ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI

Guerra politica, disinformazione e disattivazione neuronale

Marco Rota

RESEARCH PAPER
Marzo 2019

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI
www.fondazionegermani.org

L'Istituto Gino Germani, un ente senza fini di lucro costituito a Roma nel 1981 ha lo scopo di promuovere una sempre maggiore sinergia tra le scienze sociali e gli studi strategici.
L'Istituto svolge, in collaborazione con centri di ricerca, Istituzioni accademiche e organismi governativi in Italia e all'estero, attività di studio e ricerca interdisciplinare sui processi di modernizzazione e globalizzazione nel mondo contemporaneo.
L'Istituto dedica particolare attenzione all'analisi dei problemi dello sviluppo socio-economico, della democrazia e dell'autoritarismo, della sicurezza e della conflittualità nelle società contemporanee.

Marco Rota, consulente di business intelligence e political intelligence, è stato amministratore pubblico e membro di consigli di amministrazione sin da giovanissimo. Laureato con una tesi di storia moderna, dirige il Centro studi sull'intelligence "Mondi" ed è ricercatore associato dell'Istituto Gino Germani di Scienze Sociali e Studi Strategici di Roma. Collabora con il Laboratorio di Intelligence dell'Università della Calabria, con Babilon Magazine e Formiche. Da molti anni è a contatto con i massimi esperti di sicurezza e di intelligence, italiani e stranieri, con i quali studia le correlazioni tra spionaggio e sviluppo dei sistemi istituzionali, nonché la storia dello Stato in relazione al contrasto dei fenomeni criminali ed eversivi.

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI

GUERRA POLITICA, DISINFORMAZIONE E DISATTIVAZIONE NEURONALE

Marco Rota

RESEARCH PAPER
Marzo 2019

Le opinioni espresse sono strettamente personali e non riflettono necessariamente le posizioni dell'Istituto Gino Germani.

ISBN: 978-88-909073-7-1

ISTITUTO GINO GERMANI DI SCIENZE SOCIALI E STUDI STRATEGICI
Via di Valle Corteno 60 - 00141 Roma
fondazionegermani@gmail.com
www.fondazionegermani.org

«[…] history is clear: Nations with allies thrive.
America's alliances are a durable, asymmetric advantage
that no competitor in the world can match»
James Norman Mattis

«War is a means of communication»
Vladislav Surkov

Il quadro internazionale dopo il 1989

Il processo di Globalizzazione raggiunse l'apice del suo sviluppo con la vittoria atlantica sul Comunismo e il trionfo dei princìpi statuiti a Bretton Woods, coerenti con la visione di Wilson per «sécuriser le monde pour la démocratie […] contre la révolution irrationnelle»[1].

Questo fenomeno incontrò i primi ostacoli dopo l'attentato alle Torri Gemelle di New York ma soprattutto allo scoppio della crisi dei crediti *subprime* del 2008. In Occidente, dal 1945 ad oggi, la democrazia politica ha dato prova di funzionare in modo abbastanza ordinato, grazie al consolidamento della distinzione dei poteri, del suffragio universale e del *welfare state*. Un esito convalidato anche dalle transizioni relativamente pacifiche dei paesi dell'Europa orientale dopo il 1989, fatta eccezione per il caso jugoslavo.

L'articolazione dei poteri pubblici, tuttavia, versa in una crisi profonda. Per usare un gioco di parole, i *policy maker* hanno permesso la concentrazione di una ricchezza dissennata nelle mani di pochi (le élites private) a danno di molti (i cittadini). Questa sperequazione ha sospinto i molti ai margini della sopravvivenza, mentre i pochi continuano ad accedere a informazioni e risorse, *in primis* per ostacolare la prospettiva di un cambiamento dei rapporti di forza. Dal *Global Wealth Report 2018* di Credit Suisse possiamo estrapolare qualche dato.

> While the bottom half of adults collectively owns less than 1% of total wealth, the richest decile (top 10% of adults) owns 85% of global wealth, and the top percentile alone ac-

[1] Woodrow Wilson, *Le Président Wilson, la guerre, la paix. Recueil des déclarations du Président des Etats-Unis d'Amérique sur la guerre et la paix. 20 décembre 1916 – 6 avril 1918*, Librairie Berger-Levrault, Parigi 1918.

> counts for almost half of all household wealth (47%). The shares of the top 1% and top 10% in world wealth fell significantly between 2000 and 2008: the share of the top percentile, for instance, declined from 47% to 43%. However, the trend reversed after the financial crisis. The share of the top 10% was little affected. But in 2016 the share of the top 1% rose back above the level we estimate for 2000. The trend in the share of the top 1% partly reflects the trend in the share of financial assets in the household portfolio, which fell during 2000–08 and then began to rise after the global financial crisis, raising the wealth of many of the richest countries, and of many of the richest people.[2]

Fukuyama, che dopo il 1989 previde la «fine della storia» come esito felice per la civiltà occidentale, non comprese la questione dirimente: non c'era una fine della storia, ma l'avvento di problemi giganteschi, a cominciare dalle trasformazioni digitali e dai cambiamenti climatici, che diventavano problemi politici. Il *populismo* altro non è che una reazione a fenomeni complessi che si sono sedimentati per decenni e che ora sono esplosi. I flussi di rifugiati politici e di migranti economici dal Medio Oriente e dall'Africa, il sovvertimento minskyano delle «regole del gioco»[3] monetarie e finanziarie, la fine del lavoro, la crisi del welfare state, l'Intelligenza Artificiale, il bioterrorismo, le pandemie, le guerre per l'energia, il Jihādismo, sono questioni che potranno essere affrontate con politiche democratiche o tecnocratiche o autocratiche.

La digitalizzazione, inoltre, ha esteso il terreno di battaglia a livello globale, dove la proiezione del potere e l'interesse nazionale sono già regolati da dinamiche all'interno di reti più che dai comportamenti dei singoli Stati-nazione.

La sicurezza delle *infrastrutture critiche*, peraltro, è messa a repentaglio dalle stesse diseconomie cibernetiche. Emanuele Severino disse a proposito della tecnica: «L'incremento senza fine della potenza è destinato a diventare lo scopo del pianeta. Nessuna di quelle forze può avere pertanto la capacità di regolamentare quell'incremento. È esso a regolamentare sé stesso, cioè a espungere tutto ciò che lo ostacola o lo rallenta».

Per un lungo periodo, comunque, questi fenomeni saranno difficilmente governabili e produrranno insicurezza, instabilità, conflittualità sociale.

Le élites pubbliche hanno cessato di essere composte da «esseri eccezionali» e hanno fallito perché il loro modello di governance è stato superato dalla rivoluzione digitale. Il loro carisma, in senso "magico", non è più istitutivo di nulla, «cessa di compiere cose ritenute impossibili»[4].

La crisi politico-istituzionale europea è giunta all'apice ed è prevedibile che si determini una profonda trasformazione del modello di Maastricht perché il Vecchio Continente come sostiene George Friedman: «historically conflict is due to emerge again»[5]. Le istituzioni comuni europee, poi, sono state concepite per ammini-

[2] Credit Suisse, Global Wealth Report 2018, p. 9.

[3] Hyman Minsky, *John Maynard Keynes*, Bollati Boringhieri, Torino, 2009.

[4] Franco Ferrarotti, *Max Weber e il destino della ragione*, Laterza, Bari, 1985.

[5] George Friedman, *Flashpoints: The Emerging Crisis in Europe*, Geopolitical Futures paperback, Austin, 2016.

strare la prosperità nella libertà, più che per governare spirali recessive, e non hanno saputo governare le trasformazioni connesse alla Globalizzazione, proprio mentre la Cina si candida alla guida di un ben diverso processo di mondializzazione.

> From a mercantilist perspective, China's policy banks are often seen as agents of Chinese statecapitalism that employ subsidised capital to achieve a combination of commercial and geopolitical aims, while Chinese policy-makers claim that these banks simply serve to provide mutually beneficial 'development' opportunities for China and (often) its developing country partners. Without question, however, they are key tools in China's mixed, state-capitalist system and, as such, policy banks receive privileged access to capital, which they deploy globally for a combination of diplomatic and commercial goals.[6]

La crisi istituzionale dell'UE ha già definito dei blocchi regionali, che somigliano all'antica tetrarchia della Roma morente dopo Diocleziano: Germania e Francia in una dimensione, militare e industriale, di tipo neo-carolingio; un gruppo mediterraneo più marginale; il gruppo di Visegrad e i baltici o un'area geopolitica più articolata che colleghi Adriatico, Mar Baltico e Mar Nero.

Le élites franco-tedesche propugnano l'introduzione di un consiglio di sicurezza formato da un nucleo ridotto di Stati, un organo agile incaricato di migliorare capacità innovative ed efficienza dinamica nella temperie in un nuovo *Mercantilismo*. Questo nuovo ordine, però, presuppone che assurgano a nazioni di rango solo quegli Stati in grado di auto-riformarsi rapidamente, a livello centrale e periferico.

