



CYBER E TECH

La cyberwar e le guerre senza limiti

L'Italia di fronte alla complessità dei conflitti di ultima generazione

A cura di *Salvatore Santangelo*

30 SETTEMBRE 2021

Le disposizioni normative relative all'Architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale cercano di affrontare le attuali trasformazioni tecnologiche e organizzative che investono ogni dimensione – da quella economica, a quelle politica e sociale – evidenziando un processo che pone in discussione le stesse fondamenta delle strutture operative e decisionali di uno Stato. È fondamentale accompagnare l'iter di attuazione e di implementazione con un dibattito di ampio respiro che sappia rendere l'Opinione pubblica nazionale consapevole della complessità delle sfide che dovrà affrontare il Sistema-Paese.

Leggere l'evoluzione del contesto

«Il cyberspazio è un luogo definito da prassi originate spontaneamente da *fantasmi guerrieri* e da *sogni comunitari*»; questa evocativa definizione appartiene a Paul Mathias, professore dell'*Institut D'Etudes Politiques*.

E proprio il **cyberspazio** - nel momento in cui non può essere identificato come una semplice infrastruttura di rete - presenta una natura (e una struttura) assai simile (con le dovute differenze) a quelle dell'Universo, in continua espansione: un nuovo universo e, dunque, una nuova *polis*; quella *polis* che probabilmente ha la stessa radice di *polemos*.

È stato Carl Schmitt a esplorare lo stretto nesso tra *polis*, *politike*, *polemos*, partendo dal fatto che le sintesi politiche sono più coese proprio quando sono impegnate in un conflitto con un eventuale nemico/avversario: «tutti i concetti, le espressioni e i termini politici hanno un senso polemico; essi hanno presente una conflittualità concreta, sono legati a una situazione concreta, la cui conseguenza estrema è il raggruppamento in amico-nemico (che si manifesta nella guerra e nella rivoluzione)».

Come evidenziava perfettamente Alain de Benoist in un articolo apparso su *Diorama Letterario* già nel novembre '97: «Ogni evoluzione tecnologica secerne la propria ideologia, e questa ideologia guida il cambiamento». Per secoli la relazione tra uomini è stata di tipo territoriale, e si dispiegava all'interno di uno spazio continuo; con l'avvento delle reti il motore essenziale di ogni legame sociale è la comunicazione.

Non si appartiene più, non si aderisce più; l'imperativo categorico è: "essere in connessione".

Infatti, se è vero che una società è una collettività organizzata di individui che condividono interazioni di vario tipo, è anche vero che l'avvento delle tecnologie digitali ha permesso l'abbattimento di quelle frontiere naturali o politiche che - in passato - hanno plasmato i rapporti di ogni natura: la prima rivoluzione è stata sicuramente quella di natura **geopolitica**; la dissoluzione dell'Urss (e del Patto di Varsavia) ha di fatto reso improbabile qualsiasi minaccia diretta e simmetrica contro gli Stati Uniti e l'Europa ("la geopolitica presuppone sempre una metapolitica; una metastrategia").

La seconda è stata quella della **tecnologia dell'informazione**, che costituisce il principale volano della globalizzazione culturale ed economica: trasferimento di tecnologie o diffusione di media - come internet, in precedenza coperto dal segreto militare (*arpanet*).

Il terzo dato da tener presente è che **l'interdipendenza** dei sistemi e la crescente competizione globale hanno profondamente modificato non solo le forme, ma anche gli stessi contenuti della politica.

Siamo di fronte a una trasformazione che investe ogni dimensione, da quella economica, a quelle politica e sociale; un processo che culmina nell'affermazione del "Villaggio Globale" e che pone in discussione le stesse fondamenta delle strutture operative e decisionali di uno Stato, evidenziando l'esigenza di modificarle radicalmente, in

modo da eliminare il centralismo burocratico dalla politica e dagli apparati amministrativi per orientarsi verso modelli decisionali decentrati e strutture operative reticolari.

Come auspicato dal testo normativo in esame.

Allo stesso tempo occorre valutare come la diffusione dello spazio cibernetico ha profonde implicazioni per gli equilibri della politica interna e internazionale, l'attività economica mondiale, le relazioni sociali nazionali e transnazionali, e dunque sulle dinamiche geopolitiche globali nel loro complesso.

