotect-project.eu.

ISSN 2280-6164

Taranto e quello di Trieste, mentre a livello europeo si riporta il caso del Porto del Pireo, in posizione strategica, controllato ad oggi con oltre il 51 per cento delle quote dalla società cinese Cosco e nel quale Pechino controlla anche l'Autorità portuale[45].

2.3 Settore bancario e infrastrutture dei mercati finanziari

Il settore bancario e le infrastrutture dei mercati finanziari sono due categorie fortemente interconnesse, il cui funzionamento dipende largamente dalle infrastrutture digitali. La direttiva non fornisce una definizione delle due categorie in oggetto, pur facendo riferimento a enti creditizi e gestori di sedi di negoziazione per il settore dei mercati finanziari. Le istituzioni e la serie di relazioni e interconnessioni che caratterizzano questi due settori sono un fondamento su cui si basa il funzionamento dell'economia globale e della società contemporanea, nonché la credibilità dello stesso sistema finanziario internazionale[46]. Il settore bancario è infatti solitamente l'elemento più importante all'interno di un sistema finanziario, considerando che, attraverso l'erogazione del credito ai soggetti privati, funge da motore dell'economia di cui usufruisce la popolazione ed è quindi fattore di sviluppo della società[47].

Le tecnologie digitali sono intrinsecamente connesse ai sistemi bancario e finanziario e stanno cambiando i processi e il modello di *business* di questi ultimi, si pensi ad esempio all'online e al *digital banking*. Si tratta infine di due categorie che fungono da connettore tra diversi settori della società e dell'economia[48] e questo aumenta il loro livello di interdipendenza con altri settori essenziali[49].

2.4 Salute

Nella categoria Salute la Cer si riferisce ai prestatori di assistenza sanitaria, ai laboratori e ai soggetti che svolgono attività di ricerca e sviluppo relative a determinati medicinali.

La pandemia da Covid-19, come precedentemente illustrato, ha dimostrato come un evento di tipo biologico, ovvero "B" nella categoria delle minacce non convenzionali

[45] Claudio Paudice, "La privatizzazione del Pireo è stata un affare, ma solo per i cinesi, non per i greci", in *HuffPost Italia*, 5 settembre 2021, https://www.huffingtonpost.it/economia/2021/09/05/news/la_privatizzazione_del_pireo_e_stata_un_affare_ma_solo_per_i_cinesi_non_per_i_greci-5267417.

[46] Aleksi Aho, Catarina Midões e Arnis Šnore, "Hybrid Threats in the Financial System", in *Hybrid CoE Working Papers*, n. 8 (giugno 2020), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-8-hybrid-threats-in-the-financial-system.

[47] Laurențiu Mihail Grigore, "The Banking Financial System as a Critical Infrastructure of the Current and Future Society", in *Land Forces Academy Review*, vol. 26, n. 4 (dicembre 2021), p. 418-422, https://doi.org/10.2478/raft-2021-0054.

[48] Aleksi Aho, Catarina Midões e Arnis Šnore, "Hybrid Threats in the Financial System", cit.

[49] In questo contesto, vale la pena menzionare il Regolamento 2022/2554/UE, che obbliga operatori finanziari, banche, assicurazioni e fornitori di servizi ICT ad attuare misure per la resilenza digitale.

DOCUMENTI IAI 24 | 11 - OTTOBRE 2024
ISSN 2280-6164

Cbrn, può mettere sotto pressione la popolazione e il sistema sanitario nazionale in maniera tale da impedirne e/o limitarne il funzionamento. La sanità è un settore che assorbe mediamente una parte ingente di risorse pubbliche nell'UE, con un peso significativo sull'economia degli Stati anche in situazioni non emergenziali e questo vale in particolar modo per l'Italia.

La pandemia ha inoltre accresciuto la sensibilità e la consapevolezza non solo della popolazione, ma anche dello stesso personale operante negli ospedali, che ha messo in atto protocolli e procedure non ordinarie di decontaminazione. La formazione del personale per una corretta conoscenza e applicazione di tali misure dovrebbe essere parte di un approccio sistemico che miri ad una preparazione più solida, diffusa e continuativa, di fronte al possibile verificarsi in futuro di emergenze simili. Inoltre, altri eventi che causano un numero estremamente elevato di feriti e vittime, come un attacco terroristico o un disastro naturale, possono saturare le capacità di servizi sanitari. Un'infrastruttura sanitaria rischia quindi di trovarsi in difficoltà di fronte alla possibile saturazione delle sue capacità di risposta, in termini di spazi, personale ed equipaggiamenti, come si è visto durante il Covid.

In aggiunta a questa circostanza, una seconda categoria di minaccia al sistema sanitario riguarda gli attacchi *cyber*. Le strutture sanitarie hanno ampliato l'uso di sistemi digitali e l'innovazione negli ultimi anni, utilizzando oggi in maniera diffusa un vasto numero di tecnologie e l'*Internet of Medical Things* (IoMT) che, tuttavia, le espongono a vulnerabilità di tipo cibernetico importanti in un momento in cui gli attacchi *cyber* a IC sono in grande aumento[50]. Questi ultimi possono riguardare, oltre che il regolare funzionamento della struttura, la confidenzialità e l'integrità dei dati medici o il controllo di dispositivi medici capaci anche di causare la morte di un paziente, come i peacemaker[51]. Ne è un esempio l'attacco informatico tramite *ransomware*[52] a danno del sistema sanitario nella Regione Lazio a luglio 2021 che, oltre a risultare in una notevole fuga di dati, ha provocato blocchi d'accesso a servizi sanitari come la gestione delle prenotazioni e dei pagamenti, il ritiro dei referti e la registrazione delle vaccinazioni[53]. Tre anni dopo, il caso CrowdStrike ha causato disagi in strutture ospedaliere, ad esempio negli Stati Uniti e nel Regno Unito. Nonostante il problema informatico fosse stato identificato rapidamente, le operazioni di ripristino in alcuni ospedali hanno richiesto interventi manuali su ogni computer allungando considerevolmente i tempi per il ritorno a un funzionamento normale[54].

[50] Roberto Setola e Giacomo Assenza, "Infrastrutture critiche: la vulnerabilità del settore sanitario", in *ISPI Commentaries*, 8 ottobre 2019, https://www.ispionline.it/it?p=40091.

[51] Ibid.

[52] Con il termine ransomware si intende un programma informatico dannoso che può infettare un dispositivo digitale, bloccando l'accesso ai suoi contenuti con minaccia volta a ottenere un riscatto.

[53] Dario Fadda, "Attacco Regione Lazio, il garante privacy conferma i gravi errori", in *Cybersecurity360*, 10 aprile 2024, https://www.cybersecurity360.it/?p=75303.

[54] TaRhonda Thomas, "Penn Medicine Official Details How Hospital Stayed Afloat during Tech Outage", in *6abc Philadelphia*, 26 luglio 2024, https://6abc.com/post/15095746.

ISSN 2280-6164

2.5 Acque reflue e acqua potabile

Nel caso del settore delle acque reflue la Cer si riferisce a quelle "imprese che raccolgono, smaltiscono o trattano acque reflue urbane, acque reflue domestiche o acque reflue industriali"[55]. Si tratta infatti di acque che, dopo l'utilizzo, diventano inquinanti e non possono essere riutilizzate né reimmesse nell'ambiente, rappresentando un pericolo per la salute pubblica e l'ambiente circostante e richiedendo interventi di depurazione[56]. I trattamenti di depurazione riducono il carico inquinante e permettono il riutilizzo delle acque reflue per alcune finalità specifiche come l'irrigazione di colture, il lavaggio delle strade nei centri urbani o l'alimentazione dei sistemi di riscaldamento o raffreddamento, oltre che in processi di tipo industriale[57].

I fenomeni sempre più frequenti di scarsità idrica e siccità che negli ultimi anni sono in aumento nell'Italia meridionale e, in maniera più estesa, anche nell'Europa meridionale, rendono le acque reflue una risorsa molto preziosa. Questo è particolarmente importante nel contesto italiano dove, per via dell'impatto del cambiamento climatico, la siccità e desertificazione secondo le previsioni colpiranno in maniera sistematica alcune parti del territorio nazionale. Allo stesso tempo, lo sversamento improprio delle acque reflue non depurate porta con sé il rischio di disastro ambientale e potrebbe essere sfruttato anche da attori malevoli.

I potenziali rischi e le problematiche legati all'acqua potabile, inserita nella Cer, sono anch'essi collegate, tra gli altri elementi, alla siccità e scarsità idrica derivante dai cambiamenti climatici. La mancanza di acqua potabile, il suo inquinamento intenzionale o non, e/o una sua ridotta qualità espongono a rischi di contrarre malattie come colera, dissenteria o febbre tifoide, aumentando quindi la minaccia biologica e, a catena, la potenziale pressione sulle strutture sanitarie[58].

Sono dunque particolarmente importanti le reti di distribuzione idrica che, nel contesto nazionale, presentano tuttavia dei livelli altissimi di perdite, dovute anche a impianti datati. Si calcola che la perdita media per dispersione dell'acqua per uso civile sia del 40 per cento, con picchi di oltre il 50 per cento al Sud[59]. A livello nazionale, il Piano nazionale di ripresa e resilienza (Pnrr) ha predisposto 4,3 miliardi di euro per il settore idrico, tanto per la creazione di nuovi impianti, quanto

[55] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., p. 196.

[56] Vincenzo Moschetto, "Acque reflue: normative, trattamento e riutilizzo per una gestione sostenibile", in *Blog Polistudio*, 22 marzo 2024, https://blog.polistudio.it/acque-reflue-gestione-sostenibile.

[57] Ibid.

[58] WaterWide, *Why Government Must Investment in Water, Sanitation, and Hygiene (WASH)*, 13 settembre 2023, https://www.waterwide.org/?p=8209.

[59] ItaliaDomani, *Dal PNRR 4,3 miliardi di euro per il settore idrico*, 11 luglio 2022, https://www.italiadomani.gov.it/content/sogei-ng/it/it/news/dal-pnrr-4-3-miliardi-di-euro-per-il-settore-idrico.html.

ISSN 2280-6164

per la manutenzione e l'innovazione di quelli esistenti[60]. A titolo comparativo, i fondi Pnrr stanziati per il settore spaziale sono stati in totale 2,3 miliardi. I rischi in questo settore, sia di natura intenzionale che non, hanno potenzialmente un impatto molto ampio per la popolazione e che si potrebbe ricollegare a catena ad altre infrastrutture, come quelle del settore Salute individuato dalla Cer.

