Sul concetto di
Cyberterrorismo e di Cyber(in)sicurezza.

da Pablo A. Mazurier

Abstract in English:

The purpose of this paper is to highlight how cybersecurity and cyberterrorism are *constructed* concepts, serving to the interests of those cyber actors who are capable to impose their own discourse and logic to the rest of the digital social ecosystem. In the second part, the concept of cyberterrorism is analyzed focusing on the four main approaches, putting in evidence the different needs, interests and benefits involved and offering a better analysis of this multifaceted phenomenon and its effects not only in cyberspace and in society.

Abstract in Italiano:

L'obiettivo di questo articolo è duplice. Da un lato mette in evidenza, con l'aiuto di tre esempi, come la cybersicurezza e il cyberterrorismo sono concetti *costruiti*, che rispondono agli interessi dei cyber attori che sono in grado d'imporre i loro discorsi e posizioni al resto dell'ecosistema sociale digitale. Nella seconda parte, si approfondisce la concettualizzazione del cyberterrorismo, proponendo quattro modalità di studio di tale fenomeno, che rispondono a diverse necessità ed interessi e che, se utilizzate in modo equilibrato, permettono una miglior analisi del fenomeno e dei suoi effetti non solo sul cyberspazio ma anche sulla società stessa.

Abstract en Español:

El objetivo de este artículo es doble. Por un lado muestra, con la ayuda de tres ejemplos, cómo la ciberseguridad y el ciberterrorismo son conceptos *construídos*, que responden a intereses de aquellos ciber actores que pueden imponer sus discursos y puntos de vista al resto del ecosistema social digital. En la segunda parte del artículo se busca profundizar en la conceptualización del ciberterrorismo, proponiendo cuatro modalidades de estudio de tal fenómeno, que responden a distintas necesidades e intereses y que, si usadas en modo claro y equilibrado, pueden permitir un mejor análisis del fenómeno y de sus efectos no sólo en el ciberespacio sino también en la sociedad actual.

1. Sulla costruzione del concetto di cyberterrorismo.

Terrorismo e cyberterrorismo hanno da sempre avuto uno speciale vincolo con lo Stato, dato che essi rappresentano una minaccia aperta all'ordine pubblico e alla sovranità statale. In questo contesto, i governi costruiscono delle narrative sul terrorismo, adattandolo ai propri messaggi, interessi e contesto. Nel caso del cyberterrorismo, esso non solo implica una re-edizione della vecchia minaccia di terrorismo con nuovi strumenti, ma significa anche un'opportunità per i governi di riposizionarsi nel nuovo e tanto incerto contesto di digitalità globale. Nonostante la

globalizzazione le nuove tecnologie hanno eroso il potere sovrano degli Stati, la guerra contro il cyber terrore crea un forte consenso pubblico, legittimando il controllo del governo e la sorveglianza sul cyberspazio, e toglie l'attenzione sulle carenze ed inadeguatezze del settore pubblico per centrarle su un target specifico. Puntando direttamente su un antagonista specifico, i governi possono controllare la narrativa, l'agenda-setting ed i processi di policy-making, ottenendo più legittimità per imporre misure di controllo, sorveglianza e attacco cibernetico. [1] Ecco tre esempi che illustrano questa prassi.

Durante gli anni Novanta, gli Stati e i media hanno creato le più colorite metafore per inflazionare la minaccia cyberterroristica, avvertendo del pericolo di un "Phanthom Menace", "Cyber-Scare", "Cyber Doom", "Cyber-Katrinas", "Guerrilla Warfare in Cyberspace" and "Digital Pearl Harbor". [2] In modo indiretto, questi termini servirono per sottolineare quanto importante era il ruolo preventivo del potere statale nel controllare le attività degli utenti su Internet mentre rafforzavano nell'inconscio collettivo l'idea che, se non erano ancora avvenute queste tragiche evenienze, era solo dovuto al lavoro delle forze dell'ordine. Nonostante la costruzione di questo scenario d'insicurezza digitale, il cyberterrorismo continua ad essere non più di una minaccia astratta[3] e, di conseguenza, i settori pubblici e privati sono spesso più "carenti in cybersicurezza che in caffè"[4]