Questa sperimentazione istituzionale vuole scongiurare due rischi: il ripiegamento sul vecchio modello nazionale e il pericolo di secessione di pezzi di territorio, sull'esempio catalano. Dualità quali città/campagna, centro/periferia, inclusione/esclusione, sono le vere incubatrici dell'odio verso la Globalizzazione. Durante la prima metà del Novecento, anche i Totalitarismi hanno rappresentato una reazione nazionalistica e dispotica a fenomeni complessi di mondializzazione, provocando le conseguenze che conosciamo[7].

Possono essere tracciati due scenari possibili: o la fine del *Mercatismo* scuoterà l'establishment finanziario, probabilmente con una nuova crisi finanziaria, riequilibrando il dualismo tra élites private ed élites pubbliche, che vede queste ultime regolarmente sopraffatte dalle prime; o assisteremo a trasformazioni di tipo autocratico, con un deterioramento dei diritti individuali.

La crisi della liberaldemocrazia e le forze dispotiche

Dopo il crollo del muro di Berlino, Stati dittatoriali, partiti estremisti, fazioni terroristiche, criminalità organizzate, hanno acquisito una forza eccezionale e,

[6] Various Authors, *Hybrid Conflict: The Roles of Russia, North Korea and China*, Clingendael Institute, The Dutch National Network of Safety and Security Analysts (ANV), L'Aia, 2018, p. 29, https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf

[7] Vittorio Strada, *Totalitarismo e totalitarismi*, Marsilio, Venezia, 2003.

sfruttando la crisi delle élites pubbliche, hanno gradualmente logorato il sistema liberaldemocratico.

Russia, Cina, Iran, non sono Stati democratici. E in paesi europei come Italia e Ungheria, nonché in Turchia, Sudafrica, Bangladesh, Tanzania, nelle Filippine, si assiste al declino della *legal civilisation*, al diffondersi di una disposizione naturale dei cittadini all'accettazione di comportamenti xenofobi, antisemiti, populisti, che stanno spianando la strada all'introduzione di modelli illiberali.

Per facilità di espressione, chiamiamo tutti questi attori statali e non statali con la locuzione *forze dispotiche*, soggetti capaci di armonizzare i propri interessi geostrategici in funzione antioccidentale.

Giovanni Sartori, che rilesse e ridefinì i contributi teorici di Schumpeter e Downs, spiegò: «In passato il dittatore rovesciava la democrazia, il passaggio all'autocrazia era manifesto, rivoluzionario. Oggi questo processo avviene senza alcuna rivoluzione, senza neppure bisogno di riforme. Il caso più potente è la Russia di Putin: formalmente resta un sistema semipresidenziale, ma di fatto un uomo solo si è impadronito del potere e di tutti i contropoteri previsti per contrastarlo»[8].

In Russia, Vladimir Putin ha rimesso in primo piano il nesso tra *Civilizzazione* o *Civiltà* e Occidente; un argomento tutt'altro che nuovo nella cultura russa, utilizzato con efficacia per fini politici[9].

Il primo a introdurre il concetto di slavofilia e a parlare di «spirito russo» fu Aleksej Chomjakov[10]. A cavallo tra XIX e XX secolo, le questione del panslavismo e della singolarità della civiltà russa fu sollevata da Vladimir Solov'ëv e Nikolaj Berdjaev, da Nikolaj Danilevskij e Konstantin Leont'ev, mentre per tutti gli anni Novanta fino ai nostri giorni chi ha cercato di istituzionalizzare la tesi della Russia come civiltà piuttosto che come nazione è l'ideologo Aleksandr Dugin[11], un intellettuale con posizioni minoritarie poi allineatosi all'establishment e all'industria della comunicazione statale.

Dugin ha contribuito a fornire la necessaria base culturale alla nuova Russia di Putin. Egli, spinto dallo studio di autori "identitari" europei, ha contribuito in modo radicale a far riscoprire la cultura più anti-occidentale della storia intellettuale russa, fino ad abbracciare le teorie etnogenetiche di Lev Gumilëv.

Putin, dal suo ritorno alla presidenza nel 2012, ha puntato sul ruolo storico della Russia nelle relazioni internazionali. Parole come civiltà, moralità, spiritualità, ricorrono in ogni suo discorso pubblico, mentre valori come la famiglia eterosessuale, la nascita di molti figli e quindi la salute demografica della nazione; la lot-

[8] Giovanni Sartori, *Democrazia cos'è*, Rizzoli, Milano, 2007, p. 132.

[9] Cfr. http://www.au.af.mil/au/awc/awcgate/fmso/dialect.htm

[10] Natalino Valentini, *Volti dell'anima russa. Identità culturale e spirituale del cristianesimo slavo-ortodosso*, Paoline Editoriali Libri, Torino, 2012.

[11] Marlene Laruelle, *Aleksandr Dugin: A Russian Version of the European Radical Right?*, Woodrow Wilson International Center for Scholars, Kennan Institute, Washington, 2006, https://www.wilsoncenter.org/sites/default/files/OP294.pdf

ta all'alcolismo; il rispetto per la gerarchia e la burocrazia intese come tradizioni, stanno alla base della sua comunicazione con il popolo.

In Occidente, le élites pubbliche hanno sottovalutato a lungo l'attacco sferrato da queste forze per manipolare l'opinione pubblica europea e americana, così come il livello dello scontro tra la *società aperta* e i suoi nemici. I mezzi di penetrazione usati sono antichi e moderni: la televisione, la radio, la carta stampata, l'incremento di istituti di studio e di cultura, gli investimenti nel business sportivo, la penetrazione commerciale, l'aiuto occulto fornito a partiti e movimenti politici europei, tramite informazioni, affari, denaro.

> Russia's support for anti-establishment, populist, mostly far-right (but also sometimes far-left) political parties in Europe has become an established fact, proven by regular contacts with Russian parties and sometimes by financial contributions as well. In its hybrid conflict with the West, Russia uses such parties and movements pragmatically, whenever it suits its political agenda and without any ideological consistency. Parties could share Russia's agenda of promoting conservative values or show understanding for Russia's revisionism and more assertive foreign policies. Often they share a nationalist, anti-EU agenda and oppose anti-Russian sanctions or NATO's Enhanced Forward Presence. In the Netherlands, Russia has mainly focused on cultivating ties with the PVV, as its leader Wilders is looking at Russia as a potential ally against islamist terrorism and mass migration.[12]

La Cina investe ogni anno nella cosiddetta "informazione internazionale" un budget colossale di miliardi di Euro, usato per plasmare una realtà parallela ad uso e consumo del pubblico occidentale. Cina e Russia investono in quelle infrastrutture capaci di avere una proiezione globale: gran parte della programmazione di holding della comunicazione come RT in Russia e CGTN in Cina, è finalizzata a criticare l'Occidente e a pronosticarne il declino.

La stabilità tra le aree di influenza è perturbata; essa produce un'oscillazione perché siamo vicini ad un punto di rovesciamento che sposterebbe l'equilibrio a favore delle forze dispotiche. Se un simile cambiamento si verificasse, la nostra libertà cederebbe il passo a una definitiva prospettiva panottica.

L'ordine liberaldemocratico sta degenerando con un'accelerazione mai vista, benché sia riuscito a imporsi su *totalitarismi* come il Nazismo e il Comunismo sovietico.

La saldatura tra visioni di tipo sovranista, populista, neo-dirigista e attori come Russia e Iran è evidente e riguarda anzitutto le *dinamiche di influenza* di questi Stati.

Il Mediterraneo orientale resta per Mosca il principale punto nevralgico del proprio disegno geopolitico e geoenergetico, e la guerra in Siria ne è la conferma. L'obiettivo è quello di mantenere le posizioni acquisite ai tempi dell'Urss, in particolare la presenza della flotta navale nei porti siriani, in ossequio allo storico bisogno di uno sbocco nei mari caldi.