2.6 Infrastrutture digitali

Per quanto riguarda le infrastrutture digitali, la Cer include in questa categoria i fornitori di punti di interscambio Internet, di servizi di *Domain Name System* (Dns), servizi di *cloud computing* e di *data center*, oltre che i registri dei nomi di dominio di primo livello. La categoria comprende anche fornitori di servizi di comunicazione elettronica, di reti pubbliche legate a essa e di reti di distribuzione dei contenuti (*content delivery network*). La caratteristica probabilmente più sottovalutata di questa categoria di infrastrutture riguarda, forse in maniera contro-intuitiva, la sua componente fisica. Sebbene i servizi forniti dalle infrastrutture digitali appaiano ancora diffusamente nell'immaginario collettivo come immateriali, questi hanno un fortissimo impatto "materiale" ed è la dimensione fisica che abilita la fornitura e il loro funzionamento.

L'importanza di queste infrastrutture è legata alla crescente rilevanza anche geopolitica dei dati, incluso il loro *storage*, fusione e archiviazione. Le Nazioni Unite hanno stimato che oltre il 95 per cento dei dati globali viaggia attraverso cavi sottomarini in fibra ottica[61]. Questi cavi presentano delle caratteristiche fisiche e vulnerabilità simili ad altri tipi di infrastrutture. Essendo posti sui fondali marini, sono a rischio di essere danneggiati da atti non intenzionali, come succede frequentemente a causa dell'attività dei pescherecci. Inoltre, negli ultimi anni, si sono verificati in Europa alcuni incidenti la cui origine più probabile è il sabotaggio intenzionale di cavi da parte di attori statali[62]. In uno di questi casi, in una zona marittima tra le isole artiche contese da Norvegia e Russia, il cavo non solo è stato tranciato, ma anche fisicamente rimosso, per un totale di 4 chilometri e mezzo di cavo scomparsi[63].

Nella complessa rete di infrastrutture digitali rientrano non solo i cavi, ma anche i *data center* destinati all'archiviazione e allo scambio dei dati, i quali sono in gran parte infrastrutture terrestri, nonostante esistano già anche *data center* sottomarini[64]. I *data center* terrestri sono estremamente dispendiosi in termini

[60] Ibid.

[61] United Nations Office on Drugs and Crime, *Key Actions to Protect Submarine Cables from Criminal Activity Identified at UNODC Global Expert Meeting*, 7 febbraio 2019, https://www.unodc.org/unodc/en/frontpage/2019/February/key-actions-to-protect-submarine-cables-from-criminal-activity-identified-at-unodc-global-expert-meeting.html.

[62] Antonio Deruda, *Geopolitica digitale. La competizione globale per il controllo della Rete*, Roma, Carocci, 2024.

[63] Ibid.

[64] Ibid.

ISSN 2280-6164

di acqua per via degli impianti di raffreddamento, e a forte impatto inquinante a causa della produzione di anidride carbonica. Tra le problematiche di sostenibilità che caratterizzano i *data center* vi sono quindi quelle legate a un grande consumo di acqua, come nel caso, in maniera diversa, di due settori individuati dalla Cer, quelli delle acque reflue e dell'acqua potabile.

Similmente ad altri tipi di infrastrutture, quelle digitali sono controllate, gestite e/o possedute per lo più da privati e i tentativi di regolamentazione di questo settore hanno dovuto far fronte a grandi difficoltà, per cui non esiste ad oggi un sistema di norme condiviso e attuato pienamente in modo legalmente vincolante. Queste difficoltà dipendono da vari fattori. Si tratta infatti di un settore che abbraccia vari aspetti di per sé complessi e in parte nuovi, come la regolamentazione dell'intelligenza artificiale, la protezione dei dati e i diritti di proprietà intellettuale, in un mercato digitale che per natura è dinamico e in continua evoluzione[65].

Si tratta di una situazione simile a quella riscontrabile in un'altra categoria di IC, quella dello spazio. Ad esempio, fuori dalle acque territoriali di uno Stato vige la piena libertà di posa dei cavi sottomarini, sia nelle zone economiche esclusive che nelle acque internazionali. Come nel caso dello spazio, si tratta quindi di un settore in cui la debolezza dell'assetto normativo si interseca da un lato con un margine di manovra notevole in termini di espansione per quegli attori che hanno le capacità e le risorse per sfruttare tale grado di libertà, e dall'altro con una nuova arena geopolitica in cui occupare e controllare infrastrutture ad oggi vitali ad esempio per la comunicazione, o gli scambi commerciali e finanziari. In altre parole, si può parlare metaforicamente di soggetti critici che operano in una condizione non regolamentata (cavi sottomarini e satelliti), ma che sono fortemente legati ad una dimensione terrestre (*data center* e segmento di terra) che, di per sé, presenta specifiche vulnerabilità sia di tipo fisico che *cyber*.

2.7 Pubblica amministrazione

La pubblica amministrazione (PA) è alla base del funzionamento dello Stato che garantisce una serie di servizi ai cittadini. In questo campo, la Cer si riferisce a "Enti della pubblica amministrazione delle amministrazioni centrali come definiti da Stati membri conformemente al diritto nazionale"[66]. La PA è composta da enti pubblici che svolgono l'attività amministrativa al fine di perseguire interessi pubblici. Si tratta di una categoria sui generis rispetto le altre IC e riguarda, tra le altre cose, l'efficacia e la resilienza delle istituzioni e della *governance* nazionale. Nel caso italiano, i principi che dovrebbero regolare il suo funzionamento si riscontrano direttamente nella Costituzione, quali ad esempio legalità e imparzialità. Anche la PA è stata oggetto di crescenti attacchi *cyber* che possono causare fughe di dati sensibili o interrompere l'erogazione di un servizio e, tuttavia,

[65] Anna Albanese, "EU Competition Rules in Digital Markets: A Difficult Fit", in *MediaLaws*, 3 marzo 2023, https://www.medialaws.eu/?p=19275.

[66] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., p. 197.

ISSN 2280-6164

rischia di essere più trascurata in termini di resilienza[67], ad esempio per la difficoltà intrinseca nel rendere più flessibile e *responsive* l'apparato burocratico dietro la PA. Il Pnrr ha stanziato 6,14 miliardi di euro per la digitalizzazione della PA, ai quali si aggiungono 600 milioni di euro previsti dal Piano nazionale per gli investimenti complementari al PNRR[68]. In questo settore, la Cer prevede l'esclusione dalla sua applicazione degli gli enti della PA che si occupano di difesa e sicurezza (Art. 1.6).

2.8 Spazio

I sistemi spaziali e le infrastrutture ad essi connesse rappresentano un settore ad altissimo contenuto di tecnologie, la cui importanza strategica è aumentata negli ultimi anni di pari passo con il progresso tecnologico che ha caratterizzato il settore. Gli assetti spaziali forniscono oggi una serie di servizi imprescindibili, quali: (i) geoposizionamento e navigazione utilizzati ampiamente per il trasporto di persone e merci; (ii) comunicazione satellitare, non solo per le esigenze quotidiane della popolazione ma anche per garantire comunicazioni sicure governative; (iii) osservazione della terra, anche per una più accurata previsione di disastri naturali e fenomeni meteorologici estremi sempre più frequenti, per l'agricoltura e per il monitoraggio e la predizione dei cambiamenti climatici. Si tratta inoltre di tecnologie fondamentali per le attività di sorveglianza e intelligence, oltre che per lo svolgimento delle missioni delle forze armate[69].

Questa categoria di IC è ricompresa nella Cer, con un'importante eccezione: sono esclusi dall'ambito di applicazione della direttiva i programmi spaziali dell'UE (Galileo, Copernicus e Egnos). La Cer specifica, infatti, che i soggetti interessati sono gli "operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica"[70]. Nell'ambito di applicazione della direttiva ricade quindi il segmento di terra e le infrastrutture di terra, ma non il segmento spaziale che include i satelliti in orbita.

L'Italia è leader nel settore spaziale, caratterizzato tipicamente da un'ampia presenza di attori privati e commerciali che stanno guidando la spinta all'innovazione. L'applicazione della Cer al settore dello spazio in Italia dovrà tener conto del processo in atto di elaborazione di una legge spaziale nazionale e, in parallelo, della formulazione di una legge spaziale dell'UE (*EU Space Law*) che disciplini il settore anche a livello europeo[71].

[67] Arjen Boin e Martin Lodge, "Designing Resilient Institutions for Transboundary Crisis Management: A Time for Public Administration", in *Public Administration*, vol. 94, n. 2 (giugno 2016), p. 289-298, DOI 10.1111/padm.12264.

[68] Andrea Baldassarre, "PNRR e trasformazione digitale: ecco gli investimenti e le riforme previste per la digitalizzazione della PA", in *Forum PA*, 26 ottobre 2023, https://www.forumpa.it/?p=110352.

[69] Alessandro Marrone e Michele Nones (a cura di), The Expanding Nexus between Space and Defence, in *Documenti IAI*, n. 22|21 (febbraio 2022), https://www.iai.it/it/node/14669.

[70] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., p. 197.

[71] Si veda Karolina Muti, Ottavia Credi e Giancarlo La Rocca, "Il sistema-Paese Italia di fronte alle

ISSN 2280-6164

2.9 Produzione, trasformazione e distribuzione di alimenti

Per quanto riguarda la produzione, trasformazione e distribuzione di alimenti, la Cer indica delle imprese alimentari impegnate esclusivamente all'ingrosso e nella produzione e trasformazione industriale su larga scala. Questa categoria si collega al concetto di sicurezza alimentare che comprende quindi non solo la disponibilità di materie prime, ma anche la sicurezza della catena di approvvigionamento alimentare e dei processi produttivi.

Un numero crescente di rischi esogeni legati alle conseguenze delle crisi e conflitti degli ultimi anni si sommano agli effetti dell'emergenza climatica. Eventi come la pandemia e l'invasione russa dell'Ucraina hanno provocato interruzioni delle catene di approvvigionamento. Il blocco delle rotte dell'esportazione del grano ucraino da parte delle forze armate russe, con in particolare l'interruzione delle esportazioni dal porto di Odessa come snodo fondamentale, sono risultate in una riduzione dell'offerta e un conseguente aumento dei prezzi, con effetti su ampia scala tanto per l'impatto sulla resilienza economica dell'Ucraina in quanto paese esportatore, quanto per la minore disponibilità di questo alimento fondamentale in Stati già molto vulnerabili dal punto di vista della sicurezza alimentare, come alcuni paesi dell'Africa. Si può interpretate il blocco delle esportazioni alimentari ucraine da parte russa come un caso di "*weaponization*" del grano.

