https://doi.org/10.6092/issn.1825-1927/20774 ISSN 1825-1927

Il Dominio dell'Informazione nell'Era della Cognitive War*

Fabrizio Corona [1]

[1] Università degli Studi di Brescia, Italia

Abstract: L'articolo esplora l'intersezione tra tecnologia digitale e dinamiche di conflitto, evidenziando come l'era digitale abbia trasformato i tradizionali scenari di guerra in un contesto dominato da cyber warfare e manipolazione dell'informazione. Dopo una definizione introduttiva del problema, si analizza l'impatto della tecnologia digitale sulla sicurezza globale, con un focus sulla crescente rilevanza della guerra cognitiva. L'analisi offre una riflessione sulle strategie di difesa e resilienza, enfatizzando il ruolo delle normative europee nel mitigare i rischi e promuovere un ambiente digitale sicuro. Infine, l'articolo pone lo sguardo alle prospettive future, suggerendo approcci integrati per affrontare le sfide di un mondo sempre più interconnesso.

Parole chiave: Cyber Warfare, Cognitive War, Information, Data Analytics.

1 Introduzione e definizione del problema

Nell'era contemporanea, l'informazione è diventata un'arma potente all'interno di una nuova forma di conflitto conosciuta come guerra cognitiva. Essa si distingue dalle forme tradizionali di conflitto per il suo focus sulla capacità di influenzare le emozioni, i comportamenti e le percezioni delle persone, con l'obiettivo di raggiungere scopi politici e strategici. In tale contesto, l'informazione è una risorsa chiave, capace di modellare opinioni pubbliche, destabilizzare governi e influenzare il comportamento delle masse.

La guerra cognitiva si basa sulla manipolazione di tali informazioni attraverso una serie di tattiche sofisticate, tra cui propaganda, disinformazione e guerra psicologica. Le piattaforme digitali, come i social media e i motori di ricerca, fungono da campo di battaglia virtuale dove si svolgono guerre di influenza e manipolazione delle opinioni. La propaganda mira a diffondere informazioni che supportano una determinata posizione, mentre la disinformazione cerca deliberatamente di ingannare il pubblico con informazioni false o fuorvianti[1].

L'emergere della guerra cognitiva è legato a una serie di sviluppi tecnologici e sociali. La diffusione di internet e dei dispositivi mobili ha permesso la rapida circolazione delle informazioni su scala globale.

La democratizzazione dell'informazione ha portato a benefici significativi, ma ha anche aperto la porta ad una manipolazione delle informazioni senza precedenti.

fabrizio.corona@unina.it (Fabrizio Corona);
(Fabrizio Corona);

*I risultati di questo articolo sono stati presentati al Convegno interuniversitario "L'informazione e il diritto", 29-30-31 maggio 2024, Università Federico II, Orientale, Parthenope, Suor Orsola Benincasa, Napoli. Comitato scientifico: Prof. Francesco Romeo (Uni Federico II Napoli). Prof.ssa Vania Maffeo (Uni Federico II Napoli), Prof.ssa Roberta Montinaro (Università degli Studi L'Orientale di Napoli), Prof. Roberto Carleo (UNI Parthenope); Prof. Agostino De Caro (Uni Molise), Prof. Giuseppe Di Chiara (Uni Palermo), Prof.ssa Lucilla Gatt (Uni Suor Orsola Benincasa), Prof. Mariano Menna (Uni Campania).

1. T. Chen, M. Glick, *China's Information Campaigns: What the United States Can Learn. RAND Corporation,* 2019. Sul Tema vedi anche; A. Klimburg, *The Darkening Web: The War for Cyberspace.* Penguin, 2017; B. Nimmo, S. Bradshaw, *The False Information Ecosystem.* Oxford University, Project on Computational Propaganda, 2019.

La velocità e l'ampiezza della diffusione dell'informazione online hanno reso più difficile distinguere tra verità e falsità, creando un ambiente fertile per la proliferazione della disinformazione e delle teorie del complotto. Inoltre, la frammentazione dei media tradizionali e la crescente importanza dei social media hanno alterato radicalmente il panorama dell'informazione, rendendo difficile per il pubblico accedere a informazioni affidabili e verificate[2].

Un esempio emblematico della potenza della guerra cognitiva è rappresentato dagli attacchi di disinformazione condotti durante la pandemia di COVID-19. La diffusione di notizie false[3] riguardanti trattamenti inefficaci, teorie del complotto sull'origine del virus e informazioni fuorvianti sulle misure di prevenzione ha avuto un impatto significativo sulla salute pubblica e sulla fiducia nelle istituzioni sanitarie. La guerra dell'informazione ha contribuito a polarizzare ulteriormente l'opinione pubblica ed ostacolare gli sforzi per contenere la pandemia, dimostrando come la manipolazione delle informazioni possa avere conseguenze dirette e gravi sulla società.

Questo studio si propone di analizzare il fenomeno della guerra cognitiva, evidenziandone le dinamiche, le implicazioni e le strategie utilizzate per la manipolazione dell'informazione nell'era digitale. L'obiettivo è quello di esaminare come la disinformazione e la propaganda, amplificate dall'uso pervasivo delle piattaforme digitali, possano influenzare le percezioni e i comportamenti collettivi, con conseguenze politiche e sociali di vasta portata giungendo a ciò che oggi possiamo definire con il lemma "guerra cognitiva".

