Guerre ibride: quali le risposte possibili?

di Giuliana Giuseppina Carboni

Abstract: *Hybrid wars: the possible answers* - The contributions presented in the session dedicated to hybrid wars have concerned three fundamental aspects: the definition of the topic, the formants to regulate it, the plurality of systems involved in the regulation. The authors have called attention to the criticism of the concept of hybrid warfare. The term hybrid warfare underscores the importance of the combination of conventional and irregular tactics. Ambiguity is the main element of this definition. Consequently, the question of how to fight hybrid threats with the tools of the law is difficult. Traditional rules-based order seems to be insufficient, both at the international and European levels.

Keywords: Hybrid warfare; International law; Ius in bellum; Cyberwarfare; International humanitarian law.

1. Le guerre ibride: la difficoltà della definizione

I contributi presentati nella sessione dedicata alle guerre ibride hanno riguardato tre aspetti fondamentali: la definizione del tema, i formanti, la pluralità degli ordinamenti coinvolti nella regolazione.

Il concetto di guerra ha subito, negli ultimi decenni, una sostanziale estensione, di cui sono testimonianza le diverse espressioni usate come equivalenti del termine guerra (conflitto e intervento armato, operazioni di peace keeping, guerra preventiva, guerra al terrorismo, per citarne alcuni[1]) che ha condotto autorevole dottrina a parlare di rimozione della nozione stessa di guerra[2]. Non sono d'aiuto, a questo fine, le Costituzioni democratiche, che regolano le dichiarazioni di guerra senza definirla. E non manca chi ritiene addirittura impossibile una definizione precisa di guerra[3].

[1] Da ultimo, la guerra in Ucraina ha proposto un'altra tipologia di azione, ovvero la cessione di equipaggiamenti militari. Si veda l'attenta disamina di G. Marazzita, "*Guerra vietata, legittima e necessaria*", in *federalismi.it*, 2022, n. 22. Per una lettura di alcuni conflitti recenti, condotti sotto la bandiera della NATO, collocabili tra le guerre c.d. umanitarie, di difesa, e simili, si veda F. Bilancia, C. De Fiores, P. Marsocci, L. Ronchetti, M. Ruotolo, *Guerra e Costituzione*, in *costituzionalismo.it*, 2023, n. 1.

[2] A. Vedaschi, *Guerra e Costituzioni: spunti dalla comparazione*, in *Osservatorio AIC*, 2022, n. 3, 47 ss. L'autrice chiama in causa sia alcune debolezze strutturali delle Carte democratiche, sia le applicazioni che di esse hanno dato gli organi costituzionali.

[3] Nel loro contributo, Andrea Gatti e Matteo Giannelli ricordano nel suo noto libro, K. Von Clausewitz, *Della guerra*, Milano, 2005, sottolinea come sia lo Stato sovrano a decidere se e come entrare in guerra. Ancor prima negava la possibilità di definizione

DPCE online
ISSN: 2037-6677

Se i confini della guerra appaiono sempre meno chiari per i conflitti "classici", il compito definitorio si presenta quanto mai arduo per le guerre ibride[4].

E tuttavia, appare necessario, e i casi dell'Ucraina e quello recentissimo di Israele lo dimostrano, riconoscere e denunciare l'inizio di una guerra[5]. Necessario perché si possano applicare, anzitutto, le norme del diritto internazionale e del diritto interno. Il primo, per il tramite dell'art. 2 par. 4 della Carta delle NU, qualifica come illeciti la minaccia e l'uso della forza armata «contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite»[6]. Il secondo, in virtù dell'art. 11, indica i limiti entro i quali il nostro ordinamento consente l'uso della guerra[7]. Il diritto costituzionale nazionale appare però sempre meno adeguato a fornire risposte efficaci a guerre atipiche e globali[8].

Partendo dalla considerazione che ogni guerra comporta l'uso deliberativo della forza da parte di uno Stato o di altra organizzazione, per ottenere un certo risultato a danno di altri Stati o organizzazioni[9], si deve constatare che negli ultimi decenni sono emersi nuovi obiettivi e nuovi mezzi di conflitto, che è quantomeno problematico inquadrare nello ius in bellum. Le minacce ibride rappresentano un rischio reale per gli Stati perché il loro obiettivo è destabilizzare l'avversario attraverso mezzi e tattiche sempre più numerose, che non sono facili da individuare, né tantomeno da attribuire a un autore, sia esso o meno uno Stato[10].

