“La minaccia della disinformazione: panoramica introduttiva”

di Luigi Sergio Germani

Tratto da: AA. VV. (a cura di L. S. Germani),
Disinformazione e manipolazione delle percezioni: una nuova minaccia al sistema - paese,
Edizioni EURILINK, 2017

LA MINACCIA DELLA DISINFORMAZIONE: PANORAMICA INTRODUTTIVA

LUIGI SERGIO GERMANI
Direttore, Istituto Gino Germani di Scienze Sociali e Studi Strategici

Questo è il primo libro pubblicato nel nostro Paese, dedicato alla disinformazione come minaccia alla sicurezza e alla competitività del sistema-Italia. La disinformazione è un'arma di lotta politica, militare ed economica adoperata da attori statali e non-statali, la cui potenza ed efficacia viene moltiplicata dalle nuove tecnologie ICT (informatiche e della comunicazione) e dallo sfruttamento del cyberspazio.
Il volume nasce dal convegno "*Disinformazione e manipolazione delle percezioni: una nuova minaccia al sistema-Italia*", promosso nel gennaio 2015 dall'Istituto Gino Germani e dalla Link Campus University, e ne raccoglie i contributi, successivamente approfonditi e aggiornati dagli Autori.

Uno strumento di potere e di lotta competitiva

La disinformazione é uno strumento di potere e lotta competitiva che viene adoperato nei più svariati campi: la guerra, la politica interna e internazionale, il mondo degli affari e della finanza, la pubblicità, ma anche nella competizione per il potere all'interno di qualsiasi organizzazione complessa pubblica o privata. Essa si può definire come la falsificazione intenzionale di dati e notizie al fine di manipolare le percezioni di un bersaglio, influenzarne le decisioni, e indurlo ad agire nel modo desiderato dal disinformatore. Talvolta viene anche utilizzata per indebolire le capacità cognitive e decisionali del *target* diffondendo notizie che generano in esso confusione e incertezza.

In altre parole, si costruiscono e si diffondono informazioni false o fuorvianti per indurre il bersaglio a prendere decisioni (o ad adottare atteggiamenti o idee) che sono contrari ai suoi interessi e che favoriscono gli interessi del disinformatore.

E' un'arma che consente a chi la usa con successo di esercitare la "eterodirezione" o "manipolazione". Quest'ultimo termine é stato definito dal teorico della politica Mario Stoppino come "una relazione di potere caratterizzata dal fatto che chi esercita il potere lo fa di nascosto, tenendo celato all'altro il proprio intervento, e chi lo subisce non si rende conto che il suo comportamento è determinato dall'esterno e crede di scegliere in piena libertà"[1].

Come ha osservato François Géré, esperto francese di studi strategici, "Se, secondo la formula di Francis Bacon del XVII secolo 'sapere é potere', la disinformazione, azione occulta di natura ostile, mira a provocare l'impotenza o indebolimento dell'avversario interferendo con le sue informazioni e disorientando le sue capacità decisionali. La disinformazione ha come risultato di accrescere il potere di chi se ne serve grazie alla diminuzione delle capacità di azione dell'avversario"[2].

Il tema è di grande attualità oggi, nell'era del *cyber-power*[3]. Lo sviluppo di nuove tecnologie informatiche e dei "nuovi media" (Google, YouTube, Twitter, Facebook, etc.) ha determinato un notevole potenziamento degli strumenti per orientare l'opinione pubblica e gli stessi decisori politici e militari di un paese tramite la disinformazione. La rete facilita e rende sempre più efficaci le azioni disinformative. Essa consente la diffusione massiccia, incontrollata e pressoché istantanea di notizie deliberatamente falsificate o manipolate. Il che aumenta la vulnerabilità di governi, aziende, gruppi sociali e individui nei confronti di dette azioni, che sfruttano alcune debolezze cognitive molto estese nelle società contemporanee dominate dal web: la tendenza ad accedere e diffondere informazioni

---

[1] Mario Stoppino, *Potere e Teoria Politica* (Genova, ECIG, 1982).

[2] François Géré, *Dictionnaire de la Desinformation* (Paris, Armand Collin, 2011). Una parte del saggio di Géré è stato tradotto dal CESTUDEC www.centrostudistrategicicarlodecristoforis.wordpress.com/2012/01/30/francois-gere-la-disinformazione/

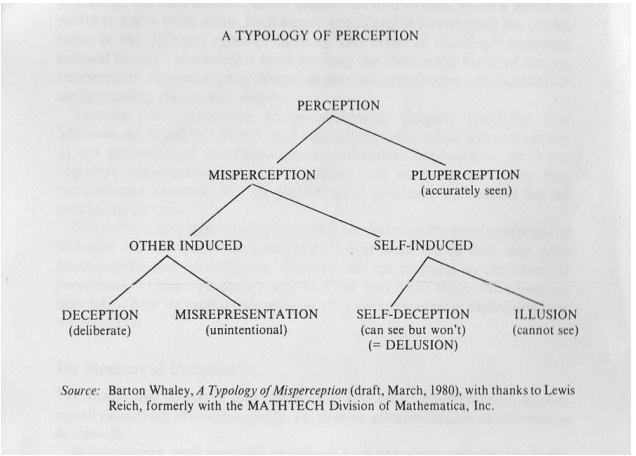
[3] Joseph Nye Jr., *Cyber Power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Maggio 2010.

