La minaccia del cyberterrorismo e i suoi limiti

L'interesse per il cyberterrorismo

Nella nostra epoca, la minaccia del «cyberterrorismo» (*cyberterrorism*) o terrorismo cibernetico ha attirato notevole attenzione e preoccupazione (cf. Golose 2022; Shandler et al. 2023; Onat et al. 2023).

Questi timori raggiunsero probabilmente l'apice all'inizio di questo secolo (Jacobsen 2022, p. 62); la paura per attacchi terroristici su vasta scala (all'epoca, specialmente di matrice jihadista), tanto più a seguito della catastrofe dell'11 settembre, si combinava con i sospetti nei confronti delle nuove tecnologie (Weimann 2005). Negli anni successivi la preoccupazione per questo genere di minaccia probabilmente si è andata progressivamente riducendo. Nondimeno, per esempio, ancora nel 2012, prima dell'ascesa del cosiddetto Stato Islamico (*Islamic State*, IS) o *Daesh*, i risultati di un questionario somministrato a specialisti di sicurezza delle tecnologie informatiche mostravano che il 79% di questi esperti si attendeva un "grande attacco terroristico cibernetico" entro un anno (Conway 2014, p. 103).

Ad oggi, appare invece difficile menzionare in modo inequivocabile un solo atto di cyberterrorismo che abbia provocato vittime o abbia causato direttamente danni materiali.

Prima di discutere la natura e la portata della minaccia posta da questo fenomeno nella nostra epoca, appare utile soffermarsi sulla definizione, non ovvia, di cyberterrorismo.

Il concetto di cyberterrorismo

Il termine "cyberterrorismo" è infatti elusivo (Jarvis e Macdonald 2015; Macdonald et al. 2022). *In primis*, è il concetto stesso di terrorismo a essere notoriamente sfuggente e controverso (tra i molti altri, da ultimo, Schmid 2023). In questa sede, si può sostenere che il terrorismo sia una forma di violenza impiegata deliberatamente da un attore non-statale (un'organizzazione, un gruppo sociale o anche un singolo individuo) contro altre persone (Merari 1993; si veda anche Marone 2013, capitolo 1), sulla base di motivazioni politico/ideologiche, allo scopo di influenzare, intimidire o trasmettere un messaggio a un pubblico più vasto delle vittime immediate della violenza (Vidino et al. 2017, p. 38).

Alla luce di questa definizione, il cyberterrorismo può essere considerato come una specie del più ampio genere del terrorismo, basata sull'uso di attacchi informatici che si traducano in violenza fisica contro persone.

Alcuni studiosi ed esperti, specialmente negli ultimi anni, hanno preferito ampliare la definizione di cyberterrorismo sino ad abbracciare pratiche svolte sul web che, per quanto potenzialmente collegate ad attività terroristiche, non sono immediatamente associate all'effettivo esercizio della violenza (per esempio, propaganda estremistica, reclutamento di militanti, raccolta di fondi per attività terroristiche, ecc.) (cfr. Marone 2019), o persino fenomeni non riguardanti direttamente il terrorismo, come forme radicali di *hacktivism* (*hacking* + *activism*) a fini di protesta (per esempio, Romagna 2020; Mazzini 2023). Come hanno rimarcato altri studiosi (Kenney 2015), tali definizioni di cyberterrorismo in senso estensivo rischiano di essere imprecise e di produrre confusione.

Sebbene ad oggi non vi sia ancora stato nulla che possa vagamente assomigliare a un «11 settembre cibernetico», appare chiaro che organizzazioni terroristiche potrebbero essere interessate ad approfittare di internet per lanciare azioni distruttive. A titolo di esempio, un'organizzazione terroristica potrebbe essere in grado di compromettere il sistema di controllo informatico di una centrale idroelettrica e di aprire le paratoie di una diga, producendo l'improvvisa inondazione di

un'area densamente popolata (per esempio, Giacomello 2004, p. 397 e *passim*). Altri esempi potrebbero essere attacchi cibernetici ai sistemi di controllo del traffico aereo, ferroviario o di altre infrastrutture critiche di un Paese (nel complesso, peraltro, sempre più dipendenti da tecnologie digitali), come strutture sanitarie o infrastrutture energetiche (Venkatachary et al. 2018), comprese persino centrali nucleari (cfr. Kim 2014), con effetti potenzialmente disastrosi.