Il secondo esempio ci mostra come lo Stato modella il concetto di cyberterrorismo per adattarlo alle proprie convenienze. Durante i primi anni dello sviluppo d'Internet, quando gli Stati Uniti erano visti come pilastri del mondo libero, gli analisti in sicurezza del presidente Clinton aumentarono la narrativa della paura[5] e puntarono l'attenzione sui cyberterroristi che si opponevano alla egemonia statale. La prima presidenza di G.W. Bush, invece, decise di virare verso un approccio più tradizionale e stato-centrico, raddrizzando la narrativa verso gli "Stati canaglia" che avevano la capacità di progettare e lanciare cyberattacchi contro infrastrutture critiche degli USA e dei suoi alleati. Dopo l'11 Settembre, sulla base della logica discorsiva di "guerra contro il terrorismo", quasi tutte le minacce contro interessi pubblici e privati nel cyberspazio che riguardavano "il commercio internazionale o le comunicazioni degli Stati Uniti" erano considerate atti di cyberterrorismo. [6] Da quel momento in poi, i governi americani hanno usato indistintamente i termini cyberterrorismo e cyberguerra per descrivere differenti tipi di cyber minacce, adattando i loro discorsi alla gravità e percezione di ogni situazione specifica sotto analisi.

Il terzo esempio mette in evidenza come sia il governo di Bush che quello di Obama hanno costruito una forte narrativa simbolica basata sulla semplice idea che i terroristi usano la cyber pirateria come fonte di raccolta di fondi per finanziare le loro attività terroristiche, "derubando l'economia americana di miliardi di dollari". [7] In

[1] Erikson, J. (2007), p. 61.
[2] Morozov, E. (2009).
[3] *"The destruction of byts and bytes never directly killed anybody or destroyed any buildings."* Erikson, J. (2007), p. 78. Anche su questo argomento Rid, T. (2013).
[4] Ozeren, S. et al. (2007), p. 263.
[5] Erikson, J. and Giacomello, G. (2007), p. 67.
[6] Erickson, J. (2007), p. 72.
[7] McCarthy, D. (2015), p. 137.

questo modo, il governo è riuscito a mettere assieme tre interessi nazionali nello stesso discorso: la lotta contro il terrorismo, la protezione internazionale del settore dell'innovazione e la legittimità per il governo d'implementare misure straordinarie di controllo, sorveglianza e di attacco nel dominio cyber.

Come illustrato attraverso questi tre esempi, il cyberterrorismo risulta un fenomeno più complesso che la semplice combinazione fra terrorismo e cyberspazio.

2. I quattro approcci per definire il cyberterrorismo.

Come costruzione sociale, esso può essere descritto in modo più preciso attraverso l'analisi congiunta di quattro approcci: quello oggettivo, quello soggettivo, quello basato sull'obiettivo e quello a forma di griglia o matrice.

a) Da un punto di vista oggettivo, ovvero basato sull'azione concreta, l'atto cyberterroristico si configura attraverso la concorrenza di tre fattori materiali essenziali: 1) la presenza di strumenti elettronici, di tecnologia informatica e/o di strutture internet e loro dati, utilizzati sia come strumento per portare avanti degli attacchi che come objettivo di essi; [8] 2) una motivazione terroristica –ideologica, etnica o religiosa, 3) l'esecutore dell'atto deve essere una persona o gruppo di persone non vincolate ad uno Stato né agenzia governativa alcuna.

Ognuno di questi tre elementi è necessario per la configurazione dell' atto cyberterroristico. Se l'azione manca del primo elemento, l'atto sarà considerato semplicemente come un atto terroristico. Se manca la motivazione, potrà essere considerato come un cyber attacco o un cyber crimine. E se viene a mancare il terzo elemento, cioè se l'esecutore è vincolato ad uno Stato, si considererà più un atto di cyberguerra o di *informationl warfare*.[9]

Questi tre elementi essenziali si completano con le azioni tipiche: portare avanti degli attacchi o altre azioni comunemente vincolate col terrorismo.

Focalizzato sulla descrizione dell'azione, l'approccio oggettivo è comunemente usato dai settori legislativi e di disegno di politiche pubbliche, grazie alla sua applicabilità universale, la sua chiarezza e precisione concettuale, imparzialità, coerenza interna ed integrità nella descrizione di cos'è e cosa non è il cyberterrorismo.

[8] L'immagine tradizionale dell'attacco cyberterrorista consiste, infatti, nell'uso di ICTs e/o strutture d'internet sia come strumento d'attacco che come obiettivo da colpire. Gordon, S. and Ford, R. (2003), p. 7.

[9] Quando l'azione è condotta da parte di uno Stato contro reti e dispositive di un'altro Stato, si considera un atto di cyberguerra. Ayala, L. (2016), p. 49.