senza valutarle criticamente, la refrattarietà all'approfondimento, la sindrome da deficit di attenzione (*Attention Span Deficit Disorder*).
La disinformazione é un argomento centrale del pensiero politico e strategico occidentale e orientale sin dall'antichità. Basti pensare ai trattati di strategia militare di Sun Tzu, secondo cui "tutta la guerra si basa sull'inganno"; all' *Arthasastra*, il trattato di scienze politico-strategiche dell'antica India, scritto da Kautilya, ministro del re Chandragupta Maurya, che offre numerosi consigli sull'importanza dell'inganno nell'arte del governo; alle riflessioni di Platone sul ricorso alla "nobile menzogna" da parte dei governanti per rafforzare la coesione dello Stato e della società; a Machiavelli, che sostiene l'uso politico della menzogna finalizzata al mantenimento del potere[4].
Nella letteratura accademica americana e britannica sul tema viene privilegiato il termine *deception* (inganno), che si riferisce al fenomeno della disinformazione in campo militare, diplomatico, e dell'intelligence. Secondo lo psicologo e filosofo Paul Watzlawick, un'azione di *deception* mira a "indurre un avversario a pensare qualcosa di errato, a percepire una 'realtà sbagliata', e occorre avere estrema cura affinché egli non si renda conto in tempo utile delle sue premesse errate… Le regole normali della comunicazione vengono capovolte"[5].
Abram Schulsky, esperto americano di intelligence, definisce la *deception* come "lo sforzo teso a indurre un avversario a credere a una falsità, a una *cover story*, anziché alla verità, allo scopo di provocarne una reazione favorevole ai propri interessi… Ciò richiede la creazione di una 'realtà alternativa' che si vuole fare percepire al bersaglio"[6].
In altre parole, ogni disinformatore si proporre di distorcere il modo in cui il bersaglio percepisce la realtà, di instillare in lui una *misperception*, un errore di percezione, al fine di ottenere un vantaggio competitivo. La disinformazione, pertanto, é un fenomeno

[4]Introduction to David Charters and Maurice A.J. Tugwell (eds), *Deception Operations: Studies in the East-West Context* (London, Brassey's UK, 1990), p. 2-3.
[5]Paul Watzlawick, *How Real is Real: Confusion, Disinformation, Communication* (New York, Random House, 1976), p. 118-119.
[6]Abram Schulsky, "Elements of Strategic Denial and Deception", in Roy Godson e James Wirtz (eds), *Strategic Denial and Deception: the 21st Century Challenge* (Transaction Publishers, New Brunswick and London, 2003).

diverso dall'autoinganno, nel quale un soggetto si auto-induce una percezione sbagliata della realtà, senza l'intervento di un altro soggetto (vedi la "tipologia della percezione" nella figura n. 1)[7]. Va sottolineato, tuttavia, che le campagne disinformative sono efficaci nella misura in cui si basano sulla conoscenza approfondita, e lo sfruttamento, delle vulnerabilità psicologiche e rigidità cognitive del *target*, e, in particolare, delle sue tendenze all'autoinganno.

Immagine 1



Fonte: Barton Whaley, "Toward a General Theory of Deception", in *Journal of Strategic Studies*, n. 1, 1982 (vol. 5), p. 180.

E' essenziale distinguere nettamente la disinformazione dalla malainformazione non-intenzionale (denominata *misrepresentation* nell'immagine), vale a dire l'informazione errata o viziata che viene inconsapevolmente presentata come vera a causa dell'ignoranza, confusione, superficialità o pregiudizi di chi la diffonde. La disinformazione, invece, é una azione ostile, deliberata e pianificata, che persegue un vantaggio in maniera occulta , costruendo e diffondendo informazione falsa o distorta. Detto questo, va sottolineato che le operazioni disinformative

[7]Barton Whaley, "Toward a General Theory of Deception", *Op. Cit.*, p. 180.

spesso sono coronate da successo perché sfruttano ingegnosamente la malainformazione che circola negli ambienti presi di mira.
E' importante chiarire il rapporto tra disinformazione e propaganda, un concetto più ampio che include qualsiasi azione comunicativa che mira a influire sulle opinioni, gli atteggiamenti, le emozioni, e i comportamenti di uno o più settori della società per trarne un beneficio. Una campagna propagandistica può avvalersi della disinformazione oppure può diffondere esclusivamente notizie vere, ma selezionate e interpretate in maniera tale da favorire determinati interessi.

Scopi, bersagli e modalità della disinformazione

Qualsiasi azione disinformativa richiede uno sforzo di pianificazione. Quanto più complessa e ambiziosa é una operazione tanto più essa richiederà una pianificazione meticolosa. Il primo passo è la definizione dello scopo finale, l'obiettivo strategico o tattico, che si vuole raggiungere : qual é precisamente il vantaggio che si vuole ottenere? Una volta chiarito lo scopo (che di solito viene indicato dai massimi dirigenti di uno Stato o entità non-statale), gli esecutori o *deception planners* devono mettere a punto gli elementi fondamentali del piano, tra cui i seguenti[8]:

1) La reazione autolesionista del bersaglio che si vuole provocare.
2) La falsa percezione che si vuole creare nel bersaglio.
3) La creazione di contenuti (messaggi, segnali) atti a far percepire la falsa realtà al bersaglio.
4) L'individuazione dei canali, palesi o occulti, da utilizzare per comunicare tali messaggi e segnali al bersaglio (media tradizionali e/o nuovi media, organizzazioni non-governative, *think tank*, canali diplomatici, agenti di influenza, servizi d'intelligence).