C. Schmitt, *Inter pacem et bellum nihil medium*, in *L'unità del mondo e altri saggi*, Roma, 1994 (1939).

[4] L'espressione venne adotta per la prima volta da F. Hoffman, *Conflict in the 21-st century. The rise of hybrid wars*, Potomac Institute for Policy Studies, Arlington, USA, 2007, che ha individuato la caratteristica delle guerre ibride nell'essere una combinazione di armi convenzionali, tattiche irregolari, terrorismo e comportamenti criminali.

[5] Lo sottolinea M. Iovane, *Il conflitto ucraino e il diritto internazionale: prime osservazioni, in Osservatorio AIC*, 2022, n. 3, 6 ss, ricordando che a queste affermazioni consegue l'applicazione dello ius belli.

[6] All'Art. 2, para. 4, della Carta delle NU. La definizione di guerra di aggressione è affidata alla Risoluzione 3314 adottata dall'Assemblea Generale (AG) delle NU il 14 dicembre 1974 «1. For the purpose of this Statute, "crime of aggression" means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations».

[7] Il tema della compatibilità con l'art. 11 della Costituzione italiana delle operazioni militari è ricorrente. Da ultimo P. Rossi, *La compatibilità con la costituzione italiana e il diritto internazionale dell'invio di armi all'Ucraina*, in *SIDIBlog*, 8 marzo 2022, disponibile all'indirizzo http://www.sidiblog.org/2022/03/08/la-compatibilita-con-la-costituzione-italiana-e-il-diritto-internazionale-dellinvio-di- armi-allucraina/.

[8] G. Azzariti, (a cura di), *Il costituzionalismo democratico moderno può sopravvivere alla guerra?*, Napoli, 2022.

[9] I protagonisti dell'uso della forza sono principalmente gli Stati, ma come dimostra il conflitto tra Israele e Hamas, non è questa l'unica possibile declinazione soggettiva della guerra.

[10] S. Sanz-Caballero, *The concepts and laws applicable to hybrid threats, with a special focus on Europe*, in *Humanities and Social Sciences Communications*, 2023, 10:360 | *https://doi.org/10.1057/s41599-023-01864-y*.

Ibrida è la guerra che colpisce beni eterogenei, diversi dalla vita delle persone e dalle cose materiali, e/o utilizza mezzi non convenzionali di attacco e difesa. Il confine tra guerra convenzionale e guerra ibrida è sottile, ed è determinato dal fatto che le armi non convenzionali vengano usate in un contesto di guerra convenzionale[11]. Colpire le fonti di approvvigionamento energetico e alimentare non è propriamente guerra ibrida, ma lo è attaccare le banche dati dei sistemi sanitari mentre i paesi di appartenenza sono coinvolti in un conflitto. Quanto ai mezzi, la gestione dei flussi migratori e gli attacchi ai sistemi informatici sono alcune delle nuove "armi" di cui si servono i Paesi belligeranti. Potremo aggiungere fenomeni come il lobbying nelle istituzioni di governo (pensando alla UE) e le politiche di acquisto di risorse sui mercati internazionali. In definitiva, anche se non esiste un elemento univoco di definizione, le guerre ibride comprendono atti illegali o che violano principi etici, portati a compimento da attori statali e non per destabilizzare una società.

Alcuni esempi di guerra ibrida sono stati descritti nelle relazioni della sessione, ma va subito precisato che si tratta di un numero limitato di casi, rispetto alle esperienze registrate negli ultimi anni.

In una linea di classificazione che parte dall'esame di obiettivi e mezzi lontani dalla guerra tradizionale, per avvicinarsi al prototipo dell'aggressione materiale, si colloca il ricorso all'immigrazione come mezzo di pressione, descritti nella relazione di Claudia De Simone. Il dato da sottolineare è che i migranti, essendo arma e vittima al contempo, possono essere oggetto di politiche di aiuto e di respingimento. La pressione esercitata sull'Unione europea da sud (Tunisia) e da est (Turchia e Bielorussia) da organizzazioni criminali manovrate da Stati intenzionati a ottenere vantaggi, e a costringere altri Stati a scelte indesiderate, può configurarsi come un attacco alla stabilità e al diritto degli ordinamenti attaccati.

