Geopolitica.info

FARO ATLANTICO

Cyberterrorismo: approcci della NATO e dell'UE a confronto

Un'analisi delle principali definizioni e misure di contrasto al fenomeno

A cura di *Davide Lo Prete*
Coordinamento di *Alessandro Savini*

20 GIUGNO 2021

Negli ultimi anni, il fenomeno del cyberterrorismo è stato sotto i riflettori dei media dei paesi occidentali, in primis degli Stati Uniti. Questo interesse ha, però, sollevato molteplici perplessità da parte degli esperti di terrorismo. Nello specifico, ci si è chiesti se il fenomeno possa essere ritenuto un pericolo concreto per gli Stati. Per le sue caratteristiche, il cyberterrorismo è difficile da definire e racchiudere entro classificazioni ben delineate. Come per il fenomeno terroristico, gli Stati hanno adottato differenti misure. In questo contesto, si analizzerà il differente approccio della NATO e dell'Unione Europea.

DOMINO – Geopolitical Brief n. 27/ giugno 2021 | Aut. Trib. Roma n. 88 - 6 marzo 2008
Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info
Direttore responsabile: Lorenzo Termine

Un fenomeno di ardua definizione

In quanto fenomeno ibrido, il cyberterrorismo non ha ancora trovato una definizione globalmente riconosciuta come valida[1]. Il termine è stato coniato negli anni '80 da Barry Collin[2] per indicare la convergenza tra cyberspazio e terrorismo[3]. Il primo può essere definito, secondo il *National Institute of Standards and Technology* (NIST), come "rete interdipendente di infrastrutture delle tecnologie dell'informazione che include Internet, le reti di telecomunicazione, i sistemi informativi, i processori e i controllori integrati nelle industrie critiche".[4] Il secondo elemento risulta di più ardua classificazione.

La NATO lo definisce come l'illegale utilizzo o minaccia di utilizzare la forza o la violenza, instillare paura e terrore contro individui o contro le proprietà, al fine di obbligare o intimidire i governi, le società o per ottenere il controllo sulla popolazione, perseguendo scopi politici, religiosi o ideologici[5].

La definizione dell'Unione europea, invece, si ricollega prettamente agli obiettivi, in quanto classifica come atti terroristici tutte quelle azioni che hanno come scopo:

- intimidire gravemente la popolazione;

[1] Plotnek, J., Slay, J., *Cyberterrorism: A homogenized taxonomy and definition,* Elsevier, 2020.
[2] Allora *Senior Research Fellow* dell'*Institute for Security and Intelligence* della California.
[3] Emery, N. E., *The Myth of Cyberterrorism,* Journal of Information Warfare Vol. 4, No. 1 (2005), pp. 80-89.
[4] NIST, *Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5.*
[5] NATO, *NATO's military concept for defence against terrorism,* 2016, (https://www.nato.int/cps/en/natohq/topics_69482.htm#:~:text=a.,political%2C%20religious%20or%20ideological%20objectives

- costringere indebitamente i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto;
- destabilizzare gravemente o distruggere le strutture politiche, costituzionali, economiche o sociali fondamentali di un paese o di un'organizzazione internazionale[6].

La continua evoluzione del fenomeno terroristico rende difficile definire cosa sia esattamente il cyberterrorismo. Alcuni autori ne hanno dato una definizione molto ampia, mentre altri hanno adottato un approccio più restrittivo. Inoltre, gli studi sul fenomeno sono relativamente recenti. Solo a metà degli anni '90 il cyberterrorismo ha iniziato a essere oggetto di studio da parte del mondo accademico e a ricevere attenzione mediatica. In particolare, a partire dagli attentati dell'11 settembre, il termine è stato utilizzato per fare riferimento a una pluralità di atti criminali perpetrati nel dominio cibernetico. Per avere una visione più chiara del fenomeno, è utile – quindi – evidenziare gli elementi che lo differenziano dalle altre minacce informatiche.

