PAPER
2018

LO STRUMENTO MILITARE E LE CEMA (CYBER ELECTROMAGNETIC ACTIVITIES)

ANDREA STRIPPOLI LANTERNINI

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

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.

Center for Cyber Security and International Relations Studies

LO STRUMENTO MILITARE E LE CEMA (CYBER ELECTROMAGNETIC ACTIVITIES)

Andrea Strippoli Lanternini

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

2018

LO STRUMENTO MILITARE E LE CEMA (CYBER ELECTROMAGNETIC ACTIVITIES)

I confronti tradizionali, che vedevano gli Stati scontrarsi sul tradizionale campo di battaglia, sono ormai terminati da tempo. Oggi, la conflittualità ha assunto forme diverse rispetto al passato, caratterizzandosi per la presenza di elementi di asimmetricità, irregolarità e non convenzionalità. Le dimensioni del tempo e dello spazio sono state fortemente distorte dall'avvento di sistemi tecnologici in grado di far viaggiare le informazioni in modo sicuro, anonimo, praticamente in tempo reale e in ogni parte del globo. Il termine *Connectography* (*Connectivity* + *Geography* = *Connectography*), coniato da Paragh Kanna nel suo *Connectography: Mapping the Future of Global Civilization*[1] esprime bene, e in modo semplice, la capacità della tecnologia di mettere in comunicazioni le migliaia di nodi geografici, fisici e non, oggi presenti sulla Terra. Ciò rappresenta sicuramente un vantaggio ma, allo stesso tempo, fa emergere importanti vulnerabilità in determinati ambiti. Tra questi la difesa e la sicurezza nazionale ed internazionale.

La minaccia alla sicurezza di una nazione ha, infatti, assunto forme e caratteristiche differenti, venendo oggi definita ibrida proprio per evidenziarne il carattere multiforme in un contesto altamente dinamico e mutevole.

In un tale cornice, lo strumento militare mantiene un'elevata rilevanza quale mezzo attraverso il quale uno Stato assicura la difesa e la sicurezza dei propri confini nazionali e partecipa alla tutela dei principi e degli interessi strategici delle organizzazioni internazionali delle quali fa parte. Anch'esso però, nel corso del tempo, ha subito delle evoluzioni. Tra queste, da un punto di vista concettuale ed operativo, quella più evidente risiede nel passaggio da operazioni militari di tipo cinetico ad operazioni definite non cinetiche (*non-kinetic operations*). In tal senso

[1] P. Khanna, *Connectography*, Fazi Editore, 2016

emergono, quali attività particolarmente rilevanti, ed oggi ancora in fase di sviluppo, quelle relative ad azioni poste in essere nel *cyberspace*, ed azioni di guerra elettronica. Le attività che rappresentano l'unione di queste due componenti, nell'ambito di un contesto operativo, vengono definite CEMA (*Cyber Electromagnetic Activities*). Per spiegare compiutamente l'articolazione delle CEMA appare utile analizzare preliminarmente, e separatamente, le due componenti chiave.

La comprensione dello spazio cyber passa necessariamente per una, seppur breve, analisi del più grande ambiente di cui questo fa parte, ossia quello informativo (*Information Enviroment* - IE). Il Department of Defense *Dictionary of Military and Associated Terms* definisce l'IE come: "*the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information*". Questo ambiente è costituito da tre dimensioni: fisica, informativa, cognitiva. Tutte e tre sono altamente interconnesse, ed interagiscono con individui, organizzazioni e sistemi, ponendosi in una relazione di interdipendenza con l'ambiente operativo.

La dimensione fisica è composta da sistemi di comando e controllo (C2), *key decision makers*, ed infrastrutture di supporto, che consentono agli individui e alle organizzazioni di creare effetti in questa dimensione in cui le piattaforme fisiche e le reti di comunicazione sono connesse. La dimensione fisica include, ma non è limitata a, esseri umani, strutture C2, giornali, libri, unità di elaborazione del computer, computer portatili, smartphone, tablet. L'importanza di questa dimensione è oggi data dal fatto che le reti non connettono soltanto sistemi confinati in un'unica nazione. Oggi le connessioni sono internazionali, intra-nazionali, ma anche trasversali in quanto connettono sistemi economici, di comunicazione, di difesa, infrastrutturali, al di là dei confini geografici[2]. È l'intera geografia ad essere connessa.