Un altro fattore fondamentale che porterà a una vulnerabilità crescente di questo settore riguarda le conseguenze dell'emergenza climatica, che ha un impatto molto grave sull'agricoltura, tanto per i danni provocati dalle temperature sempre più alte e dalla siccità, quanto per quelli imprevedibili legati a sempre più frequenti eventi meteorologici estremi, come inondazioni, o incendi, anche in zone geografiche non interessate storicamente da questi fenomeni[72].

3. I principali elementi della direttiva Cer

Come illustrato, la direttiva Cer si inserisce in un contesto internazionale caratterizzato da minacce alla sicurezza in continua evoluzione, unitamente agli avanzamenti tecnologici delle IC sempre più essenziali per l'erogazione di servizi, fortemente interconnesse e spesso dipendenti dalla dimensione digitale. La direttiva è tuttavia per sua natura e base giuridica una normativa del mercato interno europeo, in quanto mira a garantire la fornitura di servizi essenziali aumentando la resilienza dei soggetti critici che li somministrano all'interno dell'Unione. Dopo aver analizzato le categorie di IC che rientrano nell'ambito di applicazione della

sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity", in *Documenti IAI*, n. 23|15 (luglio 2023), https://www.iai.it/it/node/17272.

[72] Agnieszka de Sousa, "Europe's New Security Nightmare Is Food Supply", in *Bloomberg*, 6 marzo 2024, https://www.bloomberg.com/news/newsletters/2024-03-06/europe-s-new-security-nightmare-is-food-supply.

ISSN 2280-6164

Cer, si evidenziano di seguito le principali novità, misure e obblighi introdotti che dovranno applicarsi ai soggetti critici identificati.

3.1 Ampliamento dei settori di attuazione

Come precedentemente sottolineato, la direttiva identifica infatti undici settori (rispetto ai due della già citata direttiva del 2008): energia, trasporti, banche, infrastrutture dei mercati finanziari, salute, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Il 25 luglio 2023, a integrazione della Cer, la Commissione europea ha inoltre adottato il Regolamento delegato (UE) 2023/2450[73]: quest'ultimo fornisce un elenco "non esaustivo di servizi essenziali"[74] ricompresi nella definizione data dalla direttiva. Il regolamento stabilisce, inoltre, che l'elenco viene fornito al servizio dalle autorità competenti per effettuare una valutazione del rischio, e successivamente sarà utilizzato per individuare i soggetti critici. In questo modo, il regolamento mira a fornire chiarezza e a supportare gli Stati nell'identificazione non solo dei settori, ma anche delle sottocategorie di settori rilevanti ai fini della direttiva.

Un'importante precisazione sull'applicazione della normativa riguarda gli enti che operano nell'ambito della sicurezza e difesa. Considerata la responsabilità degli Stati membri al riguardo, è prevista l'esclusione dalla direttiva di quegli "enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati"[75]. Per quanto riguarda altri soggetti critici specifici operanti nei suddetti settori, la direttiva lascia la facoltà agli Stati membri di escluderli dalla applicazione di parte delle misure presenti nella normativa stessa.

3.2 Rafforzamento della resilienza

Un secondo elemento da sottolineare è il passaggio da un approccio incentrato sulla protezione (com'era nella direttiva 2008/114/CE) a favore di un focus sulla resilienza. L'accento sulla resilienza mira a coprire l'intero processo di gestione delle crisi, dalle prime fasi della risposta al ripristino dell'operatività, con l'obiettivo di garantire una continuità dell'erogazione dei servizi improntata sulla ridondanza dei sistemi[76]. Per sostenere gli Stati membri nell'identificazione delle misure da attuare, la direttiva interviene fornendo la seguente definizione di resilienza: "la capacità di un soggetto critico di prevenire, attenuare, assorbire un incidente, di proteggersi da esso, di rispondervi, di resistervi, di adattarvisi e di ripristinare le

[73] Commissione europea, *Regolamento delegato (UE) 2023/2450 del 25 luglio 2023, che integra la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio stabilendo un elenco di servizi essenziali*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32023R2450.

[74] Ibid., Art. 1.

[75] Ibid., p. 1.

[76] Intervista, 8 luglio 2024.

ISSN 2280-6164

proprie capacità operative"[77].

3.3 Dall'infrastruttura critica al soggetto critico

Il testo fornisce una definizione di "infrastruttura critica" intesa come un elemento, un impianto, un'attrezzatura, una rete o un sistema, oppure una parte di un elemento, di un impianto, di un'attrezzatura, di una rete o di un sistema, necessari per la fornitura di un servizio essenziale (Art. 2.4). Fermo restando la suddetta definizione di IC, le misure si rivolgono al cosiddetto soggetto critico, inteso come l'operatore, pubblico e privato, responsabile della gestione delle infrastrutture critiche nei settori indicati.

Ai sensi della direttiva, l'obbligo di individuare i "soggetti critici", ricade sugli Stati membri, tanto che la direttiva definisce "soggetto critico" "un soggetto pubblico o privato che è stato individuato da uno Stato membro" (Art. 2.1) e rispondente ai seguenti criteri fissati all'Art. 6.2: "a) il soggetto fornisce uno o più servizi essenziali", laddove per "servizio essenziale" si intende "un servizio fondamentale per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente" (Art. 2.5); "b) il soggetto opera, e la sua infrastruttura critica è situata, sul territorio di tale Stato membro; e c) un incidente avrebbe effetti negativi rilevanti [..], sulla fornitura da parte del soggetto di uno o più servizi essenziali, o sulla fornitura di altri servizi essenziali nei settori [...] che dipendono da tale o tali servizi essenziali".

Inoltre, soggetti critici di particolare rilevanza "europea" sono definiti come quei soggetti che erogano servizi a sei o più Stati membri. Un soggetto critico che si qualifica come soggetto critico europeo, deve comunicare alla autorità competente nazionale quali servizi fornisce e a quali paesi. Se i paesi interessati confermano di ricevere servizi di natura essenziale, il soggetto critico deve attenersi agli obblighi previsti dalla direttiva.

Vengono inoltre introdotte due figure preposte al coordinamento delle azioni per la resilienza a livello nazionale e verso l'UE: una o più autorità competenti per settore (Autorità settoriali competenti) e un punto di contatto unico (Pcu), responsabile del coordinamento fra i soggetti critici e verso l'Unione europea. Spetta infatti alle autorità competenti, con il supporto degli Stati membri, di effettuare controlli e vigilare sulla corretta applicazione delle misure adottate dai soggetti critici e di prevedere l'applicazione di sanzioni in caso di inadempienza.

3.4 Adozione di una strategia nazionale per la resilienza dei soggetti critici

La direttiva introduce l'obbligo per gli Stati membri di sviluppare una strategia nazionale (entro il 17 gennaio 2026) da aggiornare ogni quattro anni. Nel testo si forniscono anche gli elementi minimi che devono essere presenti nella strategia

[77] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., Art. 2.2.

ISSN 2280-6164

(Art. 4), fra questi: una descrizione del processo di individuazione dei soggetti critici, di obiettivi strategici e priorità volti ad accrescere la resilienza complessiva dei soggetti critici, unitamente a un piano di *governance* per la loro realizzazione; una definizione delle misure necessarie per la resilienza complessiva dei soggetti critici, inclusa una valutazione del rischio, come illustrato di seguito.

3.5 Valutazione del rischio da parte degli Stati membri

L'individuazione dei soggetti critici deve derivare, secondo la direttiva, da una valutazione del rischio a livello nazionale, da svolgersi entro il suddetto termine del 17 gennaio 2026, e successivamente "ogniqualvolta necessario e almeno ogni quattro anni" (Art. 5.1). La valutazione del rischio, come descritta dalla direttiva, deve essere attuata in primis da parte dello Stato membro, e poi dai soggetti critici sulla base di quanto stabilito a livello statale.

La direttiva prevede che la valutazione del rischio "tenga conto di tutti i rischi rilevanti naturali e di origine umana che potrebbero causare un incidente, compresi quelli di natura intersettoriale o transfrontaliera, gli incidenti, le catastrofi naturali, le emergenze di sanità pubblica, le minacce ibride e altre minacce antagoniste, inclusi i reati di terrorismo" (Art. 12.2). Alla luce della valutazione del rischio, le autorità competenti procedono a individuare i soggetti critici per poi supportarli nell'adottare le misure di resilienza. È importante sottolineare che gli Stati membri possono elaborare molteplici strumenti al fine di fornire un sostegno aggiuntivo ai soggetti critici. Fra questi, una mappatura a livello UE dei rischi transfrontalieri e intersettoriali, oltre che metodologie per la formazione transfrontaliera ed esercitazioni per testare la resilienza dei soggetti critici (Art. 10).

3.6 Notifica in caso di incidente

Una novità rilevante introdotta dalla direttiva riguarda l'obbligo di notifica in caso di incidente. Esistono attualmente diverse piattaforme per la segnalazione di incidenti, ma la direttiva introduce un approccio più dettagliato in un'ottica di armonizzazione delle procedure fra gli Stati membri. In caso di incidente, il soggetto critico interessato deve informare l'autorità nazionale competente entro 24 ore. La notifica deve riportare informazioni sulla natura dell'evento, la causa principale, le possibili conseguenze e i potenziali impatti transfrontalieri, il numero di utenti colpiti, la durata dell'interruzione e l'area geografica.

Le informazioni trasmesse con la notifica devono consentire all'autorità competente di avere un quadro completo dell'incidente e di poter valutare se si sia verificato o meno un impatto transfrontaliero. In tale caso, l'autorità competente è tenuta a comunicare l'incidente – nel rispetto della riservatezza – alle autorità degli Stati interessati e a fornire supporto per un'efficace risposta all'incidente. È inoltre previsto che i soggetti critici presentino un ulteriore rapporto entro un mese dal momento in cui sono venuti a conoscenza dell'incidente (Art. 15.1).

ISSN 2280-6164

3.7 La relazione con la Nis2 e la collaborazione per l'attuazione della direttiva

La direttiva Cer richiede la collaborazione dell'UE con altre agenzie competenti e le relative iniziative, in particolare per quanto riguarda la direttiva 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, conosciuta come Nis2. Questa collaborazione è fondamentale dato l'aumento dei rischi e delle sfide per le infrastrutture critiche causato dalla digitalizzazione dei servizi. La direttiva Nis2 mira ad aumentare il livello di resilienza informatica delle imprese che operano in tutti i settori rilevanti e a garantire il loro allineamento in termini di capacità appunto di resilienza. Oltre ai settori già coperti dalla precedente direttiva Nis (sanità, trasporti, finanza, acqua, energia, servizi e infrastrutture digitali), la Nis2 amplia l'attenzione a una serie di altre aree, tra le quali spazio, produzione chimica e farmaceutica, pubblica amministrazione.