In realtà, secondo molti studiosi ed esperti (per esempio, Kenney 2015; Jacobsen 2022), attualmente la minaccia del cyberterrorismo sembra essere «inflazionata» sotto molti aspetti. Ad oggi, infatti, le organizzazioni terroristiche e tantomeno i terroristi "solitari" (*lone-actor terrorists*) (per esempio, Weimann 2012; si vedano anche, tra gli altri, Hamm e Spaaij 2017; Kenyon et al. 2021), non hanno dimostrato né le capacità né l'intenzione di lanciare attacchi informatici distruttivi.

Le prossime due sezioni esaminano le ragioni per cui attori impegnati in attività terroristiche non abbiano potuto e/o voluto utilizzare questo tipo di arma.

Capacità

Da un lato, persino organizzazioni sofisticate, dotate di ampie risorse, e influenti – come il sedicente Stato Islamico, specialmente all'apice del suo potere ai tempi dell'auto-proclamato «Califfato» in Siria e Iraq (2014 - 2019), non hanno mostrato le capacità per eseguire veri e propri atti di cyberterrorismo (Bernard 2017). Ad oggi, le innegabili esperienze e competenze ostentate da organizzazioni terroristiche come l'IS nell'ambito della comunicazione e propaganda sul web non si sono trasferite alla capacità di lanciare attacchi informatici distruttivi.

La ragione più ovvia di questo fatto chiama in causa il fattore delle competenze tecniche (per esempio, Giacomello 2020; Jacobsen 2022). L'esecuzione di attacchi informatici, in grado di tradursi immediatamente in violenza fisica nel mondo reale, richiede infatti conoscenze e *skills* decisamente superiori a quelle necessarie per confezionare e distribuire online prodotti di propaganda attraenti o anche per guidare simpatizzanti jihadisti sul web con pratiche di «*mentoring*» a distanza[1].

I «cyberterroristi» devono essere, infatti, in grado di «trasformare in arma» (*weaponize*) il sistema informatico preso di mira. Non è quindi sufficiente che sappiano come individuare le vulnerabilità in un sistema informatico e come accedere allo stesso, ma devono anche possedere conoscenze specifiche sui processi tecnici (per esempio, sui complessi sistemi di controllo del trasporto aereo o ferroviario) che possano produrre l'effetto della distruzione fisica nel mondo reale (Jacobsen 2022, p. 63).

In linea di principio, le organizzazioni terroristiche potrebbero superare questo problema acquisendo dall'esterno i servigi di *hackers* altamente specializzati, in cambio di denaro o con altri metodi. La costruzione di un rapporto di collaborazione con tali "consulenti esterni", se così si può dire, appare tuttavia complicata.

Da una parte, sul lato della domanda, a causa dell'esigenza di mantenere la clandestinità (si vedano Marone 2021; Marone 2023), l'organizzazione terroristica trova solitamente difficoltà nel costruire un rapporto di stretta cooperazione con attori esterni (in particolare, Vertigans 2011; Marone 2021), tanto più se non è nelle condizioni di controllare un territorio (cfr. Lia 2015; Doboš et al. 2019). Oltretutto, la costruzione di una relazione di fiducia nella sfera virtuale tende a essere ancora più complessa, a causa delle opportunità di anonimato e di altri fattori (come l'assenza di segnali di comunicazione non verbale) (per esempio, Green 2009).