La dimensione informativa è quella in cui le informazioni sono raccolte, processate, archiviate, disseminate e protette. È il luogo dove il comando e controllo delle forze militari viene esercitato e nella quale viene influenzato il contenuto ed il flusso informativo.

Infine, la dimensione cognitiva, è quella relativa alla percezione mentale di colui che gestisce l'informazione, in entrata o in uscita.

[2] U.S. Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*, 27 November 2012, aggiornato al 20 Novembre 2014

Gli strumenti da utilizzare nell'IE possono essere diversi e sono definiti come *Information Related Capabilities* (IRC). Con tale termine ci si riferisce agli strumenti, tecniche o attività impiegate per influenzare ogni aspetto dell'ambiente informativo e sono orientate a creare gli effetti e le condizioni operative desiderate[3]. Le IRC comprendono: *operations security* (OPSEC), *military deception* (MILDEC), *military information support operations* (MISO), *electronic warfare* (EW), *cyberspace operations* (CO), e *special technical operations* (STO).

All'interno della struttura info-tecnologica, nell'ambito della quale vengono svolte le operazioni militari, il cyberspace assume un ruolo chiave tanto che la NATO, durante il summit di Varsavia nel 2016, ne ha dichiarato l'elevazione a 5° dominio delle operazioni militari[4].

Secondo il Manuale di Tallin, con il termine cyberspace ci si riferisce all'ambiente formato da componenti fisici e non fisici, caratterizzati dall'uso di computer e dallo spettro elettromagnetico, per archiviare, modificare e scambiare dati utilizzando reti di computer.

Le operazioni nel cyberspazio (*cyber operations* – CO) si basano su una infrastruttura IT (*Information Technology*) interconnessa, autonoma e integrata; oltre a ciò vi è la presenza dei dati che risiedono all'interno di questa e che vengono trasmessi attraverso determinati componenti per consentire lo svolgimento di operazioni militari all'interno dello stesso dominio. Tali operazioni sfruttano i nodi e le connessioni eseguendo operazioni logiche per creare effetti prima nel cyberspace e poi, se necessario, nei vari domini fisici. Posto l'elevato livello di interconnessione tra i vari sistemi che sono inseriti all'interno dell'ambiente operativo, le *cyber operations* sono finalizzate a conseguire una libertà di azione nei domini fisici attraverso il preventivo attacco verso assetti IT dai quali essi dipendono in varia misura.

Secondo la Joint Publication 3-12 del Joint Chief of Staff U.S.A. il cyberspace può essere suddiviso in tre *layers* così individuati: *physical network*, *logical network* e cyber-persona.

Il *layer physical network* include due componenti: una componente geografica e una componente fisica della rete. Con la prima ci si riferisce alla localizzazione fisica delle infrastrutture e dei sistemi che supportano il cyberspace; con la seconda, invece, si fa riferimento alle strutture attraverso le quali i dati viaggiano. Queste ultime sono costituite da

[3] *Ibidem.*
[4] Gli altri domini sono terrestre, navale, aereo, spaziale.

hardware, sistemi e infrastrutture (reti wireless, collegamenti cablati, collegamenti EMS, satellite e ottico), che supportano la rete e i connettori fisici (fili, cavi, radiofrequenze, router, switch, server e computer).

Il *layer logical network* è rappresentato dagli elementi che consentono lo scambio di informazioni nel cyberspace come software, sistemi operativi, dati di sistema, protocolli.

Infine, il *layer* cyber-persona comprende la componente umana all'interno del cyberspace, non come entità fisica individuale ma come dimensione virtualizzata avente una o più rappresentazioni digitali. Queste includono: email, social media, numeri di telefono o presenze web, che possono essere legate ad un individuo o gruppo. L'esempio più emblematico è rappresentato da social media, come facebook, dove, al suo interno possono celarsi più persone in grado di accedere allo stesso account, oppure una persona con più profili che condivide quindi più nodi, *links* ed informazioni.

Il cyberspace ha quindi reso ancora più complessa la conduzione di operazioni militari, posta la necessaria, ed ormai imprescindibile, interconnessione tra i vari domini operativi.