La sempre più ampia diffusione dei sistemi per la condivisione di informazioni ha permesso, infatti, a un numero sempre crescente di attori di far emergere con maggior forza le proprie prerogative e le proprie necessità e recriminazioni.

Come spesso accade nella Comunità internazionale, quando si verifica una variazione reale o percepita del peso relativo tra le Potenze o uno squilibrio delle forze nel panorama geopolitico si innesca una destabilizzazione; con un successivo riadeguamento per la ridefinizione delle posizioni stesse.

Nuovi attori si affacciano oggi sulla scena insieme con quelli già noti, contendendo loro lo spazio che era proprio (o quello disponibile), fino ad arrivare a una tensione che investe i rapporti economici e diplomatici con il rischio di causare uno scontro aperto.

Anche la tensione diplomatica può sfociare in crisi, dato il ricorso, sempre più diffuso e aggressivo, all'applicazione di "contromisure", "sanzioni", se non di vere e proprie rappresaglie.

In estrema sintesi, l'evoluzione tecnologica è da un lato uno strumento fondamentale per la creazione del benessere sociale e per la sua diffusione a livello globale, con positivi effetti sul prolungamento della vita, sulla sua miglior qualità e sull'incremento della ricchezza individuale, ma - di contro - può costituire l'elemento decisivo attraverso il quale una tensione (interna o esterna) fra individui, società, Stati e/o Alleanze sfoci in conflitti e guerre: la globalizzazione economica, sospinta dall'avanzamento tecnologico che a sua volta viene dalla stessa alimentato, cambia radicalmente le carte in tavola e aggiunge nuove dimensioni alla guerra, sottraendola spesso ai militari e ai professionisti delle tecnostutture propriamente vocate a presidiare le dimensione e la sfera della Difesa; oggi non esiste più un campo di cui la guerra non possa servirsi, e non vi è quasi nessun ambito che non abbia fatto proprio il suo modello offensivo.

Dinamiche operative

Esplorare il dominio dello spazio cibernetico punta a valutare le **implicazioni teoriche e pratiche** di questa peculiare arena di confronto. Un'arena in cui si affrontano non solo i tradizionali attori statuali, ma anche protagonisti emersi dal settore privato (sia i cosiddetti OTT come *Google*,

Amazon e Facebook, sia i ranghi delle legioni di utenti che si muovono all'interno del *cyber spazio* animati dalle più svariate intenzioni e dotati di alte competenze tecniche: quelli che, per semplicità, definiamo *hacker*).

La “**collisione**” tra le intenzioni/azioni di questi diversi protagonisti ridisegna gli spazi di manovra e di azione, riconfigurando le premesse stesse su cui tradizionalmente si basa il rapporto tra gli Stati.

In questo senso, la capacità di operare efficacemente nella dimensione Cyber diventa la preconditione per implementare (o contrastare) ogni approccio “ibrido”: per “guerra asimmetrica” non possiamo più intendere infatti solo gli approcci che abbiamo imparato a conoscere studiando i vietnamiti o le modalità con cui le milizie jihadiste agiscono nei contesti urbani nel Medio Oriente contro eserciti regolari.

Oggi occorre confrontarsi con la pervasività dei dati, con il fatto che sono prodotti da ogni azione (consapevole o inconsapevole) dei singoli e dalla relativa facilità con la quale - questi stessi dati - possono essere raccolti e utilizzati. Anzi, agli aspetti prettamente militari, come già detto, ne vanno “sovrapposti” altri che - sempre in tempo reale e in forma globale - sono anch'essi diventati sostanzialmente atti di guerra: la pirateria informatica, l'uso di strumenti finanziari per distruggere l'economia di un Paese, la manipolazione dell'opinione pubblica.

Il terreno di scontro, nelle “nuove guerre”, è ovunque.

Nel *Prometeo Incatenato*, Eschilo affida al suo eroe tragico questa potente affermazione: “*la Tecnica è di gran lunga più debole della Necessità*”.

In realtà - come ci hanno insegnato Jünger e Spengler - attraverso gli strumenti tecnici, gli uomini possono emanciparsi dalla *necessità*, inaugurando la *Storia*, o, per dirla ancora con Eschilo, “*il tempo che invecchia*”.