[1] È noto che lo Stato Islamico, specialmente durante l'epoca del suo «Califfato» territoriale in Siria e Iraq, ha affidato ad alcuni suoi esponenti, come il francese Rachid Kassim (1987 - 2017), il compito di entrare in contatto su internet con simpatizzanti jihadisti residenti in vari Paesi, supervisionare il loro percorso di radicalizzazione a distanza e guidarli persino nell'esecuzione di attacchi terroristici, senza la necessità di alcune relazione faccia a faccia nel mondo reale tra le due parti. In letteratura questa pratica è nota con il nome di *virtual entrepreneurship* o *virtual planning*. Si vedano, in particolare, Hughes e Meleagrou-Hitchens (2017), Cragin e Weil (2018) e Marone (2019, pp. 19-20).

Dall'altra parte, sul lato dell'offerta, appare generalmente improbabile che *hackers* qualificati, anche qualora già impegnati in attività criminali su internet per scopi di lucro (*cybercrime*), abbiano interesse ad assumersi il rischio di stabilire una collaborazione con un'organizzazione terroristica, che porterebbe con sé anche l'attenzione non desiderata degli apparati di sicurezza nazionale (Jacobsen 2022, p. 64).

In modo analogo, ipoteticamente, organizzazioni terroristiche potrebbero essere sostenute da Stati anche nell'impiego del cyberterrorismo, come già può avvenire per altre attività terroristiche (tra gli altri, Byman 2005). Nondimeno, com'è stato notato, appare piuttosto improbabile che uno Stato decida di affidare questo compito delicato a un attore non-statale, fornendogli risorse umane e finanziarie, quando potrebbe occuparsene direttamente in maniera clandestina (Giacomello 2020, pp. 6-7).

Intenzioni

In aggiunta alle capacità, anche l'intenzione di utilizzare il cyberterrorismo non è ben documentata (Egloff 2021; si veda anche Marone 2019).

Alcuni studiosi ed esperti, presupponendo la natura razionale dei «terroristi» nell'impiego della violenza, hanno sostenuto che, rispetto ad altre tattiche, il cyberterrorismo non sarebbe vantaggioso sulla base di un'analisi costi / benefici (Giacomello 2004; Conway 2014; Giacomello 2020). Secondo questa prospettiva, attacchi più convenzionali, come quelli attraverso autobombe, sarebbero più economici, più semplici da realizzare, più distruttivi nell'immediato e dotati di un maggiore potere simbolico rispetto al cyberterrorismo (Conway 2014, p. 118).

Una ragione di questa apparente riluttanza potrebbe essere legata alla ben nota natura spettacolare del terrorismo (per esempio, Juergensmeyer 2000); numerosi studiosi (per esempio, Conway 2014) hanno sottolineato che attacchi informatici non avrebbero lo stesso elemento di natura «scenografica». Com'è stato osservato (Stohl 2007; Jacobsen 2022, p. 65), inoltre, vi può essere il rischio che un attacco cibernetico possa essere percepito dalla popolazione come un semplice incidente non intenzionale, vanificando lo sforzo di promozione della causa estremistica.

Oltretutto, in generale, le effettive responsabilità per azioni offensive nell'arena virtuale non sono sempre identificabili e aprono quindi la questione generale della rivendicazione della paternità. Nel mondo reale, «offline», un'organizzazione terroristica può già «mentire» in diversi modi (in particolare, Kearns et al. 2014): assumendosi il «merito» di un attacco che non ha eseguito; disconoscendo, all'opposto, la paternità di un attacco che ha effettivamente compiuto; o anche attribuendo falsamente la responsabilità di un attacco (indipendentemente dal fatto che lo abbia effettivamente commesso) a un altro attore.

Il «problema dell'attribuzione» (*attribution problem*) è, però, ancora più acuto nello spazio cibernetico (per esempio, Rid e Buchanan 2015). Un attore potrebbe far apparire alcune attività online di natura offensiva come eseguite da altri attori, comprese organizzazioni terroristiche (o collettivi *cyber* associati a tali organizzazioni), *a danno delle organizzazioni terroristiche* (o quantomeno *non nel loro interesse*) (Alexander e Clifford 2019, p. 24; Marone 2019), anche nel contesto di «operazioni sotto falsa bandiera» (*false flag operations*). Nell'ottobre 2018, ad esempio, le autorità britanniche annunciarono che il gruppo virtuale chiamato «CyberCaliphate», generalmente considerato associato allo Stato Islamico, era stato in realtà promosso dal GRU, il famigerato servizio di *intelligence* delle Forze armate russe (Government of the United Kingdom 2019, citato in Marone 2019, p. 14).