Cybercrime

Spesso si fa confusione con il concetto di *cybercrime*. Per capire la differenza sostanziale, è necessario concentrarsi sugli obiettivi dei due fenomeni. I cyberterroristi perseguono scopi politici e ideologici, perlopiù riconducibili a quelli individuati dalla NATO e dall'UE. Una definizione ampiamente condivisa è quella data da Mark Pollitt, ex-

[6] Direttiva UE 2017/541 sulla lotta al terrorismo (https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32017L0541&from=EN

agente dell'FBI, secondo cui il cyberterrorismo consiste in "un attacco premeditato e dovuto a ragioni politiche, contro sistemi informatici, software e dati, che si concretizza in violenza contro obiettivi civili da parte di gruppi subnazionali o attori clandestini"[7]. I *cyber-criminals*, invece, sono spinti da finalità di lucro. Essi considerano la rete non come un obiettivo, ma come un mezzo attraverso cui acquisire informazioni, attuare frodi ed estorsioni. Come sottolineato da Maura Conway, professoressa della Dublin City University, ciò non esclude che i crimini informatici possano essere perpetrati per supportare azioni di terrorismo, ma questo non permette di classificarli come atti di cyberterrorismo[8].

Criminal hacking

Nella letteratura, si discute se sia possibile equiparare i *criminal hackers* ai terroristi. Le finalità di tali gruppi possono essere molteplici, così come gli strumenti. Il problema più grande, in questo caso, è rappresentato dai "cybermercenari", ovvero da *hackers* assoldati da gruppi terroristici per condurre le proprie attività attraverso strumenti cibernetici. Se questo genera enormi vantaggi, quali la possibilità di condurre attacchi molto efficaci e nascondere l'identità dei responsabili, allo stesso tempo, ci sono complicazioni non trascurabili. Innanzitutto, come evidenzia Greg Rattray[9], gli *hackers* agiscono, solitamente, per compromettere i dispositivi target e per ottenere un effetto *disruptive*. Diverso è, invece, compiere azioni con

[7] Pollitt, M., *Cyberterrorism — fact or fancy?*, National Academy Press, 1991
[8] Conway, M., *Cyberterrorism: hype and reality*. In: Armistead, Leigh, (ed.) Information warfare: separating hype from reality. Potomac Books, Inc., 2007, pp. 73-93
[9] Ex-direttore della Cybersecurity del *National Security Council (NSC)*

finalità distruttive che possono portare all'uccisione di civili. Questo rende maggiormente difficile, per i terroristi, trovare *hackers* disposti ad essere assoldati. La seconda problematica riguarda l'essenza dei mercenari: gli *hackers* lavorano per soldi e non per fini politici o ideologici. Questo espone i gruppi terroristici a dei rischi operativi molto alti. Infine, conseguenza di quanto appena detto è la possibilità che questi attori, esterni all'organizzazione, lavorino come agenti sotto copertura per governi ostili[10].

Cyberspazio: arma o obiettivo?

Le differenziazioni fatte fin qui sono necessarie per comprendere meglio in cosa consiste il fenomeno del cyberterrorismo. Le finalità sono considerate, dalla maggior parte della letteratura, l'elemento distintivo. Tuttavia, permane una grande questione aperta: si può considerare cyberterrorismo qualsiasi atto terroristico che concepisca i sistemi informativi sia come arma che come obiettivo? Una delle definizioni più celebri di cyberterrorismo è quella data da Dorothy Denning, durante la testimonianza di fronte allo *Special Oversight Panel on Terrorism* della Camera dei Rappresentanti degli Stati Uniti. Nel 2000, la professoressa della Georgetown University ha definito cyberterrorismo, "qualsiasi attacco o minaccia contro i computers, le reti e le informazioni conservate nelle stesse, per intimidire o minacciare il governo o la popolazione, perseguendo

[10] Rattray G. J., *The Cyberterrorism Threat,* in. Smith J. M. e Thomas C. W., The Terrorism Threat and US Government Response: Operational and Organizational Factors, Colorado, US Air Force Institute for National Security
Studies, 2001

obiettivi politici o sociali. Infine, un attacco di cyberterrorismo deve comportare violenza contro persone o proprietà, oppure generare danni sufficienti a creare paura"[11].