Infatti, oltre all'impatto sulle comunità e gli apparati di accoglienza, la penetrazione di flussi migratori nel territorio dell'Unione europea, ha costretto quest'ultima a rivedere la normativa sull'accoglienza e dunque ne ha condizionato la politica per le migrazioni. Gli Stati coinvolti direttamente dalle migrazioni, e la stessa Unione, sono costrette inoltre a un impegno economico e diplomatico per contrastare fenomeni che, in tempi e misura ordinaria, sarebbero gestiti secondo le regole del diritto internazionale.

Proseguendo sulla linea che dalle ordinarie attività umane conduce verso la guerra si segnala la relazione di Maria Rita Anglani, che nell'esaminare gli attacchi al comparto sanitario evidenzia come all'attacco contro gli ospedali e i dispositivi sanitari, codificato dal diritto umanitario come crimine di guerra, si affianchino gli attacchi informatici agli health data. Benché all'apparenza questi secondi appaiano meno cruenti, sono in grado di minare in profondità la capacità dei sistemi sanitari di rispondere alle emergenze e alle crisi causate da un conflitto.

La risposta del diritto internazionale nel caso degli attacchi a strutture e persone del sistema sanitario è chiaramente tracciata dal diritto

[11] F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, cit.; A. Mumford, P. Carlucci, *Hybrid warfare: The continuation of ambiguity by other means*, in *European Journal of International Security*, vol. 8, n. 2, maggio 2023, 192-206.

DPCE online
ISSN: 2037-6677

internazionale umanitario[12]. I principi di umanità, distinzione, proporzione, limitazione e precauzione, che dovrebbero regolare il conflitto armato, si propongono di circoscrivere gli effetti aberranti della guerra. L'estensione degli stessi al conflitto cibernetico pongono problemi applicativi evidenti. La relazione di Maria Rita Anglani fa riferimento, a titolo di esempio, al furto di dati sanitari, per dimostrare la difficoltà di ricondurre questa fattispecie alla categoria dei reati penalmente rilevanti ai sensi del DIU. La strada alternativa, della necessità di una Convenzione digitale di Ginevra, è posta come necessaria da una parte delle potenze mondiali e dalla Croce Rossa internazionale, per la tutela dei dati come diritti umanitari.

Problemi non dissimili, ovvero quale norma e con quale efficacia per il caso concreto, pongono le operazioni di *targeted killing* svoltesi in Germania e Italia in operazioni statunitensi contro Al Quaeda, e Isis (che hanno causato diverse vittime)[13].

Si pongono, in questo caso, problemi di definizione del ruolo degli Stati medesimi (si tratta di un atto di guerra) e di responsabilità per i fatti commessi. I casi descritti nella relazione di Giacomo Belisario vengono diversamente trattati in virtù di sistemi costituzionali differenti. Quello tedesco prevede all'art. 2.2 della GG il dovere di garantire la vita delle persone anche oltre i confini della Germania. Quello italiano non prevede un dovere corrispondente e le vittime hanno ritenuto di far valere la responsabilità penale del comandante italiano della sede di Sigonella (base di partenza del drone) per i reati contestati. Pur nella diversità del contesto nazionale, le due vicende richiamano il diritto internazionale e la tutela della dignità umana e dei diritti fondamentali.

2. Il quid novi delle guerre ibride

Un secondo aspetto che emerge dalle relazioni presentate è il ruolo preponderante assunto dall'informatica e dalle nuove tecnologie come mezzi e obiettivi di guerra. Lo studio del diritto di guerra deve riguardare e degli apparati di difesa/attacco impone di considerare non solo l'esercito tradizionale ma anche l'esercito informatico. Senonché, l'esercito informatico si presenta come anonimo, opera in un terreno indefinito, con armi invisibili ma capaci di nuocere [14].

La *cyber warfare* ha potenzialità enormi, se è vero che tutti gli ambiti della vita economica e sociale sono interessati dal crescente uso dell'informatica e dell'intelligenza artificiale. La reazione degli ordinamenti e del diritto internazionale alle nuove manifestazioni della guerra appare al momento molto carente. Una prima risposta si basa sull'interpretazione adeguatrice del diritto di guerra esistente, coniato per la guerra tradizionale.