L'approccio coordinato con la Nis2 implica anche l'esclusione delle questioni già disciplinate dalla Cer, con alcune precisazioni. Ovvero, considerata la connessione e l'importanza del supporto che le infrastrutture digitali danno agli altri soggetti critici, la Cer prevede che gli Stati membri identifichino, fra le infrastrutture digitali, quelle che si qualificano come soggetti critici ai sensi della Cer e valutino l'adozione di misure di resilienza anche nei loro confronti. Le autorità competenti per le due direttive sono inoltre chiamate a cooperare con lo scambio di informazioni e con l'intento di attuare le misure delle rispettive normative in maniera complementare.

Una importante misura di collaborazione introdotta dalla Cer è la possibilità di missioni di consulenza svolte sotto la direzione della Commissione, su sua iniziativa o su richiesta degli Stati membri e con il consenso del soggetto critico interessato. Le missioni hanno lo scopo di valutare la conformità delle misure adottate ai requisiti della direttiva. Inoltre, viene istituito il Gruppo per la resilienza dei soggetti critici, composto dalle autorità e da esperte ed esperti provenienti dagli Stati membri coinvolti, che discuterà le disposizioni della direttiva e i suoi effetti diretti e indiretti, nonché tutte le altre questioni relative alla resilienza delle IC (Art. 19).

4. Un quadro europeo a supporto degli Stati membri

Nel complesso, la direttiva Cer amplia e approfondisce le tendenze sovranazionali in questo settore, e riflette la direzione generale dell'integrazione europea a europeizzare ulteriori aree rispetto a quelle già esistenti. Non pregiudica tuttavia la competenza degli Stati membri e delle rispettive autorità in termini di autonomia amministrativa, né la loro responsabilità di salvaguardare la sicurezza e la difesa nazionale o il potere di salvaguardare altre funzioni essenziali dello Stato, in particolare quelle di sicurezza pubblica e l'integrità territoriale.
La direttiva prevede la messa in atto di meccanismi regolari a livello europeo e nazionale per garantire un'adeguata comunicazione, nonché il coinvolgimento di tutti i soggetti interessati e il coordinamento fra le parti interessate a livello UE, nazionale, regionale, locale e di singole IC. La valutazione del rischio e la sua

ISSN 2280-6164

attuazione sono ampiamente trattati nella Cer, che fa un significativo passo avanti nel fornire criteri comuni per gli Stati membri e illustrare gli elementi chiave al riguardo. La direttiva fa inoltre un riferimento specifico ai principali strumenti che devono essere considerati per la valutazione del rischio da parte degli Stati membri, invitando gli Stati a considerare innanzitutto la decisione n. 1313/2013/UE su un meccanismo UE di protezione civile[78], essendo il principale strumento di coordinamento a livello europeo delle emergenze, e altre valutazioni svolte in conformità con atti settoriali dell'UE.

Sebbene gli Stati membri rimangano in ultima istanza responsabili di garantire la sicurezza e la fornitura di servizi vitali, e quindi del funzionamento delle IC nazionali, si può affermare che è visibile un maggiore coordinamento in questo campo a livello di Unione. Gli sviluppi positivi in materia di sicurezza e resilienza delle infrastrutture critiche riflettono i miglioramenti nella comprensione, nella consapevolezza e nella gestione delle sfide da affrontare da parte dei diversi attori coinvolti.

5. Sfide in ambito di attuazione

Come precedentemente accennato, la direttiva Cer fornisce una cornice unica e omnicomprensiva ponendosi come obiettivo il raggiungimento di un livello di "armonizzazione minima" (Art. 3). Armonizzazione necessaria di fronte alla natura spesso ibrida della minaccia e ad attori malevoli che sfruttano sistematicamente proprio la frammentazione e le differenze politiche, legislative ed economiche tra gli Stati membri. Come evidenziato, la Cer dedica attenzione alla natura intersettoriale, interconnessa e transfrontaliera dei fenomeni che interessano le IC in Europa, ma allo stesso tempo lascia margine di manovra e autonomia ai singoli Stati membri, per garantire un approccio sufficientemente flessibile che tenga conto delle specificità e volontà nazionali e che eviti un'eccessiva rigidità, in linea con un contesto europeo e globale che è in continuo mutamento e in cui i tempi dell'emergere di nuove minacce non corrispondono a quelli legislativi.

Una sfida non irrilevante deriva dal raccogliere in una stessa cornice normativa e decisionale un così alto numero di tipi di soggetti critici diametralmente diversi tra loro, riuscendo comunque a coglierne le rispettive specificità e le differenti modalità di funzionamento. La frammentazione che ne potrebbe derivare, nonostante le misure presenti nella direttiva stessa, rischia di rendere la sua attuazione un processo lungo e centrifugo, in particolare in quegli Stati membri dove manca un solido coordinamento tra i vari dicasteri e un approccio sistemico e inter-agenzia.

[78] Parlamento europeo e Consiglio dell'UE, *Decisione n. 1313/2013/UE del 17 dicembre 2013, su un meccanismo unionale di protezione civile*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32013D1313.

© 2024 IAI
ISSN 2280-6164
DOCUMENTI IAI 24 | 11 - OTTOBRE 2024

Il rischio di frammentazione è di natura molteplice. In primis, riguarda l'approccio interno allo Stato membro, per l'intrinseca diversità dei soggetti critici da attenzionare e la loro probabile collocazione decentrata sul territorio nazionale. In secondo luogo, vi è il rischio di una frammentazione tra singoli Stati membri e tra questi e la Commissione, che può derivare dalla libertà di interpretazione della direttiva da parte delle autorità nazionali, ad esempio, nell'individuare i rispettivi soggetti critici. Gli elementi nella direttiva che descrivono tale individuazione sono infatti necessariamente generici. In terzo luogo, potrebbe emergere una divisione tra quei soggetti ritenuti già in precedenza "critici" e quindi con una certa dimestichezza ed esperienza nell'adattarsi alle nuove disposizioni di legge (come potrebbero essere alcuni soggetti nel settore energetico o dei trasporti), e quelli che verranno classificati per la prima volta come critici (come potrebbe essere anche nel caso di alcuni operatori di infrastrutture digitali) con tutto quello che ciò comporta: l'ottenimento di nulla osta di sicurezza per il personale dove necessario, l'adeguamento ex novo a processi, organizzazioni e pratiche che garantiscano la resilienza ai livelli richiesti.

Tutto ciò porta a prevedere che alcuni di questi soggetti, essendo operatori privati che devono stare sul mercato, potrebbero non vedere incentivi nell'essere classificati come "soggetto critico". Ciò comporta infatti significative responsabilità a loro carico e maggiori controlli, a fronte di un supporto che dovrebbe essere fornito dalla Commissione e dallo Stato membro ma che, nei termini descritti nella direttiva, non sembra sufficiente a compensare la mole di adempimenti, inclusi quelli burocratici di responsabilità del soggetto critico. Questo rischia di influire, inoltre, sulla propensione alla notifica di incidenti che per un operatore privato potrebbe risultare non conveniente. Lo stesso discorso varrebbe per l'adeguamento delle procedure interne di gestione delle informazioni al fine di garantire la notifica nella forma e nei tempi previsti, nonché delle attività operative alla luce della richiesta di una maggiore resilienza e individuazione dei rischi. Per un operatore privato tutto ciò potrebbe rendere lo svolgimento delle proprie attività più farraginoso e complesso.

Va evidenziato tuttavia che questi adempimenti andrebbero interpretati non come un costo, ma come un investimento in sicurezza, considerando che i danni generati dagli incidenti e attacchi hanno spesso un costo superiore a quello degli adempimenti, come dimostrano diversi esempi nel settore cyber. Se la direttiva può quindi contribuire a indirizzare i soggetti critici verso una più elevata "cultura della sicurezza", quest'ultima andrebbe sviluppata anche con altri strumenti, per evitare che lo sforzo di aumentare la resilienza e la sicurezza siano vissuti dai soggetti critici esclusivamente come costi.

Il potere degli Stati membri di "effettuare ispezioni e controlli, il potere di vigilanza, il potere di richiedere ai soggetti critici di fornire informazioni e prove riguardanti le misure adottate per adempiere ai loro obblighi" e di "emettere provvedimenti per porre rimedio alle violazioni riscontrate" per la corretta applicazione ed esecuzione" della direttiva, richiederà un adeguamento anche della macchina statale in termini di formazione e competenze del personale preposto, tempo e risorse necessarie. La

ISSN 2280-6164

direttiva suggerisce, in questo senso, che gli Stati membri sviluppino "materiali e metodologie di orientamento", contribuiscano "all'organizzazione di esercitazioni per testare la resilienza dei soggetti critici e fornire consulenza e corsi di formazione per il personale dei soggetti critici", prevedendo, dove necessario, "risorse finanziarie" e di "agevolare la condivisione volontaria di informazioni"[79].

Inoltre, gli Stati membri "dovrebbero sostenere i soggetti critici, compresi quelli che si qualificano come piccole e medie imprese, nel rafforzamento della loro resilienza" evitando "oneri amministrativi eccessivi"[80]. Considerando il contesto italiano, il rischio di un peso burocratico e amministrativo scaricato sui soggetti critici, specialmente quelli "nuovi" e di piccole dimensioni, andrebbe attenzionato fin da subito.

Nonostante la direttiva indichi che la Commissione dovrebbe sostenere, "ove lo ritenga opportuno", le autorità competenti e i soggetti critici "allo scopo di agevolare l'adempimento dei loro rispettivi obblighi", non è chiaro se questo prevederà delle risorse finanziarie ad hoc che possano sostenere l'adeguamento e, in generale, il supporto che fornirà la Commissione è formulato in maniera piuttosto generica. La suddetta istituzione di un Gruppo per la resilienza dei soggetti critici per agevolare la cooperazione tra Stati membri è senz'altro un punto di partenza.

Un ulteriore elemento di criticità riguarda il rischio di un doppio binario tra l'attuazione della direttiva Nis2 sulla cybersicurezza e della Cer. Ciò può e deve essere evitato, in quanto è fondamentale che ci sia coordinamento e complementarità nell'attuazione delle due normative: in molti casi le vulnerabilità *cyber* possono avere un impatto negativo sull'integrità fisica dell'infrastruttura in oggetto e viceversa, rendendo queste due dimensioni della resilienza – *cyber* e materiale – non separabili.

Per una piena ed efficace attuazione della direttiva è necessario uno scambio di informazioni sistematico e aperto tra soggetti critici, autorità competenti degli Stati membri e Commissione europea, in particolare ma non solo per quello che riguarda le missioni di consulenza. L'invito allo scambio di informazioni è presente in molti passaggi della direttiva, ma questa pratica potrebbe risultare problematica e di non facile attuazione, se si considera la sensibilità dei tipi di IC coinvolti e le esperienze in altri ambiti contigui.