[8]Barton Whaley, "Toward a General Theory of Deception", in *Journal of Strategic Studies*, n. 1, 1982 (vol. 5), p.

La letteratura accademica sul tema in Occidente, si é focalizzata prevalentemente sulla disinformazione in campo militare e della politica estera, mettendone a fuoco i più ricorrenti scopi. In tempi di guerra, ad esempio, se un Stato si prepara a sferrare un attacco decisivo la disinformazione deve convincere le forze nemiche che nessun attacco é imminente, affinché esse siano impreparate a fronteggiarlo. Oppure, se è consapevole che un attacco sia inevitabile, egli deve essere indotto credere che l'attacco si concretizzerà in data e luogo, e con modalità, diversi dal vero piano, e pertanto a commettere un errore fatale nella concentrazione delle sue forze.

In tempi di pace un obiettivo comune della disinformazione politico-militare è, ad esempio, quello di indurre il governo dello Stato "A" a fare concessioni politiche allo Stato "B" convincendolo che quest'ultimo é più forte e temibile militarmente di quello che è in realtà. Oppure, di far si che lo Stato "A" si astenga dal rafforzare le proprie capacità militari, e/o dal condurre una politica estera guardinga nei confronti di "B", convincendo i decisori politici di "A" che "B" é più debole di quello che è in realtà, e non ha alcuna intenzione ostile nei confronti di "A".

La disinformazione posta in essere da governi in tempi di pace non di rado mira a promuovere fenomeni destabilizzanti all'interno di Paesi concorrenti o fomentare tensioni fra Stati. Il Generale Mario Mori sintetizza così alcune delle più diffuse finalità delle campagne disinformative: "confondere con dati e notizie false i decisori istituzionali di un Paese; creare turbamenti nella pubblica opinione di un Paese concorrente; suscitare contenziosi tra Stati tra loro amici; denigrare personalità e uomini politici ostili; ingannare gli organi di controspionaggio del paese obiettivo"[9].

[9]Mario Mori, "Controinformazione: la protezione dei processi decisionali del sistema-Paese", Research Paper dell'Istituto Gino Germani di Scienze Sociali e Studi Strategici, settembre 2016, p. 6. Il Gen. Mori sottolinea, inoltre, che i regimi autoritari sono avvantaggiati rispetto a quelli democratici nell'utilizzo della disinformazione come strumento di politica estera: "La disinformazione si caratterizza per i tempi non brevi che richiede la sua corretta applicazione e la complessità della sua elaborazione, che può essere gestita solo da apparati in grado di svilupparla avendo il totale sostegno di organismi politici coesi e tali che

Gli attori che praticano la disinformazione sono, in primo luogo, gli Stati e i governi, che se ne servono come strumento di politica estera o interna, in maniera sistematica oppure occasionale, spesso affidandone la pianificazione e attuazione ai loro apparati d'intelligence. Tuttavia, come ha osservato Vittorfranco Pisano, la disinformazione non è più un'arma in esclusiva dotazione degli Stati e dei loro servizi d'intelligence: "essa rimane, particolarmente nell'attuale contesto storico caratterizzato da martellamenti mediatici, un mezzo alla portata di qualunque centro di interessi intento a raggiungere i propri scopi influenzando e sfruttando uno o più settori della compagine sociale"[10] .
Quest'arma oggi viene utilizzata da molteplici attori non-statali sia leciti (partiti e movimenti politici, aziende e società finanziarie, gruppi di interesse e di pressione, organizzazioni religiose, organizzazioni non-governative) che illeciti (gruppi terroristici ed eversivi, organizzazioni criminali, "poteri occulti", sette religiose estremiste). Per dirla con le parole di François Géré, "Di norma, chiunque disponga di un potere politico-sociale, aspiri a conservarlo, a incrementarlo o, in caso contrario, a impossessarsene, è tentato di utilizzare la disinformazione per perseguire i suoi fini"[11]
Gli esperti distinguono tra due tipi di operazioni disinformative a seconda della natura del bersaglio:[12]

1) Le operazioni finalizzate a manipolare le percezioni di un target più o meno ampio (la leadership politica e governativa di un Paese, l'opinione pubblica, determinati settori di una società). In questo caso gli strumenti più comuni sfruttati dai disinformatori sono i mezzi di comunicazione e il web.

---

possono contare su di una lunga permanenza al potere. In pratica: regimi dittatoriali".
[10]Vittorfranco Pisano, "Terrorismo e disinformazione", in *Per Aspera ad Veritatem: Rivista di Intelligence e di Cultura Professionale, n. 21,* settembre-dicembre 2001.
[11] François Géré, *Dictionnaire de la Desinformation,* op. cit.
[12]Si veda, ad esempio, Richards J. Heuer, Jr., "Commentary", in Roy Godson e James Wirtz (eds), *Strategic Denial and Deception: the 21st Century Challenge,* Op. Cit., p. 33-36.