[12] Various Authors, *Hybrid Conflict: The Roles of Russia, North Korea and China*, Clingendael Institute, The Dutch National Network of Safety and Security Analysts (ANV), L'Aia, 2018, p. 12, https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf

La Russia, davanti all'opinione pubblica mondiale, cerca di accreditarsi come potenza alternativa alla gestione politico-militare americana in Medio Oriente: gli accordi bilaterali di partenariato economico o militare, siglati dalla Federazione Russa con Egitto, Turchia, Qatar, Iran, Israele e Arabia Saudita ne sono la dimostrazione, sebbene essi dipendano in larga misura da un'iniziale rimodulazione della presenza armata statunitense in Asia Minore:

> The American commandos would be shifted to neighboring Iraq, where an estimated 5,000 United States forces are already deployed, and "surge" into Syria for specific raids, according to two military officials who spoke on the condition of anonymity. The strike teams are one of several options — including continued airstrikes and resupplying allied Kurdish fighters with arms and equipment — in a new strategy for Syria that the Pentagon is developing as officials follow the order Mr. Trump gave on Wednesday for a military drawdown even as it tries to maintain pressure on the Islamic State.[13]

La Russia si è posta al centro di un preciso disegno internazionale e per costruirlo sta condividendo con altri Stati e attori dispotici informazioni d'intelligence, ricerca scientifica, infrastrutture, tecnologie militari e civili; Mosca non si è limitata a reprimere le voci del dissenso, ma ha cominciato dalla fine degli anni Novanta a influenzare la politica dei paesi democratici. Dal *Munich Security Report* del 2019 si può apprendere con chiarezza il ruolo svolto da Mosca nell'ambito delle nuove tensioni internazionali.

> At the same time, the Russian government has aggressively used its limited but significant leverage as a disruptive force and scored some impressive short-term victories in recent years, taking the rest of the world by surprise in Ukraine and Syria. Other recent examples of Moscow's increasing assertiveness under Vladimir Putin's leadership, who was re-elected for a fourth term in May 2018, are the Skripal Affair, an escalation of hostile cyber activities, attempts to interfere in democratic elections in various countries, or the most recent confrontation in the Kerch Strait.[14]

Il concetto di *political warfare* degli Stati e delle multinazionali

La *guerra politica*, classicamente, indica una gamma di operazioni diverse da quelle di tipo militare, ed è finalizzata a conseguire specifici obiettivi di natura politica[15]. Nella guerra politica, che rappresenta il "genere", le "specie" che la compongono sono la diplomazia coercitiva, la diplomazia pubblica, la propaganda

[13] Cfr. https://www.nytimes.com/2018/12/21/us/politics/pentagon-syria-iraq-kurds.html

[14] Cfr. https://www.securityconference.de/en/publications/munich-security-report/munich-security-report-2019/, p. 9.

[15] Angelo Maria Codevilla, *Political Warfare: Means for achieving political ends, Strategic Influence: Public Diplomacy, Counterpropaganda and Political Warfare*, The Institute of World Politics Press, Washington, 2008.

bianca o nera, la corruzione, la sovversione, l'inganno (che in origine gli americani definirono con l'acronimo MILDEC (*Military Deception*)[16]. Washington riprese questa classificazione dai britannici, che nel 1941 diedero vita al *political warfare executive*, un lungimirante spettro di attività tese a influenzare potentemente lo stato sensorio-percettivo degli abitanti del Terzo Reich, in Germania e negli Stati occupati. George Frost Kennan, durante la Guerra Fredda[17], fece proprie e perfezionò queste elaborazioni, che trovarono applicazione su larga scala nella difesa della cortina di ferro fino al 1991.

Le operazioni peculiari della guerra politica e più in generale la *guerra ibrida* (*hybrid warfare*) consentirono di fronteggiare, successivamente, la prima fase tecnologica della guerra ibrida russa, la *guerra senza limiti* cinese[18], quella *asimmetrica* iraniana con le sue capacità "non cinetiche", rimodulando ciclicamente gli studi e le operazioni in ordine a minacce come la *disinformazione* e le dinamiche d'influenza.

Con la fine del bipolarismo internazionale, i governi occidentali misero in sottordine la *political warfare*, ma da allora persero la capacità di condizionare nel senso voluto il corso degli eventi politici e geopolitici in alcune aree del mondo. Si trattò, con evidenza, di una scelta dovuta al venir meno della tensione ideologica tra i blocchi contrapposti. Una preferenza che iniziò ad esporre gli Stati democratici all'influenza di potenze come la Cina, che gli stessi americani avevano riconosciuto politicamente a partire dal *comunicato di Shangai*, in funzione anti-sovietica.

Gli Stati utilizzano la guerra politica a supporto di obiettivi interni o esterni, attraverso interventi palesi o occulti; essa consiste nell'uso di informazioni, messaggi, espedienti, al fine di modificare la volontà del pubblico target attraverso la propaganda, la contro-propaganda, l'ideologia, la disinformazione. François Géré, in un pregevole saggio sugli aspetti sociali della guerra politica, ne chiarisce le modalità.

> Ci sono tantissimi tipi di disinformazione, ma tutte sfruttano le debolezze e le angosce profonde dell'essere umano, i suoi desideri, le sue ansie e paure. Vi sono molteplici temi legate alle debolezze umane che vengono sfruttate nelle campagne di disinformazione come ad esempio i bambini, la salute (ad esempio la paura di epidemie), il sesso, il denaro, l'«Altro» (ebrei, neri, musulmani, etc.).[19]

Le attività di *deception* possono avere un orizzonte temporale limitato nel tempo, cioè a medio o breve termine, e obiettivi più o meno contenuti, coinvolgendo

[16] Cfr. https://apps.dtic.mil/dtic/tr/fulltext/u2/a470825.pdf

[17] *Policy Planning Memorandum, Records of the National Security Council*, NSC 10/2, RG 273, National Archives and Records Administration, 4 May 1948.

[18] Liang Qiao, Xiangsui Wang, *Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e Globalizzazione*, Libreria editrice Goriziana, Gorizia, 2001.

[19] François Géré, "L'avvenire radioso della disinformazione", in *Disinformazione e manipolazione delle percezioni. Una nuova minaccia al Sistema-Paese*, a cura di Luigi Sergio Germani, Eurilink University Press, Roma, 2017, p. 43.

la sfera politica, diplomatica, economico-finanziaria e attori plurali come uomini di partito, diplomatici, ministri, vertici di apparati burocratici, membri dell'intelligence, soggetti dello stato maggiore delle forze armate[20].

Va messo in luce, tuttavia, uno scenario inedito che non riguarda gli attori statali. La sconfitta delle élites pubbliche a vantaggio delle élites private ha segnato il trionfo delle classi dirigenti a capo di giganti dell'energia e del web, multinazionali oligopolistiche capaci di influenzare tutto il sistema dei media non solo in ordine alle preferenze commerciali dei consumatori. Pertanto, le élites private sono diventate esse stesse *policy maker*, non sono più solo operatori del mercato riuniti in gruppi d'interesse.

Il concetto di guerra politica è antico ma a partire dalla fine degli anni Sessanta la sua applicazione è stata mutuata e ottimizzata anche dalle grandi corporation, dotate di mezzi finanziari ciclopici. I regolatori, i regolati, le regolamentazioni, nel tempo sono divenuti quasi indistinguibili. I detentori del potere reale controllano i media, influenzano la quasi totalità delle decisioni economiche e di quelle politiche, che hanno un'incidenza sullo sviluppo della società umana.

Per poterlo fare, queste élites private beneficiano anzitutto i loro sostenitori politici, a difesa della propria quota di ricchezza dentro il perimetro del *Crony Capitalism*[21]. Non sorprende che esse si servano degli strumenti della *guerra economica*, ma preoccupa che possano accedere a quelli della guerra politica con il possesso di file - riguardanti non solo la privacy personale - per manovrare l'opinione pubblica, corrompere la burocrazia, suggellare o modificare accordi commerciali e relazioni internazionali.

Si configura un'attività sofisticata, da parte di soggetti privati, sottesa alla *manipolazione delle percezioni*. L'obiettivo è indebolire le élites di genesi elettiva o burocratica, alterare le sensazioni e le convinzioni, con effetti sulla vita politica e, a cascata, sul *decision-making* statale in relazione ad ambiti come quello legislativo, commerciale, militare[22]. Le multinazionali utilizzano con abilità gli strumenti dell'intelligence, in particolare quel ventaglio di opzioni che comprende *business intelligence, competitive intelligence*, *political intelligence*, ma anche altri interventi di natura occulta e più pervasiva.

Quando la platea dei governanti non è più in grado di auto-riformarsi, prende il sopravvento l'anarchia dei governati. E laddove il modello liberaldemocratico si disgrega, in specie per mancanza di velocità nelle decisioni - da parte di coloro che dovrebbero esigere il rispetto dell'ordinamento giuridico e dell'autentica concorrenza per il mercato - proliferano e si cementano le giustizie private, i predomini privati, le ramificazioni delle criminalità organizzate.

[20] Edward Waltz, *Information Warfare: Principles and Operations*, Artech House on Demand, London and Norwood, 1998.

[21] Joseph Stiglitz, *Il prezzo della disuguaglianza. Come la società divisa di oggi minaccia il nostro futuro*, Einaudi, Torino, 2013.

[22] Richard Posner, *A Failure of Capitalism*, Harvard University Press, Cambridge, 2009.

L'Occidente è terreno di conquista politica ed economica per *rogue states*, gruppi terroristici, mafie, ma anche per corporation assurte a soggetti politici globali privi di una legittimazione politica, in un crescendo in cui controllori e controllati migliorano ogni giorno le proprie strategie offensive e difensive, nello spazio fisico e in quello cibernetico.

