La minaccia di attacchi a infrastrutture critiche nel settore energetico

Le esplosioni contro Nord Stream 1 e 2

Il 26 settembre 2022, nello spazio di alcune ore, si sono succedute alcune esplosioni ai gasdotti sottomarini Nord Stream 1 e Nord Stream 2, che trasportano gas naturale dalla Federazione Russa alla Germania attraverso il Mar Baltico. Le esplosioni hanno provocato ingenti perdite di gas in mare.

Come suggerito anche dalle dichiarazioni di alcuni *leader* di Stati e di organizzazioni internazionali come la stessa NATO (NATO 2022), le esplosioni appaiono come l'esito di azioni intenzionali di sabotaggio; verosimilmente il responsabile sarebbe un attore statale, considerate le elevate risorse e competenze richieste per l'operazione. Per quanto, secondo le informazioni disponibili, numerosi Stati occidentali abbiano sospettato un intervento della Federazione Russa (si veda Collinson 2022), al momento non vi sono indicazioni chiare sulla responsabilità di tali azioni, che comprensibilmente non sono state rivendicate da alcun attore.

Le indagini in corso sono complicate dal fatto che i gasdotti Nord Stream 1 e 2 sono controllati, rispettivamente per gran parte (51%) e totalmente, dall'impresa russa Gazprom e le esplosioni sono avvenute in acque internazionali, per quanto all'interno delle zone economiche esclusive (*exclusive economic zone*, EEZ) della Danimarca e della Svezia (Braw 2022).

Nell'immediato, le perdite di gas hanno causato un incremento del prezzo del gas naturale, nonostante il fatto che Nord Stream 1 non trasportasse più gas dall'estate 2022 e che Nord Stream 2 non sia ancora entrato in funzione. Inoltre, le perdite di metano nel Mar Baltico hanno provocato seri danni ambientali.

Più in generale, questi danneggiamenti potrebbero aggravare la crisi energetica già manifestatasi in Europa e potrebbero avere l'effetto di rendere ancora più tese le relazioni tra Russia e Stati occidentali.

Infrastrutture critiche e guerra ibrida

Se fosse confermata la responsabilità intenzionale di uno Stato, gli attacchi configurerebbero un caso rilevante di "guerra ibrida" (*hybrid warfare*), basata sull'attacco a infrastrutture critiche.

Si tratterebbe di un atto ostile in "zona grigia" (*gray zone*) che, pur avendo obiettivi coercitivi, non raggiunge ancora la soglia dell'azione militare convenzionale.

Non si può nemmeno escludere del tutto l'eventualità che gli attacchi siano stati pianificati ed eseguiti clandestinamente con lo scopo di attribuire la responsabilità del sabotaggio ad altri attori non implicati nella vicenda, nel quadro di un'operazione sotto falsa bandiera (*false flag operation)* (Jones e Bachmann 2022).

Com'è stato sottolineato, laddove i sabotaggi di Nord Stream fossero opera della Federazione Russa, essi marcherebbero un'*escalation* delle iniziative ostili organizzate da Mosca contro gli Stati occidentali, da sforzi sovversivi come attività di disinformazione a veri e propri attacchi contro infrastrutture critiche (Majkut e Palti-Guzman 2022).

Rischi e sfide per il futuro

Altri casi simili di guerra ibrida potrebbero manifestarsi in futuro. Per esempio, recenti sviluppi di tecnologie subacquee, come droni sottomarini, potrebbero essere impiegati a questo scopo. Com'è stato notato, in aggiunta a gasdotti (tra cui anche Baltic Pipeline, entrato in funzione il giorno successivo al sabotaggio di Nord Stream 1 e 2), un altro obiettivo potenziale di grande rilievo sarebbe

costituito dai cavi sottomarini, cruciali anche per le connessioni di internet (Bueger e Liebetrau 2022; si veda anche Bueger et al. 2022).

Nel settore energetico, attacchi potrebbero riguardare pure infrastrutture per la liquefazione, il trasporto o la rigassificazione di gas naturale liquefatto (GNL), divenuto ancora più saliente per Paesi occidentali come l'Italia dopo lo scoppio dell'attuale guerra in Ucraina.

Attacchi a infrastrutture critiche possono essere lanciati da attori non-statali, come gruppi ribelli o organizzazioni terroristiche (da ultimo, Lee 2022). Si può pensare, ad esempio, agli attacchi eseguiti con droni dal gruppo yemenita degli Huthi contro impianti petroliferi e obiettivi industriali in Arabia Saudita e negli Emirati Arabi Uniti a partire dal 2018. Un altro esempio recente è costituito dall'offensiva scatenata nella primavera del 2021 da jihadisti associati al cosiddetto Stato Islamico / *Daesh* nella città di Palma, nel nord-est del Mozambico; la battaglia ha comportato anche la sospensione di un ampio progetto per la produzione di gas naturale liquefatto nella vicina penisola di Afungi.