Da ultimo, la Cer si rivolge a dei soggetti specifici e sembra affrontare il tema della resilienza ancora come materia per pochi addetti ai lavori. I grandi cambiamenti e le tendenze del contesto internazionale legati alla resilienza delle IC mostrano invece come ci sia un terzo soggetto che non può più essere trascurato, la popolazione. La mancanza di disposizioni relative alla diffusione di una maggiore consapevolezza sulla resilienza delle IC da parte di cittadine e cittadini europei

[79] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022*, cit., punto 25.
[80] Ibid.

ISSN 2280-6164

appare come un'occasione persa. Ciò è particolarmente il caso in paesi dove manca la cultura della sicurezza e in cui gran parte della popolazione non conosce i soggetti che garantiscono i servizi alla base del funzionamento della loro società. I temi legati al settore della difesa possono essere ancora divisivi a causa delle diverse percezioni delle minacce da parte dei cittadini europei, ma le questioni relative alla resilienza delle IC sono tradizionalmente parte di una sfera legata alla sicurezza interna, meno divisiva e sulla quale verosimilmente c'è maggiore convergenza delle opinioni pubbliche, in quanto tutta la società fa affidamento su determinati servizi. In un momento in cui le IC sono obiettivo sistematico di attacchi e sono esposte a rischi crescenti, la responsabilizzazione, declinata come maggiore consapevolezza, dei cittadini, oltre che degli Stati membri e dei soggetti critici, sarebbe stata un'aggiunta opportuna.

6. La dimensione italiana: il recepimento della direttiva 2022/2557 e l'attuazione a livello nazionale. Sfide e opportunità

6.1 Rischi e minacce alle infrastrutture critiche: contesto e documenti strategici

L'Italia è soggetta a rischi sia naturali che antropici, in particolare eventi geofisici come i terremoti, i rischi meteo-idrogeologici o derivanti dall'attività vulcanica. Tra i recenti avvenimenti che hanno seriamente compromesso la fornitura dei servizi in Italia, va ricordata l'interruzione di corrente del 28 settembre 2003 derivata dalla caduta di un albero su un tratto di rete elettrica in Svizzera, causata da forte vento, che ha innescato una catena di eventi che hanno portato a un blackout totale in Italia per diverse ore[81]. Negli ultimi anni, si assiste con sempre maggior frequenza al verificarsi di danni causati da eventi naturali estremi. Secondo uno studio pubblicato dall'Osservatorio Città Clima di Legambiente e Unipol, nel 2023 gli eventi meteorologici estremi sono cresciuti del 22 per cento rispetto al 2022. Fra i casi più tragici degli ultimi anni, si ricordano il terremoto in Abruzzo nel 2009 e più recentemente l'alluvione in Emilia-Romagna, quest'ultima con una stima di danni alle infrastrutture pubbliche e private di circa 8 miliardi di euro[82].

L'emergenza in Emilia-Romagna ha dimostrato la rilevanza dell'interdipendenza fra alcuni settori di IC, e gli effetti "a cascata" che possono derivare dall'interruzione della fornitura di un servizio connesso con altri servizi. L'alluvione ha infatti messo in evidenza come a partire dalla mancanza di alimentazione elettrica si sono verificati malfunzionamenti nelle reti di comunicazione, e di conseguenza nell'organizzazione delle operazioni di intervento. Il ripristino dell'energia è stato

[81] "Il 28 settembre 2003 ci fu il più grande blackout elettrico della storia d'Italia", in *SkyTG24*, 28 settembre 2023, https://tg24.sky.it/cronaca/2023/09/28/blackout-italia-2003.

[82] Agenzia per la sicurezza territoriale e la protezione civile, *Alluvione. Oltre 8,8 miliardi di euro: è la stima provvisoria dei danni, di cui 1,8 per interventi necessari a fare fronte all'emergenza*, 15 giugno 2023, https://protezionecivile.regione.emilia-romagna.it/notizie/2023/giugno/alluvione-oltre-8-8-miliardi-di-euro-la-stima-provvisoria-dei-danni-di-cui-1-8-per-interventi-necessari-a-fare-fronte-emergenza.

ISSN 2280-6164

inoltre messo in difficoltà dalle condizioni delle vie di trasporto che hanno reso inaccessibili le aree che necessitavano di intervento.

Inoltre, per la sua collocazione nel Mediterraneo, l'Italia si trova in una posizione strategica sia dal punto di vista geografico, sia per quanto riguarda il suo inserimento in una fitta rete di gasdotti ed elettrodotti la cui tutela è da considerarsi una priorità per la sicurezza nazionale. Gran parte dell'export italiano inoltre avviene via mare attraverso il Mediterraneo, dove transita il 20 per cento del traffico marittimo mondiale, rendendo la sicurezza e stabilità di quest'area vitale per gli interessi nazionali del paese. La Strategia di sicurezza e difesa per il Mediterraneo 2022 del Ministero della Difesa si riferisce al concetto di "Mediterraneo allargato" che si estende dall'Europa continentale al Medio Oriente, fino all'Africa subsahariana e riconosce che le potenziali minacce in quest'area sono per lo più di natura ibrida[83]. Per quanto riguarda le IC, la Strategia ricorda che sia il petrolio che il gas per soddisfare il fabbisogno energetico nazionale vengono importati quasi totalmente con navi specializzate attraverso il Mediterraneo e che le minacce nell'area riguardano le vie di comunicazione, l'accesso ai porti, la sicurezza energetica e quella cibernetica. La natura multidimensionale della minaccia in quest'area ha portato la "sicurezza domestica e quella internazionale a convergere" e richiede un approccio sistemico con un coinvolgimento di vari dicasteri e inter-agenzia. Il documento ricorda l'importanza della stabilità e sicurezza dei paesi fornitori di energia. A tal proposito, il Piano Mattei, iniziativa di punta del governo Meloni rivolta all'Africa, menziona tra le sue direttrici sei settori che coincidono con quelli attenzionati dalla Cer, ovvero la salute, il settore energetico, l'acqua (sia potabile che processi e impianti di depurazione), lo spazio e le infrastrutture digitali anche per la cybersicurezza.

Inoltre, Il Piano del mare per il triennio 2023-2025, curato dal Comitato interministeriale per le politiche del mare, nella sezione Sicurezza si riferisce alla sicurezza dei terminali portuali, a quella marittima e a quella cibernetica[84]. Il Piano indica anche la necessità di proteggere "il complesso sistema produttivo e di trasporto marittimo, composto dalle linee di comunicazione, dai porti, dagli interporti, dai centri nodali di smistamento e dal retroterra della catena logistica, dalla flotta mercantile, crocieristica e peschereccia, dagli oleodotti e gasdotti sottomarini, dalle navi e piattaforme petrolifere offshore e dai parchi eolici marini"[85]. Il documento pone anche l'attenzione sul mantenimento del controllo di assetti strategici quali i principali porti italiani, compresi gli scali di Taranto e di Trieste obiettivo nel recente passato dell'interesse di attori extra-UE.

[83] Ministero della Difesa, *Strategia di sicurezza e difesa per il Mediterraneo 2022*, maggio 2022, https://ciram.unimc.it/it/focus/diritto-geopolitica-mare/italia-sicurezza-spazi-marittimi/litalia-e-la-sicurezza-degli-spazi-marittimi/StrategiaMediterraneo2022.pdf.

[84] Comitato interministeriale per le politiche del mare, *Piano del mare*, 31 luglio 2023, p. 211, https://www.strutturapolitichemare.gov.it/it/il-piano-del-mare/piano-del-mare-2023-2025.

[85] Ibid., p. 215.

ISSN 2280-6164

6.2 IC in Italia: identificazione e iniziative nazionali

Attualmente, in Italia vi sono numerosi atti normativi relativi a specifici settori di IC, ma manca un quadro di riferimento univoco che raccolga tutte le misure nazionali rilevanti per la protezione e resilienza delle IC[86]. Nel quadro di riferimento precedente alla Cer, il decreto di attuazione della direttiva 2008/114/CE si limitava a riportare alla lettera la definizione data dalla direttiva stessa.

In questo contesto, va notato come esista in Italia un'agenzia per la cybersicurezza nazionale, mentre al momento è la Presidenza del Consiglio l'ente di coordinamento per la protezione delle infrastrutture critiche nel caso specifico delle minacce nella dimensione fisica. Non è stata quindi finora istituita un'autorità dedicata e competente per il complesso delle IC. Questo aspetto dimostra la grande rilevanza attribuita nel Paese al settore cibernetico, e più precisamente la maggior attenzione rivolta alle minacce nel cyberspazio rispetto ad altri ambiti. Ciò è anche sintomo, secondo alcuni esperti, di un mancato interesse politico in Italia per la tematica della sicurezza e della protezione fisica. A questo si unisce purtroppo una certa mancanza di consapevolezza della tematica sia a livello degli *stakeholder* che del legislatore, e più in generale una limitata cultura della sicurezza nella società che porta a una scarsa conoscenza e sensibilità verso le sue molteplici dimensioni[87].

Nella prospettiva italiana, la sicurezza nazionale sembra essere imprescindibile dallo sviluppo tecnologico, come evidenziato dalla relazione annuale del Dipartimento delle informazioni per la sicurezza (Dis) del 2023[88], che si riferisce alla digitalizzazione come portatrice di crescita economica e allo stesso tempo causa di maggiore vulnerabilità. Nella relazione, ampia rilevanza viene data alle iniziative e agli interventi volti alla creazione di una infrastruttura digitale nazionale e, anche in questo caso, al potenziamento della sicurezza nazionale cibernetica. In relazione alla protezione delle infrastrutture critiche, il documento dedica una particolare attenzione alle telecomunicazioni e ai trasporti.

Sullo sfondo del conflitto in Ucraina e della necessità di garantire non solo la sicurezza energetica ma anche la sostenibilità economica e ambientale, la relazione del Dis per il 2023 sottolinea anche come sia rilevante garantire una diversificazione delle importazioni di gas naturale, il che implica la tutela delle infrastrutture esistenti e l'attuazione dei piani per la realizzazione di infrastrutture aggiuntive. La rilevanza e il valore critico della dimensione digitale e dei servizi IT e di quelle dei trasporti e dell'energia sono evidenti di fronte al verificarsi di un aumento di attacchi contro questo tipo di infrastrutture volti a causare un'interruzione di servizi. Un elemento di particolare interesse è relativo al profilo degli attori responsabili di tali azioni: si

[86] Patrizia Di Micco e Giulia Pascuzzi, "Resilienza, ecco la chiave per proteggere le infrastrutture critiche", cit.