Il cyberspace come strumento

Sarah Gordon e Richard Ford, partendo da questa definizione, danno una diversa interpretazione del fenomeno. I due autori, infatti, sostengono che non si può parlare di cyberterrorismo solo quando gli attacchi prendono di mira i computer. La definizione data dalla Denning corrisponderebbe al "Pure Cyberterrorism[12]", ovvero a quegli atti terroristici che si svolgono puramente nel mondo virtuale e che hanno come target i sistemi informativi. Ma il cyberspace può essere utilizzato anche come strumento. Le organizzazioni terroristiche utilizzano in modo sempre più massiccio Internet per condurre campagne di radicalizzazione e di reclutamento, per aumentare le proprie finanze attraverso attività illecite (quali la vendita di armi e droghe), riuscendo a nascondere la propria identità dietro a server proxy. A questa visione, si oppone quella di Nelson[13] e altri autori che, nel report Cyberterror Prospects and Implications delineano due tipologie di attività: "cyberterror support" e uso terroristico della rete. La prima tipologia fa riferimento all'utilizzo illegale dei sistemi informativi da parte dei terroristi, non

[11] Denning D., Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000 (https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[12] Conway, *Cyberterrorism: hype and reality*

[13] Bill Nelson, ex-direttore del dipartimento *Cyberspace Operations and Defense* dell'*Air Force Space Command*

finalizzato a minacciare le vittime. Queste attività rafforzano altri atti terroristici, amplificandone gli effetti. L'utilizzo della rete per diffondere l'ideologia dei gruppi terroristici e ampliare le loro attività, invece, non è classificabile come cyberterrorismo[14].

Nel report citato, gli autori hanno cercato di delineare le risorse e le abilità necessarie alle organizzazioni terroristiche per compiere determinati atti. Per farlo, il gruppo di ricerca ha definito tre livelli di cyberterror:

- ***Simple-Unstructured***. Indica la capacità di compiere attività di hacking molto semplici contro sistemi individuali, utilizzando strumenti già esistenti. Le organizzazioni hanno scarse capacità di *command and control*, di analisi degli obiettivi e di apprendimento.
- ***Advanced-Structured***. A questo livello, le organizzazioni sono in grado di portare avanti attacchi più sofisticati contro molteplici sistemi e creare o modificare strumenti primitive di hacking. Le organizzazioni possiedono capacità elementari di *command and control*, di analisi degli obiettivi e di apprendimento.
- ***Complex-Coordinated***. Le organizzazioni che raggiungono tale livello possiedono la capacità di mettere in atto attacchi coordinati, in grado di provocare danni su larga scala a strutture ben difese, oltre a saper creare strumenti di hacking molto sofisticati. Le organizzazioni possiedono elevate

[14] Nelson et al., *Cyberterror Prospects and Implications,* Center for the Study of Terrorism and Irregular Warfare, Monterey, 1999

capacità di *command and control*, di analisi degli obiettivi e di apprendimento.

Una definizione comune

Nell'individuare un filo comune a tutte le definizioni di cyberterrorismo presenti in letteratura, Plotnek[15] e Slay[16] hanno delineato alcuni elementi essenziali che caratterizzano il fenomeno. Essi riguardano gli attori, le motivazioni, gli intenti, i mezzi, gli effetti e gli obiettivi. Volendo dare una definizione che metta d'accordo la maggior parte degli esperti, i due autori definiscono il cyberterrorismo come "un attacco o una minaccia premeditata da parte di attori non statali con l'intento di utilizzare il *cyberspace* per produrre conseguenze concrete al fine di infondere paura o minacciare civili, governi o obiettivi non governativi, cercando di raggiungere scopi sociali o ideologici"[17]. Un ulteriore aspetto controverso, come precedentemente riportato, riguarda la differenza tra l'utilizzo terroristico della rete e il cyberterrorismo. Mentre al secondo è stata data un'attenzione mediatica molto importante, il primo è stato ampiamente ignorato[18]. Nonostante ciò, il pericolo maggiore è rappresentato dall'utilizzo del cyberspazio come mezzo attraverso cui diffondere contenuti terroristici. La propaganda online, infatti, permette a tali organizzazioni di reclutare nuovi