In aggiunta ad azioni cinetiche, occorre naturalmente considerare anche gli attacchi cibernetici. Alcuni attacchi *cyber* hanno già colpito infrastrutture energetiche di Stati occidentali, tanto in Europa quanto in Nordamerica. Oltretutto, il processo di transizione energetica (si veda Hafner e Tagliapietra 2020), che richiede la digitalizzazione di reti elettriche, potrebbe condurre a vulnerabilità ancora più pronunciate nel settore energetico (cfr. Overland 2019). Già nel dicembre del 2015 un attacco cibernetico, non rivendicato ufficialmente, colpì la rete elettrica dell'Ucraina, in pieno inverno (si vedano Van de Graaf e Colgan 2017; Sullivan e Kamensky 2017).

Conclusioni

La recente sequenza di esplosioni avvenuta ai danni dei gasdotti Nord Stream 1 e 2 nel Mar Baltico conferma la rilevanza del tema della protezione delle infrastrutture critiche, a fronte di minacce potenziali poste tanto da attori statali, oltre che da attori non-statali (come organizzazioni terroristiche). Nell'attuale contesto politico ed economico, assume ancora più salienza il ruolo delle infrastrutture critiche nel settore energetico (inclusi i sottosettori dell'elettricità, del petrolio e del gas) (cfr. Consiglio dell'Unione Europea 2008).

Bibliografia

- Braw, E. (2022). Russia May Use Nord Stream Aftermath to Cause More Trouble. *Foreign Policy*, 3 ottobre, testo disponibile al sito: https://foreignpolicy.com/2022/10/03/nord-stream-russia-sabotage-investigation/ (consultato il 6 ottobre 2022).
- Bueger, C., Liebetrau, T. (2022). Nord Stream sabotage: the dangers of ignoring subsea politics. *The Loop. ECPR's Political Science Blog*, 7 ottobre, testo disponibile al sito: https://theloop.ecpr.eu/nord-stream-sabotage-the-dangers-of-ignoring-subsea-politics/ (consultato il 10 ottobre 2022).
- Bueger, C., Liebetrau, T., Franken, J. (2022). *Security threats to undersea communications cables and infrastructure – consequences for the EU*. In-Depth Analysis requested by the European Parliament, 1° giugno, testo disponibile al sito: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 (consultato il 10 ottobre 2022).
- Collinson, S. (2022). US and Europe condemn 'sabotage' as suspicion mounts that Russia was behind pipeline leaks. CNN, 29 settembre, testo disponibile al sito: https://edition.cnn.com/2022/09/29/politics/pipeline-leaks-russia-suspicion-analysis/index.html (consultato il 6 ottobre 2022).
- Consiglio dell'Unione Europea (2008). Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.
- Hafner, M., Tagliapietra, S. (a cura di) (2020). *The Geopolitics of the Global Energy Transition*. Cham: Springer.
- Jones, M. P., Bachman, S.-D. (2022). 'Hybrid warfare': Nord Stream attacks show how war is evolving. *The Conversation*, 5 ottobre, testo disponibile al sito: https://theconversation.com/hybrid-warfare-nord-stream-attacks-show-how-war-is-evolving-191764 (consultato il 6 ottobre 2022).
- Lee, C. Y. (2022). Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure. *Energy Research & Social Science* 87 102459.
- Majkut, J., Palti-Guzman, L. (2022). Security Implications of Nord Stream Sabotage. Center for Strategic and International Studies, 9 marzo, testo disponibile al sito: https://www.csis.org/analysis/security-implications-nord-stream-sabotage (consultato il 6 ottobre 2022).
- NATO (2022). Statement by the North Atlantic Council on the damage to gas pipelines. Press release, NATO, 29 settembre, testo disponibile al sito: https://www.nato.int/cps/en/natohq/official_texts_207733.htm (consultato il 6 ottobre 2022).
- Overland, I. (2019). The geopolitics of renewable energy: Debunking four emerging myths. *Energy Research & Social Science* 49: 36-40.
- Sullivan, J. E., Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. *The Electricity Journal* 30: 30-35.
- Van de Graaf, T., Colgan, J. D. (2017). Russian gas games or well-oiled conflict? Energy security and the 2014 Ukraine crisis. *Energy Research & Social Science* 24: 59-64.