La guerra ibrida russa come economia della forza

Gli analisti citano l'espressione *guerra ibrida* spesso in sostituzione di altre locuzioni come *gray zone strategies*, *competition short of conflict*, *new generation warfare*. La dottrina della guerra ibrida russa, che comprende le operazioni della *guerra convenzionale*, della guerra politica, della *cyberwarfare* e della *guerra irregolare*, confonde la separazione tra tempo di pace e tempo di guerra: «The infosphere, understood as a body of general and specialized programs for creating, processing, and storing computerized data, is bound to become one of the most likely objects of military confrontation»[23].

La *guerra dell'informazione* russa ha un carattere *olistico* e si connota come un'attività perennemente in corso, a prescindere dalle relazioni internazionali e diplomatiche intrattenute con gli altri Stati.

Nikolaj Ogarkov, capo di Stato Maggiore sovietico durante gli anni Ottanta, fu tra i primi analisti militari a evocare i mutamenti della guerra, coniando il termine *Military-Technical Revolution* (MTR) per spiegare il passaggio epocale dall'esercito tradizionale (di massa) alle operazioni della *guerra elettronica*, gettando le basi per l'estensione della *strategia russa di inganno* (*Maskirovka*) a tutti i livelli e a tempo indefinito. Nell'analisi *Russia's Approach to Cyber Warfare*, elaborata per CNA da Michael Connell e Sarah Vogler, si legge che

> The information contained in the comments and posts by the trolls ranges from misleading to verifiably fraudulent. Western observers and Russian anti-government activists have noted, however, that the role of the Russian internet troll is not necessarily to persuade its audience to a pro-Russian perspective but rather "to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space[24].

L'uso di strategie ibride da parte della Russia è cresciuto notevolmente durante gli ultimi due decenni; ciò è dovuto ad un aumento delle capacità militari russe ma anche all'indebolimento delle strategie convenzionali sovietiche usate durante la Guerra Fredda. Dallo studio delle elaborazioni teoriche di Sergej G. Čekinov e Ser-

[23] A.N. Kukashin e A.L. Yefimov, "The Security of the Infosphere of Strategic Defense System", in *Military Thought*, n. 5, 1995.

[24] Michael Connell, Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA Analysis &Solutions, Arlington, 2016, p. 19, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

gej A. Bogdanov, si evince come queste operazioni, attraverso campagne politiche, informative, economiche, cibernetiche, ecologiche, abbiano lo scopo di riequilibrare lo svantaggio competitivo rispetto ai paesi occidentali, causato fondamentalmente da un divario tecnologico più ancora che economico.

> Despite Russia's strengths in the sphere of armaments production, the deficiencies evident across the wider range of civilian technology are likely to serve as a source of economic weakness in the future. Economic development - often labelled as modernization and diversification - at home will be shaped much more by rising levels of technology of investment and production across the civilian economy, than by any niche areas of comparative advantage in the military sphere, contrary to hopes expressed by Vladimir Putin that the Russian defence industry might serve as a 'locomotive of technological development'.[25]

Nel 2006, in occasione di un messaggio annuale all'Assemblea Federale, Vladimir Putin ebbe a dire: «Dobbiamo tenere conto dei piani e delle direzioni di sviluppo delle forze armate di altri paesi […] Le nostre risposte devono essere basate sulla superiorità intellettuale, esse saranno asimmetriche e meno costose»[26]. Russia e Cina, a grandi linee, utilizzano operazioni ibride per obiettivi rispettivamente difensivi e offensivi[27], in maniera ciclicamente più o meno aggressiva. La Cina, che pure è alle prese con molte criticità strutturali al suo interno, è una potenza che ha una visione geostrategica globale.

> La Cina sta attraversando una trasformazione essenziale sebbene complessa, diretta a una crescita più sostenibile attraverso un riequilibrio degli investimenti e della produzione manifatturiera a favore dei consumi e dei servizi. […] Inoltre, l'interdipendenza economica probabilmente produrrà alcuni effetti di ricaduta che varieranno a seconda dei paesi e delle regioni. L'integrazione globale è fondamentale per tutte le economie e non vi è alcun interesse in una guerra commerciale o nel protezionismo. La conservazione della proprietà pubblica quale pilastro dell'economica cinese non è sostenibile. Si rendono inevitabili riforme per affrontare le cause all'origine dell'eccesso di capacità produttiva in vari settori industriali e il ruolo delle imprese statali. Occorre affrontare problematiche nazionali, come sollevare milioni di persone dalla povertà e ridurre le diseguaglianze economiche in continua crescita nonché la corruzione endemica.[28]

Inoltre, si può evidenziare qualche elemento degno di nota.

> China has moved from being a developing economy before the Great Recession to a developed economy a decade later. Not only the speed of the growth of debt, but also the debt's

[25] Natasha Kuhrt, Valentina Feklyunina, *Assessing Russia's Power: A Report*, Bisa, King's College London, Newcastle University, 2017, p. 23, https://www.bisa.ac.uk/files/working%20groups/Assessing_Russias_Power_Report_2017.pdf

[26] *Krasnaya zvezda*, 11 maggio 2006.

[27] Cfr. https://rand.org/pubs/perspectives/PE310.html

[28] Anna Saarela, *La trasformazione della Cina e l'interdipendenza economica globale*, Direzione delle politiche esterne, Parlamento Europeo, 2017,
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/570484/EXPO_STU(2017)570484_IT.pdf

composition is a concerning issue. Almost half of it comes from the real estate sector and related industries, and at least another 30 percent is the product of shadow-banking intermediaries, whose financial discretion is highly doubtful.[29]

In questo scenario, la Cina, divenuta più aggressiva a causa della guerra commerciale con gli Usa, dopo un periodo di relativa tregua instaurata durante l'amministrazione Obama, rappresenta il vero pericolo per il sistema liberaldemocratico[30]. Il suo disegno di dominio, la ricerca di una nuova egemonia nel Pacifico, la penetrazione economica e finanziaria in Europa e in Africa, indicano che Pechino non è solo alla ricerca di energia e materie prime per mantenere la propria struttura nazionale e la propria geopolitica regionale, ma vuole soppiantare la leadership americana a livello mondiale.

La Russia, al contrario, fa uso della guerra ibrida per fornire risposte a interrogativi politici, connessi alla sopravvivenza stessa dello Stato, e per farlo punta a ottenere obiettivi mirati e di medio-periodo: orientare la politica estera ed economica dei governi europei più fragili; creare pretesti per sviluppare conflitti armati in ambito regionale; annettere territori confinanti; garantire agli Stati europei l'accesso al mercato russo (gas, armamenti, ecc. ecc.) a condizioni vincolanti.

Secondo James Wirtz, esperto di studi strategici, la Federazione Russa più di ogni altro attore statale è riuscita ad escogitare un modo per integrare la guerra cibernetica in una più ampia strategia per raggiungere questi fini: «Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives»[31]. Nell'ultimo *Global Threat Report Adversary Tradecraft and the importance of speed* si sottolinea che «It is quite remarkable to see that Russia-based threat actors are almost eight times as fast as their speediest competitor — North Korea-based adversaries, who themselves are almost twice as fast as intrusion groups from China," CrowdStrike says in the threat report»[32].

Il conflitto ibrido russo è caratterizzato da alcune specifiche caratteristiche. La guerra è *perpetua*: il grado d'intensità del conflitto che resta in perenne evoluzione. Le strategie ibride sono sempre in corso, sebbene in certi momenti possano acutizzarsi, intensificarsi o incrociarsi con operazioni convenzionali. C'è un'*economia del ricorso alla forza*: la Russia è consapevole di avere poche possibilità di vincere un conflitto convenzionale con la NATO, e cerca di perseguire il proprio interesse nazionale senza ingaggiare un conflitto militare, laddove sia possibile. La Rus-

[29] Cfr. https://mises.org/wire/chinese-bomb-are-we-really-threshold-another-global-financial-crisis?fbclid=IwAR1YMWhV6jutwdWS8JqArA9u9V3Pjzo-Aj9EabbQ4BDVN3pCXS5Qf-0s9HE

[30] Cfr. https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836

[31] James Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power Into Grand Strategy", in *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications, Tallinn, 2015, p. 31.

[32] Cfr. https://assets.documentcloud.org/documents/5743766/Global-Threat-Report-2019.pdf

sia può ancora usare la minaccia nucleare come parte di una strategia ibrida, ma preferisce ridurla al minimo così come l'impiego della forza militare tradizionale. L'uso della cyberwar è un esempio illuminante di come la Federazione Russa faccia economia dell'uso della forza, razionalizzando le risorse umane ma soprattutto quelle economiche. Inoltre, la guerra dell'informazione russa è il risultato di una lunga osservazione poiché durante l'ultimo quarto di secolo i suoi studiosi e i suoi militari hanno osservato e analizzato le tecniche di combattimento degli Stati Uniti e dei suoi alleati nei Balcani e in Medio Oriente.