[87] Intervista, 26 giugno 2024.

[88] Dipartimento delle informazioni per la sicurezza, *Relazione annuale 2023*, febbraio 2024, https://www.sicurezzanazionale.gov.it/contenuti/relazione-2023.

ISSN 2280-6164

tratta in maggior misura di gruppi statuali o sponsorizzati da Stati, frequentemente nell'ambito di azioni di spionaggio.

La particolare rilevanza delle reti di comunicazione e di fornitura di energia, oggetto di recenti atti di sabotaggio a livello internazionale, e la posizione strategica dell'Italia, rendono necessario guardare con priorità alla dimensione subacquea nella quale si diffonde la rete articolata di cavi e dotti che circonda il Paese[89]. Tale dimensione sta rivestendo sempre maggior rilevanza strategica, come evidenziato dalle diverse iniziative mirate al monitoraggio delle infrastrutture che si trovano nei mari adiacenti l'Italia, fra queste l'operazione Fondali Sicuri del Ministero della Difesa, il memorandum di intesa fra la Marina Militare e l'azienda Sparkle per il monitoraggio dei cavi di telecomunicazione di quest'ultima e l'istituzione del Polo nazionale della dimensione subacquea (Pns) a La Spezia.

6.3 Gli strumenti e le strutture responsabili dell'attuazione in Italia

Per quanto riguarda la normativa di attuazione, la direttiva Cer è stata recepita in Italia con il decreto legislativo n. 134 del 4 settembre 2024[90]. Si presentano di seguito alcuni degli elementi più significativi che delineano quali saranno le misure per l'attuazione della Cer, così come descritti nel decreto legislativo.

Per quanto riguarda l'ambito di applicazione, è previsto che siano individuati specifici soggetti critici che svolgono attività principalmente nei settori della pubblica sicurezza, della protezione civile, della difesa o dell'attività di contrasto compresi l'indagine, l'accertamento e il perseguimento di reati al fine di escluderli dall'ambito di applicazione della direttiva Cer[91].

In base al decreto attuativo della direttiva, le misure di resilienza da adottare comprendono misure tecniche, di sicurezza e di organizzazione. Queste includono le azioni necessarie a evitare il verificarsi dei rischi, facendo specifico riferimento a catastrofi naturali e collegate ai cambiamenti climatici, oltre a misure volte a contrastare e mitigare le conseguenze di eventuali incidenti e garantire la continuità operativa. A ciò si aggiungono interventi di realizzazione di protezione fisica (barriere, controllo degli accessi, impianti di rilevamento) e a favore della sicurezza del personale. Quest'ultima dovrebbe prevedere l'individuazione di personale con funzioni critiche per garantire il rispetto delle misure, nonché adeguata e continua informazione e formazione tramite corsi ed esercitazioni.

[89] Elio Calcagno e Alessandro Marrone (a cura di), "The Underwater Environment and Europe's Defence and Security", in *Documenti IAI*, n. 23|13 (giugno 2023), https://www.iai.it/it/node/17225.

[90] Decreto legislativo n. 134 del 4 settembre 2024: *Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici...*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;134.

[91] Ibid., Art. 1.

ISSN 2280-6164

La responsabilità dell'attuazione della direttiva è del Presidente del Consiglio dei ministri. In particolare, l'Art. 3 del decreto specifica che il Presidente ha l'alta direzione e la responsabilità delle politiche di resilienza nonché dell'adozione della strategia nazionale per la resilienza. In aggiunta, è prevista l'istituzione di enti e organi ad hoc: il Punto di contatto unico (Pcu), le Autorità settoriali competenti (Asc), il Comitato interministeriale per la resilienza (Cir) e la Conferenza per la resilienza dei soggetti critici (Crsc).

Il Punto di contatto unico sarà istituito presso la Presidenza del Consiglio dei ministri (Pcm), mentre le Asc saranno corrispondenti ai Ministeri competenti per gli 11 settori. Il Pcu, in coordinamento con le Asc, sarà responsabile per la valutazione del rischio a livello nazionale. Entrambi avranno inoltre un ruolo di sostegno ai soggetti critici, con i quali condivideranno linee guida e metodologie di analisi, e supporto tramite attività di formazione ed esercitazioni. I rappresentanti del Pcu potranno partecipare alle attività del suddetto Gruppo per la resilienza dei soggetti critici, istituito a supporto della Commissione europea e a sostegno alla cooperazione fra gli Stati.

Le Asc avranno il compito di individuare i soggetti ritenuti critici, entro il 17 gennaio 2026, ciascuna per i rispettivi settori e sottosettori di competenza. Alla base dell'identificazione dei soggetti critici, le Asc dovranno considerare, come previsto dall'Art. 8 del decreto legislativo: (i) la valutazione del rischio effettuata dallo Stato; (ii) la strategia nazionale per la resilienza; (iii) il carattere 'essenziale' del servizio fornito; (iv) la collocazione o operatività nel territorio nazionale; (v) gli effetti negativi rilevanti sull'erogazione dei servizi di un eventuale incidente. Saranno poi i soggetti critici stessi a svolgere una successiva valutazione del rischio sulla cui base adottare le misure tecniche di resilienza. La direttiva fornisce quindi gli elementi chiave di cui sopra a supporto degli Stati membri per l'identificazione dei soggetti critici, ma l'individuazione di criteri specifici è rimandata a livello nazionale. Rimane una sfida l'impostazione di una procedura di identificazione basata su una metodologia che sia funzionale e che bilanci realismo (e quindi la selezione di un numero di soggetti non superiore alle capacità istituzionali di gestione, anche amministrativa) e completezza (che riesca quindi a individuare quei soggetti che sembrano secondari ma che possono acquisire una rilevanza "critica" in determinati scenari caratterizzati da effetti a cascata imprevisti).

Un altro ente previsto presso la Pcm è il Cir, Comitato interministeriale per la resilienza, con compiti di proposta di politiche di resilienza, sorveglianza sull'attuazione della relativa strategia, e promozione di misure di rafforzamento della resilienza e di collaborazione fra i soggetti istituzionali e critici (Art. 4). Il Comitato avrà una composizione essenzialmente politica, in quanto riunisce, sotto coordinamento della Pcm, i ministri competenti per i settori di riferimento dei soggetti critici. È tuttavia previsto che possano parteciparvi anche gli operatori stessi dei soggetti critici, oltre che il Presidente della Agenzia per la cybersicurezza nazionale.

© 2024 IAI
ISSN 2280-6164
DOCUMENTI IAI 24 | 11 - OTTOBRE 2024

Presso la Presidenza del Consiglio dei ministri verrà istituita inoltre la Conferenza per la resilienza dei soggetti critici (Crsc), coordinata dal Pcu e composta principalmente da: un rappresentante per ciascuna delle autorità settoriali; un rappresentante del Ministero dell'Interno; uno del Dipartimento della Protezione civile e uno dell'Acn[92]. La Conferenza rappresenterà un momento di condivisione fra gli attori coinvolti e dovrebbe, grazie alla sua composizione, agevolare lo scambio di informazioni e di misure per il rafforzamento della resilienza.

Il termine di 18 mesi per il recepimento nazionale è ritenuto, da alcuni esperti, stringente rispetto alla complessità dei meccanismi dell'attuazione a livello italiano[93]. L'Italia, tuttavia, è attualmente in linea con i termini. Ha inoltre anticipato alcune delle scadenze definite dalla direttiva, come evidenziato da alcuni esperti del settore[94]. Nello schema nazionale, ad esempio, l'adozione della strategia nazionale per la resilienza dei soggetti critici e della analisi del rischio necessaria alla ricognizione, da parte delle autorità settoriali, dei soggetti critici è prevista con sei mesi di anticipo rispetto a quanto previsto dalla Cer (il termine indicato nella direttiva è il 17 gennaio 2026, il decreto legislativo italiano lo anticipa al 17 luglio 2025)[95].

Sotto il profilo della *governance*, è stato evidenziato in modo positivo l'accentramento nella Presidenza del Consiglio in quanto autorità designata alla supervisione dell'attuazione della direttiva, e l'istituzione della Crsc. Viene infatti evidenziato il coordinamento così garantito a livello orizzontale alle autorità competenti per gli specifici settori, sia nell'eventualità di un attacco fisico sia con Acn per la materia *cyber* e per eventuali impatti nella dimensione digitale[96].

Alcuni esperti hanno evidenziato come nella Cer venga ancora mantenuto un approccio settoriale e in un certo senso individualistico, che potrebbe non garantire la giusta attenzione agli aspetti di interdipendenza. In questo contesto, risulta quindi centrale ed essenziale la collaborazione fra i vari ministeri coinvolti e le autorità competenti, e la partecipazione al Comitato per la resilienza dei soggetti critici, sotto il forte coordinamento della Presidenza del Consiglio.

La partecipazione degli operatori al Crsc è un importante elemento che permette di concretizzare il confronto tra settore pubblico e privato nonché un raccordo con la parte cibernetica. Come sottolineato da alcuni esperti, la collaborazione pubblico-privato implica la necessità di stabilire rapporti di fiducia reciproca e di condivisione. Alcuni buoni esempi e pratiche di successo sono dati dai sopracitati accordi di cooperazione tra la Marina Militare e Sparkle nell'ambito delle IC subacquee.

[92] Ibid., Art. 11.3.
[93] Intervista, 26 giugno 2024.
[94] Intervista, 8 luglio 2024.
[95] Decreto legislativo n. 134 del 4 settembre 2024, cit., Art. 6.1.
[96] Intervista, 8 luglio 2024.

ISSN 2280-6164

In questo contesto, i grandi operatori del settore possiedono un'attenzione e una cultura della sicurezza più approfondita, che permette loro di agire con consapevolezza nei confronti delle minacce e delle misure di resilienza da attuare[97]. Diversamente, i piccoli e medi operatori attivi su scala regionale o in ambiti settoriali non tradizionalmente identificati come IC – è il caso ad esempio dei servizi per le acque reflue o della fornitura alimentare – è probabile debbano ancora sviluppare o potenziare tale cultura. È importante, quindi, agire affinché tutti gli operatori raggiungano maggiore consapevolezza del loro ruolo e del contributo che possono dare alla sicurezza nazionale, a supporto e in coordinamento con le istituzioni.