[15] Jordan J. Plotnek, assistente di ricerca presso la *University of South Australia* e dottorando presso *La Trobe University*
[16] Jill Slay, professoressa presso la *School of Engineering and Mathematical Sciences* de *La Trobe University* ed esperta di *Cybersecurity*
[17] Plotnek e Slay, *Cyberterrorism: A homogenized taxonomy and definition*
[18] Conway, *Cyberterrorism: hype and reality*

membri senza dover attraversare i confini nazionali. Questo rende ancora più difficile combattere il fenomeno terroristico, che in tal modo si diffonde più facilmente e riesce a creare nuove alleanze transnazionali. L'analisi fin qui fatta delle varie interpretazioni del termine cyberterrorismo è essenziale al fine di procedere alla comprensione della minaccia rappresentata da tale fenomeno. È altresì utile per capire quali possono essere gli strumenti legislativi, diplomatici, di polizia e di intelligence fondamentali per contrastare questa nuova forma di terrorismo. Una volta chiariti alcuni aspetti più teorici, quindi, è necessario comprendere se il cyberterrorismo, in quanto tale, rappresenta una minaccia concreta e quali misure hanno adottato gli Stati per contrastarlo, verificando se queste si siano rivelate efficaci o meno. Quanto detto finora, infatti, permetterà una comprensione più profonda dell'approccio di due attori sovranazionali al cyberterrorismo: la NATO e l'Unione Europea.

La NATO e l'evoluzione delle minacce cibernetiche

Sebbene la NATO abbia riconosciuto il *cyberspace* come dominio operativo soltanto nel 2016, le prime minacce cibernetiche per l'Alleanza risalgono ai primi anni 2000. Durante la guerra in Kosovo, infatti, i server della NATO sono stati vittima di molteplici attacchi informatici da parte di hacker al servizio dell'ex Repubblica di Jugoslavia. Nello specifico, circa 100 server dell'organizzazione sono stati

colpiti da attacchi di tipo DDoS (*Distributed Denial of Service*) dopo i bombardamenti operati dai paesi alleati ai danni delle forze jugoslave. Gli attacchi alle reti della NATO hanno generato effetti particolarmente distruttivi per le comunicazioni esterne e interne.

Soltanto nel 2007, però, l'Alleanza ha acquisito consapevolezza della distruttività delle minacce cibernetiche. La campagna di attacchi informatici che ha colpito l'Estonia in quell'anno, infatti, ha messo in luce la vulnerabilità delle infrastrutture critiche degli Stati. I siti web di vari parlamenti, banche, ministeri e giornali sono stati vittime di attacchi DDoS da parte di attori *nation-state* russi. Ciò ha determinato una risposta concreta della NATO, che ha istituito – nel 2008 – il *Cooperative Cyber Defense Center of Excellence (CCDCOE)*. Il fine ultimo del centro è quello di fungere da propulsore per il rafforzamento delle capacità cibernetiche difensive della NATO. Il fatto che abbia sede in un paese confinante con la Russia è significativo della sua funzione di deterrente. Nel 2013, un gruppo di esperti, sotto l'egida del *CCDCOE,* ha realizzato un manuale, il Tallinn Manual, che raccoglie le norme di diritto internazionali applicabili alla guerra cibernetica. Nonostante non sia considerato un documento ufficiale della NATO e quindi non abbia carattere vincolante per i Paesi membri, il manuale – di cui è stata pubblicata una seconda edizione rivisitata nel 2017[19] – rappresenta, forse, il più importante documento giuridico in questo ambito. Sebbene l'attacco russo non sia

[19] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, editore generale Schmitt N. M, 2017

configurabile come cyberterrorismo, in primis perché condotto da attori *nation-state*, esso è emblematico delle potenzialità distruttive del *cyberspace*. I terroristi potrebbero utilizzare gli attacchi DDoS per colpire infrastrutture critiche di interi Stati, creando una crisi cibernetica nazionale. In questo senso, sono emblematici i casi del *Colonial Pipeline*, il più grande oleodotto statunitense, e quello della JBS, la più grande azienda di lavorazione della carne al mondo. Entrambe le società, a maggio 2021, sono state colpite da un attacco *ransomware*, un *malware* (software malevolo) installato su un *device* che è in grado di bloccare la *business continuity*[20] aziendale finché non viene pagato un riscatto (*ransom*). In entrambi i casi, le società hanno pagato il riscatto, anche se l'FBI è riuscita a recuperare la metà del denaro nel caso del Colonial Pipeline. Questi attacchi mettono in luce come i gruppi di *criminal hackers* siano in grado di paralizzare le infrastrutture critiche di uno Stato. Gli attacchi sono stati ricollegati ad attori russi, probabilmente sponsorizzati dal governo. Ciò farebbe venir meno la matrice terroristica di tale attacco. Tuttavia, il Dipartimento di Giustizia americano ha dichiarato di voler adottare, contro tali azioni, lo stesso approccio aggressivo messo in atto contro il terrorismo[21]. Questo rappresenta un passo in avanti nella strada verso una nuova consapevolezza delle minacce cibernetiche. A dispetto di ciò, è necessario