Su questa dinamica oggi se ne impone un'altra: nell'era della globalizzazione la conflittualità non si manifesta solo nella vecchia dimensione spaziale/istituzionale, ma anche attraverso una verticalizzazione delle contrapposizioni all'interno di ogni singola realtà.

La disponibilità e l'accesso a nuove tecnologie ha contribuito in misura determinante a ridefinire gli equilibri internazionali, spesso contemporaneamente a immani tragedie. Si pensi, per esempio, al primo Conflitto Mondiale nel quale la massiva applicazione di nuove tecnologie (dalla produzione di nuovi armamenti, al movimento delle truppe con migliaia di treni sincronizzati, alla conservazione del cibo in scatola, all'affermazione del mezzo aereo) ha enormemente aumentato il numero dei belligeranti e la capacità distruttiva delle forze in campo, e purtroppo, accanto a tale miglioramento, si è perfezionata l'efficienza della distruzione e l'esponenziale crescita del numero di vittime, almeno fino al momento in cui le nazioni che avevano una maggior disponibilità di nuovi strumenti bellici e capacità economico-produttive hanno potuto sfruttarle per arrivare alla vittoria finale.

La conquista di questa nuova dimensione diventa un'*escalation* per ottenere la supremazia dei dati (sia specifici che appartenenti alla sfera dei *big data*) e guadagnare un sostanziale vantaggio competitivo nel ciclo OODA (Osservazione, Orientamento, Decisione e Azione - codificato da John Boyd).

Dall'attacco *Botnet* del 2007 contro l'Estonia a *Stuxnet* contro il programma nucleare iraniano, fino alla sistematica diffusione di notizie (a prescindere dal fatto che siano vere, verosimili o assolutamente false) che condizionano le opinioni pubbliche, i processi decisionali e le stesse procedure elettorali, proveremo a esplicitare alcune priorità che dovrebbero accompagnare il percorso normativo su un tema così delicato.

Il **doppio shock** geo-pandemico e geo-cibernetico può generare uno sconvolgimento sociale e organizzativo statale e interstatale, variando gli stessi assetti all'interno dei singoli Stati e di questi nell'ambito delle alleanze (così come le abbiamo storicamente conosciute).

Le due scosse non generano solo disfunzionalità e disequilibri (sociali e politici) ma amplificano - sommandosi nell'effetto di profonda incertezza nella visione del futuro - su un particolare ambiente evolutivo della società moderna: il cosiddetto spazio cibernetico (o cyberspace).

La dinamica geopandemica ha infatti dato ancora maggiore impulso alla frequentazione e occupazione umana dello

spazio di manovra virtuale, soprattutto eco-socio-politico, offerto dal web.

La Pandemia ha spinto alla dematerializzazione del segmento fisico delle attività umane e tutto ciò che era iniziato con gli anni '90 con le prime dinamiche net-centriche ed era approdata recentemente all'“*Internet of Thing*” sta portando la società (almeno la parte più evoluta di essa) al cosiddetto “*Internet of Behavior*”.

L'internet dei comportamenti quindi, l'infrastruttura digitale a supporto dell'orientamento del comportamento delle masse rispetto ai gusti, alle mode, alle tendenze, alle scelte in qualsiasi campo dell'esistenza umana (dall'ambiziosa corsa dei risparmiatori alle monete virtuali, al lancio delle degeneri sfide sui social che provocano tra i più giovani stati di esaltazione o di depressione fino a spingerli a un mortale autolesionismo).

Bruce Sterling e William Gibson - visionari narratori - si interrogano sull'impatto della *Tecnica*, generatrice di nichilismo per eccellenza: non tanto, e non solo, sulla vita, quanto sulle coscienze e sulle percezioni delle creature umane.

I loro universi hanno saturato immaginari: film, serie tv, giochi di ruolo e *videogame*, nell'ultimo dei quali - *Cyberpunk 2077* - l'*avatar* di Keanu Reeves interpreta il rocker ribelle Johnny Silverhand.

Proprio il genere ***Cyberpunk*** è il più lucido tentativo di definire i protagonisti del *Medioevo prossimo* venturo con una lingua nata nel/dal futuro per parlare del presente.

Una nuova lingua, e dunque un nuovo stile sorto dalla frammentazione del tempo vettoriale della nostra esperienza quotidiana, fatta di una narrazione lineare, che implode in una prassi dettata dalla compresenza simultanea dei momenti e delle differenze, resa possibile dall'avvento dei media elettrici.