Infine, segnalo la mia definizione di *congiunzione dei tavoli paralleli* o *partita su molti tavoli* (*poker on many tables*). Dal 1989 ogni Stato ha giocato e gioca sulla scacchiera internazionale una singola partita contro un altro Stato, su tavoli diversi ma paralleli ed egualmente importanti, cioè la partita energetica, geopolitica, commerciale, militare, finanziaria (quella legata ai fondi sovrani, *sovereign wealth fund*). Solo gli Stati forti possono sopravvivere a tutte le partite contemporaneamente; gli Stati deboli, invece, sono esposti in continuazione alle minacce della guerra dell'informazione (*information warfare*) e più di altri a quelle della *guerra economica*.

La Russia predilige l'adozione di schemi e approcci semplificati, cioè congiungere i tavoli, costruire alleanze e pianificare strategie con Stati storicamente alleati o prossimi, ideologicamente affini, *Stati-cuscinetto* confinanti.

Gli Stati più vulnerabili - tra cui l'Italia - sono quelli tradizionalmente più esposti alla corruzione politica o quelli in cui alcuni soggetti politici ed economici, pubblici e privati, condividono gli interessi e gli obiettivi geostrategici russi. Anche attori statali forti come Stati Uniti, Regno Unito, Germania, Francia, sono minacciati da queste operazioni.

> The main challenge is not that Russia's media and security services have highly sophisticated new instruments to influence the German or European public; it is how they use and promote existing anti-US, anti-EU, anti-media, anti-establishment and anti-migrant feelings. Most elements of the narratives pushed by Russia already exist in growing parts of European societies, which criticise the inability of the governing elites to solve their countries' problems in an increasingly complex world. This self-doubt is supported by Russia's international media, whose main goal is to 'build up a counter-public as well as show media manipulation' in the German public discourse.[33]

Nel 2014, la Russia ha impiegato operazioni ibride culminate con l'annessione della Crimea, territorio facente parte dell'Ucraina. Sebbene il conflitto abbia avuto dei precedenti politici, risalenti all'epoca della dissoluzione dell'URSS, Mosca ha capitalizzato le instabilità interne dell'Ucraina per infiltrare un gran numero di *little green men* - forze armate non convenzionali e non identificabili, ritenute inqua-

[33] Various Authors, *Hybrid Conflict: The Roles of Russia, North Korea and China*, Clingendael Institute, The Dutch National Network of Safety and Security Analysts (ANV), L'Aia, 2018, p. 9, https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf

drate nelle forze speciali russe - che hanno occupato i punti chiave geografici e istituzionali, proclamandosi come forza separatista.

La Russia ha sempre negato la responsabilità di queste azioni, ma nel marzo 2014 gli eventi hanno subìto un'accelerazione finché le proteste filorusse e antiucraine si sono militarizzate e i separatisti nel Donbas (o Donbass) hanno dichiarato unilateralmente l'indipendenza dall'Ucraina. Tutto questo è avvenuto in modo tale da evitare le ritorsioni e senza provocare un'incursione militare da parte della NATO o delle singole potenze occidentali, facendo leva sul supporto di una massiccia campagna di disinformazione, sul web e con i mezzi di comunicazione tradizionali come la televisione.

Il ministro degli Esteri russo Lavrov, in risposta alle accuse rivolte alla Russia a proposito degli eventi ucraini e alla richiesta di un *cessate il fuoco*, ha risposto: «Before demanding from us that we stop doing something, please present proof that we have done it». La Russia ha sperimentato queste operazioni sin dal 2008 con l'invasione della Georgia e prima ancora in Cecenia.

> The term hybrid was first linked with warfare by William Nemeth in his Naval Postgraduate School thesis on the Chechen war in which he proposed that for the Chechens the war amounted to much more than the battlefield itself. Militarily they brought together regular and irregular methods in a highly flexible combination. However, they also perceived war "in a wider, non-linear sense and hence, in addition to field tactics, they also employed all the means of the information age to gain an advantage over their enemies." In Nemeth's estimation this style of warfare was made possible by the structure of Chechen society and was specific to it.[34]

I *conflitti congelati* in Ucraina e il teatro georgiano-osseto hanno minato gli sforzi politici ed economici esercitati da queste nazioni, finalizzati a integrarsi con l'Occidente e con l'Unione Europea sul piano delle relazioni internazionali ed economiche. Un altro obiettivo è quello di creare il pretesto per un'azione militare: l'annessione della Crimea ha generato preoccupazioni rispetto alla possibilità che il Cremlino utilizzi le stesse operazioni ibride creando il pretesto per un'azione militare anche altrove, ad esempio al confine con gli Stati baltici.

La Russia potrebbe fare pressioni sulla minoranza russa della popolazione in uno Stato come l'Estonia, costruendo una narrativa dei media che descriva questo governo come repressivo, quindi sfruttando le divisioni interne di uno Stato sovrano per giustificare un intervento militare a protezione della minoranza di lingua russa.

Considero un caso di guerra ibrida quello dei cosiddetti *gilets jaunes*, in Francia. Un movimento legato all'estrema destra internazionale, sostenuto da evidenti sforzi di manipolazione delle percezioni finalizzati alla sovversione, posti in essere in funzione anti-francese.

[34] Martin Murphy, *Understanding Russia's Concept for Total War in Europe*, 2016, https://www.heritage.org/node/10472/print-display.

> La deuxième vague de l'enquête sur le complotisme confirme plusieurs enseignements par rapport à la précédente, dont celui-ci : le positionnement politique, notamment à l'extrême droite, reste une des variables induisant une adhésion plus forte que la moyenne aux représentations conspirationnistes.[35]

Il coordinamento della guerriglia urbana è composto anche da ex combattenti filo-russi già operativi nel Donbas[36]; questo movimento serve ad influenzare l'opinione pubblica francese ed europea su argomenti di natura politico-economica al fine di indebolire il governo di Parigi, le riforme della presidenza Macron e l'integrazione con le politiche tedesche nel nuovo assetto neo-carolingio. Oggi la Repubblica francese, insieme al Regno Unito, è il principale avversario europeo della Russia di Putin. Mark Galeotti ha sintetizzato che

> One distinctive aspect of recent Russian campaigns, from political operations against the West to military operations in Ukraine, has been a blurring of the borders between state, paramilitary, mercenary, and dupe. The Putin regime evidently believes that it is at war with the West — a geopolitical, even civilizational struggle — and is thus mobilizing every weaponizable asset at its disposal. This extends to mining society as a whole for semi-autonomous assets, from eager internet trolls and "patriotic hackers" to transnational banks and businesses to Cossack volunteers and mercenary gangsters.[37]

Un aspetto particolarmente interessante è anche il nesso tra guerra ibrida russa e criminalità organizzata. Questa correlazione affonda le sue radici nel periodo sovietico, quando alcuni *apparatčik* della *nomenklatura* instaurarono relazioni e affari, reciprocamente vantaggiose, con il mondo della criminalità. La burocrazia non solo tollerò l'attività criminale ma la supportò e la protesse. Gli stessi membri del Partito Comunista e i funzionari pubblici furono indirettamente alla guida del crimine organizzato, abusando delle posizioni di potere, del livello informativo e delle risorse statali. Secondo un articolo pubblicato dal Centro Studi Internazionali di Roma, che sintetizza uno studio di Mark Galeotti:

> Le connessioni con lo Stato russo e gli apparati di intelligence e sicurezza governativi e la presenza sul territorio europeo rendono il RBOC [*Russia-Based Organized Crime*] uno strumento flessibile ed efficace per le azioni del Cremlino nell'ambito della guerra ibrida. Nello specifico, diverse sono le attività che Mosca può commissionare agli esponenti del crimine organizzato. Innanzitutto, i criminali possono essere assoldati per eseguire omicidi di personalità rilevanti quali ex spie, giornalisti anti-governativi, oppositori politici e imprenditori o oligarchi invisi alla cerchia di potere statale. In secondo luogo, gli elementi del RBOC, qualora dispongano di spiccate capacità informatiche, possono essere utilizzati per la condu-

[35] Cfr. https://jean-jaures.org/nos-productions/enquete-complotisme-2019-le-conspirationnisme-et-l-extreme-droite

[36] Cfr. https://www.francetvinfo.fr/economie/transports/gilets-jaunes/enquete-franceinfo-quand-l-ultra-droite-tente- d-infiltrer-les-gilets-jaunes_3180061.html

