

**COMMISSIONE III
AFFARI ESTERI E COMUNITARI**

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

6.

SEDUTA DI MARTEDÌ 21 LUGLIO 2020

PRESIDENZA DEL VICEPRESIDENTE **PAOLO FORMENTINI**

INDICE

	PAG.		PAG.
Sulla pubblicità dei lavori:		Billi Simone (LEGA)	12
Formentini Paolo, <i>Presidente</i>	3	Boldrini Laura (PD)	9
INDAGINE CONOSCITIVA SULLE EVENTUALI INTERFERENZE STRANIERE SUL SISTEMA DELLE RELAZIONI INTERNAZIONALI DELLA REPUBBLICA ITALIANA		Cabras Pino (M5S)	10
Audizione di Stefano Mele, esperto di cybersecurity:		Mele Stefano, <i>esperto di cybersecurity</i>	3, 13
Formentini Paolo, <i>Presidente</i>	3, 9, 13, 17	Romano Andrea (PD)	11
		<i>ALLEGATO: Documentazione depositata dall'avvocato Mele</i>	18

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Forza Italia - Berlusconi Presidente: FI; Partito Democratico: PD; Fratelli d'Italia: FdI; Italia Viva: IV; Liberi e Uguali: LeU; Misto: Misto; Misto-Noi con l'Italia-USEI-Cambiamo!-Alleanza di Centro: Misto-NI-USEI-C!-AC; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Centro Democratico-Radicali Italiani-+Europa: Misto-CD-RI-+E; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE; Misto-Popolo Protagonista - Alternativa Popolare: Misto-PP-AP.

PAGINA BIANCA

PRESIDENZA DEL VICEPRESIDENTE
PAOLO FORMENTINI

La seduta comincia alle 12.40.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione di Stefano Mele, esperto di cybersicurezza.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle eventuali interferenze straniere sul sistema delle relazioni internazionali della Repubblica Italiana, l'audizione dell'avvocato Stefano Mele, esperto di cybersicurezza.

Do quindi il benvenuto all'avvocato Mele, che ringrazio per la disponibilità a contribuire ai nostri lavori.

Stefano Mele è il responsabile del Dipartimento di diritto delle tecnologie, *privacy*, *cybersecurity* e *intelligence* presso lo studio legale associato Carnelutti. È, inoltre, presidente dell'Autorità per le tecnologie dell'informazione e della comunicazione della Repubblica di San Marino. La sua attività accademica in materia di *cybersecurity* si svolge presso il Dipartimento di studi giuridici dell'Università Bocconi e anche presso le cattedre di informatica giuridica e informatica giuridica avanzata della facoltà di giurisprudenza dell'Università degli studi di Milano. È altresì membro del Consiglio direttivo e presidente della Commissione sicurezza cibernetica del Co-

mitato atlantico italiano, nonché presidente del gruppo di lavoro sulla *cybersecurity* della Camera di commercio americana in Italia. È docente presso istituti di formazione e di ricerca del Ministero della difesa italiana e della NATO e autore di numerose pubblicazioni scientifiche e articoli sui temi della *cybersecurity*, *cyberintelligence*, *cyberterrorismo* e *cyberwarfare*. In ragione della sua ampia e approfondita competenza su questi temi, nel 2014 la NATO lo ha inserito nella lista dei suoi *key opinion leaders for cyberspace security*.

Ciò premesso do la parola al nostro ospite affinché svolga il suo intervento.

STEFANO MELE, *esperto di cybersicurezza*. Grazie mille, presidente. Per me è un privilegio essere qui oggi con voi a parlare di un tema che ritengo davvero molto importante, e quindi assolutamente un plauso a questa Commissione che ha deciso di approfondire il tema della propaganda, della disinformazione in linea generale legata alle potenziali attività – e vedremo sotto il punto di vista dell'*on line*, della *cybersecurity* se sono potenziali o se sono molto attuali – e non solo, addirittura già svolte da parte di Governi nelle nostre relazioni internazionali.

Effettivamente viviamo nell'era della disinformazione. Noi siamo già dentro la disinformazione e siamo già dentro un'era, da tanti anni, che è caratterizzata essenzialmente da un'enorme produzione tecnologica e da un'enorme produzione di informazioni. Queste informazioni sono manipolate costantemente, da molti anni, da numerosi attori statali, sia europei sia extraeuropei. Del resto, è sotto gli occhi di tutti – ritengo – quante e quali tipologie di informazioni vengano costantemente sottratte per essere date ai giornalisti o messe *on line* con un intento prettamente male-

volo di screditare un Governo, una persona fisica, un'azienda e così via. È sotto gli occhi di tutti quanto, attraverso le tecnologie e quindi attraverso la propaganda e la disinformazione fatta attraverso le tecnologie, oggi più che mai sia facile creare dei cunei all'interno della nostra democrazia e all'interno delle nostre istituzioni, infiammando il dibattito.

Per questo è assolutamente importante, secondo me, analizzare questi fatti — e vi ringrazio davvero per l'invito, perché per me è un privilegio — e analizzarli nel campo di battaglia — perdonatemi il termine — più attuale, che è appunto il cyberspazio. In particolar modo c'è da evidenziare, anzitutto, che sicuramente non si tratta di qualcosa di innovativo, di nuovo, di un fenomeno inedito che è nato attraverso *internet*. In realtà, quando parliamo di propaganda e di disinformazione, parliamo della cosiddetta politica *warfare*, che è un concetto che nasce nel 1920, in particolar modo all'interno degli ambienti della CIA, dell'Agenzia *d'intelligence* americana che tutti quanti conosciamo. È qualcosa che è stato fatto ed è stato applicato, in particolar modo dagli Stati Uniti d'America, non soltanto nel periodo delle due guerre mondiali, ma soprattutto dalla seconda guerra mondiale e ovviamente durante la guerra fredda, come tutti quanti sappiamo, con ricadute note a tutti anche in relazione, per esempio, all'attività russa nel settore della disinformazione. Però c'è un tema fondamentale: quella vecchia arte della politica *warfare* era caratterizzata fondamentalmente da un'influenza molto lenta, costruita a tavolino con grande attenzione, fatta avvicinandosi alle persone, parlando, influenzando la loro sfera psicologica. Oggi la capillarità di *internet* e delle tecnologie ha cambiato completamente questo paradigma e non abbiamo più una politica *warfare*, e non la chiamiamo nemmeno più politica *warfare*, così strutturata; abbiamo una serie di misure attive che vengono utilizzate costantemente da Governi nel e attraverso il cyberspazio, in maniera veloce, in maniera istantanea, più che altro con scarsa qualificazione in alcuni casi; soprattutto, questa azione viene compiuta

da remoto, sempre di più. Inevitabilmente queste attività sono, come ho detto, misure attive, ma più che mai questo cambio di paradigma, che è avvenuto principalmente attraverso le tecnologie, ha trasformato un lavoro lento e certosino in un lavoro di massa, quindi in un'influenza psicologica di massa data appunto dalla capillarità di *internet*.

Questo ha reso la disinformazione e la propaganda una minaccia molto peggiore rispetto a quella che era durante la seconda guerra mondiale, durante la guerra fredda e praticamente fino agli inizi del 2010, quando *internet* e le tecnologie sono cominciate a diventare un nuovo strumento nell'arco della politica di qualsiasi nazione. Questo, di conseguenza, fa sì che nel momento in cui vengono strutturate questo genere di operazioni e vengono fatte tramite *internet* e le tecnologie, anche per il Governo che le predispone è molto complicato non soltanto immaginarne gli effetti, ma anche controllarne gli effetti, controllarne il risultato; e questo mi fa dire che le rende ancora più pericolose di quelle fatte *ante* 2010.

Qual è l'obiettivo della guerra attraverso le informazioni, come la chiamo io? Gli obiettivi sono essenzialmente molteplici. Evidentemente c'è quello di creare divisioni fra nazioni alleate; manipolare i gruppi etnici; creare attrito fra soggetti, fra individui, fra gruppi; erodere la legittimità di un Governo o erodere la reputazione di una persona; facilitare determinate scelte politiche, che sarebbero complicate da attuare senza un'attività di propaganda e di disinformazione. Lo si fa — scusate il gioco di parole — con la propaganda, che quindi è una attività tesa a coinvolgere emotivamente il soggetto che la riceve, oppure con la disinformazione, che è un'attività tesa invece a forgiare delle informazioni false per manipolare la percezione. Ovviamente, questa attività è sempre di più fatta attraverso *internet* e le tecnologie. L'abbiamo conosciuta tutti e abbiamo imparato a definirla — con il termine scorretto, dal mio punto di vista, di *fake news* — a parlarne e conoscerla nel 2016, durante le elezioni del Presidente Trump, ma in realtà è qualcosa

che come abbiamo detto esiste da tantissimi anni. È una minaccia molto coerente e molto profonda: è molto coerente con le politiche di chi la pone in essere e molto profonda all'interno delle nostre società. Se avessimo studiato... Gli Stati Uniti, come sapete, accusano in maniera diretta la Russia attraverso un *report*, il primo *report* nella storia sottoscritto dalle diciassette agenzie di *intelligence* americane dove si punta il dito in maniera diretta e dichiarata contro il Governo russo; è un *report*, peraltro pubblico, molto interessante da leggere. Se avessimo studiato le metodologie e le tecniche del Governo russo di infiltrazione e di manipolazione delle elezioni presidenziali dell'Ucraina due anni prima, avremmo capito tranquillamente e in maniera molto semplice lo schema di azione del Governo russo quando cerca di manipolare delle elezioni presidenziali.

Se seguite, come io amo fare, la politica americana oltre a quella italiana, saprete benissimo che da un anno a questa parte non c'è quotidiano, non c'è telegiornale, non c'è programma informativo negli Stati Uniti d'America che non apra parlando del rischio delle infiltrazioni da parte di Governi stranieri nelle prossime elezioni del Presidente degli Stati Uniti d'America, che come sapete probabilmente saranno entro la fine di quest'anno.