2) Le operazioni, di carattere più specializzato e occulto, finalizzate a ingannare gli apparati d'intelligence di un determinato paese (o entità non-statuale) o i suoi massimi decisori politici, propagando notizie false o inducendo il target a commettere errori di analisi e interpretazione delle informazioni. Spesso questo tipo di operazione mira a sfruttare i servizi segreti dell'avversario per manipolare i suoi *decision-makers*.

Vi sono sostanzialmente due diverse modalità per costruire messaggi ingannevoli: la prima è la "fabbricazione di falsità", ossia la creazione di informazioni false presentate come vere; la seconda é la "manipolazione informativa", ossia l'uso di notizie vere ma con alterazioni e omissioni, o la presentazione di informazioni fuori contesto al fine di indurre il bersaglio a trarre implicazioni fuorvianti[13].
Le azioni disinformative si possono anche distinguere in base al tipo di distorsione percettiva che si vuole provocare nel bersaglio:[14]

1) Operazioni che riducono la percezione di incertezza e ambiguità nel bersaglio, rafforzando ai suoi occhi la credibilità di una falsa ipotesi. Il bersaglio così acquisisce delle certezze (false) e sulla base di queste ultime prende decisioni autolesioniste (tipo "M" o *"misleading variety*").
2) Operazioni che accrescono l'incertezza del bersaglio, il quale viene sommerso da notizie ambigue e contraddittorie che provocano confusione, sbandamento, e paura, e paralizzano il suo processo decisionale (tipo "A" o "*ambiguity increasing*").

Un esempio classico di disinformazione di tipo "M" é l'operazione FORTITUDE, condotta dagli Alleati prima e durante lo sbarco in Normadia nella Seconda Guerra Mondiale, che diede un contributo

[13]Joseph W. Caddell, "Deception 101: Primer on Deception", US Army War College - Strategic Studies Institute, dicembre 2004 (www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=589).
[14]Ibid.

determinante alla vittoria alleata. FORTITUDE - componente di un più ampio piano di *deception* denominato BODYGUARD - riuscì a far credere ai tedeschi che lo sbarco degli Alleati avrebbe avuto luogo sullo stretto di Calais e non sulle spiagge della Normandia. Inoltre, la campagna disinformativa instillò nei tedeschi la convinzione, nel periodo subito dopo lo sbarco in Normandia, che quest'ultimo fosse un depistaggio e che la vera invasione si sarebbe svolta successivamente nello stretto di Calais[15].
Un esempio di operazione di tipo "A" è, secondo diversi esperti, la campagna disinformativa condotta da Al-Qa'ida nei confronti dei servizi d'intelligence americani nei mesi precedenti gli attacchi alle Torri Gemelle l'11 settembre 2001. Nella primavera-estate di quell'anno i vari apparati informativi statunitensi - CIA, NSA, FBI, DIA e altri organismi - furono sommersi da notizie contraddittorie relative a imminenti attacchi terroristici contro obiettivi americani. L'NSA, ad esempio, intercettò molteplici comunicazioni tra esponenti di Al-Qa'ida che facevano pensare alla possibilità di attentati di tutti i tipi, che poi si rivelavano falsi allarmi. La proliferazione di informazioni allarmanti captate dai servizi segreti americani sarebbe stata promossa dalla stessa Al-Qa'ida per diffondere confusione e panico all'interno della comunità d'intelligence, riducendone la capacità di percepire chiaramente la minaccia e di venire a conoscenza del vero piano di attacco[16].

La disinformazione all'epoca della Guerra Fredda: il caso della dezinformacija sovietica

La disinformazione era un tema centrale del pensiero politico e strategico del Novecento: l'epoca dei totalitarismi nazista e comunista, i quali la istituzionalizzarono come strumento di

[15] FORTITUDE utilizzò diversi metodi per creare false percezioni, tra cui: 1) la costruzione di finti aeroporti e aeroplani; 2) false comunicazioni radio; 3) creazione di un intero esercito fittizio (FUSAG - First United States Army Group); 4) notizie false trasmesse ai servizi d'intelligence tedeschi dai loro informatori occulti in Inghilterra, che in realtà erano "agenti doppi" controllati dal servizio segreto inglese MI5.
[16] Eli J. Lake, "Al Qaeda's Disinformation War", *The New Republic*, 11/04/2001.

governo, praticandola nei confronti della propria popolazione, come evidenziò Hannah Arendt, che analizzò la natura profonda dei sistemi totalitari[17]. Il filosofo polacco Leszek Kolakowski giunse a una conclusione simile quando caratterizzò il comunismo come "la prima civiltà nella storia in cui l'intero sistema di potere - e cioè il controllo della popolazione da parte dei governanti - si basa sul controllo delle informazioni. Colui che controlla tutto ciò che al popolo viene dato sapere è senza dubbio il padrone[18]"

Durante la Guerra Fredda il regime sovietico utilizzava sistematicamente la disinformazione non solo sul piano interno, ma anche come strumento di politica estera. L'obiettivo di fondo della strategia globale sovietica era l'espansione mondiale del sistema comunista e il logoramento progressivo delle democrazie occidentali. Lo strumento privilegiato per raggiungere questi obiettivi erano le cosiddette "misure attive" (*aktivnye meroprijatija)*: un termine che abbracciava molteplici attività di influenza e guerra psicologica - tra cui la *dezinformacija* - intraprese nei confronti di paesi esteri dal KGB e altri apparati d'intelligence comunisti[19].