Su tutto, il reticolo delle informazioni e sullo sfondo la lotta per l'egemonia del futuro basata sull'innovazione: «Ogni millennio ha la sua apocalisse, e quella temuta nel Terzo millennio non poteva che essere un apocalisse tecnologica, così come quella attesa per l'anno mille avrebbe dovuto essere un'apocalisse destinata a coincidere con la liberazione di Satana dalle catene impostegli, per mille anni, al momento della nascita di Cristo» (Giuseppe Sacco).

Oggi, i timori non sono più quelli dell'olocausto termonucleare, come si è paventato per più di cinquant'anni, ma quelli appunto di un'apocalisse elettronica: l'intera saga di "Terminator", "ex-Machina", "Alien Covenant": il grande schermo ci ha ormai abituato alle trasposizioni cinematografiche dei rischi connessi allo sviluppo incontrollato dell'Intelligenza Artificiale. Un tema che ha spaccato il mondo dei tecno-guru con pezzi da novanta come Peter Thiel ed Elon Musk schierati dalla parte dei catastrofisti: attacchi da hacker informatici sulle auto a guida autonoma e AI - le macchine pensanti appunto - che

prendono il sopravvento e si rivoltano contro l'uomo. È questo lo scenario, o meglio il timore, espresso dal patron di Tesla per il futuro. È dello scorso anno la notizia che Facebook ha interrotto un esperimento sulle macchine senzienti quando i due processori coinvolti hanno cominciato a comunicare tra di loro in un linguaggio non comprensibile agli sviluppatori. Quello che è chiaro è che intorno a questo tema - e più in generale sull'innovazione - si giocherà la lotta per l'egemonia del futuro. Un concetto che Putin ha recentemente codificato di un assioma geoeconomico: «Chi controllerà lo sviluppo dell'Intelligenza Artificiale controllerà il mondo (Una sentenza lapidaria che ridefinisce i parametri di una Geopolitica 2.0 dove l'immateriale prende il sopravvento sulle coordinate geografiche)».

Priorità

Non è un caso che **Russia** e **Cina** come potenze revisioniste siano i Paesi più impegnati su questo versante: la vera **competizione** del futuro, che ruota appunto attorno alle biotecnologie, ai calcolatori quantistici, all'intelligenza artificiale, alle reti di comunicazione sempre più performanti e sulla capacità di collezionare e analizzare dosi sempre più massicce di dati.

Quello che per oggi è ancora di fantascienza, esprime già i primi segnali all'orizzonte e non sono pochi i pensatori che chiedono una regolamentazione che impedisca un uso immorale di una tecnologia che si affermerà un istante dopo

la sua invenzione. In questo senso, come ha affermato Germano Dottori: «Il 5G è una tecnologia che espanderà considerevolmente l'universo del possibile, a beneficio di individui e sistemi, pubblici e privati, aziendali e politici. Ne diventeremo tutti dipendenti, molto rapidamente, anche nella gestione della nostra vita quotidiana, a partire dall'ambiente domestico. Le nostre case e il governo della viabilità ne saranno fortemente influenzati, così come la gestione di attività sensibili incluse quelle connesse alla salute personale o all'impiego dei risparmi. Il 5G sarà infatti l'architettura del cosiddetto internet delle cose, o *internet of thing*. Rispetto a questo tipo di evoluzione, al contrario di ciò che si dice non sarà certo la protezione dei dati la sfida principale. I dati possono essere carpiri in una grandissima quantità di modi già oggi. Persino con applicazioni che scarichiamo sui nostri telefonini per giocare, penso per esempio a quel periodo in cui tanti di noi giocavano a fabbricare immagini "invecchiate" di sé stessi, fornendo a chi gestiva il programma una gran quantità di dati biometrici. Lo stesso accade quando vincoliamo la sicurezza di un telefono al riconoscimento dell'iride. In generale, per carpire o trasferire dati bastano le applicazioni, applicazioni che spesso possiamo scaricare direttamente dalla rete senza dover superare particolari controlli. Il vero problema è un altro, del tutto diverso: ed ha a che fare con l'identità del gestore del sistema, o meglio della sua infrastruttura. Chi venderà il proprio, infatti, avrà il potere di riprogrammare da remoto o minacciare anche la negazione del servizio. In questo senso, il 5G odierno potrebbe essere l'*enabler*, ciò che