Anche l'Italia ha subito delle attività — evidenti dal mio punto di vista — sotto il profilo della propaganda e della disinformazione durante l'emergenza COVID-19. In particolare, abbiamo subito in maniera evidente, a mio avviso, delle attività da parte del Governo cinese. Questi (*slide n. 7*) sono dei *tweet* originali dove uno dei portavoce del Ministero degli Affari esteri cinese usa ciò che noi abbiamo fatto — cioè cercare una coesione nazionale cantando l'inno durante l'emergenza COVID-19 dai nostri balconi, cercando di darci coraggio — per fare propaganda all'interno della Cina sull'apprezzamento che i cittadini italiani stavano dando agli aiuti cinesi. Vediamo come questo sia fatto anche ufficialmente — e, peraltro, in maniera anche abbastanza dilettantesca, passatemi il termine, perché evidentemente si credeva che mettendo

l'*hashtag #Italy* nessuno se ne sarebbe accorto nel nostro Paese —, soggetti legati istituzionalmente ad alte figure governative cinesi hanno utilizzato *internet* e le tecnologie per fare propaganda all'interno del proprio Paese e quindi, di conseguenza, per cercare di influenzare la percezione che i cittadini cinesi hanno di quello che è avvenuto.

In particolar modo, infatti, vorrei approfondire le attività del Governo cinese e poi anche quelle del Governo russo in un'ottica proprio di propaganda e di disinformazione. Sotto questo punto di vista dobbiamo sapere, per esempio, che durante il 2019 il Governo cinese ha puntato enormemente su questo genere di attività. Ha puntato enormemente su questo legando addirittura il progetto della *Belt and Road Initiative*, quindi della Nuova Via della Seta, estendendolo anche all'ambito delle comunicazioni, della propaganda e della disinformazione. Questo non lo dice l'avvocato Stefano Mele, non lo dicono i *report* americani, non lo dicono i *report* occidentali. Lo dicono i *report* ufficiali di *Reporter senza Frontiere*, quindi un'organizzazione che dovrebbe essere presa come esempio di apoliticità. Se noi andiamo ad analizzare questi *report*, scopriamo che normalmente il Governo cinese organizza dei viaggi all'interno della *Belt and Road*, dei viaggi per giornalisti a livello internazionale, di indottrinamento. Negli ultimi dieci anni vengono investiti per ogni anno 1,4 miliardi di dollari... Ripeto, ogni anno negli ultimi dieci anni, 1,4 miliardi di dollari vengono investiti dal Governo cinese proprio sulla questione della comunicazione. È stato creato addirittura un *News Network* legato alla Via della Seta, cioè un'associazione che prevede l'interconnessione di giornalisti in ottantasei Paesi differenti e non dico che siano a libro paga, però comunque sono vicini alle politiche della Cina attraverso questa metodologia. È chiaro ed evidente quanto il Governo cinese abbia puntato negli ultimi dieci anni, ma soprattutto negli ultimi quattro o cinque, a questo strumento come uno strumento di potere, come uno strumento di influenza, come uno strumento per ottenere risultati politici all'in-

terno dell'Italia, all'interno dell'Unione europea, all'interno dell'Occidente, all'interno dei Paesi africani e così via, ed è sotto gli occhi di tutti. Chi non vuole vedere questi dati, questi documenti e queste prove, che abbiamo visto quanto abbiano impattato enormemente anche il nostro Paese durante l'emergenza COVID-19, a mio avviso o non vuole vedere o non può vedere la realtà di questi fatti.

In particolar modo, se guardiamo l'attività strettamente legata alla propaganda durante l'emergenza COVID-19, sia interna sia esterna, possiamo trarre delle linee politiche, delle linee strategiche del Governo cinese che sono state attuate in maniera molto chirurgica durante l'emergenza COVID-19. Innanzitutto una prima linea politica è quella di cercare di allontanarsi dall'essere imputabile come la nazione che ha coperto, almeno in una prima fase, l'emergenza COVID-19. La seconda linea politica è quella di far vedere la Cina come un buon attore all'interno dello scenario internazionale. Qui la propaganda si è concentrata, in particolar modo, nel dire che il Governo cinese è stato quello impattato all'inizio, ha già risolto la problematica e adesso si pone come cittadino del mondo per dare ed elargire degli aiuti; ma in un'ottica di propaganda questo deve essere letto non come dare semplicemente degli aiuti, ma dimostrare come il modello cinese di *governance*, il modello politico di gestione di una minaccia, sia migliore rispetto a quello degli Stati occidentali e quindi cercare di esportarlo.

Questa immagine che vedete (*slide n. 12*) è il quantitativo di informazioni, il quantitativo di *tweet*, il quantitativo di articoli che il Governo cinese ha sviluppato giorno per giorno, dall'inizio di gennaio agli inizi di marzo di quest'anno, relativi alla questione COVID-19, quindi concentrati soltanto sull'*hashtag* *#covid-19*. Vedete come si impenna sempre di più e come, soprattutto dalla metà di febbraio fino agli inizi di marzo, sia davvero molto rilevante in termini numerici. Questo sta ad indicare quanto effettivamente il Governo cinese stia puntando su questo e soprattutto c'è un elemento che io ritengo molto impor-

tante da approfondire e da sottolineare in questo caso: quanto la propaganda cinese contro l'Occidente e la propaganda russa contro l'Occidente stiano convergendo. Questa immagine che vedete (*slide n. 13*) è relativa a un tema molto caro al Governo russo, legato agli Stati Uniti d'America che avrebbero aperto nel corso degli anni centinaia di laboratori di biosicurezza in venticinque Paesi differenti per sviluppare armi biologiche da utilizzare in caso di conflitto. Questo è un tema classico della propaganda russa. Recentemente abbiamo notato come, sempre *on line*, sempre attraverso *internet* e le tecnologie, la Cina si sia allineata sul messaggio russo, abbia ripreso temi cari al Governo russo, li abbia rilanciati attraverso CGTN — che è il *network* internazionale di televisione cinese —, legato inevitabilmente al principale *network* nazionale di comunicazione televisiva. La Cina ha evidenziato questo tema e successivamente il Governo russo si è inserito su questa logica cinese e ha approfondito e sottolineato le preoccupazioni cinesi in un'ottica di propaganda russa, quindi spingendole sempre di più. Quindi notiamo un allineamento tra Cina e Russia, in particolar modo su questi e su altri temi, ma in ogni caso sull'utilizzo della propaganda e della disinformazione come strumento di politica internazionale.

Infatti la Russia è il secondo Stato di cui vorrei approfondire oggi alcuni tratti. Lo Stato russo non ha bisogno di presentazioni, quando parliamo di propaganda e di disinformazione. Dal punto di vista storico è stata la CIA, quindi gli Stati Uniti d'America, a inventare nel 1920 la politica *warfare*, come avevo detto, e ad utilizzarla ampiamente in particolar modo durante la seconda guerra mondiale e ovviamente durante la guerra fredda. In ogni caso la *disinformatia* russa, come normalmente viene chiamata, è sicuramente, da sempre, uno strumento importantissimo del Governo russo.

In particolar modo, in realtà, se noi guardiamo ancora una volta la politica russa in generale, possiamo evidenziare come la Russia non abbia alcuna intenzione di fare una politica di forza nei

confronti dei Paesi europei, nei confronti dell'Occidente. La Russia non ha mai intenzione di arrivare a un conflitto aperto — giustamente peraltro — contro determinati Paesi occidentali, contro gli Stati Uniti d'America, contro l'Unione europea. Dove la Russia investe enormemente? In propaganda e disinformazione per fare attività di ingerenza, di propaganda, di manipolazione informativa, di tutto ciò che comporta lo stadio delle informazioni, delle cosiddette *information operation*: cioè colpire le informazioni di un avversario attraverso le informazioni. Colpire attraverso i *computer*, attraverso i sistemi o attraverso dei cyberattacchi veri e propri, la capacità di un sistema di erogare un servizio essenziale, per esempio per una comunità, ma anche di utilizzare *internet* e le tecnologie proprio per questa attività di influenza e di propaganda.

Quali sono gli obiettivi strategici del Governo russo? (*slide n. 16*) Il primo è quello di ripristinare il grande impero russo, e quindi dare una percezione del Governo russo maggiore rispetto a quella che realmente è. Il secondo è quello di insistere sulle attività di influenza politica, in particolar modo in tutte le aree di influenza ritenute in questo momento sensibili e interessanti per il Governo russo: sicuramente, quindi, l'Occidente, ma non solo, sicuramente anche i cosiddetti « Paesi cuscinetto » e quindi tutti gli *ex* Paesi dell'Unione Sovietica, che sono aree di influenza ancor oggi molto evidenti del Governo russo. Proteggere il regime di Putin è il terzo obiettivo, e inevitabilmente questo ci fa ritornare alla memoria un elemento fondamentale che è quello legato al fatto che le operazioni di propaganda e disinformazione agiscono all'esterno e hanno un obiettivo all'esterno, ma in determinati Paesi hanno anche, contestualmente, un obiettivo verso l'interno, di mantenimento del potere politico di chi in quel momento sta amministrando, e in questo caso del Presidente Putin. L'ultimo obiettivo è quello di migliorare la percezione che si ha all'estero della capacità militare della Russia. Questi sono i quattro obiettivi fondamentali, ma in realtà sono solo i quattro basilari. Sono i

quattro obiettivi per cui ho utilizzato il termine « fondamentali » proprio perché sono i quattro principali.