[37] Cfr. https://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/

zione di operazioni di cyber-warfare, incluse violazioni di archivi e banche dati, sottrazione di informazioni preziose o attacchi a reti e infrastrutture critiche. Come se non bastasse, l'abilità di muoversi attraverso i canali finanziari legali ed illegali permette alla criminalità di movimentare ingenti quantità di denaro e aggirare gli ostacoli e le limitazioni poste in essere dal regime sanzionatorio imposto al Cremlino dopo l'annessione della Crimea. Infine, grazie al controllo del territorio e alle reti di contatti con le criminalità locali dei singoli Paesi europei, le organizzazioni russe possono partecipare ad attività che rientrano sotto l'ombrello delle cosiddette "misure attive" (*aktivnye meroprijatija*), ossia le operazioni illegali all'estero di FSB, GRU e SVR. Tra queste, possono essere menzionate l'esfiltrazione di individui di alto valore politico o militare, l'influenza e il controllo sulle comunità russe all'estero, il monitoraggio e la sorveglianza di soggetti posti sotto osservazione. La Russia utilizza il RBOC per minimizzare i costi delle operazioni e i rischi politici derivanti dall'assunzione di responsabilità diretta di determinate azioni illegali. Questo porta a risultati efficienti in qualsiasi questione di stampo politico ed economico a livello internazionale e fornisce consistenti benefici agli obbiettivi di penetrazione del Cremlino.[38]

Due gli scenari possibili: lo scenario dello *scontro indiretto* o *per procura* (*proxy*) della Russia con l'Occidente, e in specie con gli Stati Uniti. Oppure lo scenario *inerziale*, che si basa sulla difesa delle posizioni e dei risultati geopolitici raggiunti in questi anni, con repentine operazioni di disturbo/contrasto rispetto agli interessi occidentali, sempre in un'ottica di rapporto asimmetrico in alcuni casi coordinato con altri Stati come Cina, Iran e altri paesi sudamericani e africani.

La manipolazione delle percezioni e le conseguenze sociali

In procinto di assistere all'applicazione su vasta scala delle prime forme di *Artificial Intelligence* (AI), sia nell'ambito militare sia nell'ambito del controllo e della sorveglianza civili, l'influenza e la manipolazione delle percezioni, che si stanno evolvendo in maniera parallela allo sviluppo dell'informazione, sono tematiche fondamentali per gli analisti d'intelligence ma anche per gli studiosi dell'AI applicata ai robot umanoidi.

I conflitti militari convenzionali, che sono sempre finalizzati a garantire risultati politici, rappresentano ormai la minima parte della guerra perpetua contemporanea. Andrea Zapparoli Manzoni così descrive gli aspetti più salienti delle guerre cibernetiche in corso:

L'aspetto più problematico del *"new normal*" è la possibilità per gli Stati di far "scivolare" senza troppo clamore la gestione dei propri conflitti sempre più verso il piano "cyber", innalzando continuamente il livello dello scontro senza dover fare ricorso ad eserciti ed armamenti tradizionali. In un mondo multipolare del quale Internet e l'ICT sono ormai parte integrante (ed insostituibile), questo significa entrare in una fase storica di cyber-guerriglia permanente, sempre più feroce, ovviamente non dichiarata ed anzi sistematicamente negata (sia dagli attaccanti che, in alcuni casi, addirittura dalle vittime).

[38] Cfr. https://cesi-italia.org/articoli/909/la-criminalit-organizzata-al-servizio-della-guerra-ibrida-russa

Per la natura dei mezzi utilizzati, questa dinamica non provoca particolare allarme o rifiuto da parte delle opinioni pubbliche e dà ai partecipanti la sensazione di poter esercitare forme di pressione sempre maggiori senza doverne rendere conto, dato che il rischio di subire le conseguenze di una loro attribuzione rimane remoto - ritenendo anche in caso di attribuzione di poter comunque evitare ritorsioni troppo costose, il che naturalmente è un incentivo ad alzare continuamente la posta. Basti pensare ad ExPetr/NotPetya, il singolo attacco più grave di sempre (costato oltre 10 miliardi di dollari), che ha avuto conseguenze planetarie (pur essendo mirato inizialmente all'Ucraina) ed è stato ufficialmente attribuito alla Russia da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda (c.d. "Five Eyes").

In altri tempi e contesti, una simile provocazione avrebbe causato una risposta militare, oggi invece dopo un fatto del genere molti Paesi (inclusi molti considerati minori) invece che protestare lavorano silenziosamente al prossimo NotPetya, trasformando così il mondo intero in un campo di battaglia, con la linea del fronte che passa (non incidentalmente, ma by design) dalle case dei cittadini, dagli uffici, dalle fabbriche e dalle infrastrutture critiche di tutto il pianeta. Va detto senza troppi giri di parole che questi crescenti livelli di cyber-attrito rappresentano ormai un "*clear and present danger*" per la nostra civiltà digitale e possono in qualsiasi momento, per un errore di valutazione o a causa di un'escalation tra due o più parti, determinarne il collasso. [....] Un secondo elemento di grave preoccupazione è legato alle attività di cyber-spionaggio e sabotaggio, che sono in netta crescita ed assumono ormai le forme più svariate, dalla ormai costante "guerra della percezione" realizzata tramite *fake news* amplificate via Social Media all'infiltrazione di infrastrutture critiche , aziende ed istituzioni , al furto sistematico di ogni genere di informazioni per finalità geopolitiche, di predominio economico e tecnologico, di ricognizione e di "preparazione del terreno" in vista di ulteriori attacchi. Questo genere di minaccia è sempre più diffuso per due ragioni fondamentali: da un lato le vittime non sono assolutamente strutturate per difendersi da questa tipologia di attaccanti, e dall'altro forze dell'ordine e servizi di sicurezza non hanno le risorse sufficienti per presidiare efficacemente questo fronte, anche considerato che la superficie di attacco potenziale è sostanzialmente infinita. Un ulteriore motivo di preoccupazione legato alle attività di cyber-spionaggio e sabotaggio scaturisce dal fatto che per gli attaccanti, con particolare riferimento a potenze minori/emergenti come Russia e Cina, ma anche Iran e Corea del Nord, le "barriere all'ingresso" sono molto basse ed il rapporto costi-benefici è molto favorevole, il che tra l'altro ha stimolato la proliferazione di gruppi mercenari *state-sponsored* che realizzano campagne su commissione come *subcontractor* di strutture governative, e di un ecosistema globale di fornitori di tecnologie e soluzioni "chiavi in mano" che sviluppano strumenti sempre più potenti e sofisticati, di una qualità ben diversa rispetto a quelli utilizzati dal Cybercrime, a supporto di queste operazioni. L'affermarsi di questo modello, che potremmo definire di "*espionage-as-a-service*", aumenta ulteriormente i livelli di rischio complessivi derivanti da questo genere di attività, di per sé già particolarmente dannose, dal momento che questi mercenari sono difficilmente controllabili e spesso si comportano come cybercriminali, in alcuni casi addirittura compiendo cyber-rapine per finanziarsi o per aumentare i propri profitti, il che rappresenta un ulteriore moltiplicatore di danno.[39]

Alessandro Magno ci ha consegnato una delle prime interpretazioni del problema, secondo la quale l'impiego della propaganda è utile a proteggere le vittorie an-

[39] Andrea Zapparoli Manzoni, Introduzione al *Rapporto Clusit 2019*, Security Summit, Milano, 12 Marzo 2019.

che al cessare delle ostilità[40]. Le attività odierne di manipolazione, dirette a mutare le percezioni degli abitanti di un altro Stato - come ha spiegato Valery Gerasimov - assumono un valore particolarmente importante grazie al fatto che rafforzano indirettamente le capacità militari e il vantaggio competitivo di chi ne fa uso: «The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy»[41]. Lo Stato che raggiunge obiettivi politici senza ricorrere all'uso della coercizione, non solo evita i costi economici e sociali connessi ad un conflitto (la già citata economia del ricorso alla forza), ma spesso depotenzia o neutralizza le capacità militari del suo avversario. In ordine alle tecniche di combattimento, normalmente gli istruttori di tattica militare discutono di come interrompere la cosiddetta *kill chain*[42] cioè in origine la struttura a fasi di un attacco. La catena è costituita dall'identificazione del bersaglio, l'esercizio di una forza sul bersaglio, la decisione, l'ordine di attaccare il bersaglio, la neutralizzazione del bersaglio. La corporation Lockheed Martin ha adattato questo concetto alla sicurezza del livello cibernetico, come metodo per neutralizzare l'intrusione in una rete di computer[43].

L'economia del ricorso alla forza ha trasformato la *kill chain*, per necessità, in una *strategia di contenimento*. Gli americani, come abbiamo visto, la usano al fine di proteggersi da una minaccia cibernetica (e non solo), i russi per rendere sostenibile la guerra ibrida.