Fig. 1: Struttura dell'atto cyberterroristico secondo l'approccio obiettivo.

Elementi Essenziali	Azioni	Applicazione
1. computer and internet technology used as tool or as target 2. Terrorist motivation (ideological, ethnical, religious) 3. Actor: Single person or Group (not States nor its agents)	A) to perpetrate attacks	In real life: intimidation, blackmailing, threatens human lives,[10] to cause relevant material damage[11] or public fear and concern,[12] challenging or jeopardizing the State security.
		To online networks/systems, communication infrastructures and data[13]
	B) to act in support or promotion of terrorism	Propaganda, fundraising, recruitment, communication, plotting, indoctrination, radicalization, logistics, planning, material dissemination, support infrastructure.

b) L'approccio soggettivo non punta verso l'azione ma analizza l'esecutore. Questa prospettiva è la preferita da molte istituzioni governative, in particolar modo di quelle che devono portare avanti le investigazioni, non solo per prevenire futuri cyber attacchi ma anche per smantellare reti di propaganda, indottrinamento, progettazione di attacchi e reclutamento di lupi solitari.[14]

Quando un potenziale terrorista o gruppo di terroristi è identificato, molte delle volte grazie al suo vincolo con un'organizzazione terroristica già riconosciuta, le autorità di solito applicano tecniche di sorveglianza cibernetica e data mining su tutta la rete sociale dei soggetti, nonostante la crescente preoccupazione pubblica sulla stigmatizzazione sociale e la violazione della privacy di cittadini innocenti ignari di essere a contatto con soggetti potenzialmente pericolosi. Negli Stati Uniti, ogni dispositivo, posto, azione, comunicazione e persona connessa fino al terzo grado di contatto col soggetto sorvegliato è considerato un rischio potenziale per la sicurezza nazionale.

Alcuni autori considerano che qualsiasi utilizzo d'internet e di tecnologie da parte di un terrorista costituisce *per se* un atto di cyberterrorismo. [15] Tuttavia, altri sottolineano che è preferibile utilizzare una definizione *actor-neutral* di cyberterrorismo,[16] mettendo in rilievo la necessità di muoversi da una visione tipicamente centrata sul soggetto per tener conto della "natura intersoggettiva e

[10] La legge della Nuova Zelanda stabilisce che l'attacco contro un'infrastruttura deve "essere in grado di mettere in pericolo vite umane". Chen, T.M. et al. (eds.) (2014), p. 20-21.
[11] Per molte fonti legislative ed academiche, la violenza contro persone o il forte danneggiamento economico sono elementi esenziali del cyberterrorismo. Conway, M. (2004) "Cyberterrorism: media myth or clear and present danger?" in: Kan, P.R. and Irwin J (eds)(2004), p. 84.
[12] Ai cyberattacchi manca una dimensione simbolica di teatralità, e quindi risultano meno attraenti per I terroristi che gli attacchi convenzionali. Chen, T.M. et al. (eds.) (2014), p. 114-5.
[13] Secondo Addicott, "i cyberattacchi comprendono attività che sono in grado di arrestare, corrompere, inabilitare e distruggere informazione contenuta in computer o reti di computer." In Ozeren, S. (2007), p. 260.
[14] "Lo scenario più probabile del quale dobbiamo preoccuparci è quello di un lupo solitario e non di una grande e bene organizzata operazione terroristica.." Discorso del Presidente Obama Aug. 16, 2011, cit. in Weimann, G. (2015).
[15] Desouza KC, Hensgen T (2003), p. 388.
[16] Stohl, in Chen, T.M. et al. (eds.) (2014), p. 90.

costruita della conoscenza da parte dei terroristi", ovvero "le motivazioni ed esperienze personali dei terroristi, la loro mentalità e visione del mondo." [17]

c) *L'approccio incentrato sull'obiettivo,* o *target approach,* considera come cyberterrorismo "l'utilizzo di strumenti di reti di computer per il danneggiamento o messa fuori uso di infrastrutture critiche." [18] In questo modo, si sta definendo una tipologia di azione attraverso il vincolo fra un intermediario specifico con un obiettivo specifico, evitando ogni discussione sull'esecutore, sull'azione e sulla motivazione. Sebbene questa definizione di *per se* risulta frammentata ed incompleta, [19] essa ci serve come adeguato complemento degli altri due approcci analizzati prima. Mettendo in evidenza la criticità dell'obiettivo a colpire, questo approccio permette alle autorità, da una parte, di distinguere fra cyberterroristi e attivisti politici, [20] e, dall'altra di focalizzare le politiche sulla prevenzione, attraverso l'identificazione e protezione delle infrastrutture critiche, la pronta individuazione di vulnerabilità e la progettazione di un piano di protezione, risk management e misure di deterrenza contro cyber attachi di questo tipo.