Recentemente è stato pubblicato un *report*, questa volta da parte di una società americana — se qualcuno è interessato, volentieri lo condividerò perché è un *report* pubblico —, che ha posto in evidenza una campagna di propaganda e di disinformazione russa attuata negli ultimi sei anni e l'ha analizzata. Come vedete da questa *slide* (*slide n. 17*), in realtà gli obiettivi nel corso dei sei anni sono stati maggiori dei quattro principali che io vi ho evidenziato, ne vediamo nove. Vediamo, per esempio, quello di far apparire l'Unione europea come ormai disgregata e come un attore non più *trustable*, non più affidabile. Per esempio, ci sono anche campagne contro il *doping* degli atleti russi: si è lavorato per evitare che la percezione degli atleti russi di essere tutti quanti dopati forse quella che andasse per la maggiore. L'ultimo dei nove obiettivi che vedete all'interno di questa *slide* — per non dirli tutti — è quello di contrastare chiunque cerchi di parlare pubblicamente *on line* contro il regime russo all'estero, ma anche all'interno dei confini russi. Ci preoccupa ancora di più quello che viene fatto all'interno del territorio, sempre perché l'obiettivo principale dei quattro che abbiamo visto è anzitutto mantenere il potere e il controllo sui propri cittadini.

Ovviamente, anche durante il COVID-19 la Russia ha fatto attività di disinformazione in Occidente, anche in Italia, ma in particolar modo contro gli Stati Uniti d'America. Questa (*slide n. 18*) è una *slide* molto « simpatica », piena di informazioni — di disinformazione, anzi — nei confronti di Bill Gates: « Bill Gates ha creato il COVID-19, Bill Gates metterà dei *microchip* all'interno di tutti noi per combattere il COVID-19 » e così via. Sono cose anche abbastanza banali, ma poi vedremo — e mi avvio alle conclusioni — se effettivamente questa banalità ha presa oppure no. Guardiamo ai *report* ufficiali dell'Unione europea, quindi ancora una volta di un'istituzione che dal 2015 ha cominciato a prendere davvero sul serio il problema della propaganda e della disinformazione: noi abbiamo un sito *in-*

internet che può essere consultato costantemente e che tiene traccia di tutte le operazioni di propaganda e di disinformazione rivolte soprattutto contro i Paesi dell'Unione europea: vengono analizzate, in particolar modo, le attività di russi e cinesi. Se guardiamo a questi *report* ufficiali, possiamo scoprire quanto questo genere di operazioni, in particolar modo durante il COVID-19, abbia avuto effetti reali sui cittadini europei e sui cittadini in giro per il mondo. Per esempio, se guardiamo agli ultimi *report*, scopriremo che il 23 per cento circa dei cittadini russi — quindi stessa propaganda fatta da russi che influenza i cittadini russi — ritengono che il COVID-19 sia una finzione, che non sia mai esistito. Senza andare troppo distanti, proprio ieri all'interno del TG1 è stato intervistato un ragazzo italiano di vent'anni, che ha detto una cosa in maniera molto infantile (io l'ho considerato un effetto di un'operazione di propaganda in relazione al COVID-19, fatta all'interno dei confini italiani): «Noi stiamo soltanto cercando di divertirci, tanto questo COVID-19 non è mai esistito». Vedete come ci sia un effetto subdolo, ma reale, di un'attività di propaganda e di disinformazione fatta attraverso *internet* e le tecnologie, perché inevitabilmente — sappiamo meglio di chiunque altro che abbiamo di fronte a noi un cellulare costantemente, a dieci centimetri dal volto, per ore durante la giornata, se facciamo il conteggio — è chiaro che se riesco a catturare l'attenzione dei giovani che perdono addirittura più tempo di noi all'interno dei *social network*, è chiaro che io posso manipolare la loro percezione di che cosa stia succedendo all'interno del mondo. Una minaccia serissima come quella del COVID-19, che ha causato — non ve lo devo dire — centinaia di migliaia di morti nell'Unione europea, sentire che qualcuno possa pensare che non sia addirittura esistita o che sia soltanto un'esagerazione mette davvero i brividi e dovrebbe far accendere dei campanelli d'allarme molto rilevanti.

Non le voglio leggere tutte con voi perché lascerò sicuramente queste *slides* agli atti; però sappiate, per esempio, che un terzo dei cittadini del Regno Unito ha ri-

tenuto, tra febbraio e marzo, che la vodka fosse un disinfettante utile per le mani, a causa di attività di propaganda fatta attraverso *internet* e le tecnologie. In Italia la società di sondaggi italiana SWG ha prodotto un *report* in cui ha evidenziato che, in conseguenza delle attività di propaganda e disinformazione che sono state fatte durante il COVID-19, la percezione dei cittadini italiani della Cina come un Paese amico è passata dal 10 per cento nel gennaio del 2020 al 52 per cento a marzo del 2020, in due mesi. Così come la sfiducia nei confronti dell'Unione europea è scesa dal 42 per cento di settembre 2019 al 27 per cento di marzo 2020: quindi queste attività funzionano.

In conclusione, io ritengo che questi temi siano davvero importanti da trattare e vi ringrazio per il tempo che mi avete dedicato. Noi esperti di *cybersecurity* facciamo questo lavoro e guardiamo a questo genere di minacce nell'ambito più complessivo, ma anche e soprattutto a minacce legate alla propaganda e disinformazione, e negli ultimi anni notiamo un errore che viene fatto spesso: credere che questi strumenti influenzino esclusivamente il mondo virtuale, colpiscano esclusivamente il mondo virtuale. In questo caso è esattamente il contrario, perché inevitabilmente, quando viene inserito un documento falso all'interno di un documento autentico, l'effetto che quel documento avrà è nel mondo reale. Inevitabilmente, quando si riesce a far passare una determinata tipologia di linguaggio, determinate ideologie estremiste, determinate tipologie di epiteti razziali attraverso un'operazione di propaganda e disinformazione, l'effetto è raggiunto e l'effetto è reale. Quando dei soggetti decidono di scendere in piazza perché si sono organizzati attraverso *internet* e le tecnologie sulla base di informazioni manipolate, l'effetto di quell'operazione è reale, e così via. Inevitabilmente, è chiaro che ci troviamo di fronte a una minaccia — e qui chiudo davvero — che impatta sul nostro Stato democratico, impatta sulla realtà dei fatti, impatta sulla nostra capacità di distinguere ciò che è vero da ciò che è falso. Se avessimo più tempo, approfondiremmo in

maniera sicuramente molto più precisa questo genere di operazioni fatte da questi Stati, ma anche da altri in maniera minore. Io ritengo che quando si perde la scientificità delle prove, quando viene persa la capacità di distinguere tra vero e falso, l'emotività colma quel vuoto tra ciò che è realmente e ciò che invece non è, ciò che è stato forgiato ad arte.

Ritengo, ancora una volta, che questa sia una sfida di libertà e una sfida di democrazia nel 2020 per il nostro Stato, per l'Unione Europea, per l'Occidente e per qualsiasi nazione che è oggetto di questo genere di attacchi. Non possiamo più tirarci indietro, è una « chiamata alle armi » legata alla sensibilità di comprendere, oggi più che mai, che la nostra libertà e la nostra democrazia passano anzitutto da questa capacità di distinguere tra vero e falso, tra giusto e sbagliato. Il percorso tra vero e falso e giusto e sbagliato è quello che porta a una logica di guerra e di pace. Sappiamo perfettamente che alcuni conflitti, soprattutto nel passato, sono nati in conseguenza di informazioni manipolate e di una percezione sbagliata di determinati argomenti.

Io vi ringrazio ancora una volta per l'attenzione che mi avete prestato e sicuramente attendo con molta ansia le vostre domande. Del resto — come amo dire sempre, presidente —, un avvocato *gratis* non vi ricapiterà mai più, quindi, di conseguenza, spero che ci siano davvero tantissime domande. Vi ringrazio soprattutto per aver avuto la sensibilità di capire che oggi più che mai propaganda e disinformazione sono legate a *internet*, alla tecnologia e alla capillarità di *internet* e delle tecnologie di entrare nelle nostre vite, a dieci centimetri dalla nostra faccia, in qualsiasi momento, da qualsiasi parte del mondo, e soprattutto di poter fare questo genere di operazioni in maniera anonima e quindi di riuscire anche a negare eventuali responsabilità. Grazie mille.

PRESIDENTE. Grazie, si sono prenotati già quattro colleghi per le domande. La prima è l'onorevole Boldrini.

LAURA BOLDRINI. Grazie, signor presidente. Ringrazio l'avvocato Mele per la sua relazione. Io condivido l'analisi che Lei ha fatto. Ritengo da anni, caro avvocato, che la disinformazione sia la più grande minaccia contemporanea per una democrazia. Prima delle elezioni del Presidente Trump io organizzai in questa Camera un incontro con molti *stakeholders* sul tema della disinformazione. All'epoca sembrava qualcosa di completamente campato in aria il diritto ad essere informati correttamente contro il rischio della disinformazione, sembrava una cosa di nicchia. Chiamammo direttori di giornali, direttori di telegiornali, il Consiglio nazionale delle ricerche, quindi luoghi della scienza, perché a quell'epoca la disinformazione era scientifica. Nel tempo abbiamo visto come la disinformazione sia pervasiva, capace di influenzare la formazione del consenso e del dissenso, capace di distruggere reputazioni costruite negli anni attraverso le menzogne, le *fake news*, cioè attraverso le cose inventate. Abbiamo visto come le persone si siano anche intimidite di fronte a questo sistema e infatti molte non partecipano più al dibattito pubblico, perché temono poi l'assalto e la gogna: dunque la disinformazione incide decisamente nei sistemi democratici.

Io penso che noi abbiamo questo problema a livello internazionale, come Lei ci ha illustrato, e lo abbiamo anche a casa nostra, e in modo strutturato. Anche a casa nostra questo sistema dà ottimi risultati, caro avvocato. Nessuno qua può dirsi superiore a questo fenomeno e tutti dovremmo avere l'onestà di affrontare questo tema seriamente, perché non si salverà nessuno. Una volta che tu metti in moto il meccanismo non sai più quella macchina dove va a finire e anche chi ha messo in moto quella macchina rischia di andare a sbattere.