[20] La capacità di un'azienda di continuare a erogare prodotti o servizi a livelli accettabili in seguito a un incidente.
[21] Bing C., *Exclusive: U.S. to give ransomware hacks similar priority as terrorism*, 03-06-2021 (https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/ ultimo accesso: 21/06/2021)

capire se il cyberterrorismo costituisca una minaccia reale o solo ipotetica per l'Alleanza.

Cyberterrorismo: quale minaccia per la NATO

Nel periodo successivo agli attacchi dell'11 settembre, i media americani hanno paventato più volte la concreta possibilità di massicci attacchi cibernetici da parte di al-Qaeda. Nonostante ciò, questo non si è mai verificato. Non per questo però il pericolo del cyberterrorismo deve essere sottovalutato. Vanno tenuti in conto i fattori di vantaggio che i terroristi hanno nell'utilizzare il *cyberspace*, sia come strumento che come obiettivo. Gabriel Weimann, professore di comunicazione all'Università di Haifa, ha individuato 5 ragioni per cui il cyberterrorismo è più attraente rispetto agli atti terroristici tradizionali:

- È meno costoso;
- Permette una maggiore anonimità;
- C'è una maggiore varietà e quantità di potenziali target;
- È possibile condurre tali atti da remoto;
- Può essere colpito un più ampio numero di persone[22].

Negli ultimi anni, la NATO ha incluso la minaccia cyber tra le sue priorità. Durante il Summit del Galles del 2014, i rappresentanti degli Stati membri hanno riconosciuto la *cyber defence* come parte integrante della funzione di difesa collettiva dell'Alleanza e sono stati unanimi nell'individuare il diritto internazionale come framework normativo applicabile nel cyberspazio. Il vero *turning point* è giunto nel 2016, con il riconoscimento dello spazio cibernetico come

[22] Weimann G., *Cyberterrorism: How Real Is the Threat?,* United States Institute Of Peace, 2004

dominio operativo alla stregua di terra, aria e mare. Ciò ha significato non solo attribuire un ruolo chiave alla difesa cibernetica per la sicurezza della NATO, ma anche permettere azioni di rappresaglia. Si tratta di una misura fondamentale di *active defense*, come definita da Seymour E. Goodman, Jessica Kirk e Megan Kirk[23]. Secondo tali autori, la maggior parte di queste attività possono essere condotte dai governi nazionali e attraverso alcune forme di cooperazione intergovernativa.

NATO 2030: maggiore contrasto alle minacce cibernetiche e al terrorismo

È proprio quanto ha ribadito il Segretario Generale, Jens Stoltenberg, durante il discorso di presentazione dell'iniziativa NATO 2030[24]. Il terrorismo e gli attacchi informatici sono stati individuati come minacce di elevata intensità da parte del Segretario Generale. Nonostante l'attenzione sia stata posta sulla capacità degli Stati ostili di dotarsi di un arsenale di *cyberweapons*, non si può trascurare l'attività condotta dai gruppi terroristici nel *cyberspace*. Lo scopo dell'iniziativa NATO 2030 è proprio quello di permettere all'Alleanza di adattarsi ai cambiamenti e all'evoluzione del panorama delle minacce. Una misura chiave di questo adattamento è sicuramente la creazione di un *Cyberspace Operations Centre*. Il nuovo centro, che dovrebbe diventare operativo a partire dal 2023 e la cui creazione è stata stabilita nel 2018 durante il vertice di Bruxelles, sarà lo strumento principale per l'attuazione di contromisure nel