A quei tempi i governi e servizi segreti occidentali ravvisavano nella *dezinformacija* sovietica una minaccia alla propria sicurezza nazionale, e di conseguenza dedicavano considerevoli risorse alle attività di controspionaggio e controinfluenza atte a contrastarla. Inoltre, esperti accademici e dei *think tank*, specie

[17]Secondo Hannah Arendt, una delle caratteristiche essenziali del totalitarismo "é proprio l'inclinazione a trascurare 'il dato di fatto' e a fabbricare la verità sostituendo, attraverso la menzogna sistematica, un vero e proprio mondo fittizio a quello reale" (Diego Fusaro, "Hannah Arendt: verità e politica", www.filosofico.net/arendt9.htm).

[18]Leszek Kolakowski, "The Power of Information", *Encounter*, 1988.

[19]Un manuale interno del KGB definisce "misure attive" come "misure operative finalizzate a esercitare influenza su aspetti di interesse della vita politica di un paese-obiettivo, sulla sua politica estera, sulla soluzione di problemi internazionali, oppure intese a ingannare l'avversario, sovvertire e indebolire le sue posizioni, neutralizzare i suoi piani ostili, e conseguire altre finalità" (*KGB Lexicon: the Soviet Intelligence Officer's Handbook*, a cura di Vassilij Mitrokhin, Frank Cass, London and Portland, Oregon, 2002).

nel mondo anglosassone, elaborarono molti studi su questa e altre "misure attive" sovietiche.
E' importante studiare l'approccio sovietico in questo campo per comprendere il fenomeno della disinformazione oggi. Infatti, il KGB perfezionò una serie di tecniche operative di disinformazione che oggi vengono adoperate dai più diversi attori della disinformazione, tra cui la falsificazione di documenti ufficiali di governi stranieri e corrispondenza di natura politico-diplomatica, la pubblicazione di articoli di stampa "pilotati", la creazione di organizzazioni propagandistiche di facciata, l'uso di "agenti di influenza[20].
Le campagne di disinformazione sovietica perseguivano diverse finalità strategiche, tra cui le seguenti:[21]

1) Diffondere fra élites e masse nei paesi non-comunisti un'immagine falsamente tranquillizzante della politica estera sovietica.
2) Screditare e demonizzare determinati Paesi, governi, gruppi politici, leaders, o individui, considerati ostili agli interessi sovietici.
3) Fomentare tensioni fra i Paesi NATO e fra Stati Uniti ed Europa Occidentale.
4) Alimentare tensioni fra paesi occidentali e paesi del Terzo Mondo (e in particolare fra USA e Terzo Mondo).
5) Aizzare le popolazioni contro le Istituzioni dello Stato nei paesi occidentali e provocare la crescente ingovernabilità di questi ultimi.
6) Delegittimare e destabilizzare i servizi informativi e di sicurezza occidentali.
7) Diffondere un senso di demoralizzazione, sfiducia e pessimismo tra le popolazioni dei paesi occidentali circa il futuro delle democrazie capitalistiche, sfruttando paure e sensi di colpa.

[20] Vittorfranco Pisano, "Terrorismo e disinformazione", op. cit.
[21] Si veda, ad esempio, "Appendix: Recent Revelations of Soviet Active Measues" in *Soviet Active Measures in the Post-Cold War Era 1988-1991*, United States Information Agency, giugno 1992.

L'evoluzione del dibattito sulla disinformazione dopo la fine della Guerra Fredda

Dopo la fine dello scontro bipolare USA-URSS e il crollo dell'impero sovietico l'attenzione nei confronti della disinformazione subisce un significativo calo in tutto l'Occidente, sia nell'ambito dei Servizi segreti che nel mondo degli esperti e studiosi non-governativi.
Gli anni '90 sono caratterizzati da un diffuso ottimismo: la democrazia liberale appariva destinata ad affermarsi sempre di più in tutto il mondo, sembrava certa la transizione dei regimi autoritari e totalitari verso la democrazia, il che avrebbe molto facilitato la costruzione di un ordine internazionale più stabile e pacifico. In questo clima euforico si attenua sempre di più la percezione della disinformazione come minaccia.
Dopo gli attentati dell'11 settembre 2001, che mandano in frantumi la sopracitata visione fiduciosa del mondo post-bipolare, alcuni esperti, soprattutto statunitensi, tentano di riaccendere l'interesse per il tema, specie con riferimento a due fenomeni specifici: le tecniche di *taqqiya* (inganno) praticate dal radicalismo islamico[22], e la capacità di gruppi terroristici e "Stati canaglia" di disinformare i Servizi d'intelligence occidentali per vanificare le attività di contrasto[23].
Alcuni esperti consigliano al governo americano di impiegare in chiave offensiva la *deception* per combattere formazioni terroristiche come Al-Qa'ida, organizzazioni criminali transnazionali e Stati impegnati in programmi di proliferazione di armi di distruzione di massa[24]. Altri, invece, ritengono il ricorso alla disinformazione moralmente discutibile, oltre che rischioso