Io ritengo che per trovare un rimedio a questo sistema deviato si debba agire su più livelli e vorrei un Suo parere. Io feci il primo progetto di educazione civica digitale con l'allora Ministra Fedeli. Entrammo nelle scuole a dare strumenti ai ragazzi per stimolare il senso critico e fargli capire che

non tutto quello che è in rete è vero e che una bufala, in quanto tale, si può scoprire, basta avere strumenti e senso critico. Il *New York Times* ci dedicò la prima pagina dicendo che in Italia i ragazzini imparavano a leggere, a scrivere e a scoprire le bufale. Quel progetto fu pilota. Io ritengo indispensabile che si prosegua su quella strada, per stimolare il senso critico e dare gli strumenti tecnici ai nostri giovani per capire cosa è vero e cosa è falso; ma evidentemente non basta, perché questo è un progetto a medio e lungo termine. Nel frattempo, le nostre democrazie sono sotto scacco. Allora io chiedo a Lei, dal suo osservatorio, che cosa si potrebbe fare affinché questo sistema non fagociti la veridicità del dibattito, non lo inquinii totalmente fino a restringerlo, perché l'intimidazione è molto forte oggi.

Io ne parlo anche perché ho visto tanti giovani dire: « Sa che c'è? A questo punto, visto quello che succede ad alcuni di voi, io non faccio più politica, perché non me la sento ». Questo rende la politica meno viva e la democrazia meno capace di includere, quindi chiedo a Lei, nel frattempo, che cosa noi come legislatori e legislative possiamo fare perché questo non diventi l'inizio della fine della libertà nelle nostre democrazie. Grazie.

PINO CABRAS. Ho ascoltato con molta attenzione la Sua relazione e sono temi che mi sono familiari da molti anni. Ci sono analisi, anche se il tema è diventato di moda negli ultimi anni, che datano anche dallo scorso decennio sulle forme di manipolazione dell'opinione pubblica che si insinuano su elementi di contraddizione dei Paesi, dei sistemi informativi, per diffondere elementi di influenza che spostano il centro del dibattito pubblico verso un'altra parte. Ad esempio, il fatto che esistano legioni di *troll* che costano meno di un cacciabombardiere, ma possono essere più efficaci nello spostare le opinioni, quindi la percezione delle vicende politiche e belliche, è un tema che è attuale da molto tempo.

Io vedo molto ben organizzate quelle *slides*, la tassonomia dei problemi e dei concetti rappresentati. Però faccio a Lei la

stessa critica che ho fatto un'altra persona che è intervenuta in questo dibattito, che aveva similmente — anzi, con meno completezza — presentato questa tassonomia, questo insieme di comportamenti. È come se Lei fosse Keynes, che scopre una teoria economica generale, con grande efficacia, ma la applica soltanto al settore ittico o soltanto all'Andalusia. Io vedo questi problemi chiaramente legati al comportamento di alcune nazioni, e sicuramente la Russia li adopera investendo delle risorse significative, ugualmente la Cina. Però è una questione generale e questo è l'elemento che non capisco, a volte, nella torsione di questa discussione.

Ci sono elementi di influenza, di utilizzo anche maligno di certe forme di *soft power*, che sono proprie anche del nostro sistema. Un sistema a cui Lei sicuramente è più organico per frequentazione, per studi, per ambiente, ma anche il nostro ambiente occidentale interviene pesantemente su questo fronte. Anche nella vicenda ucraina non sono stati solo i russi a intervenire nelle dinamiche elettorali. C'era l'Ambasciatore americano che partecipava anche ai comizi e c'erano frange dell'estremismo di destra ucraino che lavoravano fianco a fianco anche con esponenti democratici europei e hanno influito su quella vicenda. È un gioco in cui intervengono tutte le potenze, ma non dobbiamo polarizzare nel senso che questa cosa la fanno soltanto certi soggetti, questo non possiamo dirlo. Ce lo rivela Edward Snowden, che ha svelato una caterva di documenti sulla mole di controllo centralizzato in capo alla *National Security Agency* e ad altre agenzie statunitensi. Ce lo rivelano le ricerche di Assange e le rivelazioni che sono emerse in quella operazione. Ovviamente, anche quell'operazione avrà margini per essere stata sporcata, per aver visto interventi di più Servizi che cercano di agire di sponda per colpire una palla o per colpirne un'altra, però questa è la dialettica di vero e falso che abbiamo nel mondo contemporaneo.

Se dobbiamo ricondurre a una verità nell'interpretazione di questi fatti, dobbiamo guardare anche a noi stessi, senza farci incantare da situazioni immaginifiche

come la vodka per pulirsi le mani. Se l'Europa è caduta nei consensi, non sarà tutto effetto della propaganda russa, sarà per contraddizioni interne di questo sistema che non ha dato risposte tempestive alle sfide estreme che si sono presentate in questi anni, perché aveva essenzialmente un grave difetto di fondo che era il sistema dell'*austerità*. Qualcun altro può fare propaganda, ma siamo stati noi a indebolirci per primi. L'altra cosa che in tutta questa analisi non mi convince è il ruolo del grande *mainstream* informativo, come se fosse immune dalla possibilità di manipolare le informazioni e come se fosse estraneo a questo gioco. Io credo che invece l'oligarchia — perché sono pochi i proprietari — che detiene la proprietà dei grandi organi di informazione entri pesantemente nel gioco della manipolazione informativa, anche con pesanti *fake news*, soprattutto quando ci sono saldature di interessi su alcune vicende politiche: penso alla guerra in Libia, in cui la stampa occidentale non ha giocato un ruolo positivo, infatti si è intossicata con le sue stesse informazioni e oggi subiamo le conseguenze del non aver rappresentato in modo corretto e veritiero le vicende che accadevano.

Queste sono le osservazioni che mi sentivo di fare e sono rivolte anche all'impostazione di tutto questo lavoro che dobbiamo fare. Dobbiamo fare un lavoro a trecentosessanta gradi. Grazie.

ANDREA ROMANO. Anch'io ringrazio l'avvocato e vado subito al punto, ricollegandomi a quanto diceva il collega Cabras. Non ho alcuna velleità di interpretare il suo intervento, che è stato molto chiaro, però c'è una lettura del fenomeno — che è quella che l'onorevole Cabras ha appena descritto e ribadito — secondo cui — mi perdonerà il collega se mi lancio in questa interpretazione — in fondo, da che mondo è mondo, è sempre stato così. Lei un po' lo ha detto: c'è il *political warfare*, tutti fanno questo gioco sporco, di cosa ci stupiamo, è una partita a tutto campo dove ognuno usa le sue cartucce. Naturalmente ognuno è libero di decidere chi è il buono e chi è il cattivo, però fondamentalmente, in termini fenomenologici, siamo di fronte alla stessa

partita, magari con una lieve o meno lieve innovazione tecnologica.

L'assunto diverso, che per esempio è il mio, ed è secondo me uno dei gli obiettivi di questo nostro lavoro — le eventuali ingerenze, ci mancherebbe altro, non è un lavoro preconstituito e viaggia certamente con una visione a trecentosessanta gradi — l'assunto è che invece siamo di fronte a qualcosa di nuovo, non tanto perché è nuovo il colore politico dei soggetti che la promuovono, ma la domanda che ci stiamo ponendo è questa: c'è stato un salto di qualità? C'è un collegamento — questa è la mia lettura — tra agenzie governative e innovazione tecnologica? Nello specifico, la domanda che Le faccio è questa: Russia e Cina, rispetto alla tradizione del *political warfare* — che come Lei ha detto giustamente risale agli anni venti e che ha visto una recrudescenza nella guerra fredda — hanno finanziato e realizzato operazioni di disinformazione con obiettivi politici e che hanno effettivamente realizzato una svolta, un *breakthrough*, un'innovazione profonda nella qualità della discussione pubblica e quindi nella qualità del dibattito democratico nei Paesi occidentali? Questa è la domanda che io mi faccio. Rispetto alla lettura che ha dato l'onorevole Cabras, io la penso in tutt'altro modo.

Pur non essendo nato ieri e pur sapendo che il novecento è attraversato da fenomeni di questo tipo, la mia preoccupazione è: ma non è che il nostro dibattito politico e democratico è influenzato non tanto dal ragazzo che va in giro a fare baldoria e siccome viene beccato dalla telecamera dice: « Il COVID-19 non esiste. ». Quello, lo dico anche da padre, è un fenomeno che mi preoccupa a livello familiare, ma mi preoccupa meno a livello democratico. Quello che mi preoccupa a livello democratico è che il nostro dibattito pubblico — qui siamo in Parlamento e per questo abbiamo tutti insieme deciso di affrontare questo tema — è intossicato, non tanto dalle tesi russe e cinesi che conosciamo. Per fare un riferimento: il fatto che la Cina investa 1,4 miliardi di dollari nelle strategie di informazione non mi scandalizza, perché anche gli Stati Uniti hanno lunghe strategie di

quelle che chiamano « *public diplomacy* »; io e tanti altri colleghi siamo stati invitati negli Stati Uniti e siamo stati blanditi; io ricordo che in un'età molto lontana venni convocato in un programma dal titolo un po' ridicolo che si chiama « *Young Leaders Programme* », dove mi dissero: « Lei è un giovane *leader* » — si sbagliavano, naturalmente — « le paghiamo un bellissimo viaggio negli Stati Uniti e vedrà che quando torna parlerà bene degli Stati Uniti. ». Io in generale parlo bene degli Stati Uniti, ma per ragioni ideologiche non perché mi invitarono lì. Comunque la Cina ha i suoi programmi di *public diplomacy*, gli Stati Uniti hanno i loro programmi di *public diplomacy*. Non è quello il tema. Il tema è: c'è una catena di comando di tipo militare, politico eccetera che condiziona il nostro dibattito pubblico? La domanda che Le faccio — con questa premessa un po' lunga di cui mi scuso — è: Lei ha detto una cosa su cui vorrei un suo approfondimento, cioè che a volte queste strategie sfuggono di mano ai loro promotori. L'ha detto all'inizio del suo intervento e quindi, siccome sappiamo — ma non noi qui, lo sappiamo perché esiste ormai una mole di documentazione importante, la NATO, Lei lo sa meglio di noi, dal 2017 ha messo a fuoco le cosiddette « influenze maligne », è di oggi la pubblicazione in Gran Bretagna del rapporto del Parlamento britannico su queste cose; negli Stati Uniti è stato fatto; è stato fatto dal Parlamento europeo; esiste questa mole di documentazione —, la domanda che Le faccio è: può articolare quel punto? Cioè, ci sono agenzie, in Russia per esempio, che sappiamo essere finanziate dallo Stato — ma gli effetti concreti non il ragazzino che dice che il COVID-19 non esiste —, quegli effetti possono essere sfuggiti alla volontà del decisore politico russo o cinese? Questa è la mia domanda specifica. Grazie.