Un elemento che ne evidenzia la complessità, e la trasversalità, è rinvenibile nella necessità di operare all'interno dello spettro elettromagnetico (EMS – *Electromagnetic Spectrum*), il quale fa da sfondo all'intero ambiente operativo. Lo spettro elettromagnetico consiste nell'insieme di tutte le possibili frequenze delle radiazioni elettromagnetiche. A sinistra dello spettro sono situate le onde radio con una frequenza superiore o uguale a 250 Mhz ed una lunghezza d'onda da 10 km a 10 cm, mentre all'estremo opposto, passando per le microonde, gli infrarossi, il visibile, l'ultravioletto e i raggi x, sono collocati i raggi gamma con una frequenza superiore o uguale a 300 Ehz e con una lunghezza d'onda minore o uguale a 1pm.

Quasi tutti i dispositivi utilizzati nel campo di battaglia funzionano attraverso lo spettro elettromagnetico; se ne comprende l'importanza se si pensa che tali dispositivi sono impiegati in ambito intelligence, comunicazioni, posizione, navigazione, comando e controllo (C2), attacco, trasmissioni, processo e archivio delle informazioni, cyber. Ciò posto appare evidente come la protezione dell'intero EMS sia fondamentale per preservare le proprie forze ed acquisire un vantaggio su quelle avversarie.

Con il termine *Electronic Warfare* (EW) ci si riferisce alle operazioni militari che coinvolgono l'uso di energia diretta elettromagnetica per controllare lo spettro elettromagnetico o per attaccare il nemico[5]. Convenzionalmente la EW è suddivisa in 3 sezioni: *electronic attack* (EA), *electronic protection* (EP), e *electronic warfare support* (EWS o ES). Tutte e tre contribuiscono al successo delle operazioni in aria, mare, terra, e cyberspace ad ogni livello di conflittualità.

L'EA coinvolge l'uso di energia elettromagnetica, energia diretta o armi antiradiazioni impiegate per attaccare personale, strutture o equipaggiamenti, con l'intento di degradare, neutralizzare, o distruggere le capacità di combattimento nemiche, ed è considerata una forma di fuoco[6].

L'EP si riferisce a tutte quelle azioni poste a difesa del personale, delle strutture e degli equipaggiamenti da ogni tipo di effetto proveniente dall'uso dello spettro elettromagnetico da parte di forze amiche, neutrali o nemiche; ma anche per proteggersi da fenomeni naturali che possono degradare o distruggere le capacità di combattimento amiche.

La EWS è caratterizzata da quelle azioni volte alla ricerca, intercettazione, identificazione e localizzazione di fonti di energia elettromagnetica, intenzionale e non, finalizzate al riconoscimento immediato della minaccia con lo scopo di consentire la pianificazione e la conduzione di operazioni future. L'*Electronic Warfare Support* sincronizza e integra la pianificazione e l'uso operativo di sensori, risorse e processi all'interno di uno specifico *battlefield* per ridurre le incertezze concernenti il nemico, l'ambiente, il tempo e il terreno. I dati acquisiti tramite EWS possono essere utilizzati per produrre SIGINT (*Signal Intelligence*), per fornire le coordinate di *targeting* per effettuare un attacco elettronico o fisico, nonché per ottenere misurazioni e firme intelligence[7].

Il dominio dello spettro elettromagnetico risulta oggi fondamentale per acquisire un vantaggio competitivo sull'avversario. Ciò è vero soprattutto in considerazione del passaggio da azioni di tipo cinetico ad azioni di tipo non cinetico mirate a sfruttare le vulnerabilità insite negli aspetti cognitivi della conflittualità. La protezione dei propri dispositivi e il contestuale controllo su quelli avversari tramite azioni di *electronic*