[12] Si fa riferimento, in particolare, alla Convenzione di Ginevra del 1949, alle convenzioni dell'Aja del 1899 e 1907, allo Statuto di Roma sulla corte penale internazionale.

[13] Definite come omicidi mirati realizzati mediante utilizzo di droni da G. Belisario, *La lesione dei diritti fondamentali posta in essere da Italia e Germania nelle operazioni di targeted killing comandate dagli USA in Stati non coinvolti ufficialmente in conflitti armati.*

[14] Si veda il contributo di Gatti e Giannelli, *Presupposti per la configurazione e la dichiarazione di guerra cibernetica*, in *questo numero speciale*, 453-468 ss.

Un altro strumento, di diritto privato, è il documento adottato dal centro NATO per la ciberdifesa, il c.d. Manuale di Tallin, dal nome della città dove ha sede l'agenzia[15].

La relazione di Matteo Gatti e Andrea Giannelli si concentra sulla definizione della guerra cibernetica e sulla sua compatibilità con l'art. 11 Costituzione italiana, a dimostrazione che le definizioni e l'inquadramento giuridico dei fenomeni che si riconducono alle guerre ibride sono presupposto necessario per l'applicazione di istituti di diritto interno e internazionale.

In assenza di adeguate codificazioni, la guerra informatica sottostà alle regole d'ingaggio di quella tradizionale, con la differenza che quest'ultima è generalmente attribuibile a Stati, mentre la prima vede coinvolti atri soggetti (gli attacchi terroristici).

In un contesto di crescente protagonismo della guerra cibernetica, ci ricorda Alessandro Lauro, si spiega la nascita di una strategia europea per la difesa dei sistemi informatici, che, secondo l'approccio della NATO, ove fossero facilmente vulnerabili esporrebbero alla vulnerabilità anche i diritti. Lauro avverte però che una equazione siffatta conduce ad un pericolo evidente: la compressione della libertà in nome della cybersicurezza. La dilatazione del concetto di sicurezza sta interessando sia il profilo oggettivo (i settori della vita umana per i quali viene richiesta protezione) sia il profilo soggettivo, perché accanto ai soggetti pubblici vengono coinvolti i soggetti privati, chiamati a mettere in atto misure di protezione e difesa nella gestione di strutture tecnologiche.

Un altro aspetto interessante, che credo sia emerso in tutte le sessioni, è che i tradizionali principi del diritto di guerra vengono messi in crisi dal superamento dei confini militare/civile, pubblico/privato (Wagner, soggetti gestori di *providers*), appropriato/esagerato, danni non necessari, ecc.

Il coinvolgimento nelle guerre di apparati civili, la cui funzione è ordinariamente estranea ai conflitti, comporta che essi vengono in varia misura ridefiniti nella struttura e nelle funzioni.

Un settore particolarmente sensibile è quello della protezione dei dati personali, che rappresenta, ordinariamente, un ambito della vita sociale ed economica dei cittadini. L'innalzamento delle esigenze securitarie sta trasformando la normativa nazionale sui siti internet e sull'accesso alla rete. Il diritto di internet rischia di diventare, da momento di espansione delle libertà, occasione di pericolo per la loro esistenza.

Se la guerra coinvolge settori della vita sociale, economica e istituzionale possiamo forse azzardare che essa si pone come fattore di co-produzione del diritto, non solo nel senso di produrre il diritto di guerra, ma anche nel senso di regolare ambiti normalmente estranei ad essa.

Si pensi alla questione migratoria e la risposta dell'Europa. Il fenomeno delle migrazioni gestite come strumento di destabilizzazione e ricatto ha determinato modifiche rilevanti del sistema di accoglienza europeo, che Claudia De Simone ha richiamato nel suo contributo. È chiaro che la disciplina del fenomeno interessa tutti i paesi e tutti i flussi, di origine economica o umanitaria che siano.

---

[15] *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*. Il Manuale è stato redato da un Gruppo di esperti internazionali, ed è perciò una fonte privata.

DPCE online
ISSN: 2037-6677

La sanità è un esempio ancor più significativo. Gli attacchi ai health data spingono a regole di protezione informatica destinate ad operare anche dopo la fine del conflitto.