SIMONE BILLI. Grazie, avvocato Mele. È vero, innanzitutto, il digitale e l'innovazione digitale stanno avendo una crescita esponenziale in questi ultimi anni, quindi anche da un punto di vista legislativo, in questo settore più che in altri, siamo assolutamente a rincorrere molto affannosa-

mente quello che succede nel mondo reale. È un'evoluzione così repentina che è difficile da seguire, soprattutto per i non esperti nel settore.

Devo dire che poche volte mi sono trovato d'accordo, ma oggi lo devo ammettere, con l'onorevole Boldrini quando definisce la *cybersecurity* come una delle più grandi minacce contemporanee per la democrazia, perché è vero: la *cybersecurity* può incidere veramente anche proprio nel concetto di democrazia di un Paese e di una regione, ma anche del mondo; quindi da questo punto di vista la *cybersecurity* è assolutamente molto importante proprio per garantire il nostro sistema democratico, del nostro Paese, del nostro Occidente e del mondo intero. Quindi è assolutamente importante.

Quanto diceva prima anche l'onorevole Cabras, sulle manipolazioni dell'opinione pubblica, è assolutamente vero. Bisogna stare molto attenti, perché con la digitalizzazione e quindi con la *cybersecurity* possono essere intraprese — come ha spiegato anche Lei prima molto bene, avvocato Mele — tantissime iniziative che possono cambiare il sentire dell'opinione pubblica. È anche vero, però, che la *cybersecurity* si rivolge anche ad altri settori, quello industriale — da cui provengo — la sicurezza nazionale, che comunque è sempre molto importante, e quindi in generale anche sui dati personali. Lei stesso, avvocato Mele, nella Sua relazione ha fatto un quadro abbastanza esaustivo anche delle problematiche che in certi Paesi sono molto più grosse e stanno venendo alla ribalta in modo molto più marcato, per esempio la Cina con le sue *fake news*.

Sembra effettivamente che la Cina stia utilizzando questo tipo di sistemi di propaganda in modo molto massiccio. Noi ne abbiamo visto un esempio durante la crisi drammatica del coronavirus, con questi aiuti che non si capisce nemmeno più bene se siano veri o presunti, perché c'è stata un'opera massiccia di comunicazione dietro a questi aiuti della Cina per fare il proprio interesse di Paese, in modo più o meno legittimo.

Quindi con un regime comunista come quello cinese, che nega i diritti umani nel proprio Paese, bisogna stare molto attenti a come questo stesso regime comunista possa utilizzare questi nuovi strumenti e bisogna cercare di porre tutte le possibili barriere che noi abbiamo a disposizione e che possiamo creare per cercare di arginare queste nuove tecnologie, affinché non possano essere utilizzate da un Paese come la Cina per i propri interessi.

Anche la Russia è stata una cosa molto interessante e ha fatto diversi esempi che vanno sempre in quella direzione lì, una direzione di controllo massiccio dell'opinione pubblica. Volevo però sottolineare un fatto che secondo me è comunque importante e su cui avrei piacere di sentire molto in breve la Sua opinione: per quanto riguarda il limite sottile che c'è tra il lecito e l'illecito, perché quando si parla di comunicazione in generale non è facile definire questo limite. Io penso alle problematiche che ci sono da decenni e alle discussioni che si fanno da decenni sulla pubblicità ingannevole, che può avere anche degli aspetti in comune con la *cybersecurity*; pubblicità ingannevole che ha cercato nel corso dei decenni di indirizzare in modo ingannevole e negativo l'opinione pubblica su determinati prodotti in modo da aumentare la commercializzazione. Quindi qual è il limite tra il lecito e l'illecito? Come noi legislatori possiamo definire parametri per cercare di regolare al meglio queste nuove problematiche, tenendo presente, però — e per me è sempre molto importante —, la libertà e la libera iniziativa?

È vero che quando si parla di un regime come può essere quello comunista cinese e questo tramite *fake news*, cioè notizie false, cerca di fare il proprio interesse e di manipolare l'opinione pubblica, questo fatto non può essere considerato rientrante nella libera iniziativa e lecito, e dovrebbe essere colpito. Quindi come si può colpire un fatto del genere e poi, soprattutto, c'è tutta una zona grigia di azioni che non si sa bene se possono essere ritenute lecite o illecite; dipende dai punti di vista, dipende anche dalle idee che ci sono dietro, dipende dal

comune sentire di una nazione, può cambiare da nazione a nazione il sentimento.

Quindi come si può colpire più efficacemente con azioni concrete questi fatti che possono essere illeciti, di vecchia maniera, oppure fatti illeciti, più di nuova maniera? Nuove azioni che prima non si erano mai viste, come quelle delle *fake news*, sono fatti palesemente illeciti che prima non c'erano: come le possiamo colpire, secondo la Sua esperienza professionale? Come possono essere colpiti per cercare di essere il più efficaci possibili, sempre garantendo la libera iniziativa delle persone, dei Paesi e delle nazioni?

Inoltre, dal Suo punto di vista particolarmente privilegiato sull'argomento, Lei vede anche dei nuovi Paesi che stanno emergendo e che possono essere delle grosse minacce per il mondo sul discorso *cybersecurity* o la situazione. Le sembra più stabile e sviluppata, cristallizzata? Sarei curioso di sapere anche una Sua breve opinione su questo. Grazie.

PRESIDENTE. Grazie, invito l'avvocato Mele ad intervenire in sede di replica.

STEFANO MELE, *esperto di cybersicurezza*. Grazie mille, innanzitutto per tutte le domande che mi sono state poste e anche per le puntualizzazioni, davvero molto interessanti.

Comincio dall'onorevole Boldrini. Grazie onorevole, sottoscrivo ogni parola del Suo approfondimento. Effettivamente, e qui mi ricollego anche a una parte dell'ultima domanda, abbiamo urgente necessità di pianificare una strategia per contrastare questi fenomeni, perché come giustamente Lei ha evidenziato, ci sono misure che io condivido pienamente, quella dell'educazione civica digitale, lanciata da Lei. Dobbiamo tornare a insegnare educazione civica all'interno delle nostre scuole e declinarla su elementi dove i nuovi cittadini — giovani — vivono in questo momento: sia nelle strade — ne abbiamo bisogno anche lì, purtroppo, ancora — ma sicuramente nel mondo digitale. Però, come giustamente evidenziato da Lei, questo è uno strumento di medio-lungo periodo. Allora una strategia occorre

farla e una strategia per essere davvero efficace, per quanto debba coprire da cinque anni in poi — per intenderci — ha comunque sempre un piano di attuazione tattico-operativo nei primi due/tre anni. Sicuramente io ritengo che un ruolo fondamentale sia giocato, per una determinata fascia di età, ancora dai *mass media*, e quindi cercare strumenti di educazione civica e dare strumenti di educazione civica attraverso i *mass media*.

Non è pensabile, oggi, trascurare gli argomenti di *cybersecurity*: in generale, di come si può attaccare un sistema informatico e spegnere l'erogazione dell'energia elettrica — è stato fatto nel dicembre del 2015 in Ucraina, secondo il governo ucraino dai russi ancora una volta —; come si svolgono le attività di spionaggio: tutti gli Stati spiano, tutti gli Stati hanno sempre spiato, tutti gli Stati vogliono continuare a spiare, ma anche lo spionaggio ha delle regole e quando lo spionaggio si rivolge alla sottrazione di informazioni digitali a vantaggio dell'economia nazionale, a vantaggio di società private nazionali, che poi partecipano ad appalti europei e internazionali consapevoli delle varie offerte, allora si violano determinate regole.

Quindi occorre contrastare questo genere di fenomeni, contrastare la criminalità informatica, il terrorismo, che sempre di più imparerà ad utilizzarli. Dobbiamo creare e piantare quei semi anche attraverso i *mass media*, perché inevitabilmente la sicurezza cibernetica e l'educazione digitale che Lei ha puntualizzato sono una responsabilità di tutti e di tutte le fasce d'età. Il problema è colpire i giovani, nel senso di colpire l'attenzione dei giovani che sono gli stessi che si allontanano purtroppo dalla politica, che si allontanano dalla voglia di partecipare alla cosa pubblica, che è un male enorme dell'Italia — io ritengo — ma di qualsiasi altra nazione europea in questo momento.

Sotto questo punto di vista io vedo, su due piedi, anzitutto come fondamentale cercare di creare delle campagne di sensibilizzazione che parlino attraverso quelle stesse piattaforme da cui vengono erogate attività di propaganda e di disinforma-

zione. Questa è una strategia che viene utilizzata per il contrasto alla propaganda terroristica: quindi combattere, tra le varie cose, la propaganda terroristica fatta *online* con messaggi diametralmente opposti, quindi facendo vedere, per esempio, durante la minaccia legata al sedicente Stato islamico, che quello che veniva detto non era in realtà la verità, e dunque venivano intervistate delle donne fuoriuscite dal sedicente Stato islamico che raccontavano la verità dei fatti, far vedere quanto male è stato fatto. Io ritengo che questo potrebbe essere un piccolo granello in una strategia più complessa.