Recentemente alcuni studiosi hanno, infine, avanzato un'altra ipotesi generale, meritevole di ulteriori riflessioni e verifiche empiriche, che chiama in causa fattori legati all'identità sociale degli attori. Lo studioso militare Jeppe T. Jacobsen (2022), in particolare, ha suggerito che le inclinazioni personali dei «terroristi» tendano a non sovrapporsi e a non essere compatibili con quelle tipiche degli *hackers*: mentre i primi non di rado sarebbero personalmente attirati dalla brama di esercitare

violenza fisica contro altre persone, persino con modalità particolarmente raccapriccianti (come il caso dello Stato Islamico ha tristemente mostrato: per esempio, Friis 2018; Lakomy 2019), i secondi sarebbero spinti piuttosto dal desiderio di risolvere una sorta di *puzzle* tecnico nella sfera virtuale (cfr. Mazzini 2023).

Conclusioni

Il contributo ha esaminato le ragioni per cui, ad oggi, la minaccia del cyberterrorismo (in senso stretto) non si è materializzata mettendone in luce i limiti all'impiego sotto il profilo sia delle capacità sia delle intenzioni degli attori.

In conclusione, attualmente rimangono vincoli salienti all'impiego del cyberterrorismo *stricto sensu*, da parte di attori non-statali. Nondimeno, occorre notare che tali vincoli non appaiono insuperabili.

Bibliografia

- Alexander A., Clifford B. (2019). Doxing and Defacements: Examining the Islamic State's Hacking Capabilities. *CTC Sentinel*, 4: 22-28.
- Bernard R. (2017). These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State. *Journal of Cyber Policy*, 2: 255-265.
- Byman D. (2005). *Deadly connections: States that sponsor terrorism*. Cambridge: Cambridge University Press.
- Conway M. (2014), *Reality Check: Assessing the (Un)Likelihood of Cyberterrorism*. In Chen T.M., Jarvis L., Macdonald S., a cura di, *Cyberterrorism: Understanding, Assessment, and Response*, New York: Springer: 103-121.
- Cragin R. K., Weil, A. (2018). "Virtual Planners" in the Arsenal of Islamic State External Operations. *Orbis: A Journal of World Affairs*, 2: 294-312.
- Doboš B., Riegl M., Hansen, S. J. (2019). Territoriality of radical Islam: comparative analysis of jihadist groups' approach to territory. *Small Wars & Insurgencies*, 3: 543-562.
- Egloff F.J. (2021). Intentions and cyberterrorism. In: Cornish P., a cura di, *The Oxford Handbook of Cyber Security*, Oxford: Oxford University Press: 187-200.
- Friis S.M. (2018). 'Behead, burn, crucify, crush': Theorizing the Islamic State's public displays of violence. *European Journal of International Relations*, 2: 243-267.
- Giacomello G. (2004). Bangs for the buck: A cost-benefit analysis of cyberterrorism. *Studies in conflict & terrorism*, 5: 387-408.
- Giacomello G. (2020). Research Note: More Bucks, Still No Bangs? Why a Cost-Benefit Analysis of Cyberterrorism Still Holds True. *Studies in Conflict & Terrorism*, online first.
- Golose P.R. (2022). A comparative analysis of the factors predicting fears of terrorism and cyberterrorism in a developing nation context. *Journal of Ethnic and Cultural Studies*, 4: 106-119.
- Government of the United Kingdom (2019). *UK exposes Russian cyber attacks*. Press release, 4 October, testo disponibile al sito: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks (consultato il 26 giugno 2023).
- Green M.C. (2009). *Trust and social interaction on the Internet*. In: Joinson A., McKenna K.Y.A., Postmes T., Reips U.-D., a cura di, *Oxford Handbook of Internet Psychology*, Oxford: Oxford University Press: 43-51.
- Hamm M. S., Spaaij, R. (2017). *The age of Lone Wolf Terrorism*. New York: Columbia University Press.
- Hughes S., Meleagrou-Hitchens, A. (2017). The Threat to the United States from the Islamic State's Virtual Entrepreneurs. *CTC Sentinel*, 3: 1-8.
- Jacobsen, J.T. (2022). Cyberterrorism. *Perspectives on Terrorism*, 5: 62-72.
- Jarvis L., Macdonald S. (2015). What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence*, 4: 657-678.
- Juergensmeyer M. (2000). *Terror in the Mind of God: The Global Rise of Religious Violence*, Berkeley: University of California Press; trad. it. *Terroristi in nome di Dio*, Roma-Bari, Laterza, 2003.
- Kearns E. M., Conlon B., Young, J. K. (2014). Lying about terrorism. *Studies in Conflict & Terrorism*, 5: 422-439.
- Kenney M. (2015). Cyber-terrorism in a post-Stuxnet world. *Orbis*, 1: 111-128.
- Kenyon J., Baker-Beall C., Binder J. (2021). Lone-actor terrorism–a systematic literature review. *Studies in Conflict & Terrorism*, online first.