[23] Seymour E. Goodman, Jessica C. Kirk, Megan H. Kirk, *Cyberspace as a medium for terrorists*, in Technological Forecasting and Social Change, Volume 74, Issue 2, Febbraio 2007, pp 193-210
[24] Discorso integrale disponibile al link: https://www.nato.int/cps/en/natohq/opinions_176197.htm

cyberspace. Questo diverrebbe il punto centrale non solo dell'*active defense*, alla luce della funzione di difesa collettiva della NATO, ma anche di azioni di tipo *offensive*. Per quanto riguarda le altre misure di difesa, Goodman mette in luce la necessità di adottare misure di *passive defense*, ovvero il rafforzamento delle infrastrutture IT. Tuttavia, mentre nel caso delle misure di rappresaglia, queste potrebbero fungere da deterrente, nel secondo caso, i terroristi saranno spinti ad innalzare il livello di minaccia, cercando nuove vulnerabilità. Sebbene questo ruolo spetti prettamente agli Stati, la NATO, oltre ad aver adottato *policies* e documenti strategici per innalzare il livello di difesa, si è dotata di alcuni strumenti chiave per il contrasto agli attacchi cibernetici. Il CCDCOE organizza annualmente importanti esercitazioni di *cyber defense* a cui prendono parte rappresentanti dei Paesi membri, principalmente in ambito militare. L'esercitazione *Locked Shields*, organizzata a partire dal 2010, è volta a far acquisire agli esperti che vi partecipano nuove capacità di difesa cibernetica, attraverso la simulazione di attacchi alle infrastrutture critiche nazionali. La *Cyber Coalition*, invece, è condotta per mettere alla prova i processi decisionali, le procedure tecniche e le capacità di cooperazione tra gli Stati membri. Infine, la *Crossed Swords* viene svolta per testare le capacità e le abilità che i partecipanti devono possedere per pianificare e mettere in atto un'operazione cibernetica che coinvolga anche elementi degli altri domini. Affrontare la minaccia cibernetica è, per la NATO, di assoluta priorità. Adattare la propria struttura e la propria strategia all'evoluzione delle organizzazioni terroristiche è uno dei

punti cardine dell'iniziativa NATO 2030. La chiave per affrontare il cyberterrorismo in modo più efficace consiste nel rafforzamento della cooperazione tra Stati. Questo deve avvenire sia attraverso la partecipazione alle esercitazioni sopra citate, strumento fondamentale della *passive defense*, sia attraverso l'elaborazione di *policies* maggiormente restrittive per limitare il cyberterrorismo.

L'UE e la difesa del cyberspace

Riprendendo la definizione di Collinn, il cyberterrorismo è caratterizzato dalla convergenza del *cyberspace* e del terrorismo. È fondamentale, quindi, comprendere quale sia lo sforzo dell'UE nel contrastare questi due fenomeni. La Direttiva UE 2017/541 – già citata – dà una chiara definizione di cosa sia il terrorismo. Esso rappresenta una minaccia per la popolazione e per le istituzioni, col fine di intimidire e perseguire obiettivi sociali, politici o ideologici. I rischi nel *cyberspace* sono aumentati costantemente negli ultimi anni. Nel 2020, in particolare, sono cresciuti in modo vertiginoso gli attacchi contro le infrastrutture critiche[25]. Gli ospedali sono stati gli obiettivi più sensibili, a causa della pandemia e del basso livello di cybersecurity di tali strutture. I recenti attacchi al Colonial Pipeline e alla JBS hanno messo in luce l'importanza di creare un perimetro di sicurezza cibernetica che garantisca il maggior livello di

[25] Walsh N. P., *Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic*, CNN, 10-06-2021 (https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html

resilienza possibile. In questo senso, nel 2016, è stata adottata la Direttiva NIS (*Network and Information Security*)[26], la quale ha innalzato il livello di *cybersecurity* degli Stati membri, stabilendo degli obblighi per gli operatori di servizi essenziali (OSE), sia in termini di misure da implementare, sia in termini di notifica degli incidenti informatici. Tali operatori sono stati individuati in settori critici, quali l'energia, la sanità, i trasporti e la finanza. Si tratta di obiettivi particolarmente sensibili, in quanto i terroristi troverebbero molto conveniente attaccare centrali elettriche, aeroporti, ferrovie. Il *cyberspace* rappresenta un vettore incredibilmente invitante per gli atti terroristici, a causa dell'anonimità e della possibilità di causare danni fisici su larga scala. A tale riguardo, l'UE si sta adoperando su più fronti per accrescere la ciberresilienza, combattere la criminalità informatica e proteggere le infrastrutture critiche[27]. Di recente, infatti, le istituzioni europee hanno presentato una proposta di revisione della direttiva NIS, considerata non più adeguata al panorama attuale delle minacce. Inoltre, la nuova direttiva dovrebbe incrementare la resilienza e la capacità di risposta agli incidenti degli enti pubblici e privati.