rende possibile la “guerra senza limiti” immaginata in Cina 21 anni fa da Wang Xangsui e Qiao Liang. Quella in cui, all’improvviso e senza preavviso, gli oggetti di uso comune nelle mani della gente si trasformano in armi letali rivolte contro di loro. E l’“*internet of thing*” è ancora poco. Sono infatti all’orizzonte l’*augmented man* e il cosiddetto *internet of human*, ovvero l’integrazione uomo-macchina anticipata dalla fantascienza, sulla quale già si esercitano le Difese meglio finanziate e più ambiziose del pianeta. Quelle che stanno lavorando alla trasmissione diretta del pensiero tra i soldati del futuro. Acquisirà maggior concretezza lo spettro agitato dal vecchio Henry Kissinger, che già da diversi anni ci ammonisce rispetto al rischio che le macchine finiscano per prendere il sopravvento su di noi. Magari opportunamente aiutate dalla manina di qualche programmatore nemico».

Risulta parimenti evidente come le potenzialità espresse dalle nuove tecnologie, se da un lato consentano di massimizzare gli effetti delle attività “tradizionali”, dall’altro introducono nuove potenziali sfide, cui è necessario saper far fronte attraverso la definizione di specifiche strategie atte a contenere e a mitigare i rischi associati con il loro impiego.

Appare chiaro, infine, come il dominio cibernetico, nonostante la sua natura virtuale, impatti, anche direttamente, sull’ambiente reale e come l’innovazione tecnologica, dato l’elevato impiego della componente informativa sui nostri strumenti di C2 e sistemi d’arma, stia cambiando la forma dei conflitti moderni, aumentando la complessità tradizionale del campo di battaglia.

Per quanto evidenziato, per acquisire un **vantaggio strategico**, che risulta già decisivo per le Strutture del Paese impegnate nel complesso tema cibernetico, occorre:

- I) non limitarsi a sapersi avvalere delle nuove tecnologie, ma concorrere al loro sviluppo, adottando un processo di trasformazione coerente e aderente alle proprie effettive esigenze, in modo da adattarsi costantemente all'evolvere delle minacce, che tra l'altro si caratterizzano sempre più per la loro volatilità e indeterminatezza e che plausibilmente diventeranno sempre più numerose e sofisticate;
- II) sviluppare diversificate competenze di natura tecnica, informatica e giuridica;
- III) ampliare le proprie capacità operative, al fine di condurre operazioni attraverso e nello spazio cibernetico, in un ambiente sempre più multi-dominio;
- IV) occuparsi non solo della propria sicurezza cibernetica ma rivolgere lo sguardo anche alla protezione delle infrastrutture critiche del Paese;
- V) preservare un approccio che persegua la centralità dell'uomo (anche nell'ambito del dominio cibernetico, l'unico, tra l'altro, creato proprio dall'uomo) e che miri a una sempre più spiccata valorizzazione della componente umana, da ricercare attraverso una crescita culturale e professionale continua, sia del personale tecnico specializzato o di "settore" che del cittadino comune la cosiddetta "utenza civile" attraverso una incessante spinta motivazionale sugli "addetti ai lavori" e una necessario

stimolo della “coscienze” a ogni livello e non solo sotto il profilo etico.

Bibliografia

Metaggiata C., “La dura legge del controspionaggio: svelati Angelo Piangente, Pterodattilo e le altre ‘cyber-creature’ della CIA”, 24.03.17, Analisi Difesa
<http://www.difesaonline.it/evidenza/cyber/la-dura-legge-del-controspionaggio-svelati-angelo-piangente-pterodattilo-e-le-altre>

Howlett W. S., “The Rise of China’s Hacking Culture: Defining Chinese Hackers”, 2016, California State University Scholar Works,
<http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1413&context=etd>

Xiaokui Shu and JR Rao, “Unleashing Cyber Reasoning Potential in The Era of AI Security”, 01.05.20, IBM,
<https://www.ibm.com/blogs/research/2020/05/cyber-reasoning/>

Modha D.S., “Introducing a Brain-inspired Computer. TrueNorth's neurons to revolutionize system architecture”, 05.08.15, IBM, <https://research.ibm.com/articles/brain-chip.shtml>

Vecchio A., “Sovranità e supremazia tecnologica nell’era post globale”, 30.11.20, Difesa Online,