- Kim D. Y. (2014). Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, 65: 141-143.
- Lakomy M. (2019). Danse macabre: Gore Images in the Islamic State's "Dabiq" Magazine as a Propaganda Device. *The International Journal of Intelligence, Security, and Public Affairs*, 2: 143-161.
- Lia B. (2015). Understanding jihadi proto-states. *Perspectives on Terrorism*, 4: 31-41.
- Macdonald S., Jarvis L., Lavis S. M. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, 8: 727-752.
- Marone F. (2013). *La politica del terrorismo suicida*. Soveria Mannelli: Rubbettino.
- Marone F., a cura di (2019). *Digital Jihad: Online Communication and Violent Extremism*. Milan: Ledizioni - ISPI.
- Marone F. (2021). Dilemmas of the terrorist underworld: the management of internal secrecy in terrorist organisations. *Behavioral Sciences of Terrorism and Political Aggression*, online first.
- Marone F. (2023). Between paradise and prison: External secrecy and visibility in terrorist organisations. *International social science journal*, 247: 89-101.
- Mazzini F. (2023). *Hackers. Storia e pratiche di una cultura*. Roma-Bari: Laterza.
- Merari A. (1993). Terrorism as a Strategy of Insurgency. *Terrorism and Political Violence*, 4: 213-251.
- Onat I, Bastug M. F., Guler A., Kula S. (2022). Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression*, online first.
- Rid T., Buchanan B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 1-2: 4-37.
- Romagna M. (2020). *Hacktivism: Conceptualization, techniques, and historical view*. In Holt T.H. e Bossler A.M., a cura di, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Palgrave Macmillan – Springer: 743-69.
- Schmid A.P. (2023). *Defining Terrorism.* ICCT Report. International Centre for Counter-Terrorism – The Hague (ICCT).
- Shandler R., Kostyuk N., Oppenheimer H. (2023). Public Opinion and Cyberterrorism. *Public Opinion Quarterly*, 1: 92-119.
- Stohl M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, law and social change*, 46: 223-238.
- Venkatachary S. K., Prasad J., Samikannu R. (2018). Cybersecurity and cyber terrorism-in energy sector – a review. *Journal of Cyber Security Technology*, 3-4: 111-130.
- Vertigans S. (2011). *The Sociology of Terrorism: People, Places and Processes*, Abingdon: Routledge.
- Vidino L., Marone F. Entenmann E. (2017). *Fear thy Neighbor: Radicalization and Jihadist Attacks in the West*. Milan: ISPI – Program on Extremism at George Washington University (PoE GWU) – ICCT-The Hague.
- Weimann G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, 2: 75-90.