Occorre, inoltre, analizzare la normativa, quindi immaginare delle norme — sono un avvocato, quindi non posso non parlare della questione normativa — che regolamentino determinati comportamenti e che soprattutto colleghino delle responsabilità in relazione a questo genere di comportamenti. Bisognerebbe vedere quale ruolo vogliamo dare alle piattaforme digitali. Sicuramente potrebbe essere una strada, dalla quale, tuttavia, le piattaforme digitali cercano di fuggire a gambe levate, perché comporterebbe per loro di essere trattate come se fossero dei direttori di una testata giornalistica. Sicuramente è un elemento da analizzare e da declinare, però qualcosa deve essere fatta, inevitabilmente, e deve passare a mio avviso per una strategia che tenga conto in maniera ampia non soltanto delle esigenze dei « vecchi », quindi della popolazione da una certa età in poi, ma anche e soprattutto dei giovani, che tenga conto dell'aspetto sociale, che tenga conto dell'aspetto normativo, che tenga conto di tutti gli altri aspetti che inevitabilmente devono essere considerati quando si vuole fare davvero una strategia seria e si capisce — come io spero di aver trasferito a voi — che siamo di fronte a una minaccia reale.

Anche perché — qui rispondo un po' all'onorevole Cabras e un po' all'onorevole Romano — questo genere di attività viene condotto dai servizi di *intelligence*, viene preparato dai servizi di *intelligence*. Nel 1920 era così, ho citato la CIA proprio perché non volevo assolutamente dare il senso che questa mia ora di approfondi-

mento con voi fosse contro soltanto la Cina e la Russia, perché non è assolutamente così. Così come tutti gli Stati fanno spionaggio informatico a seconda delle loro necessità politiche del momento, di breve, medio e lungo periodo, così una possibilità potrebbe essere di utilizzare strumenti di propaganda, a maggior ragione perché inventata dagli Stati Uniti d'America.

Però, se io dovessi scegliere in questa partita in che campo giocare — l'ha detto Lei, onorevole Cabras — io scelgo di giocare nel campo di chi ha le mie stesse regole, nel campo di chi ha la possibilità che ci sia Snowden e la possibilità che Snowden possa esistere e possa rilasciare pubblicamente, attraverso il *Guardian* e attraverso la comunità internazionale di quotidiani che hanno dato visibilità a questa attività, liberamente questo genere di cose.

Non credo che in altri Paesi ci sia la stessa libertà di cui godiamo noi — di stampa, di opinione —, gli stessi valori su cui noi ci basiamo e quindi, tenendo presente che è un comportamento che viene fatto da tutti — e lo ripuntualizzo —, con più o meno efficacia e con più o meno pressione e organizzazione di questo genere di attività, io preferisco guardare a chi ritengo essere davvero una minaccia, perché non gioca « nel nostro campionato », non gioca con le nostre regole, non gioca — è la mia personalissima opinione — con i diritti, non gioca con la libertà di espressione, non gioca con la libertà di stampa e non gioca con tantissimi altri presupposti che io ritengo fondamentali e alla base del vivere comune occidentale, e diciamo globale — dovrebbe essere, purtroppo non lo è — nel 2020.

Però sono indubbiamente delle operazioni, onorevole Romano, come dicevo all'inizio, fatte e preparate in particolar modo dall'*intelligence*, anche perché l'*intelligence* ha una mano molto più ampia in determinate tipologie di attività, risponde molto meno rispetto, per esempio, alle Forze armate, rispetto ad altri soggetti di attività che hanno connotati sotto il punto di vista anche del diritto internazionale. L'ingerenza all'interno degli affari politici di uno Stato è sicuramente un'attività che può

essere analizzata sotto il punto di vista del diritto internazionale e questo genere di analisi porta delle conseguenze per chi la svolge.

Quindi inevitabilmente io ritengo che ci sia stato un cambiamento evidente della pericolosità di questo genere di attività, perché l'abbiamo chiamata giustamente « *soft power* », ma il *soft power* è qualcosa di strutturato, è qualcosa che riguarda fondamentalmente un approccio di politica al *warfare* come l'abbiamo conosciuta e come l'abbiamo studiata durante la seconda guerra mondiale, durante la guerra fredda e fino a prima del 2010, quindi un'attività lenta, minuziosa di avvicinamento verso le persone; molte volte di *human intelligence* per intenderci, quindi addirittura tarata su una persona specifica.

Oggi invece i Governi approfittano di *internet* e delle tecnologie per fare delle vere e proprie campagne di propaganda e di disinformazione veloci, da qualsiasi parte del mondo, in maniera anonima, utilizzando anche soggetti terzi, quindi anche in maniera molto economica e anche abbastanza disorganizzata in alcuni casi, come ho analizzato precedentemente. Questo comporta che, come ho sottolineato all'interno di un passaggio, questo genere di minaccia si sia acuita, perché lo stesso Governo che organizza queste campagne, normalmente attraverso le agenzie di *intelligence*, perde il controllo di queste operazioni. Perde anche la capacità di comprendere l'efficacia di queste operazioni, i loro effetti e quindi nel momento in cui qualcosa che io ritengo essere una minaccia sfugge al controllo di chi perpetra questa minaccia è chiaro che non può che essere un qualcosa che mi preoccupa molto di più rispetto a qualcosa — mi scuso per il gioco di parole — che sia controllato e verificato nei suoi effetti.

È tutto reale, come ho dimostrato. Io ho letto alcuni esempi alla fine, ma anche politici che votano in conseguenza di campagne di propaganda e di disinformazione e che sono influenzati da questo genere di campagne di disinformazione, perché inserite all'interno di bolle informative, come tutti noi lo siamo, all'interno di un *social network*, all'interno della nostra comunità,

all'interno delle persone che ci circondano giornalmente sia *offline* che *online*: siamo influenzati e influenziamo a nostra volta. I politici influenzano a loro volta l'elettorato, giustamente. Trascinano, nel senso buono del termine, l'elettorato verso determinate ideologie. È chiaro che, di conseguenza, dobbiamo guardare alla realtà di questa minaccia, ai suoi effetti, alla sua ricaduta sulla sicurezza nazionale.

Non a caso il titolo del mio intervento è « propaganda e disinformazione *online* come minaccia alla sicurezza nazionale », perché nel momento in cui un politico vota perché influenzato — volente o nolente — da determinate campagne di propaganda e disinformazione, l'effetto è reale e il cambiamento è reale nella politica di quel Paese. Quando i giovani scendono in piazza, la manifestazione è reale. Quando ci sono dei soggetti che guardano all'estremismo politico come a una soluzione di qualsiasi problema, allora l'effetto di quella campagna è ancora una volta reale e sono tutti effetti legati alla sicurezza nazionale.

È lecito o illecito farlo? Ha ragione, onorevole, è molto complicato trovare questa linea di demarcazione, così come è molto complicato trovare una linea di demarcazione, per esempio, nell'attività di *intelligence* da parte di uno Stato, perché inevitabilmente le agenzie di *intelligence* sono lì per spiare. Lo fanno tutti. Non troverà all'interno del diritto internazionale una norma che vieta le operazioni di *intelligence*, proprio perché sul piano del diritto internazionale tutti gli Stati spiano, come ho detto precedentemente, tutti gli Stati hanno sempre spiato e tutti gli Stati vogliono continuare a spiare in ragione della loro capacità e dei loro interessi politici. Di conseguenza, è ovvio che, essendo un comportamento perpetrato da tutti a livello internazionale, non ci sia una norma che vieta questo genere di attività; però tutti quanti la regolamentiamo sotto il punto di vista del diritto interno, onorevole Boldrini, e quindi anche per quanto riguarda le attività di propaganda e disinformazione, a livello di diritto internazionale in questo caso fortunatamente alcune misure le abbiamo e le dobbiamo sfruttare, le

dobbiamo approfondire sul piano legale, dobbiamo capire come e quando farlo, ma sicuramente dobbiamo creare quell'infrastruttura normativa nazionale che permetta di portare a casa una strategia contro questa minaccia quanto mai attuale e reale.

L'ultima riflessione, onorevole, sulla *cybersecurity* in generale: mi ha chiesto se vedo altri Paesi; sì, io vedo che tutti i Paesi sono interessati, Italia compresa, a sfruttare *internet* e le tecnologie per scopi politici, per scopi militari, per scopi informativi, per scopi tecnologici, per scopi anche positivamente legati all'innovazione tecnologica, alla pubblica amministrazione digitale, all'offrire servizi ai cittadini. È chiaro che ancora una volta ci sono alcuni Stati che fanno di *internet* e delle tecnologie un campo di battaglia e altri che fanno di *internet* e delle tecnologie qualcosa per il bene dei propri cittadini, anzitutto.

È lì che noi dobbiamo andare ad analizzare ed è lì che noi dobbiamo andare a evidenziare quelle che sono le differenze tra chi gioca nel nostro campo, con i nostri valori, con la nostra casacca, all'interno del nostro « campionato » — perdonatemi ancora una volta il paragone calcistico — e chi invece fa questo per cercare di ottenere vantaggi politici sul piano internazionale.

È chiaro che se la decliniamo sotto il punto di vista dello spionaggio ci sono ancora una volta tutti gli Stati in prima linea. Ci sono sicuramente anche Stati europei che svolgono pesantissime attività di spionaggio cibernetico nei confronti dell'Italia, in particolar modo, così come ci sono Paesi extraeuropei che svolgono questo genere di attività. È sotto gli occhi di tutti la capacità cinese, russa, iraniana, nordcoreana di cercare di sviluppare sempre più capacità sotto vari punti di vista che sono quelli dello spionaggio, quelli del *warfare*, quindi del conflitto militare nel e attraverso il cyberspazio; quindi nuovi Paesi che in realtà sono vecchi Paesi, che sempre di più strutturano la loro *governance* per sfruttare quello che noi chiamiamo « il quinto dominio della conflittualità »: *internet* e le tecnologie.