La lotta alla propaganda terroristica online

Per quanto concerne il cyberterrorismo, l'UE ha profuso un grande sforzo nel contrasto alla diffusione dei contenuti terroristici online. Di recente, infatti, il Parlamento Europeo

[26] Direttiva NIS (https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=EN)
[27] Cibersicurezza: la risposta dell'UE alle minacce informatiche (https://www.consilium.europa.eu/it/policies/cybersecurity/

ha approvato il Regolamento[28] per la prevenzione di tale fenomeno. L'UE ha riconosciuto i vantaggi che il *cyberspace*, in particolare Internet, comporta per le attività terroristiche. La propaganda e il reclutamento possono essere messi in atto in modo anonimo, a livello internazionale e con costi molto bassi. Il nuovo regolamento UE concede alle autorità degli Stati membri il potere di obbligare le piattaforme di *hosting* (o prestatori di servizi) a rimuovere i contenuti terroristici online o di disabilitarne l'accesso in tutti gli Stati membri. Ciò dovrà avvenire entro un'ora e si applica a tutti i prestatori che offrono servizi all'UE. Ma cosa si intende per terrorismo? Sarebbe necessario che tutti gli Stati membri adottassero una definizione comune del fenomeno. Quella utilizzata dalla Polizia di Stato italiana è molto chiara e comprensiva delle diverse caratteristiche prese in esame nella prima parte. Il cyberterrorismo è definito come "l'utilizzo del cyberspazio (Internet) per fini terroristici, ovvero, diffondere la paura e il panico nella popolazione destabilizzando l'ordine e la sicurezza pubblica, per ragioni politiche, ideologiche o religiose. Il cyberterrorismo si manifesta con due attività prevalenti: propaganda e attività diretta." Includere anche la distinzione tra queste due attività è fondamentale. Il *cyberspace*, come ribadito più volte, può essere utilizzato sia come strumento che come obiettivo. La propaganda permette alle organizzazioni terroristiche di incrementare il proprio raggio di azione. L'attività diretta,

[28] Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0640&from=EN

invece, consente di mostrare la propria potenza di fuoco e produce effetti nel mondo fisico.

L'approccio europeo a doppio binario

Per questo, è necessario continuare sulla strada del duplice approccio. Da un lato, attraverso il contrasto alla diffusione dei contenuti; dall'altro, attraverso normative e *policies*, incrementare il livello di *cybersecurity* degli Stati membri, per prevenire gli attacchi alle infrastrutture critiche, la cui compromissione potrebbe generare una crisi cibernetica nazionale o europea. Lo scorso anno, poi, l'UE ha imposto le prime sanzioni per attacchi informatici. Nel 2019, il Consiglio dell'Unione Europea ha stabilito un framework normativo che permette di adottare sanzioni nei confronti di persone o entità responsabili di attacchi informatici o tentati attacchi informatici. Tali misure restrittive, includono il divieto per le persone che viaggiano verso l'UE e il congelamento dei beni delle persone o entità. Tali misure possono essere applicate anche per contrastare il fenomeno del cyberterrorismo. Esse fungono da deterrente, elemento fondamentale di *defense*, come definita da Goodman. L'UE è dotata, quindi, di un quadro normativo efficace per rispondere alle minacce poste. Tuttavia, il fattore fondamentale per la prevenzione e il contrasto ai *cyberattacks*, come nel caso della NATO, è la cooperazione tra gli Stati membri, che devono implementare in modo adeguato e puntuale le direttive comunitarie.

Conclusioni

Individuare una definizione globalmente condivisa di cyberterrorismo non è opera inutile. Piuttosto, questo rappresenta il primo passo per poter contrastare a livello internazionale tale fenomeno. Come evidenziato finora, il pericolo maggiore è rappresentato non dall'attività diretta, ma dalla propaganda e dalla condivisione di contenuti terroristici online. Nonostante ciò, non vanno sottovalutate le capacità dei terroristi di condurre attacchi cibernetici su larga scala, contro infrastrutture critiche.