L'approccio russo al problema, sulla scorta degli studi di Liddell Hart, studioso britannico di tattica e strategia militare nonché padre della teoria dell'*approccio indiretto*[44], insegna che il metodo *proxy* è quello decisivo nel mondo contemporaneo: il nemico deve essere colto di sorpresa e va attaccato non dove è più forte bensì dove è più debole. Mosca deve rompere la catena delle uccisioni - per usare una metafora - stando a debita distanza dall'avversario, senza ingaggiare un combattimento convenzionale.

Nel 1956 Robert Oppenheimer mise in guardia i governi dall'impiego irresponsabile della psicologia per influenzare gli esseri umani, ricordando come questo genere di attività potesse nuocere alla società più dell'uso sconsiderato della fisica e delle armi nucleari. Secondo Oppenheimer, la psicologia avrebbe potuto sviluppare «the most terrifying prospects of controlling what people do and how they think and how they behave and how they feel»[45].

[40] Haroro Ingram, *A Brief History of Propaganda during Conflict: Lessons for Counter-Terrorism Strategic Communications*, ICCT International Centre for Counter-Terrorism, L'Aia, 2016, https://www.icct.nl/wp-content/uploads/2016/06/ICCT-Haroro-Ingram-Brief-History-Propaganda-June-2016-2.pdf

[41] Valery Gerasimov, "Tsennost Nauki v Predvidenniye", in *Voenno-promyshlenni Kurier*, 27 febbraio, 2013, http://www.vpk-news.ru/articles/14632.

[42] Tarun Yadunv, Arvind Mallari Rao, *Technical Aspects of Cyber Kill Chain*, Defence Research and Development Organisation, New Delhi, 2015.

[43] Cfr. https://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125

[44] Liddell Hart, *Strategy: The Indirect Approach*, Faber and Faber, London, 1967.

[45] Robert Oppenheimer, "Analogy in Science", in *American Psychologist*, 11, n° 3, 1956, pp. 127-135.

Alcune tipiche operazioni non-convenzionali si servono della manipolazione psicologica e possono imporre una scala di priorità alla società politica e alla società civile, sfruttando la percezione dei cittadini tramite la diffusione di dati e news apparentemente credibili, anche usando messaggi distorsivi e personalizzati volti a polarizzare il dibattito e indirizzare la discussione politica tra gruppi.

Non va dimenticato che la stessa disinformazione fa leva su preesistenti convinzioni culturali, religiose, etiche, razziali, ed è peraltro «un argomento centrale del pensiero politico e strategico occidentale e orientale sin dall'antichità»[46]. Essa svilupperà nel prossimo futuro livelli di manipolazione e d'influenza inimmaginabili, con una bassa probabilità di provocare uno scontro militare ma un'alta probabilità di generare conseguenze psico-sociali.

Mosca utilizza piattaforme preesistenti come i social network per attaccare i *target*, utilizzando il web come canale capace di raggiungere senza mediazioni i singoli cittadini occidentali, con il risultato di sviluppare un'arma ibrida efficiente e a basso costo. In pratica, l'industria commerciale, le aziende pubblicitarie e i cittadini (i *target*) hanno fornito consapevolmente e inconsapevolmente il supporto primario indispensabile a questa strategia.

Le tecniche di disinformazione attuali riducono la fiducia tra cittadini e *policymakers*, inducono alla formazione di convinzioni legate a fattori più soggettivi che oggettivi.

Mark Zuckerberg, presidente e amministratore delegato di Facebook, ascoltato dal Congresso degli Stati Uniti, ha detto che sulla piattaforma di questo social network 120 milioni di americani potrebbero aver letto contenuti manipolati direttamente dalla Russia durante la campagna elettorale per le ultime elezioni presidenziali. Una stima che successivamente gli analisti hanno corretto al rialzo (circa 150 milioni). La Russia ha attuato operazioni di questo livello prima dello svolgimento delle campagne elettorali in Francia, Germania, Ucraina, durante il referendum sulla Brexit e in occasione del voto sull'indipendenza della Catalogna.

> We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign then focused on undermining her expected presidency.[47]

Queste azioni sono state segnalate in ben diciotto appuntamenti elettorali sparsi in tutto il mondo[48]. Si tratta di una pianificazione su vasta scala.

[46] Luigi Sergio Germani, "La minaccia della disinformazione: panoramica introduttiva", in *Disinformazione e manipolazione delle percezioni. Una nuova minaccia al Sistema-Paese*, Eurilink University Press, Roma, 2017, p. 11.

[47] Cfr. https://www.dni.gov/files/documents/ICA_2017_01.pdf

[48] Cfr. https://freedomhouse.org/report/freedom-net/freedom-net-2017

Nell'*attention economy*, i contenuti vengono confezionati per essere consumati rapidamente a causa di una soglia di attenzione sempre più bassa, che impedisce la possibilità di un'analisi completa ed equilibrata di dati e fenomeni. La gran maggioranza delle persone rimanda a Google il compito di fornire risposte a qualsiasi domanda, dalla meno evoluta a quella più complessa, a ulteriore riprova della teoria della *morte delle competenze*[49].

Le *fake news* prodotte dalle operazioni russe rimbalzano da un punto all'altro dell'*infosfera* e quasi sempre riguardano i temi preferiti dalla disinformazione come l'immigrazione, la crisi delle istituzioni europee, la piccola criminalità comune, la decadenza dei costumi occidentali, allo scopo di alimentare le pulsioni populiste e generare paura nell'opinione pubblica occidentale.

Notizie, studi, piattaforme, partiti e uomini politici, centri di studio, professori, esperti, diffondono a piene mani l'idea di un Occidente al tramonto e pronosticano l'ascesa di nuove potenze "spirituali" (la Russia agognata da Aleksandr Dugin, ma anche l'Iran) o economico-finanziarie (la Cina). In verità, il quadro sulla Cina risulta molto più complesso:

> Prima economia dell'Asia e terza economia a livello mondiale, la Cina svolge un ruolo significativo generando circa il 18 % della crescita globale nel 2016 (FMI). Nel 2016 l'economia cinese ha registrato la crescita più lenta dal 1990 con un tasso di crescita del PIL sceso al 6,7 % dal 6,9 % del 2015. Malgrado la crescita cinese superi quella della maggior parte delle altre economie, si prevede un rallentamento che continuerà nel medio termine.[50]

In conclusione, non si tratta solo di disinformare gli elettori a poche settimane dal voto, di spostare l'ago della bilancia in favore di una parte politica compiacente o ricattata. Si tratta di una strategia di destabilizzazione che avviene col supporto di una rete presente all'interno del Paese da monitorare e destabilizzare[51]. Internet è solo una parte del problema, certo non di poco conto: senza addentrarci in tecnicalità, basti pensare che una ricerca sulle reti *botnet* ha spiegato come la percentuale di *tweet* creata da *human-bot* corrisponda a una cifra tra il 9% e il 15%. Ciò fa pensare ad un fenomeno durevole, con un potenziale di crescita piuttosto consistente nell'immediato futuro[52].

Difendere l'opinione pubblica occidentale dalle campagne di manipolazione delle percezioni sarà molto difficile, e non è razionale immaginare che singolo Stato possa contrastare ad uno ad uno tutti i post all'interno di una discussione, i tweet, i *deep fake*, la propaganda politica ingannevole.

[49] Tom Nichols, *The Death of Expertise: The Campaign against Established Knowledge and Why It Matters*, Oxford University Press, Oxford, 2017.

[50] Cfr. https://www.bloomberg.com/news/articles/2017-01-24/slowing-china-still-added-a-fullindonesia-economy-in-2016

[51] Cfr. https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy

[52] Various Authors, *Online Human-Bot Interactions: Detection, Estimation, and Characterization*, Cornell University Library, Ithaca, 2017, https://arxiv.org/pdf/1703.03107.pdf

L'*Artificial Intelligence* (AI) verrà in soccorso svolgendo un ruolo analogo a quello del radar; le capacità crescenti dell'AI, infatti, agiranno alla stregua di un sistema di allarme per rilevare la minaccia di informazioni avversarie e segnalare subito le notizie false e le operazioni di disinformazione, imminenti o in corso. L'AI potrà allertare gli analisti umani rispetto alla minaccia, determinando la sua origine e il percorso di consegna dell'informazione, forse anche includere la pubblicazione o il reindirizzamento degli utenti a link con brevi informazioni qualificate, capaci di neutralizzare le *fake news* più dozzinali.

Tuttavia, lo scandalo legato a *Cambridge Analytica* e l'interferenza nelle elezioni politiche di Stati democratici, dimostra come la *cyberwa*r abbia effetti enormi, oltre che sull'equilibrio politico tra le nazioni, anche sulla salute psicofisica delle popolazioni colpite. L'*effetto priming «*refers to the incidental activation of knowledge structures, such as trait concepts and stereotypes, by the current situational context»[53] quindi l'attivazione inconscia di determinati legami tra rappresentazioni mentali precedentemente scollegati, ad esempio "immigrato/delinquente", può essere abbinato alla scoperta di Rizzolatti e Sinigaglia.