Questa considerazione ci conduce ad un ulteriore riflessione. Gli effetti delle guerre ibride si avvertono sui beni materiali, sulle persone, e sul modello sociale. Questa mi sembra la cosa più importante per capire le risposte alle guerre ibride.

Gli attacchi al sistema sanitario e ai big data impongono accorgimenti che incidono sui costi e sui servizi offerti ai pazienti. Il sistema di welfare è la stessa natura dello Stato sociale democratico, almeno nella parte occidentale del Mondo, subiscono una trasformazione indotta da crisi sovranazionali prodotte da tecnologie informatiche.

Quali risposte?

3. Quali risposte?

Gli Stati e le organizzazioni internazionali devono affrontare le minacce e i pericoli derivanti dalle guerre ibride con gli strumenti del diritto interno e internazionale. Il coinvolgimento di diversi ordinamenti nazionali e internazionale è connaturale ad ogni guerra, ma nel caso delle guerre c.d. ibride la combinazione tra l'ordinamento nazionale e internazionale è indispensabile.

Pur in assenza di una definizione condivisa di guerra ibrida, è necessario per prima cosa elaborare concetti e tipologia di minacce da contrastare. In secondo luogo, occorre individuare gli strumenti di difesa attraverso il diritto, compito reso difficile dal contesto internazionale, divenuto anch'esso ibrido, tanto da mettere in crisi la sua stessa funzione[16]. Da un'arena nella quale protagonisti e Stati avevano un ruolo e una posizione definita, si è passati a un contesto geopolitico instabile.

La Nato e l'UE hanno iniziato a elaborare una strategia di risposta alle guerre ibride[17], che consiste in primo luogo nel definire ciò che è illegale e contrario al diritto.

La linea di demarcazione tra legale e illegale è essa stessa obiettivo delle manipolazioni e delle strategie disinformative delle guerre ibride contemporanee. Si tratta di una modalità particolarmente odiosa per le democrazie, che non possono rispondere con gli stessi strumenti degli avversari. Infatti, i regimi autoritari non sono soggetti al controllo

[16] Di tragedia del diritto internazionale ha parlato A. Sari, *Hybrid threats and the law. Concepts, trends and implications*, in *Hybrid CoE Trend Report 3*, Apr 2020, 8. Hybrid CoE è un'organizzazione internazionale indipendente, che lavora con il patrocinio della NATO e della UE, basata su una rete che promuove un approccio interdipendente tra governi e società civile per contrastare le minacce ibride.

[17] NATO: *Active engagement, modern defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon Strategic*, November 2010, available at: https://www.nato.int/cps/en/natohq/official_texts_68580.htm; European External Action Service: *A Europe that protects: Countering hybrid threats*, June 2018, available at https://www.eeas.europa.eu/node/46393_en.

dell'opinione pubblica e ai limiti del diritto, che vincolano gli Stati democratici a una risposta secondo il diritto[18].

Nei conflitti in Ucraina e Gaza la comunicazione delle parti in conflitto ha preso di mira la legittimità delle azioni, il rispetto dei vincoli internazionali, l'estensione delle regole a un determinato caso o territorio (*lawfare*)[19].

Rispetto a questa realtà in movimento, e alle pratiche di *lawfare*, le Convenzioni di Ginevra hanno poche possibilità di venire applicate in modo efficace. Le minacce ibride hanno generato un serio problema di legalità per quanto riguarda le leggi di guerra, il diritto all'autodifesa, la legittimità delle misure preventive e l'uso di contromisure in risposta a queste opache tattiche offensive. Si pensi alla possibilità di far valere l'art. 5 del Trattato sulla NATO (sul reciproco aiuto in caso di attacco) in caso di attacco non convenzionale a uno degli Stati aderenti, di intensità tale da non apparire una minaccia alla sua esistenza, ma da compromettere alcune attività.

Tuttavia, sebbene le guerre ibride possano operare in una zona grigia, non operano in un vuoto giuridico. Il diritto internazionale in generale, e il diritto internazionale dei diritti umani in particolare, continuano ad applicarsi. È anche importante notare che contrastare le minacce ibride è una competenza e responsabilità dello Stato. Sebbene contrastare le minacce ibride richieda una stretta collaborazione tra la NATO e l'UE, la responsabilità principale della risposta spetta allo Stato attaccato.