[22]Si veda, ad esempio, Andrew Campbell, "'Taqiyya' and the Global War Against Terrorism", *National Observer: Australia and Foreign Affairs* (Primavera, 2005).
[23]Su questo argomento cfr. James Bruce, "Denial and Deception in the 21st Century: Adaptation Implications for Western Intelligence" , *Defense Intelligence Journal* (vol. 15, n. 2, 2006).
[24]Secondo questo punto di vista, è legittimo e opportuno per le democrazie occidentali ricorrere alla disinformazione per combattere avversari statali e non-statali: cfr. R. Godson e James Wirtz (eds), *Strategic Denial and Deception, a 21st Century Challenge*, op. cit.

per la democrazia, anche se destinata a colpire avversari esterni, e non la propria popolazione[25].

La ripresa di interesse per la disinformazione negli anni immediatamente dopo l'11 settembre ha, tuttavia, un carattere molto limitato. Essa coinvolge solo alcuni analisti e studiosi specializzati, prevalentemente statunitensi, mentre in Europa il tema continua a suscitare scarso interesse.

Peraltro, lo sfruttamento dello spazio cibernetico per condurre operazioni disinformative non viene considerato un tema centrale del dibattito americano ed europeo sulla sicurezza cibernetica e il *cyber-warfare*, che prende corpo nei primi anni duemila e successivamente acquisisce una rilevanza politica sempre crescente.

A differenza di quello occidentale, il pensiero strategico russo e cinese sul cyberspazio attribuisce enorme importanza alle attività di disinformazione, influenza e manipolazione psicologica: per gli esperti russi e cinesi, infatti, lo scopo primario delle aggressioni cibernetiche è aggredire la mente dell'avversario[26].

Va infatti ricordato che il concetto centrale del dibattito russo sul cyberspazio è "guerra con le informazioni" (*information warfare*, in russo *informacionnaja vojna*), che ha un significato molto più ampio e olistico rispetto al termine occidentale di *cyber-warfare*, in quanto comprende non solo gli attacchi cibernetici e le attività di penetrazione informatica, ma anche le operazioni psicologiche, la disinformazione, l'influenza strategica, la guerra elettronica, e per certi aspetti anche le attività di intelligence e counterintelligence[27].

Emblematica del profondo interesse della comunità strategica russa per l'impatto delle nuove tecnologie informatiche sulla mente umana è la pubblicazione di numerosi studi sugli aspetti

---

[25]Questa posizione fu sostenuta, ad esempio, da Elisabeth Kiss, in "Strategic Deception in Modern Democracies: The Ethical Dimension", paper presentato alla conferenza "Strategic Deception in Modern Democracies: Legal, Ethical and Policy Challenges", 31 ottobre-1 novembre 2003.

[26] Timothy L. Thomas, "Information Security Thinking: a Comparison of US, Russian and Chinese Concepts". Foreign Military Studies Office, luglio 2001.

[27] V. I. Cymbal, *O koncepcii informacionnoj vojny* (Moskva, Sbornik "Bezopasnost", 1995).

psicologici dell'*information warfare*[28] e sulle armi psicotroniche (armi per il "controllo del pensiero")[29].

A partire dai primi mesi del 2014 - con l'annessione della Crimea e la destabilizzazione dell'Ucraina orientale da parte di una Russia sempre più determinata a recuperare lo status di potenza globale, e l'ascesa di DAESH, una nuova e più temibile espressione del movimento jihadista globale - si risveglia in Occidente l'attenzione nei confronti della disinformazione, tra i decisori politici, nei servizi d'intelligence e nel mondo dei *think tank*, dopo quasi un quarto di secolo in cui prevaleva un diffuso disinteresse per il tema. Il mondo occidentale, del resto, appare sorpreso e del tutto impreparato di fronte all'impiego massiccio della disinformazione sia da parte della Russia (che se ne serve come strumento di politica interna ed estera) sia da parte di DAESH (che la utilizza per allargare la propria influenza al di fuori del Califfato e radicalizzare le masse musulmane in tutto il mondo).

La disinformazione viene percepita come componente della "guerra ibrida" o "minacce ibride", concetti che acquisiscono crescente importanza in ambito NATO e UE a partire dal 2014. Le "minacce ibride" hanno le seguenti caratteristiche[30]:

- La combinazione di azioni convenzionali e non-convenzionali, militari e non-militari, palesi e occulte.
- Lo scopo di creare ambiguità e confusione circa la natura, l'origine e l'obiettivo della minaccia.

---

[28] Per una rassegna di studi russi in materia di *information warfare* incentrati sull'influenza e la manipolazione psicologica, si veda Nerius Maliukevičius, "Geopolitics and Information Warfare: Russia's Approach", *Lithuanian Annual Strategic Review*, Vilnius, 2007.

[29] Una di queste opere, *Informacionnaja Vojna* di Sergej Rastorguev (Radio i Svjaz, Moskva, 1998), ancora oggi viene considerata fondamentale in ambienti dell'elite politica e degli apparati militari e dell'intelligence. Tra i temi affrontati dal libro vi sono gli "psico-virus" che, analogamente ai virus informatici, alterano gli algoritmi della mente e impediscono alle persone colpite di ragionare in maniera logica e obiettiva.