I due scienziati hanno dimostrato che nell'area F5 della corteccia premotoria c'è una particolare famiglia di neuroni, detti *neuroni specchio*, che si attivano non solo quando un soggetto esegue un'azione ma anche quando la vede fare da un'altra persona. Queste attività cerebrali rappresentano la base dell'imitazione sociale e la prova secondo cui il cervello si modifica con l'esperienza. La dinamica del rispecchiamento non si verifica solo nei confronti delle azioni, ma anche delle emozioni vissute dagli altri[54].

La disinformazione unitamente ad un allineamento empatico sulle emozioni negative della maggioranza delle persone esposte, agiscono sullo stress, sull'ansia, sui livelli di serotonina e sulle paure, alterando il flusso delle informazioni che ha luogo normalmente nel cervello.

Questo flusso, anziché essere inviato alla corteccia prefrontale, che valuta logicamente tutte le informazioni e decide come reagire, viene inviata direttamente alla corteccia motoria che controlla i muscoli, un sistema decisionale più automatico e veloce, che scavalca la corteccia prefrontale.

Come si evince dalle ricerche di Patricia Molina Molina, dell'Istituto di Neuroscienze dell'Università di Barcellona, quanto più il cervello sperimenta condizioni di stress cronico, tanto più la corteccia prefrontale arriva a disattivarsi definitivamente, danneggiando in questo modo il cervello[55].

[53] John Bargh, Mark Chen and Lara Burrows, "Automaticity of social behavior: Direct effects of trait construct and stereotype activation on action", in *Journal of Personality and Social Psychology*, vol. 71 (2), 1996, pp. 230-244, https://psycnet.apa.org/doiLanding?doi=10.1037%2F0022-3514.71.2.230

[54] Giacomo Rizzolatti, Corrado Sinigaglia, *So quel che fai, il cervello che agisce e i neuroni specchio*, Cortina, Milano, 2006, pp. 127-179.

[55] Patricia Molina Molina, *Effects of chronic stress on Prefrontal Cortex structure and function*, Autonomous University of Barcelona, Institute of Neuroscience (INc), Barcelona, 2015.

Come osserva Rasika Priscilla Rumor,

> diversi studi provano come l'esposizione a contenuti violenti, siano fattori causali dell'aumento di episodi violenti nella vita reale e come la violenza dei media incrementi sia l'aggressività che le esperienze emotive negative, soprattutto in età infantile, e che questa possa essere messa in relazione a comportamenti aggressivi in età adulta. Esperimenti come quelli condotti da Hummer e Wang dell'Università di Medicina dell'Indiana, evidenziano che l'esposizione (per una sola settimana) a contenuti violenti causi una minore attività del lobo frontale inferiore sinistro (un'area del cervello associata all'empatia). Hummer ha dimostrato che durante i test cognitivi si è osservato un calo degli stimoli nella corteccia cingolata anteriore, quella zona cerebrale deputata al controllo dei conflitti, all'elaborazione approfondita dei problemi e al rilevamento degli errori. La stessa ricerca, ha dimostrato come a due settimane di distanza dall'esposizione agli stimoli, gli effetti siano diminuiti ma non scomparsi definitivamente. Possiamo quindi concludere che in soggetti fortemente esposti a contenuti violenti, odio e disinformazione, tipici della *cyberwar*, la corteccia prefrontale si deattiva creando 'buchi funzionali' a favore di una risposta decisionale automatica ed impulsiva, perciò incorrendo frequentemente a stereotipi, pregiudizi e bias. Come afferma Olivia Choy, professore di psicologia alla NTU Singapore, «Stimulation of the Prefrontal Cortex Reduces Intentions to Commit Aggression», mentre restano fondamentali ulteriori approfondimenti e ricerche per il trattamento dell'età evolutiva.[56]

È necessario identificare e inviare messaggi di carattere preventivo a gruppi fortemente vulnerabili, con una campagna ad alto impatto, finanziata dagli Stati democratici o dagli organismi sovranazionali, l'UE o le agenzie dell'ONU. Si pensi al concetto di *herd immunity*, quando un numero sufficiente di persone nella popolazione deve essere vaccinato per prevenire la diffusione di una malattia (in questo caso la disinformazione): i comportamenti vanno ricondotti a una gestione basata sulla prevenzione, coordinata a livello internazionale, dunque non è sufficiente l'attività di autoregolamentazione o di contrasto attraverso la *counterintelligence*.

La prevenzione però non risulta efficace se la popolazione non la capisce, non ha consapevolezza delle implicazioni fondamentali, o, peggio, se sono state compromesse alcune capacità connesse alla sfera emozionale, causando danni neuronali alle persone. La disinformazione è ormai un problema cognitivo di massa, con conseguenze epidemiologiche.

Contro la disinformazione è necessario uno sforzo anzitutto pedagogico[57], ma in prospettiva anche sanitario. I cittadini occidentali devono tornare a comprendere funzioni e meccanismi elementari del dialogo civile e della democrazia, con l'aiuto di programmi educativi mirati delle istituzioni nazionali e sovranazionali, un po' come accaduto durante l'epoca dell'alfabetizzazione di massa, a cavallo tra l'Ottocento e la metà del Novecento. Quella delle forze dispotiche è una guerra perpetua alla società aperta, che si nutre di quel libero flusso di informazioni che l'ha generata.

[56] Rasika Priscilla Rumor è una studiosa della correlazione tra nuove tecnologie e psicologia clinica.

[57] Mario Caligiuri, *Introduzione alla società della disinformazione. Per una pedagogia della comunicazione*, Rubbettino, Soveria Mannelli, 2018.

Verso la fine del 2016, il presidente degli Stati Uniti Barack Obama firmò il *Countering Foreign Propaganda and Disinformation Act*, un disegno di legge bipartisan inizialmente chiamato *Countering Information Warfare Act*, integrato nel *National Defense Authorization Act*[58], fortemente voluto dal senatore John McCain. A partire dal marzo 2018, il Dipartimento di Stato ha accentuato il contrasto alla cyberwar russa sul territorio americano; programmi analoghi sono stati sviluppati in Francia, Germania, Regno Unito, Finlandia, Danimarca, Olanda, nei paesi baltici.

Recentemente è stato confermato che le ultime elezioni di *midterms* negli Stati Uniti si siano svolte regolarmente soltanto grazie all'attività di contrasto del *Cyber Command* dell'esercito, in sinergia con la National Security Agency (NSA), che hanno neutralizzato gli attacchi informatici di una struttura di San Pietroburgo, sostenuta da un oligarca collegato al Cremlino. Il senatore Mike Rounds ha detto: «The fact that the 2018 election process moved forward without successful Russian intervention was not a coincidence»[59].

Insistere su una strategia di controingerenza aiuterà a ridurre i danni in modo transitorio o parziale e non eliminerà il problema: le forze dispotiche continueranno ad esercitare manipolazioni a danno della salute dei cittadini occidentali, in misura e con conseguenze difficili da quantificare. Carlo Jean ha scritto: «Praticamente con il big data e con lo sviluppo delle neuroscienze, ci sarà uno sviluppo della capacità di disinformazione e di manipolazione delle percezioni e comportamenti molto superiore a quello verificatosi con la tecnologia del subliminal»[60].

Dopo l'interferenza nel sistema politico-decisionale degli Stati liberaldemocratici è ora la volta della *guerra neuronale*, attraverso la disattivazione delle funzioni cognitive dei cittadini target. Questa guerra non convenzionale investe direttamente il tema della sopravvivenza degli istituti della democrazia rappresentativa per come li conosciamo.

L'ex segretario alla Difesa degli Stati Uniti, James Mattis, ha affermato che «It is clear that China and Russia […] want to shape a world consistent with their authoritarian model - gaining veto authority over other nations' economic, diplomatic, and security decisions - to promote their own interests at the expense of their neighbors, America, and our allies»[61]. In un contesto come quello descritto, le minacce russe e cinesi rappresentano una parodia invertita delle tesi di Clausewitz: non più la guerra come prosecuzione della politica con altri mezzi ma, paradossalmente, la politica (e la guerra politica) come prosecuzione della guerra (perpetua) con altri mezzi.

[58] Cfr. https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf

[59] Cfr. https://nypost.com/2019/02/26/us-military-blocked-russian-troll-farms-efforts-to-interfere-in-2018-midterms/

[60] Carlo Jean, "La disinformazione come strumento di guerra economica", in *Disinformazione e manipolazione delle percezioni. Una nuova minaccia al Sistema-Paese*, a cura di Luigi Sergio Germani, Eurilink University Press, Roma, 2017, p. 84.

[61] Cfr. https://media.defense.gov/2018/Dec/20/2002075156/-1/-1/1/LETTER-FROM-SECRETARY-JAMES-N-MATTIS.PDF