[5] U.S. Joint Chiefs of Staff, *Electronic Warfare*, Joint Publication 3-13.1 (Washington DC: Joint Chiefs of Staff, February 8, 2012), GL-9.
[6] *Ibidem.*
[7] *Ibidem.*

warfare risulta fondamentale ad ogni livello, tattico, operativo, strategico. Sul campo di battaglia acquisire il controllo dell'EMS, sia per condurre azioni offensive che per azioni difensive, è divenuto imperativo. Si pensi ad esempio al vantaggio di ottenere il controllo, attraverso azioni nello spettro elettromagnetico, di droni che svolgono azioni di ricognizione e intelligence, oppure il controllo di apparati C2, o radar, avversari, o ancora di inserirsi nei processi relativi alle fasi di lancio, di guida, o di comunicazione tramite *data link* di un missile. La capacità di inserirsi anche nei processi che riguardano la singola unità dispiegata sul terreno implementerebbe il senso di frustrazione funzionale ad un sempre maggiore disimpegno, anche solo motivazionale, dell'avversario. Questo andrebbe ad intaccare il processo di *decision making* avversario impedendo al comandante nemico di avere una *picture* coerente dell'ambiente operativo inducendolo quindi ad intraprendere azioni non idonee alla situazione contestuale. Ma l'EW può essere impiegata anche per svolgere attività di influenza nei confronti di determinati elementi dell'ambiente operativo quali ad esempio *leaders* politici avversari, o la stessa popolazione. In scenari di *hybrid warfare/hybrid operations* questa capacità sarebbe particolarmente remunerativa in quanto permetterebbe di agire facilmente, almeno durante certe fasi, per orientare il confronto a proprio vantaggio rimanendo comunque al di sotto della soglia legale di intervento.

L'evoluzione della conflittualità ed il relativo adattamento di tattiche, tecniche e procedure ha modificato la tradizionale percezione di tempo e spazio. In funzione di ciò si comprende quanto l'implementazione dei sistemi di sfruttamento dello spettro elettromagnetico risulti importante sia per quanto riguarda attività operative di tipo cinetico, sia per ciò che concerne la realizzazione di operazioni psicologiche a supporto di azioni informatiche in un ambiente operativo in cui l'aspetto cognitivo sarà sempre più enfatizzato. Gli assetti di guerra elettronica, quindi, per come concepiti e sviluppati, andranno a incidere sia nelle fasi di conflittualità che si collocano al di sotto della soglia legale di intervento, sia nel pieno di un eventuale confronto armato inquadrato in una cornice di *hybrid warfare*. Non va mai dimenticato, infatti, che la conflittualità del futuro si svolgerà all'interno di quello che potremmo definire come *advanced & integrated multidomain battlespace*, dove l'informazione rappresenterà il pilastro su cui basare tutta la pianificazione sui vari livelli. Possedere la capacità di gestire e/o interrompere e modificare le informazioni del nemico nell'ambito dello

spettro elettromagnetico rappresenterà un moltiplicatore di forza in grado di degradare le capacità tecnologiche più avanzata.

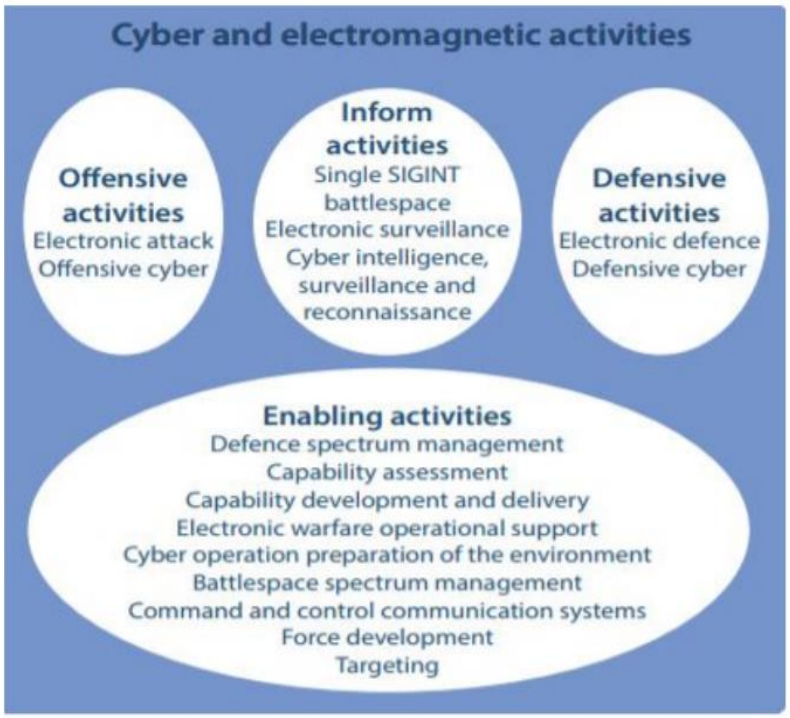
Connessa a tutto ciò, di notevole importanza, ma di relativo scarso approfondimento, è la questione concernente la conduzione di operazioni cyber e di guerra elettronica nell'ambito di quelle che vengono oggi definite come *Cyberspace Electromagnetic Activities* (CEMA). Come sostenuto dallo UK Chief of the Defence Staff - Air Chief Marshal Sir Stuart Peach "*...to understand, manage and control the electromagnetic enviroment is a vital role in warfare at all levels of intensity. The outcome of future operations will be decided by the protagonist who does this to decisive advantage*".