7. Conclusioni e raccomandazioni

7.1 Contesto europeo

Nell'introdurre alcune conclusioni e raccomandazioni, è bene sottolineare nuovamente che l'adozione della direttiva Cer amplia e approfondisce la tendenza ad affrontare un crescente numero di aspetti della sicurezza con un approccio comune a livello europeo, compreso il settore delle infrastrutture critiche. La direttiva lascia margine di manovra e autonomia ai singoli Stati membri, per garantire un approccio sufficientemente flessibile che tenga conto delle specificità e volontà nazionali e che eviti un'eccessiva rigidità, in linea con un contesto europeo e globale che è in continuo mutamento e in cui i tempi dell'emergere di nuove minacce non corrispondono a quelli legislativi.

La sinergia con altri strumenti Ue

L'approccio multi-rischio introdotto dalla Cer dovrebbe facilitare l'adozione di azioni che tengano conto della diversità e trasversalità delle minacce. Questo include anche altri strumenti messi a disposizione dall'Ue che, a vario titolo, mirano ad assicurare una maggiore resilienza e protezione delle IC, come ad esempio il meccanismo di screening degli investimenti diretti esteri, attualmente in fase di miglioramento e revisione. Il meccanismo può essere utilizzato a beneficio di diverse aree oggetto della Cer, essendo quindi complementare alla direttiva nel garantire una protezione olistica dei soggetti critici in Europa. Lo stesso può valere per strumenti, strategie e linee guida relativi a una specifica categoria di IC, come ad esempio la Strategia portuale europea globale (*Comprehensive European Port Strategy*), che dovrebbe essere approvata entro la fine del 2024.

La frammentazione da evitare

In passato, livelli e metodi di trasposizione diversi della precedente direttiva nei sistemi nazionali hanno generato un certo grado di frammentazione. È importante che quest'ultima venga evitata, andando oltre un approccio settoriale e individualistico, che potrebbe non garantire la giusta attenzione agli aspetti di

[97] Intervista, 8 luglio 2024.

ISSN 2280-6164

interdipendenza. Centrale sarà il supporto previsto dalla Commissione e dallo Stato membro che dovrà tenere conto della mole di adempimenti, inclusi quelli burocratici di responsabilità del soggetto critico. L'individuazione, secondo la direttiva, dei soggetti considerati "critici", porterà gli Stati membri non solo a dover predisporre, in raccordo con i soggetti interessati, una protezione appropriata e misure per aumentare la resilienza, ma anche di disporre di un adeguato livello di *situational awareness* che sia transettoriale e *cross-domain*, includendo anche la dimensione subacquea. Questo dovrebbe portare ad avere quello che in gergo militare viene definito come *common operational picture* che potrà essere raggiunto solo attraverso un approccio inter-agenzia e interministeriale e con la partecipazione delle Autorità settoriali competenti (Asc). Allo stesso tempo, una volta identificati i soggetti critici a livello nazionale in linea con quanto richiesto dalla Cer, questi ultimi andrebbero mappati in relazione ai domini operativi e ne andrebbero mappate anche le relative catene di approvvigionamento (*supply chain*) necessarie per il loro funzionamento.

Il rischio di frammentazione va affrontato non solo per quel che riguarda l'implementazione della direttiva negli Stati membri, ma anche nella gestione organica e integrata da parte dell'UE del dossier della resilienza e protezione delle IC, che oggi ricade sotto più direzioni generali della Commissione (ad esempio Affari interni, Protezione civile e operazioni di aiuto umanitario, Energia) in base ai settori coinvolti.

Il vicinato dell'UE e la natura transfrontaliera della minaccia

Vista la natura transfrontaliera dei rischi e minacce alla sicurezza ai quali sono esposte le IC che riguardano anche paesi extra-Ue del vicinato, i progressi e le lezioni apprese di cui gli Stati membri beneficeranno nell'attuazione della Cer andrebbero condivisi ad esempio con i Paesi dei Balcani occidentali. Questi ultimi, se lo ritengono utile e vista la prospettiva della loro adesione, potrebbero mutuare degli elementi nello spirito di armonizzazione minima presente nella direttiva. Ciò potrebbe riguardare ad esempio elementi come l'approccio alla valutazione del rischio o la creazione di una strategia di resilienza indicati dalla Cer. Paesi come l'Albania, la Bosnia Erzegovina, la Macedonia del Nord, la Moldavia, il Montenegro, la Serbia, nonché la Norvegia, la Turchia e l'Ucraina partecipano già in parte a una risposta condivisa UE di fronte a crisi e emergenze, come nel caso della loro adesione al meccanismo di protezione civile dell'Unione[98].

7.2 Contesto italiano

Rapporto pubblico-privato e civile-militare

A livello nazionale l'accentramento nella Presidenza del Consiglio in quanto autorità designata alla supervisione dell'attuazione della direttiva è un elemento

[98] Sito della Direzione generale per la Protezione civile e le operazioni di aiuto umanitario europee: *Meccanismo di protezione civile dell'UE*, https://civil-protection-humanitarian-aid.ec.europa.eu/node/584_it.

ISSN 2280-6164

positivo che può garantire il coordinamento a livello orizzontale alle autorità competenti per gli specifici settori. La partecipazione degli operatori privati alle iniziative e ai forum istituiti ad hoc è un importante elemento che permette di concretizzare il confronto tra settore pubblico e privato, nonché un raccordo con la parte cibernetica rappresentata dalla direttiva Nis2.

L'aumento delle categorie rilevanti per la Cer intensificherà e renderà ancora più urgente un buon coordinamento tra attori pubblici e privati, tanto in ciascun Stato membro quanto a livello europeo. Alla luce di questa moltiplicazione, serviranno una struttura e dei meccanismi decisionali e di risposta sufficientemente flessibili, rapidi ed efficaci. Aumentare la resilienza di una così vasta gamma di soggetti critici richiede un grado di flessibilità e tempestività e un coinvolgimento attivo di tutti i soggetti interessati. Tale coinvolgimento richiede di costruire una base di fiducia reciproca e di condivisione tra Stato e soggetti critici, per garantire un maggiore e reciproco scambio di informazioni e delle lezioni apprese dal momento che i soggetti critici, inclusi gli operatori di IC, possono essere reticenti a condividere informazioni sugli attacchi subiti per non mostrare le proprie vulnerabilità e non danneggiare la propria immagine.

A livello nazionale, poiché il numero dei settori cui ci si rivolge è passato da due a 11, nella mappatura e nell'identificazione dei soggetti sarà importante tener conto della diffusione e dispersione dei vari tipi di IC sul territorio nazionale, attraverso i cinque domini operativi (terrestre, marittimo, aereo, spaziale e cibernetico) e nella dimensione subacquea. Si dovrà tener conto anche della complessa catena logistica e di approvvigionamento dietro le IC che comprende spesso sub-componenti, soggetti secondari ma imprescindibili di una *supply chain* che sovente, per alcuni tipi di soggetti critici, è per natura transnazionale.

Per questo motivo, oltre a un'efficace rapporto pubblico-privato, va migliorata, approfondita e resa più sistematica la cooperazione tra dimensione civile e militare. Gran parte dei rischi e delle minacce cui sono esposte le IC si trovano oggi all'intersezione tra queste due dimensioni, intersezione che viene sistematicamente sfruttata da avversari statali, come dimostrato dal caso ucraino o dalla strategia adottata dalla Cina.

Investimenti in formazione e ricerca

Le misure di resilienza non possono prescindere dall'individuazione di aree di investimento prioritarie. Questo riguarda sia un'adeguata formazione e preparazione del personale, inclusi operatori pubblici e privati, sia lo sviluppo di soluzioni volte a rafforzare la resilienza fisica dei soggetti critici, quali misure di protezione e sorveglianza. La necessità di una risposta rapida di fronte a un possibile incidente da una parte va di pari passo con processi di ricerca, sviluppo e innovazione (R&S&I) sufficientemente rapidi, e dall'altra necessita dell'individuazione di aree di investimento su filoni tecnologici trasversali. Fondamentale è il continuo sostegno da parte dell'Unione europea verso i Paesi membri e verso gli enti attivi in R&S&I tramite, ad esempio, il prossimo Programma di finanziamento alla ricerca *Framework Programme 10*, il Forum strategico per

ISSN 2280-6164

importanti progetti di comune interesse europeo, e il Fondo per la sicurezza interna (*Internal Security Fund*) della Direzione generale Affari interni.

La popolazione

In un momento in cui le IC sono obiettivo sistematico di attacchi e sono esposte a rischi crescenti, e di fronte all'evidenza che tutta la società fa affidamento su determinati servizi, la responsabilizzazione, declinata come maggiore consapevolezza, dei cittadini, oltre che degli Stati membri e dei soggetti critici, dovrebbe essere valorizzata. Ciò specialmente in Paesi come l'Italia dove è carente la cultura della sicurezza e in cui gran parte della popolazione non conosce i soggetti che garantiscono i servizi alla base del funzionamento della loro società, anche attraverso campagne di sensibilizzazione e adeguate linee guida per la cittadinanza. Nel fare questo, si potrebbe guardare ad alcune iniziative verso la cittadinanza intraprese in paesi come la Finlandia e l'Estonia, che applicano un concetto di resilienza basato su una maggiore commistione tra dimensione civile e militare e la cui cittadinanza è preparata ad avere un ruolo più attivo e consapevole in caso di crisi e conosce i comportamenti da adottare. Si tratta di paesi che non possono essere paragonati all'Italia in termini di popolazione, ma ciò non vuol dire che alcune idee non possono essere mutuate o osservate per trarne insegnamenti di cui fare tesoro in vista di una sensibilizzazione a livello nazionale.

aggiornato 11 ottobre 2024

ISSN 2280-6164

Riferimenti

Simon Aebi, Andrin Hauri e Jurgena Kamberaj, "Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication", in *CSS Risk and Resilience Reports*, marzo 2024, https://doi.org/10.3929/ethz-b-000662463

Agenzia per la sicurezza territoriale e la protezione civile, *Alluvione. Oltre 8,8 miliardi di euro: è la stima provvisoria dei danni, di cui 1,8 per interventi necessari a fare fronte all'emergenza*, 15 giugno 2023, https://protezionecivile.regione.emilia-romagna.it/notizie/2023/giugno/alluvione-oltre-8-8-miliardi-di-euro-la-stima-provvisoria-dei-danni-di-cui-1-8-per-interventi-necessari-a-fare-fronte-emergenza

Aleksi Aho, Catarina Midões e Arnis Šnore, "Hybrid Threats in the Financial System", in *Hybrid CoE Working Papers*, n. 8 (giugno 2020), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-8-hybrid-threats-in-the-financial-system

Anna Albanese, "EU Competition Rules in Digital Markets: A Difficult Fit", in *MediaLaws*, 3 marzo 2023, https://www.medialaws.eu/?p=19275

Andrea Baldassarre, "PNRR e trasformazione digitale: ecco gli investimenti e le riforme previste per la digitalizzazione della PA", in *Forum PA*, 26 ottobre 2023, https://www.forumpa.it/?p=110352