[30] Jan Joel Andersson and Thierry Tardy, "Hybrid: What's in a Name?", *European Institute for Security Studies Brief*, n, 32, ottobre 2015, p. 2.

- La capacità di individuare e sfruttare le vulnerabilità del bersaglio.
- Il mantenimento del livello di ostilità al di sotto della soglia della guerra convenzionale.

Il ritorno della dezinformacija

Il rinnovato interesse al tema viene considerevolmente stimolato dal ritorno della *dezinformacija* russa, che la maggior parte degli specialisti di politica internazionale ritenevano fosse stata definitivamente archiviata con la fine della Guerra Fredda.
A partire dalla crisi ucraina Mosca ricorre in maniera sempre più intensa alla disinformazione, sia all'interno del paese, sia all'estero. La disinformazione verso l'interno é finalizzata a mantenere la stabilità del regime, mentre quella di carattere esterno è funzionale al perseguimento di due obiettivi fondamentali della politica estera russa: ricostituire una sfera d'influenza nell'"Estero Vicino", e indebolire l'Occidente fomentando divisioni e diffondendo un senso di sfiducia e insicurezza al suo interno.
Il succitato dibattito russo sulla "guerra con le informazioni" ci aiuta a capire perché la Russia di Putin abbia deciso di riattivare la *dezinformacija* in maniera così sistematica e vigorosa. Dalla metà degli anni 2000 tra i membri dell'*establishment* politico, militare e dell'intelligence russo si diffonde la convinzione secondo cui l'Occidente ricorrerebbe a tecniche di *information warfare* - dai social networks all'utilizzo di organizzazioni non-governative - per fomentare rivoluzioni e instaurare governi filo-occidentali nei paesi dell'"Estero Vicino", area che Mosca considera la propria zona d'influenza. Secondo questa teoria, l'Occidente - e soprattutto gli Stati Uniti - utilizzerebbe dette tecniche per provocare proteste anti-governative nella stessa Russia, al fine di rovesciare il regime di Putin, e indebolire, se non disgregare, lo Stato russo. Tale percezione di minaccia - giusta o sbagliata che sia - porta il Cremlino a ritenere necessario e legittimo il ricorso all'*information warfare* nei confronti

dell'Occidente, sia in chiave difensiva (all'interno) che offensiva (all'estero)[31].

Già prima della crisi ucraina il Cremlino aveva deciso di rafforzare le proprie contromisure difensive tese a neutralizzare la percepita "minaccia informativa" proveniente da Occidente, ma anche di potenziare le proprie attività offensive di *information warfare*, tra cui la disinformazione anti-occidentale, anti-americana e anti-UE.

A tale scopo l'apparato mediatico internazionale controllato dal Cremlino viene notevolmente ampliato e modernizzato in seguito a ingenti investimenti. La disinformazione russa rivolta verso l'estero viene veicolata sia dai grandi mezzi di comunicazione - come l'emittente televisiva RT e l'agenzia multimediale Sputnik - sia sfruttando tutti gli strumenti del nuovo universo dei media digitali: social media, siti e blog di "informazione alternativa", *troll* di internet (propagandisti pagati dal Cremlino), adoperati non solo per amplificare le notizie false o manipolate ma anche per intimidire e screditare chi si adopera per smascherarle[32].

Si possono individuare diversi temi ricorrenti nelle operazioni disinformative russe in Occidente, che tendono a enfatizzare le debolezze e i fallimenti delle società occidentali e del modello liberal-democratico. Nei confronti delle opinioni pubbliche europee, ad esempio, vengono veicolati i seguenti messaggi:

- "I governi europei sono completamente impotenti di fronte al terrorismo islamista".
- "La Russia di Putin è l'unico Stato che si impegna veramente nella lotta a DAESH, creato con la complicità delle potenze occidentali e in particolare degli Stati Uniti".
- "L'Europa é invasa da immigrati e profughi provenienti dal Medio Oriente e dall'Africa che sono fuori controllo e

[31]Stefan Meister, "Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign", Transatlantic Academy Paper Series, Aprile 2016, p. 3-5.

[32]EU East StratComm Task Force, "Means, Goals and Consequences of the Pro-Kremlin Disinformation Campaign", ISPI Commentary, 19 gennaio 2017. p. 2.

accrescono sempre di più il disordine e la violenza nel continente".

- "L'Europa e l'Occidente in generale sono società decadenti sotto il profilo morale".
- "I governanti dei paesi europei sono burattini degli Stati Uniti".
- "Gli Stati Uniti e il complesso militare-industriale americano vogliono dominare il mondo".

Non di rado vengono amplificate varie teorie del complotto (o della cospirazione) per accrescere l'ostilità dei cittadini nei confronti delle élites, del *establishment*, del sistema mediatico, o di altri gruppi potenti. Talvolta la *dezinformacija* destinata all'Europa mira non tanto a diffondere una tesi precisa, ma a creare confusione cognitiva, a relativizzare e screditare il concetto di "verità", facendo passare l'idea che esistono "molteplici verità", e che tutta l'informazione è manipolata, da qualunque parte provenga[33].

