



Center for Cyber Security and  
International Relations Studies

# *Minacce ibride, che sta facendo l'Europa per la sicurezza e il ruolo dell'Italia*

**Pablo Mazurier**



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

**Research Analysis**

*Luglio 2018*



## **Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici,  
Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

**<https://www.cssii.unifi.it/ls-6-cyber-security.html>**

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.



# ***Minacce ibride, che sta facendo l'Europa per la sicurezza e il ruolo dell'Italia***

**Pablo Mazurier**



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

**Research Analysis**

*Luglio 2018*

## Riguardo all'autore

**Pablo Andrés Mazurier** è Phd in "Politics, Human Rights and Sustainability" alla Scuola Superiore Sant'Anna di Pisa con un progetto di ricerca in Internet Governance. E' stato ricercatore al King's College, University of London (UK) e all'Institut d'Études Européennes of the Université Libre de Bruxelles (Belgium). Ha ottenuto una Laurea Specialistica con lode in Studi Europei e Internazionali all'Università di Trento, con una tesi in "Sociology of Legal Regimes at the Global level", e una laurea in Giurisprudenza all'Austral University (Argentina).

## **Minacce ibride, che sta facendo l'Europa per la sicurezza e il ruolo dell'Italia<sup>1</sup>**

Negli ultimi anni si è parlato molto di minacce ibride, concetto molto ampio che include casi così diversi come gli atti violenti perpetrati da civili filorussi militarizzati nell'Est dell'Ucraina, i cyber attacchi contro strutture critiche pubbliche e private nei Paesi Baltici e le massicce campagne di fake news e di manipolazione dei social network durante la Brexit e le elezioni presidenziali francesi.

### **Che cosa sono le minacce ibride**

Originariamente, in ambito militare si sviluppò il concetto di “guerre asimmetriche o ibride” per parlare di quei conflitti armati nei quali coesistevano elementi “non convenzionali” con quelli convenzionali, senza offrire una specifica tipologia di riferimento. Col passare degli anni, il dibattito mutò verso l'esistenza di “conflitti ibridi” e, più recentemente, “minacce ibride”. Mentre molti studiosi cercano ancora di sviluppare definizioni specifiche, esiste una tendenza generale a lasciare un certo grado di flessibilità nella definizione, puntando più a studiare lo specifico contesto che serve allo sviluppo di dinamiche di ibridismo. Possiamo citare qui tre di queste riflessioni.

In Cina, il libro “Guerra senza restrizioni” di Qiao Liang e Wang Xiangsui<sup>2</sup> ipotizzò, già nel 1999, la possibilità di coinvolgere nei

---

<sup>1</sup> La seguente analisi è apparsa su <https://www.agendadigitale.eu> il giorno 18 luglio 2018 ed è reperibile al seguente link <https://www.agendadigitale.eu/sicurezza/minacce-ibride-che-sta-facendo-leuropa-per-la-sicurezza-e-il-ruolo-dellitalia/>.

<sup>2</sup> Liang, Q. and Xiangsui, W. (1999), *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing.

conflitti armati dei fattori che sono stati da sempre considerati esterni al mondo militare. Soltanto attraverso una guerra non convenzionale su tutti gli ambiti della società, le potenze militarmente più arretrate potevano avere qualche possibilità di vincere contro le superpotenze globali.

Più recentemente, nel 2013, il Capo di Stato Maggiore dell'esercito russo, Gen. Valery Gerasimov, riprendendo la logica di Liang e Xiangsui, sviluppa la sua propria "dottrina Gerasimov" che stabilisce che le regole della guerra sono cambiate in modo sostanziale e che in questo stato di guerra costante dove si utilizzano mezzi non militari per raggiungere obiettivi politici e strategici in modo più efficace che attraverso le armi, si devono trovare e sfruttare tutte le vulnerabilità degli avversari in ogni momento e su ogni campo.

Anche la NATO ha sviluppato una definizione sulla base del proprio approccio onnicomprensivo verso le situazioni di crisi, definendo le minacce ibride come il "lato oscuro" di questo approccio, cioè l'utilizzo di mezzi di ogni tipo, in particolar modo di mezzi di propaganda, di movimenti popolari e risorse digitali e di attacchi cyber, con l'obiettivo di destabilizzare le società e le istituzioni dei paesi alleati<sup>3</sup>.

## **La risposta europea**

Dalla metà 2016, l'Unione europea ha cominciato a collaborare con la NATO nell'implementazione di procedure operative nelle aree di cyber sicurezza relative alle minacce ibride<sup>4</sup>.

---

<sup>3</sup> Ref. Cusumanu, E. and Corbe, M. (eds.) (2018), *A Civil-Military Response to Hybrid Threats*, Palgrave MacMillan, New York, p. 2.

<sup>4</sup> Attraverso una Dichiarazione Congiunta su un insieme di misure da implementare, vedi su <https://www.hybridcoe.fi/wp-content/uploads/2017/08/Common-set-of-proposals-for-the-implementation-of-the->

In simultaneo, la Commissione Europea, insieme al Parlamento ed al Consiglio europeo, pubblica un quadro congiunto per contrastare le minacce ibride<sup>5</sup>. In questo documento si sottolinea come il concetto di “minacce ibride” deve rimanere flessibile per rispondere adeguatamente ai cambiamenti del contesto sociale. Tuttavia si chiarisce la necessità di sviluppare difese contro le ambiguità che ostacolano i processi decisionali a livello locale, nazionale e comunitario, e contro lo sfruttamento da parte dei nemici dei punti deboli delle istituzioni e delle società.