Daniel Bellamy, "Mar Rosso: petroliera battente bandiera greca in fiamme dopo un attacco degli Houthi", in *Euronews*, 24 agosto 2024, https://it.euronews.com/2024/08/24/mar-rosso-petroliera-battente-bandiera-greca-in-fiamme-dopo-un-attacco-degli-houthi

Arjen Boin e Martin Lodge, "Designing Resilient Institutions for Transboundary Crisis Management: A Time for Public Administration", in *Public Administration*, vol. 94, n. 2 (giugno 2016), p. 289-298, DOI 10.1111/padm.12264

Elio Calcagno et al., "Le minacce cyber ed elettromagnetiche alle infrastrutture spaziali", in *Documenti IAI*, n. 24|07 (luglio 2024), https://www.iai.it/it/node/18696

Elio Calcagno e Alessandro Marrone (a cura di), "The Underwater Environment and Europe's Defence and Security", in *Documenti IAI*, n. 23|13 (giugno 2023), https://www.iai.it/it/node/17225

Comitato interministeriale per le politiche del mare, *Piano del mare*, 31 luglio 2023, https://www.strutturapolitichemare.gov.it/it/il-piano-del-mare/piano-del-mare-2023-2025

ISSN 2280-6164

Commissione europea, *EU Foreign Direct Investment Screening – 2024 Revision*, Publications Office of the European Union, aggiornato al 24 gennaio 2024, https://doi.org/10.2781/130838

Commissione europea, *La protezione delle infrastrutture critiche nella lotta contro il terrorismo* (COM/2004/702), 20 ottobre 2004, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52004DC0702

Commissione europea, *Regolamento delegato (UE) 2023/2450 del 25 luglio 2023, che integra la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio stabilendo un elenco di servizi essenziali*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32023R2450

Commissione europea-Direzione generale degli Affari interni, *Internal Security Fund (2021-2027)*, 27 agosto 2024, https://home-affairs.ec.europa.eu/node/6905_en

Consiglio dell'Unione europea, *Direttiva 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32008L0114

Decreto legislativo n. 134 del 4 settembre 2024: *Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici...*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;134

Antonio Deruda, *Geopolitica digitale. La competizione globale per il controllo della Rete*, Roma, Carocci, 2024

Agnieszka de Sousa, "Europe's New Security Nightmare Is Food Supply", in *Bloomberg*, 6 marzo 2024, https://www.bloomberg.com/news/newsletters/2024-03-06/europe-s-new-security-nightmare-is-food-supply

Patrizia Di Micco e Giulia Pascuzzi, "Resilienza, ecco la chiave per proteggere le infrastrutture critiche", in *Formiche.net*, 27 settembre 2023, https://formiche.net/?p=1580470

Dipartimento delle informazioni per la sicurezza, *Relazione annuale 2023*, febbraio 2024, https://www.sicurezzanazionale.gov.it/contenuti/relazione-2023

EU-NATO Task Force on the Resilience of Critical Infrastructure, *Final Assessment Report*, 29 giugno 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

EUR-Lex, "Quadro per il controllo degli investimenti esteri diretti", in *Summaries of EU Legislation*, aggiornato al 7 gennaio 2022, https://eur-lex.europa.eu/it/legal-

ISSN 2280-6164

content/summary/screening-framework-for-foreign-direct-investments.html

Dario Fadda, "Attacco Regione Lazio, il garante privacy conferma i gravi errori", in *Cybersecurity360*, 10 aprile 2024, https://www.cybersecurity360.it/?p=75303

Francesca Ghiretti, "China, Italy and COVID-19: Benevolent Support or Strategic Surge?", in *IAI Commentaries*, n. 20|14 (marzo 2020)2022, https://www.iai.it/it/node/11436

Georgios Giannopoulos, Bogdan Dorneanu e Olaf Jonkeren, "Risk Assessment Methodology for Critical Infrastructure Protection", in *JRC Scientific and Policy Reports*, 2013, https://publications.jrc.ec.europa.eu/repository/handle/JRC78292

Laurențiu Mihail Grigore, "The Banking Financial System as a Critical Infrastructure of the Current and Future Society", in *Land Forces Academy Review*, vol. 26, n. 4 (dicembre 2021), p. 418-422, https://doi.org/10.2478/raft-2021-0054

Lily Hay Newman, Matt Burgess e Andy Greenberg, "Come il bug di Crowdstrike ha mandato in tilt i computer di mezzo mondo", in *Wired*, 22 luglio 2024, https://www.wired.it/article/crowdstrike-microsoft-guasto-come-e-successo

Hu Luo, "La Belt and Road Initiative e lo sviluppo di China COSCO Shipping nel Mediterraneo", in *OrizzonteCina*, vol. 9, n. 1 (gennaio-marzo 2018), p. 14-17, https://www.twai.it/?p=3426

ItaliaDomani, *Dal PNRR 4,3 miliardi di euro per il settore idrico*, 11 luglio 2022, https://www.italiadomani.gov.it/content/sogei-ng/it/it/news/dal-pnrr-4-3-miliardi-di-euro-per-il-settore-idrico.html

Eric Luiijf e Marieke Klaver, "Analysis and Lessons Identified on Critical Infrastructures and Dependencies from an Empirical Data Set", in *International Journal of Critical Infrastructure Protection*, vol. 35 (dicembre 2021), articolo 100471, DOI 10.1016/j.ijcip.2021.100471

Alessandro Marrone (a cura di), *Russia-Ukraine War's Strategic Implications*, Roma, IAI, 2024, https://www.iai.it/it/node/18118

Alessandro Marrone e Michele Nones (a cura di), The Expanding Nexus between Space and Defence, in *Documenti IAI*, n. 22|21 (febbraio 2022), https://www.iai.it/it/node/14669

Sarantis Michalopoulos, "How Effective Is China's 'Mask Diplomacy' in Europe?", in *Euractiv*, 26 marzo 2020, https://www.euractiv.com/?p=1447230

Ministero della Difesa, *Strategia di sicurezza e difesa per il Mediterraneo 2022*, maggio 2022, https://ciram.unimc.it/it/focus/diritto-geopolitica-mare/italia-sicurezza-spazi-marittimi/litalia-e-la-sicurezza-degli-spazi-marittimi/

ISSN 2280-6164

StrategiaMediterraneo2022.pdf

Vincenzo Moschetto, "Acque reflue: normative, trattamento e riutilizzo per una gestione sostenibile", in *Blog Polistudio*, 22 marzo 2024, https://blog.polistudio.it/acque-reflue-gestione-sostenibile

Karolina Muti, Ottavia Credi e Giancarlo La Rocca, "Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity", in *Documenti IAI*, n. 23|15 (luglio 2023), https://www.iai.it/it/node/17272

Parlamento europeo, *Risoluzione del 17 gennaio 2024 "Costruire una strategia portuale europea globale"* (2023/2059(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0025_IT.html

Parlamento europeo e Consiglio dell'UE, *Decisione n. 1313/2013/UE del 17 dicembre 2013, su un meccanismo unionale di protezione civile*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32013D1313

Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva Nis 2)*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2555

Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2557

Parlamento europeo e Consiglio dell'UE, *Regolamento (UE) 2019/452 del 19 marzo 2019 che istituisce un quadro per il controllo degli investimenti diretti esteri nell'Unione*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32019R0452

Claudio Paudice, "La privatizzazione del Pireo è stata un affare, ma solo per i cinesi, non per i greci", in *HuffPost Italia*, 5 settembre 2021, https://www.huffingtonpost.it/economia/2021/09/05/news/la_privatizzazione_del_pireo_e_stata_un_affare_ma_solo_per_i_cinesi_non_per_i_greci-5267417

Henrik Praks, "Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage", in *Hybrid CoE Working Papers*, n. 32 (maggio 2024), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage

Steven M. Rinaldi, James P. Peerenboom e Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", in I*EEE Control Systems Magazine*, vol. 21, n. 6 (dicembre 2001), p. 11-25, DOI

ISSN 2280-6164

10.1109/37.969131

Roberto Setola e Giacomo Assenza, "Infrastrutture critiche: la vulnerabilità del settore sanitario", in *ISPI Commentaries*, 8 ottobre 2019, https://www.ispionline.it/it?p=40091

Andrius Sytas e Anne Kauranen, "Three Baltic Pipe and Cable Incidents 'Are Related', Estonia Says", in *Reuters*, 27 ottobre 2023, https://www.reuters.com/world/europe/three-baltic-pipe-cable-incidents-are-related-estonia-says-2023-10-27

Paola Tessari, "La doppia minaccia nucleare che grava sull'Ucraina", in Alessandro Marrone et al., *La guerra russo-ucraina, la sicurezza dell'Europa e la difesa europea*, Roma, IAI, 2022, https://www.iai.it/it/node/16243

Paola Tessari e Karolina Muti, "Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations", in *European Parliament Studies*, luglio 2021, https://doi.org/10.2861/179721

TaRhonda Thomas, "Penn Medicine Official Details How Hospital Stayed Afloat during Tech Outage", in *6abc Philadelphia*, 26 luglio 2024, https://6abc.com/post/15095746

UE e Nato, *Dichiarazione congiunta sulla cooperazione UE-NATO*, 10 gennaio 2023, https://www.consilium.europa.eu/it/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023

United Nations Office on Drugs and Crime, *Key Actions to Protect Submarine Cables from Criminal Activity Identified at UNODC Global Expert Meeting*, 7 febbraio 2019, https://www.unodc.org/unodc/en/frontpage/2019/February/key-actions-to-protect-submarine-cables-from-criminal-activity-identified-at-unodc-global-expert-meeting.html

WaterWide, *Why Government Must Investment in Water, Sanitation, and Hygiene (WASH)*, 13 settembre 2023, https://www.waterwide.org/?p=8209

Brian Wong, "China's Mask Diplomacy", in *The Diplomat*, 25 marzo 2020, https://thediplomat.com/2020/03/chinas-mask-diplomacy

David J. Yu et al., "Logical Interdependencies in Infrastructure: What Are They, How to Identify Them, and What Do They Mean for Infrastructure Risk Analysis?", in *Risk Analysis*, 1 agosto 2024, https://doi.org/10.1111/risa.16555

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 24 | 11 - OTTOBRE 2024

Istituto Affari Internazionali (IAI)

L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, economia internazionale e *governance* globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*AffarInternazionali*), due collane di libri (*Trends and Perspectives in International Politics* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17 - I-00186 Roma, Italia
T +39 06 6976831
iai@iai.it
www.iai.it

Ultimi DOCUMENTI IAI

Direttore: Alessandro Marrone (a.marrone@iai.it)