Io ancora una volta vi ringrazio. Spero di non avervi annoiato troppo e grazie ancora, presidente.

PRESIDENTE. Ringrazio molto l'avvocato Mele, anche per la documentazione, che sarà pubblicata in allegato al resoconto

stenografico della seduta odierna (*vedi allegato*), e dichiaro conclusa l'audizione.

La seduta termina alle 13.50.

*Licenziato per la stampa
il 13 ottobre 2021*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO



**PROPAGANDA E DISINFORMAZIONE ONLINE
COME MINACCE ALLA SICUREZZA NAZIONALE**

Avv. Stefano Mele

Commissione Affari Esteri — Camera dei Deputati

Roma — 21 Luglio 2020

@MeleStefano

- ▶ **Avvocato specializzato in Diritto delle Tecnologie, Privacy, Cybersecurity e Intelligence presso Carnelutti Studio Legale Associato (Milano)**
- ▶ **Presidente dell’Autorità ICT della Repubblica di San Marino**
- ▶ **Socio fondatore e Partner della società HUMINT Consulting**
- ▶ **Membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano**
- ▶ **Presidente del «Gruppo di Lavoro sulla Cyber-security» della Camera di Commercio Americana in Italia (AMCHAM)**
- ▶ **Docente presso numerosi Istituti di formazione e di ricerca del Ministero della Difesa italiano e in ambito NATO**
- ▶ **Nel 2020, ha partecipato al prestigioso International Visitors Leadership Program (IVLP) del Dipartimento di Stato americano**
- ▶ **La NATO lo ha inserito nella lista dei suoi Key Opinion Leaders for Cyberspace Security**
- ▶ **La rivista americana Forbes lo ha inserito tra i 20 migliori Cyber Policy Experts al mondo da seguire in Rete**



#Propaganda e Disinformazione

La vecchia arte della **'political warfare'**, ovvero quella caratterizzata da un'influenza psicologica lenta, altamente qualificata, fatta a distanza ravvicinata e costruita con grande sforzo e meticolosità, si è trasformata grazie alla capillarità di Internet e delle tecnologie in un'arte ad alta velocità, economica, spesso anche poco qualificata e compiuta da remoto

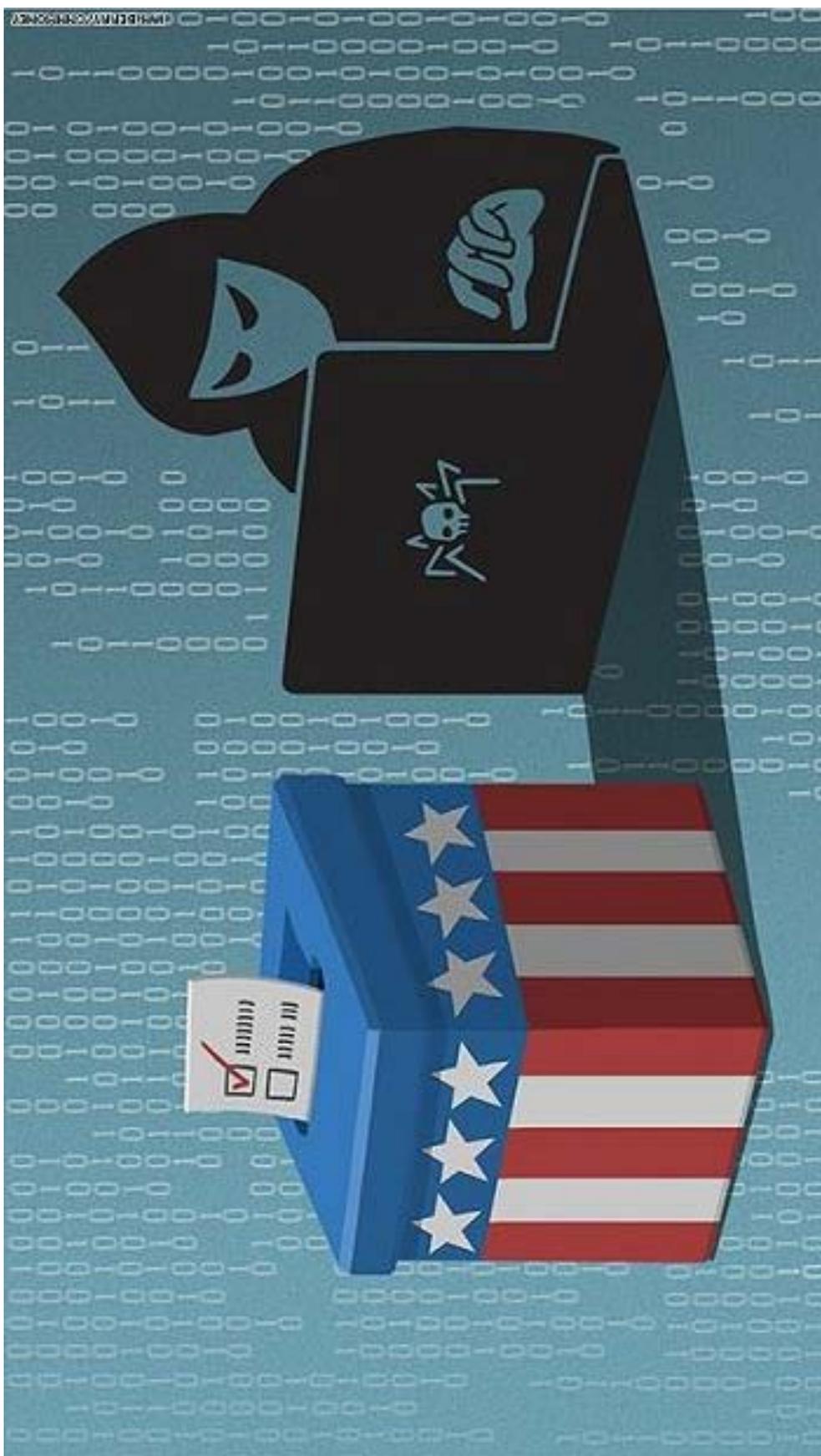
Queste attività - chiamate in gergo **'misure attive'** - sono diventate non solo più attive che mai, ma anche meno controllabili e più difficili da valutare una volta lanciate. La disinformazione, di conseguenza, è diventata ancora più pericolosa

#Propaganda e Disinformazione

La “**guerra attraverso le informazioni**” ha obiettivi variegati, come:

- Creare divisioni tra nazioni alleate
- Manipolare tensioni tra gruppi etnici
- Creare attrito tra individui in un gruppo o in un partito
- Minare la fiducia che gruppi specifici di una comunità hanno nei confronti delle loro istituzioni
- Erodere la legittimità di un governo o la reputazione di un individuo
- Facilitare una specifica decisione politica

Questi obiettivi vengono attuati attraverso operazioni di **propaganda** (che cerca di coinvolgere emotivamente i bersagli) e di **disinformazione** (che cerca invece di manipolare la parte razionale dei bersagli attraverso, ad esempio, informazioni false) attuate oggi giorno principalmente - anche se non esclusivamente - per mezzo di Internet



The image shows a screenshot of a tweet and a video. The tweet is from Hua Chunying (@SpokespersonCHN) and contains the text: "Amid the Chinese anthem playing out in Rome, Italians chanted 'Grazie, Cina!'. In this community with a shared future, we share weal and woe together." Below the tweet is a video titled "Aula Radiofonica Confucio CRI-Uni-Italia" with a timestamp of 14 marzo alle ore 21:38. The video shows a building with a balcony where a Chinese man is playing the Chinese national anthem. The video has 22 likes and 3 shares. The video player interface shows a progress bar at 0:13 and a volume icon.

Hua Chunying 华春莹
@SpokespersonCHN

Amid the Chinese anthem playing out in Rome, Italians chanted "Grazie, Cina!". In this community with a shared future, we share weal and woe together.

Traduci il Tweet

Aula Radiofonica Confucio CRI-Uni-Italia 🎧 cool.
14 marzo alle ore 21:38

A Roma, qualcuno ha suonato l'inno cinese nel balcone per ringraziare gli aiuti cinesi all'Italia. 🇮🇹