Sebbene queste istituzioni europee riconoscano che la responsabilità principale ricada sugli Stati membri, esse sottolineano la necessità di affrontare in modo più efficace queste minacce attraverso una risposta coordinata, sulla base dei principi di solidarietà ed assistenza reciproca stabiliti nel trattato di Lisbona.

Imitando la vincente esperienza e il successo dei Centri d’Eccellenza della NATO, l’Unione Europea ha creato, nell’aprile 2017, un Centro di eccellenza sulle minacce ibride a Helsinki<sup>6</sup>, che conta attualmente 15 paesi partecipanti: Estonia, Finlandia, Francia, Germania, Italia, Latvia, Lituania, Norvegia, Polonia, Spagna, Svezia, Danimarca, il Regno Unito e gli Stati Uniti.

Col supporto istituzionale della NATO, questo CoE cerca di sviluppare, da una parte, una rete istituzionale a livello diplomatico ed intergovernamentale, mentre, dall’altra parte, promuove la ricerca e

---

[Joint-Declaration-2.pdf](#).

<sup>5</sup> Commissione Europea, JOIN (2016) 18 FINAL, Bruxelles, 6 giugno 2016, vedi su <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016JC0018&from=EN>.

<sup>6</sup> Sito online ufficiale: <https://www.hybridcoe.fi>.

la formazione di funzionari pubblici ed altri quadri delle amministrazioni locali.

## **Le opportunità per l'Italia**

L'Italia partecipa alle operazioni del CoE dallo scorso aprile 2018, quando l'ambasciatore in Finlandia Gabriele Altana firmò il Memorandum d'Intesa<sup>7</sup>. In quell'occasione, il direttore del CoE, Matti Saarelainen, sottolineò come la partecipazione dell'Italia sin dalla creazione del Centro, "ha migliorato il bilancio geografico del Center". Sebbene esiste ancora un chiaro sbilanciamento verso il Nord-Est europeo, soprattutto a causa della necessità e preoccupazione dei paesi di quell'area di contrastare le minacce russe, l'inclusione dell'Italia può contribuire alla creazione di un asse Roma-Madrid per portare ad Helsinki una voce comune sulle problematiche più consone all'area mediterranea.

Nello specifico, una crisi così rilevante come quella dell'immigrazione illegale attraverso il Mediterraneo, può essere interpretata e gestita anche come una minaccia ibrida, dato che al suo trattamento prettamente militare e transfrontaliero, si aggiungono pressioni geopolitiche (come la minaccia di Erdogan), diverso trattamento dei media, manifestazioni popolari, divisioni, conflitti sociali interni e la proliferazione di fake news<sup>8</sup> sulla quantità degli sbarchi, sulla pericolosità dei migranti, e su tanti altri versanti.

Inoltre, l'Italia dovrebbe guardare anche alla Spagna per imitare alcune misure politiche davvero innovative. Ad esempio, da marzo

---

<sup>7</sup> Riferimento dalla sezione "Notizie" del Centro di Eccellenza:  
<https://www.hybridcoe.fi/news/italy-joins-hybrid-coe/>.

<sup>8</sup> Vedi <https://www.agendadigitale.eu/tag/fake-news/>.



2018, il governo dell'ormai ex premier Rajoy decise di nominare la diplomatica Julia Alicia Olmo y Romero come la prima ambasciatrice in missione speciale per le minacce ibride e la cyber sicurezza<sup>9</sup>. Inquadrata all'interno della Strategia di Sicurezza Nazionale del 2017, questa innovazione istituzionale ha contribuito al dibattito ed alla pubblicità su queste tematiche, e l'ambasciatrice Olmo è stata una presenza fissa in tutte le conferenze, atti istituzionali e congressi accademici relativi alle tematiche cyber.

Un'alternativa alla misura governativa spagnola è quella adottata dal governo della Repubblica Ceca, il cui Ministero dell'Interno ha creato un Centro contro il Terrorismo e le Minacce Ibride, attivo dal primo gennaio 2017. Tuttavia, come specifica la normativa ceca, questo Centro non ha competenze legislative, né di polizia cyber né di intelligence<sup>10</sup>.

## **Lo sviluppo in Italia del trattamento delle minacce ibride**

Resta ancora un ultimo e cruciale punto sul quale risulta essenziale discutere lo sviluppo in Italia del trattamento delle minacce ibride. Se, come sottolineano Cederberg ed Eronen<sup>11</sup>, ci troviamo in uno stato globale di lotta perpetua dove la battaglia si lotta in ogni settore della società, il nostro paese ha bisogno, soprattutto in ambito digitale e di cyber sicurezza, di un grande accordo fra tutti gli attori sociali per

---

<sup>9</sup> Vedi <https://www.agendadigitale.eu/tag/cyber-security/>.

<sup>10</sup> Vedi <http://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx>.

<sup>11</sup> Cederberg, A. and Eronen, P. (2015), "How can Societies be Defended against Hybrid Threats?", in Strategic Security Analysis, Sept. 2015 N. 9, GCSP, Geneva, disponibile su [http://www.defenddemocracy.org/content/uploads/documents/GCSP\\_Strategic\\_Security\\_Analysis\\_-\\_How\\_can\\_Societies\\_be\\_Defended\\_against\\_Hybrid\\_Threats.pdf](http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf).

costruire linee di difesa integrali e onnicomprensive, per costruire una società sempre più sicura e resiliente.



**Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

<https://www.cssii.unifi.it/ls-6-cyber-security.html>