d) *L'approccio a forma di griglia o matrice*, o *matrix approach*, considera una lista di elementi comuni senza una gerarchia uniforme né una struttura classificatoria. Questi elementi sono: persone (o gruppi), posti (esecutori, complici e vittime), metodologie/modalità di azioni, strumenti, obiettivi, affiliazioni e motivazioni. [21] Un'altro studio simile offre un elenco diverso, includendo: origine dell'attacco-gravità (identità dell'attaccante), origine dell'attacco al sistema (tipo di IT e sistemi), motivazione, obiettivo-gravità (popolazione, organizzazione, identità), obiettivo-tipologia, risultato desiderato e risultati ottenuti. [22] Il vantaggio di questo approccio aperto è radicato nella sua flessibilità, una caratteristica necessaria per comparare diverse definizioni da parte di diversi governi e per determinare come queste si adattano ai parametri comuni. [23]

Da una prospettiva costruttivista, il cyberterrorismo costituisce una realtà sociale in costante cambiamento, elaborata sulla base di discorsi, simboli, esperienze, riflessioni, identificazione e coinvolgimento sociale. L'analisi di questo fenomeno, quindi, si sposta da quello che il cyberterrorismo in realtà è, a più complesse domande su come il cyberterrorismo è percepito, come è visuto, se viene esagerato o ignorato. Per tutto ciò, i discorsi sulla cyber sicurezza in generale, e sul cyberterrorismo in particolare, devono tener conto della forte strumentalizzazione di cui è oggetto.

[17] Hülsse, R. and Spencer, A. (2008), p. 574.
[18] Lewis, J. A. (2002).
[19] Cyberterrorismo e cyberguerra hanno lo stesso obiettivo: danneggiare l'infrastruttura critica e I sistemi di controllo vincolati l'uno con l'altro nei confine del cyberspazio. Ayala, L. (2016), p. 49.
[20] Quasi tutti sono d'accordo che arrestare o bloccare un sito web del governo, per motive politici, non sia un atto di terrorismo, bensì una dimostrazione di attivismo politico. Chen, T.M. et al. (2014), p. 2.
[21] Gordon, S. and Ford, R. (2003), p. 5.
[22] Ariely, in Chen, T.M. et al. (2014), p. 178.
[23] Gordon, S. and Ford, R. (2003), op. cit., p. 5.

Bibliografia.

- Ayala, L. (2016), *Cybersecurity Lexicon*, Apress, New York.
- Carr, M. (2016), *US Power and the Internet in International Relations*, Palgrave MacMillan, New York.
- Chen, T.M. *et al.* (eds.) (2014), *Cyberterrorism. Understanding, Assessment, and Response*, Springer, New York.
- Desouza KC, Hensgen T (2003), *Semiotic emergent framework to address the reality of cyberterrorism*, Technol Forecast Soc Change 70(4):388.
- Erikson, J. and Giacomello, G. (2007), *International Relations and Security in the Digital Age*, Routledge, London - New York.
- Gordon, S. and Ford, R. (2003), "Cyberterrorism? Symantec Security Response White Paper", Cupertino.
- Hülsse, R. and Spencer, A. (2008), "The Metaphor of Terror: Terrorism Studies and the Constructivist Turn", in Security Dialogue, vol. 39, no. 6
- Kan, P.R. and Irwin J (eds)(2004), *War and virtual war: the challenges to communities*, Rodopi, Amsterdam.
- Lewis, J. A. (2002) "Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats", Centre for Strategic and International Studies (Online) http://www.csis.org
- McCarthy, D. (2015), P*ower, Information, Technology, and International Relations Theory. The Power and Politics of US Foreign Policy and Internet*, Palgrave MacMillan, London.
- Morozov, E. (2009), "Cyber-Scare:The Exaggerated Fears over Digital Warfare", Boston Review, July/August 2009. http://bostonreview.net/archives/BR34.4/morozov.php
- Ozeren, S. et al. (2007), *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, IOS Press, Amsterdam
- Rid, T. (2013), *Cyber War will not take place*, Oxford University Press, Oxford.
- Weimann, G. (2015), *Terrorism in Cyberspace. The Next Generation*, Columbia Univ. Press, New York.