Il progresso tecnologico raggiunto dalle potenze occidentali nel corso degli anni ha permesso di acquisire elevate capacità operative funzionali al raggiungimento degli obiettivi politico-strategici. Tuttavia, l'assenza di una effettiva integrazione tra tali capacità, e l'esponenziale evoluzione tecnologica, soprattutto in ambito IT, ha indotto la comunità di sicurezza e difesa a riflettere maggiormente sulla necessità di un coordinamento tra i vari strumenti a disposizione per una maggiore consapevolezza dell'ambiente operativo e per una più efficace attività di C2. L'incremento di operazioni non cinetiche, ed il ruolo sempre più importante dell'informazione sul campo di battaglia, ha portato ad una presa di coscienza concernente la necessità di integrare e coordinare attività cibernetiche, *information operations*, e attività di *electronic warfare*.

Con il termine CEMA si fa riferimento alla sincronizzazione e coordinamento di attività cyber ed elettromagnetiche di natura offensiva, difensiva, informativa ed abilitativa, al fine di ottenere un vantaggio operativo consistente in libertà di movimento e raggiungimento di effetti, impedendo e degradando, simultaneamente, la capacità dell'avversario di utilizzare l'*electromagnetic enviroment* ed il *cyberspace*[8].

Le CEMA comprendono quattro attività principali che sono condotte nel cd. EME (*Electro Magnetic Enviroment*) o nel cyberspace, o in entrambe.

[8] CEMA Capability Integration Group (CIG).



Fonte: UK Joint Doctrine Note 1/18 Cyber and Electromagnetic

Le attività offensive, difensive e informative, queste ultime destinate a produrre Intelligence, sono supportate da attività abilitanti le quali provvedono alla necessaria analisi operativa, alle risorse e alle infrastrutture. Queste attività non contribuiscono direttamente all'attività operativa ma sono di supporto. Tuttavia, una errata conduzione di tali azioni avrebbe ripercussioni sulle attività offensive, difensive e informative con conseguenti abbassamenti del livello di successo operativo[9].

La possibilità di utilizzare il cyberspace e la EW mediante un'unica pianificazione, integrazione e sincronizzazione, permette al comandante, e all'intera catena di comando e controllo, di avere una consapevolezza dell'ambiente operativo più completa, funzionale alla conduzione di attività offensive, nonché di sincronizzare le operazioni utilizzando lo stesso dominio, al fine di dispiegare una maggiore ed efficace reattività difensiva contro una speculare minaccia CEMA[10]. I sistemi di informazione e comunicazione militare, come radar e apparecchiature di navigazione, infatti, operano nel cyberspazio attraverso connessioni wireless che accedono allo spettro EM; ciò li

[9] UK Ministry of Defence, *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*, February 2018

[10] Headquarters Department of Army, FM 3-12 *Cyberspace and Electronic Warfare Operations*, April 2017

rende vulnerabili a ostili e congiunte operazioni informatiche ed elettroniche sempre più sofisticate.