<https://www.difesaonline.it/geopolitica/analisi/sovranita-e-supremazia-tecnologica-nellera-post-globale>

Salah A., “The Multiple Types of Electronic Breach of States' Domestic Policies”, 20.03.17, FARAS, <https://futureuae.com/en-US/Mainpage/Item/2601/hacking-democracy-the-multiple-types-of-electronic-breach-of-states-domestic-policies>

Pierantoni F. e Pierantoni M., “Combattere con le informazioni” (Collana del Centro militare di studi strategici, Volume 34), 1998 – Ed. Franco Angeli

Suffia G., “Effetti geopolitici del Datagate: appunti e spunti per la geopolitica della sorveglianza globale”, *Cyberspazio e diritto*, vol. 16, n. 54 (3-2015), pp. 461-508

Martino L., “La quinta dimensione della conflittualità - L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale”, *Politica & Società* 1/2018, pp. 61-76, Ed. Il Mulino

Crosston M., “Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes”, *Cyber, Intelligence, and Security* 1/2020, pp. 149-171

Darnis J.P. e Polito C., “La Geopolitica del Digitale”, 2019, Ed. Nuova Cultura

Fauceglia D., “Cybersecurity, Competition, Contracts and Cyber-Risk”, *European Journal of Privacy Law & Technologies* 1/2020, pp 1-20, Ed. Giappichelli

Salamone L.V.M., “La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell’informazione: contesto normativo nazionale di riferimento, ruolo dell’intelligence e prospettive de iure condendo”, *federalismi.it* 23/2017, pp. 2-37

Marrone A. e Sabatino E., “La difesa cibernetica nei Paesi NATO: modelli a confronto”, *Osservatorio di Politica internazionale* n. 164, 12/2020, Istituto Affari Internazionali

Rajna G., “Bio-Circuitry Neurons Computing”, raccolta di articoli scientifici, ottobre 2019

Van der Meer S., “Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signalling”, *International Affairs Forum Spring 2017*, pp. 85-90, Netherlands Institute of International Relations ‘Clingendael’

Johnson J., “The End of Military-techno Pax Americana? Washington’s Strategic Responses to Chinese AI-enabled Military Technology”, *The Pacific Review*, 10/2019, Ed. Taylor & Francis

“Scenarios for the Future of Technology and International Development”, 5/2010, Rockefeller Foundation

Whyte C. and Mazanec B., “Understanding cyber warfare : politics, policy and strategy”, 2019, Routledge

Evan H. Potter and others, “Cyber-diplomacy: managing foreign policy in the twenty-first century”, 2002, McGill-Queen’s University Press

Caravelli J. and Jones N., “Cyber security : threats and responses for government and business”, 2019, Praeger Security International

“Russian Military Intelligence - Background and Issues for Congress”, 11/2020, US Congress

Pelton J. N., “Preparing for the Next Cyber Revolution. How Our World Will Be Radically Transformed. Again!”, 2019, Springer International Publishing

Quade P., “The Digital Big Bang. The Hard Stuff, the Soft Stuff, and the Future of Cybersecurity”, 2019, John Wiley & Sons

Delerue F., “Cyber Operations and International Law”, 2020, Cambridge University Press

Thielborger P. and Heintze H.J., “From Cold War to cyber war_ the evolution of the international law of peace and armed conflict over the last 25 years”, 2016, Springer International Publishing

Daras N.J., “Cyber-Security And Information Warfare”, 2019, Nova Science Publishers

Bou-Harb E. and Neshenko N., “Cyber Threat Intelligence for the Internet of Things”, 2020, Springer Nature

“Defense Budget Overview - Fiscal Year 2021 Budget Request”, 5/2020, US DoD

“Unmanned Systems Integrated Roadmap 2017-2042”, 2017, US DoD

Salvatore Santangelo

(1976) Giornalista professionista e docente universitario. Esperto di politica internazionale e di storia del Novecento, si occupa delle nuove dimensioni dei conflitti e studia la sfera mitica dell'attualità occupandosi di "geosofia": l'esplorazione "dei mondi che si trovano nella mente degli uomini" (John K. Wright - Berkeley 1947). Tra le sue pubblicazioni: *Gerussia* (2016), *Babel* (2018) e *Geopandemia* (2020), tutte edita da Castelvechi.

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