La Russia di Putin ha senza dubbio risuscitato le tecniche della *dezinformacija* adoperate dal KGB e dal Partito Comunista dell'Unione Sovietica durante la Guerra Fredda, modernizzandole e adattandole al XXI secolo con l'introduzione delle più innovative tecnologie ICT. Va evidenziata, tuttavia, una differenza fondamentale tra la *dezinformacija* sovietica e quella della Russia putiniana: mentre la prima era strumento di una politica di espansione globale dell'ideologia marx-leninista e del potere dell'URSS, la seconda viene praticata per perseguire finalità più limitate e di carattere prettamente geopolitico e non ideologico[34].

---

[33] Peter Pomerantsev e Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Special Report, The Interpreter and Institute of Modern Russia, 2014.

[34] La politica estera russa, come abbiamo già sottolineato, punta a rilanciare Mosca come grande potenza mondiale, dotata di una propria sfera d'influenza nello spazio post-sovietico, nel quadro di sistema internazionale "multipolare" e non più sottoposto all'egemonia statunitense. Mentre l'Unione Sovietica, fino all'epoca di Gorbačëv, ambiva a conquistare una posizione egemonica a livello

Il ritorno della *dezinformacija* russa viene percepita come minaccia da diversi governi occidentali, che ne temono l'impatto potenzialmente destabilizzante, soprattutto nelle società europee, rese fragili e vulnerabili da una crisi profonda e multidimensionale. Una crisi che non è certo stata creata dalla Russia, ma che quest'ultima intende sfruttare fino in fondo in funzione dei propri interessi geopolitici.
Gli analisti hanno individuato i seguenti obiettivi strategici della *dezinformacija* russa in Europa:

1) Delegittimare e indebolire l'UE e la NATO, e minare l'efficacia dei loro processi decisionali.
2) Fomentare tensioni tra paesi all'interno dell'UE e della NATO.
3) Logorare l'autorità e la credibilità di governi europei ritenuti ostili o poco collaborativi con Mosca.
4) Aumentare l'instabilità e la conflittualità nella politica interna dei paesi dell'UE.
5) Favorire la crescita, se non l'ascesa al potere, di partiti populisti europei filo-Cremlino.
6) Alimentare la sfiducia dell'opinione pubblica in Europa nei confronti del modello liberal-democratico occidentale e nei valori fondamentali della "società aperta".
7) Screditare le voci europee critiche, in ambito politico e mediatico, nei confronti del regime russo e della sua politica estera.

La rinnovata attenzione nei confronti della disinformazione - e in modo particolare di quella russa - non ha tuttavia ancora portato i governi occidentali a investire le risorse necessarie per poter comprendere a fondo e contrastare efficacemente il fenomeno. Inoltre, continua a essere poco studiato l'uso di quest'arma da parte di attori non-statali illeciti, come gruppi terroristici, movimenti politici estremisti, organizzazioni mafiose, cartelli della droga e poteri occulti.

---

globale, e si sentiva investita della missione di espandere l'ideologia comunista in tutto il mondo.

La minaccia al sistema-Italia

Malgrado la recente ripresa d'interesse nel tema a livello internazionale, la disinformazione come minaccia alla sicurezza nazionale rimane una questione poco discussa e approfondita in Italia dal mondo accademico e dei *think tank*. La comunità d'intelligence nazionale se ne sta occupando in qualche misura, ma le risorse destinate al settore sono del tutto insufficienti rispetto ai rischi crescenti per il sistema-Italia connessi all'espansione della disinformazione di matrice sia statale che non-statale.
La disinformazione è una minaccia multiforme che comprende diversi tipi di rischi per la sicurezza nazionale che vanno sistematicamente monitorati e analizzati, tra cui i seguenti:

- Azioni promosse da potenze straniere miranti a manipolare le percezioni dell'opinione pubblica e/o dei decisori politici nazionali per portare il Paese ad assumere decisioni di politica estera contrarie all'interesse nazionale.
- Campagne di disinformazione economico-finanziaria miranti a danneggiare la reputazione dell'Italia e/o delle sue più importanti imprese, o a influire sui mercati finanziari con conseguenze destabilizzanti sul sistema economico nazionale.
- Attività disinformative promosse da gruppi e movimenti socio-politici estremisti al fine di diffondere paura, odio e confusione in determinati settori della popolazione italiana, incoraggiando comportamenti violenti.
- L'uso dello spazio cibernetico da parte di movimenti terroristici di matrice islamista per attività di propaganda e disinformazione finalizzate alla radicalizzazione di immigrati di fede musulmana presenti in Italia.
- Operazioni di *deception* promosse da organizzazioni criminali italiane o estere per falsare le analisi o depistare le indagini anti-mafia svolte da forze di polizia, dalla magistratura o dai servizi d'intelligence.

- Il ricorso, da parte di gruppi terroristici o eversivi, a minacce o falsi allarmi (anche di natura nucleare, biologica o chimica) inteso a generare disordine e panico.

È evidente, di conseguenza, che la tradizionale minaccia della disinformazione acquisisce, nell'era del *cyber-power*, connotati nuovi e inediti, rendendo necessario un potenziamento della ricerca scientifica e dell'analisi d'intelligence in questo campo. Inoltre, è indispensabile rendere sempre più consapevoli di questa sfida i decisori politici e aziendali italiani, il sistema mediatico, l'opinione pubblica, il mondo accademico e gli istituti culturali e di ricerca.