Perché, allora, non c'è mai stato un attacco terroristico di tale entità? Secondo Maura Conway[29], il cyberterrorismo non rappresenta una minaccia così concreta, per una serie di ragioni. Innanzitutto, le organizzazioni terroristiche (islamiche) non possiedono grandi conoscenze informatiche; in secondo luogo, assoldare hackers con grandi capacità comprometterebbe la sicurezza operativa. Infine, ai terroristi non interesserebbe rimanere anonimi. Ad interessanti conclusioni, è giunto anche Thomas Chen[30], che in *Cyberterrorism after Stuxnet* ha cercato di analizzare il fenomeno del cyberterrorismo indagando gli intenti e i mezzi utilizzati dalle organizzazioni terroristiche, prima e dopo Stuxnet, la prima arma cibernetica della storia, utilizzata da Stati Uniti e Israele per compromettere la centrale nucleare di Natanz, in Iran. Secondo Chen, i

[29] Professoressa di Sicurezza Internazionale presso la *School of Law and Government* dell'Università di Dublino
[30] Professore di *Cybersecurity* presso la *School of Engeenering and Mathematical Sciences* della *City University* di Londra

terroristi, pur dipendendo da Internet per condurre molte attività, non sono interessati all'attuazione di attacchi informatici sofisticati. Inoltre, nonostante le infrastrutture critiche presentino delle vulnerabilità ampiamente sfruttabili nel *cyberspace*, i terroristi continuerebbero a preferire gli attacchi fisici perché questi sono meno costosi[31]. La crescita degli attacchi informatici alle infrastrutture critiche registrata nell'ultimo anno sembrerebbe smentire queste conclusioni. È necessario comprendere se tali atti possono essere classificati come cyberterrorismo. Le dichiarazioni del governo statunitense sembrano andare in quella direzione. La volontà del Dipartimento della Giustizia di equiparare i *ransomware* che hanno paralizzato Colonial Pipeline e JBS ad atti terroristici sembra chiarire ulteriormente i dubbi a riguardo. Alla luce di ciò, la NATO e l'Unione Europea devono comprendere quali siano i rischi reali e potenziali per le infrastrutture critiche. Queste, come visto, sono il bersaglio prediletto in quanto la loro compromissione potrebbe contribuire ad infondere terrore nella società e minacciare i governi, finalità principali degli atti terroristici. Come ha sottolineato Dorothy Denning, poi, per comprendere la potenziale minaccia del cyberterrorismo, si devono considerare due fattori: la vulnerabilità degli obiettivi, che potrebbe portare a danni consistenti, e la volontà e la capacità – dei terroristi – di perpetrare attacchi contro tali obiettivi. Nell'ultimo anno, gli ospedali e le strutture sanitarie sono divenuti

[31] Chen T., *Cyberterrorism After Stuxnet*, Strategic Studies Institute e U.S. Army War College Press, 2014

particolarmente vulnerabili, come dimostrato dalla crescita degli attacchi informatici rivolti contro di essi. Uno strumento essenziale è la redazione di documenti che mappano le minacce, come ad esempio i *Threat Landscape Reports* pubblicati dalla *European Union Agency for Cybersecurity* (ENISA).

La capacità delle due organizzazioni di adottare delle misure concrete ed efficaci per prevenire e rispondere alle minacce cibernetiche sarà fondamentale per garantire la sicurezza degli Stati membri. In questo modo, la NATO si affermerebbe – anche nel *cyberspace* – quale garante del principio di difesa collettiva. L'Unione Europea, invece, raggiungerebbe gli obiettivi di creare un ciberspazio aperto e sicuro per contribuire a una maggiore fiducia dei cittadini negli strumenti e nei servizi digitali.

Geopolitica.info

Davide Lo Prete

Studente di Laurea Magistrale in Relazioni Internazionali, indirizzo Pace, Guerra e Sicurezza presso l'Università degli Studi di Roma Tre. Collabora con l'area Cyber e Tech di Geopolitica.info. Tra i suoi interessi vi sono la cybersecurity, l'Intelligenza Artificiale, gli affari militari e le relazioni Euro-Atlantiche.

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info
www.geopolitica.info | centrostudi@geopolitica.info