In un contesto conflittuale sempre meno definito, la necessità di avere una "*battlefield picture*" da rappresentare a vari livelli, da quello tattico rappresentato dall'unità sul terreno, a quello strategico, rappresentato dal decisore politico-militare, risulterà fondamentale per mantenere un vantaggio operativo sull'avversario. Oltre a ciò sarà necessario coordinare le varie azioni, di natura offensiva e difensiva, in uno scenario altamente dinamico e multidimensionale dove lo spettro elettromagnetico sarà il denominatore comune in funzione del quale condurre le varie attività. Ciò in quanto il controllo dell'EMS, oltre ad avere il governo dello scenario tattico e di compiere una serie di azioni tecniche volte a rendere inutilizzabili o a degradare l'utilizzo di determinati sistemi di combattimento, permette anche di interagire con attori che si trovano fuori dal campo di battaglia ma che, nell'ambito delle nuove forme di conflittualità, soprattutto di natura ibrida, rappresentano il reale obiettivo dell'azione nemica. La popolazione civile, infatti, poiché altamente dipendente dalle varie reti che oggi garantiscono la sopravvivenza del sistema, risulta essere il target primario per un attore che opera in un contesto di *hybrid operation/hybrid warfare*. Inoltre, l'ulteriore dipendenza dalle informazioni provenienti da internet e dai social media trasformano la società civile in un bersaglio altamente remunerativo per un attore, statale o non statale, che abbia il controllo dell'EMS. Ciò in quanto, attraverso la capacità di modificarne i contenuti, insieme alla realizzazione di azioni cyber, questo sarà in grado di orientare il *sentiment*, o l'ideologia delle masse, verso tendenze più favorevoli all'attaccante, anche attraverso azioni di *deception*.

Al fine di scongiurare la possibilità di essere oggetto di tali azioni, il raggiungimento di quella che potrebbe essere definita come *EMS joint integrated superiority*, che copra tutti i domini (cielo, mare, terra, spazio e cyber), deve passare per una efficace attività di intelligence e di ISR (*Intelligence, Surveillance and Reconnaissance*), capace di raccogliere e poi analizzare i dati raccolti in modo integrato e joint. Questo risulta fondamentale per consentire ai responsabili di ogni livello di avere una *operational awareness* completa al fine di pianificare ed eseguire operazioni cyber e di EW. Va evidenziato come, in un contesto CEMA, l'*operational awareness* includa anche il controllo delle topologie di rete, le quali illustrano il modo in cui le informazioni transitano all'interno e

all'esterno dell'area operativa e che potrebbero essere oggetto di manipolazione e sabotaggio. A questo punto appare chiaro come, nel prossimo futuro, la capacità di acquisire il controllo dello spettro elettromagnetico e del cyberspace risulterà determinante per le forze in campo al fine di assicurarsi libertà di movimento all'interno del *battlefield* negandola all'avversario; ciò sincronizzando le funzionalità tra i vari domini le funzioni di combattimento con lo scopo di massimizzare gli effetti reciproci nel, e attraverso, il cyberspace e l'EMS[11].

Attualmente, diversi Stati stanno sviluppando capacità EW e cyber in grado di essere integrate e rese interoperabili con altri sistemi nell'ambito di attività A2/AD (*Anti Access/Aerial Denial*) a tutela dei propri confini nazionali e delle aree di interesse strategico. Tra questi la Russia, l'Iran e la Cina.

Come visto finora, l'ambiente operativo continuerà, presumibilmente, ad evolversi provocando la necessità di implementare continuamente soluzioni tecnologiche funzionali ad ottenerne il controllo nel modo più completo possibile. Per fare ciò risulta fondamentale acquisire consapevolezza del fatto che i conflitti del futuro saranno sempre più liquidi, disegnando uno scenario in cui la vera battaglia si combatterà in quello spazio grigio esistente, ad oggi, tra i concetti di guerra e pace. Il confronto attraverserà in modo trasversale tutti i vari domini di ingaggio, i quali saranno interconnessi e interdipendenti seppure con differenti gradi di intensità. Ci si prepara, quindi, ad affrontare quello che è stato già definito come *advanced & integrated multi domain battlespace*, nel quale la minaccia sarà sempre più ibrida e di difficile individuazione, con ripercussioni di estrema rilevanza anche dal punto di vista giuridico ed in particolare di *ius ad bellum*.

[11] https://www.afcea.org/content/army-accelerates-cyber-ew-integration

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

Center for Cyber Security and
International Relations Studies