5:09 AM · 15 mar 2020 · Tw

Mi piace 22

Commenta 1

Condividi 3



#Cina: propaganda e disinformazione nel 2019

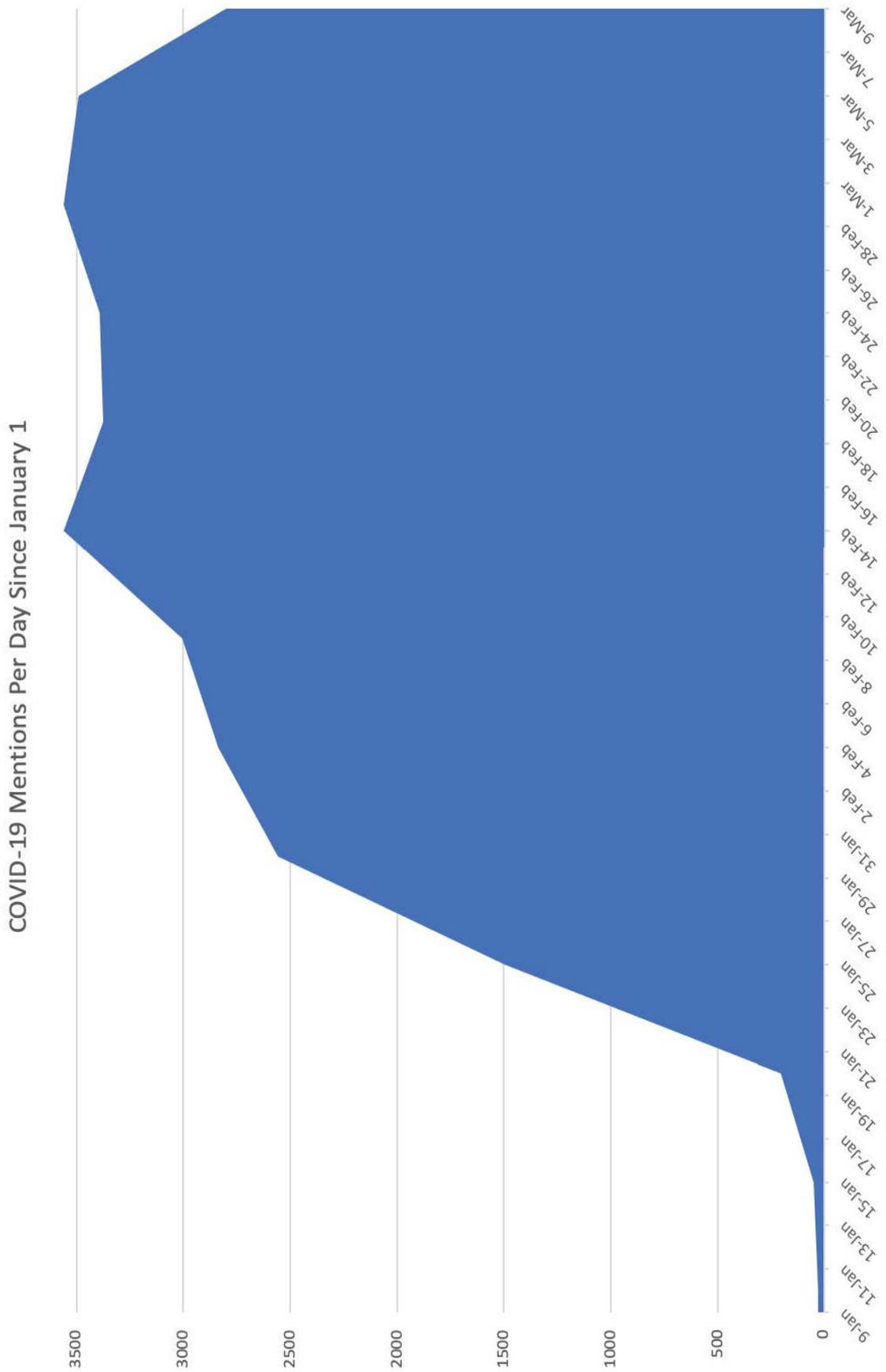
- ▶ Durante il 2019, le operazioni di propaganda e disinformazione del governo cinese all'estero hanno continuato ad avere come **obiettivo la promozione di narrazioni positive della Cina e la neutralizzazione delle critiche al PCC**, in alcuni casi configurando un **assalto diretto alle libertà di stampa e ai valori democratici**
- ▶ La Cina ha sempre di più cercato di garantirsi un'ampia copertura mediatica all'estero **acquistando quote di partecipazione nei media locali**, pubblicando annunci positivi sui giornali e offrendo **viaggi di «formazione» interamente pagati in Cina per giornalisti stranieri**, incorporando esplicitamente tali strategie nella Belt and Road Initiative

#Cina: propaganda e disinformazione nel 2019

- ▶ La Cina, nell'aprile del 2019, ha creato il «**Belt and Road News Network**», ovvero un'associazione composta da **182 media outlet** in 86 Paesi, con l'obiettivo di promuovere una copertura mediatica positiva del progetto
- ▶ Un rapporto del marzo 2019 pubblicato da **Reporters Without Borders** ha concluso che la Cina mira a costruire un «**nuovo ordine mondiale dei media**» in cui «**i giornalisti non sono altro che degli ausiliari della propaganda di Stato**»
- ▶ Secondo quanto riportato da **Reporters Without Borders**, il governo cinese ha investito circa **1,4 miliardi di dollari** (10 miliardi di renminbi) ogni anno nell'ultimo decennio per migliorare la sua presenza sui media internazionali

#Cina: propaganda COVID-19 interna ed esterna

- ▶ **Le origini del COVID-19 non sono chiare e il governo cinese non ne è responsabile**
- ▶ **La Cina ha gestito con successo l'epidemia e il suo metodo di risposta dovrebbe essere il modello per contenere la diffusione del virus in tutti gli altri Paesi. Alcuni sotto-temi di questo messaggio includono: (1) la Cina ha un sistema di **governance migliore**, che le ha permesso di rispondere meglio e più rapidamente dell'Occidente; e (2) ora che l'emergenza in Cina è finita, è il turno della Cina di aiutare il mondo (**la Cina come un buon cittadino globale**)**
- ▶ **L'Occidente utilizza l'emergenza COVID-19 come una scusa e uno strumento per contenere l'ascesa sul piano internazionale della Cina**







#Russia: propaganda e disinformazione

- ▶ Queste tipologie di attività si devono inquadrare nel più ampio approccio strategico di Mosca, teso da sempre a **destabilizzare e seminare incertezza nelle istituzioni dei Paesi considerati nemici** attraverso operazioni di influenza, ingerenza, propaganda, disinformazione e intossicazione informativa
- ▶ La strategia russa, infatti, è principalmente una **strategia di influenza e non di forza**, che mira quindi a minare la coerenza interna dei governi e non a distruggerli completamente

#Russia: propaganda e disinformazione

- ▶ **Obiettivo n. 1: Ripristinare lo stato di grande **potenza** della Russia**
- ▶ **Obiettivo n. 2: Preservare la sfera di **influenza** della Russia**
- ▶ **Obiettivo n. 3: Proteggere il **regime** di Putin**
- ▶ **Obiettivo n. 4: Migliorare l'**efficacia** militare della Russia**

Information Operations Focused on Nine Main Topics



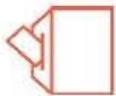
Ukraine as a failed or unreliable state



U.S. and NATO aggression or interference in other countries



European divisions and weakness



Elections



Migration and Islam



Russia's doping scandals in sporting competitions



Turkey as an aggressive, destabilizing force



Defending Russia and its government



Insulting Kremlin critics including Alexei Navalny and the Bellingcat investigative group

DISINFORMATION TARGETS BILL GATES

- X** BILL GATES FOUNDATION **MANUFACTURED** COVID-19 OUTBREAK
- X** COVID-19 VACCINES - BIG PHARMA **FRAUD** LED BY BILL GATES
- X** BILL GATES WILL USE **MICROCHIP IMPLANTS** TO FIGHT COVID-19
- X** BILL GATES & SECRET ELITES ASPIRE TO **REDUCE** THE GLOBAL POPULATION

DISINFORMATION



#UE: impatti delle attività di disinformazione COVID-19

Secondo l'EEAS Strategic Communications and Information Analysis Division, ci sono un numero sempre maggiore di prove dell'effetto delle attività di propaganda e di disinformazione operate da Cina e Russia aventi ad oggetto il COVID-19:

- ▶ Quasi un quarto dei russi (23,2%) considera la pandemia legata al COVID-19 una finzione, inventata da "soggetti interessati". Un ulteriore 9% dei russi pensa che il pericolo della **pandemia sia esagerato**
- ▶ Un terzo delle persone in 6 paesi (Argentina, Germania, Corea del Sud, Spagna, Regno Unito e Stati Uniti) afferma di **aver visto "moltissime" informazioni false o fuorvianti sul COVID-19 su social media** e applicazioni di messaggistica
- ▶ Un terzo dei cittadini del Regno Unito ritiene che la **vodka** possa essere utilizzata come **disinfettante per le mani**

#UE: impatti delle attività di disinformazione COVID-19

[...]

- ▶ **Le teorie cospirazioniste legate al 5G** come facilitatore della diffusione del COVID-19 hanno portato al vandalismo in diverse località nei Paesi Bassi, in Belgio e nel Regno Unito e a bloccare l'installazione di antenne in molti paesi italiani
- ▶ Un numero crescente di persone organizza regolarmente manifestazioni illegali a Berlino per protestare contro il **"terrorismo delle vaccinazioni"** e afferma che il COVID-19 non sia **"nient'altro che una semplice influenza"**
- ▶ La società di sondaggi italiana SWG rileva che la percentuale di intervistati che afferma di **considerare la Cina come un Paese amico dell'Italia** è salita a marzo al 52% dal 10% di gennaio, mentre la percentuale di intervistati che indica di **avere fiducia nelle istituzioni dell'UE** è scesa al 27% a marzo dal 42% di settembre 2019

#In conclusione..

- ▶ Quando le vittime di un'operazione di disinformazione **leggono e reagiscono a documenti segreti falsificati**, la loro reazione è reale
- ▶ Quando si contano i voti di **parlamentari influenzati**, il risultato è reale
- ▶ Quando falsi account sui social media invitano gli utenti inconsapevoli a **partecipare a una manifestazione per strada**, quella manifestazione è reale
- ▶ Quando i cittadini iniziano a usare **epiteti razziali offline o a condividere post estremisti**, i loro punti di vista sono reali

Le operazioni di propaganda e di disinformazione vengono chiamate ‘misure attive’, perché queste operazioni cambiano attivamente e immediatamente opinioni, decisioni e fatti sul terreno, qui, nel presente

La posta in gioco è enorme: la disinformazione corrode le fondamenta della democrazia liberale, la nostra capacità di valutare i fatti in base al merito

Ma quando l’autorità delle prove viene erosa, sono le emozioni a colmare il vuoto

E, allora, distinguere tra fatti e non fatti diventa più difficile, mentre confondere gli amici con i nemici diventa purtroppo sempre più facile



@MeleStefano



info@stefanomele.it

PAGINA BIANCA

PAGINA BIANCA



18STC0110630