Gli attacchi ibridi possono essere contrastati con il diritto nazionale, in particolare del diritto penale nazionale, compresa la legislazione antiterrorismo, il diritto nazionale sulle telecomunicazioni, le norme sul controspionaggio, i diritti di proprietà e tutta la legislazione contro l'incitamento all'odio e la criminalità informatica. e riciclaggio di denaro. Quando le minacce ibride non si qualificano come azioni militari e quindi non rientrano nell'ambito del diritto internazionale umanitario, gli Stati sono tenuti a fronteggiare gli attacchi ibridi mediante la propria legislazione nazionale, solitamente applicando il proprio codice penale nazionale, sebbene talvolta anche la legislazione civile sia utile.

Il ruolo delle organizzazioni sovranazionali è di supporto in misura proporzionale alla situazione. Ove non sia applicabile la clausola di reciproco aiuto di cui all'art. 5 Trattato sulla NATO, può essere attivata quella sulla consultazione tra gli Stati[20].

Quanto all'Unione europea, a parte le clausole di solidarietà reciproca, va notato come essa sia in grado di reagire in risposta a minacce che riguardano specifici settori, come la sicurezza dei dati e la gestione dei flussi migratori.

---

[18] European Center of Excellence for Countering Hybrid Threats, *The–future of cyberspace and hybrid threats*, in *Hybrid CoE Trend Reports, no. 6*, Apr 2021, 14, available at: *www.hybridcoe.fi*.

[19] Dopo l'annessione dei territori ucraini di confine, la Russia ha attribuito la nazionalità a intere comunità di quei territori, per poi affermare di tutelarne i diritti come comunità minoritarie.

[20] A norma dell'art. 4 del Trattato sulla NATO, Le parti si consulteranno ogni volta che, nell'opinione di una di esse, l'integrità territoriale, l'indipendenza politica o la sicurezza di una delle parti fosse minacciata".

DPCE online
ISSN: 2037-6677

Esperienze positive di contrasto delle forme non convenzionale di attacco sono l'Agenzia dell'Unione europea per la cooperazione nel settore della lotta alla criminalità organizzata (*Europol*), l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (*Eurojust*), l'Agenzia dell'Unione europea per la cibersicurezza (ENISA)[21].

La risposta agli attacchi non convenzionali richiede più spesso la combinazione tra diritto interno e internazionale. Per contrastare le minacce ibride Stati (anche Terzi) e Unione europea cooperano in settori chiave come la modernizzazione e l'armonizzazione della legislazione, il blocco dei canali di finanziamento. Le strategie vengono spesso elaborate da specialisti, non solo delle strutture di sicurezza ma anche della sfera civile, il che rende possibile valutare le conseguenze delle misure adottate per i diversi gruppi e strati della società. Un esempio di questa integrazione è offerto dalla piattaforma EMPACT (*European Multidisciplinary Platform Against Criminal Threats*), che riunisce specialisti delle forze dell'ordine e degli organi giudiziari, delle agenzie dell'UE, dei servizi doganali e fiscali e delle aziende private. Un altro esempio è offerto dall'uso dei *digital service providers* per il lavoro di investigazione e informazione delle Agenzie europee di cui sopra.

Le fonti convenzionali possono interagire tra loro, e con il diritto degli Stati.

Rispetto alla prospettiva considerata, la possibilità di creare un nuovo diritto di guerra in risposta alle guerre ibride appare al momento poco effettiva. Gatti e Giannelli si interrogano sulla possibilità di costituire una autorità internazionale per gestire le crisi informatiche. Esistono due precedenti importanti, costituiti dalla Direttiva europea NIS2 in materia di cibersicurezza e segnalazione di incidenti, e il NIST statunitense (National Institute for Standard and Technologies) che certifica le attività informatiche secondo standard di sicurezza.

I limiti di un approccio internazionale o globale derivano dalla difficoltà di individuare i soggetti responsabili, sia per gli attacchi e sia per le risposte ad essi. Alla difficoltà soggettiva si aggiunge la difficoltà oggettiva di definire minacce, attacchi e guerre ibride.

Giuliana Giuseppina Carboni
Dip.to di Scienze economiche e sociali
Università degli Studi di Sassari
carboni@uniss.it

[21] D. Yu. Bazarkina, *Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States*, in *Herald of the Russian Academy of Sciences*, 2022, Vol. 92, Suppl. 4, S315–S320.