2 L'Impatto della tecnologia digitale e la guerra cognitiva

La tecnologia digitale ha amplificato l'impatto dell'informazione come strumento di guerra, consentendo la manipolazione dei contenuti su vasta scala attraverso l'uso di bot e account falsi, con effetti diretti sul dibattito pubblico. Algoritmi sofisticati determinano il filtraggio selettivo delle informazioni, contribuendo alla polarizzazione delle opinioni e alla creazione di echo chamber digitali.[4]

I social media, in particolare, utilizzano algoritmi progettati per mostrare agli utenti contenuti in linea con i loro interessi e preferenze; questo meccanismo, se da un lato migliora l'esperienza utente, dall'altro può portare alla formazione di bolle informative chiuse, in cui gli individui vengono esposti quasi esclusivamente a contenuti che confermano le loro credenze preesistenti.

Il fenomeno è stato descritto da Eli Pariser con il concetto di *filter bubble,* che evidenzia come la personalizzazione algoritmica possa limitare la diversità delle informazioni a cui si ha accesso, riducendo il confronto con prospettive alternative[5]. I fenomeni rendono più difficile la distinzione tra verità e manipolazione, con implicazioni significative per la formazione dell'opinione pubblica e la tenuta democratica[6].

2. J. Arquilla, D. Ronfeldt, *Cyberwar is Coming!* Comparative Strategy, 12(2), 141-165, 1993. Sul Tema vedi anche: M. Fisher, S. Kelly, J.J. Albright, *Toward a doctrine of collective cyber defense.* The Brookings Institution, 2018; E. Gartzke, J.R. Lindsay, *Weaving tangled webs: Offense, defense, and deception in cyberspace. Security Studies*, 27(2), 235-268, 2018; U. Gori (a Cura di), *Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato*, FrancoAngeli, 2023.

3. Un esempio significativo è stato l'oscuramento del sito "farmacocoronavirus.it", che promuoveva la vendita di un farmaco antivirale al prezzo di oltre 600 euro, presentandolo come efficace contro il COVID-19 senza alcuna evidenza scientifica. L'AGCM ha disposto la sospensione cautelare della commercializzazione del prodotto e l'oscuramento del sito per tutelare i consumatori da informazioni ingannevoli e pratiche speculative. - Provvedimento di sospensione PS11723 (17 marzo 2020). Altro esempio emblematico è stato il Provvedimento di sospensione PS11726 (22 marzo 2020) – AGCM che ha anche affrontato pratiche scorrette nel settore delle donazioni online. Ad esempio, la piattaforma GoFundMe è stata oggetto di un provvedimento per aver preimpostato una percentuale di commissione sulle donazioni, inducendo i consumatori a credere che il servizio fosse gratuito. L'Autorità ha ritenuto tali pratiche ingannevoli e aggressive, poiché sfruttavano la sensibilità dei consumatori durante la pandemia per ottenere commissioni non chiaramente comunicate.

4. E. Dubois, B. Grant, *The Echo Chamber is overstated: The moderating effect of political interest and diverse media. Information, Communication amp*; Society 21:729–745, 2018. Sul tema vedi anche: S. Flaxman, G. Sharad, J. M. Rao, *Filter bubbles, Echo Chambers, and online news consumption.* Public Opinion Quarterly 80:298–320, 2016. R. Fletcher, T. R. Craig, K. N. Rasmus, *How many people live in politically partisan online news echo chambers in different countries?* Journal of Quantitative Description: Digital Media 1, 2021.

5. E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Books Ltd, 2012

6. K. H. Jamieson, J. N. Cappella, *Echo chamber rush limbaugh and the Conservative Media Establishment,* Oxford University Press, 2010. Sul tema vedi anche: E. Peterson, G. Sharad, I. Shanto, *Echo chambers and partisan polarization: Evidence*

I bot e gli account falsi sono strumenti utilizzati per diffondere disinformazione e propaganda; possono essere programmati per pubblicare automaticamente contenuti manipolati, influenzare le tendenze sui social media e amplificare determinate narrative.

Tale attività può avere un impatto significativo sulla percezione pubblica e sul dibattito politico; infatti, la guerra cognitiva offre nuovi mezzi per attaccare le infrastrutture critiche e compromettere la sicurezza nazionale attraverso attacchi informatici mirati e operazioni di disinformazione su larga scala. Tali attacchi possono paralizzare reti elettriche, sistemi di comunicazione e altre infrastrutture essenziali, causando danni economici e sociali significativi[7].

Gli attacchi informatici possono essere utilizzati per rubare informazioni sensibili, distruggere dati o interrompere servizi essenziali; possono essere lanciati da stati nazionali, gruppi terroristici o hacker indipendenti, rendendo difficile attribuire la responsabilità e rispondere in modo efficace.

Le operazioni di disinformazione su larga scala possono includere la diffusione di notizie false, la manipolazione dei media e la creazione di campagne di disinformazione coordinate. Un esempio significativo dell'impatto della tecnologia digitale sulla guerra cognitiva è l'uso di deepfake. I deepfake, riprendendo la definizione introdotta dall'AI ACT, sono: *"immagini o contenuti audio o video generati o manipolati dall'IA che assomiglia a persone oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona"*, possono essere utilizzati per creare contenuti estremamente convincenti che ingannano il pubblico e diffondono disinformazione su larga scala[8]. Un deepfake, ad esempio, potrebbe essere utilizzato per creare un video di un leader politico che fa dichiarazioni controverse, con conseguenze potenzialmente devastanti per la stabilità politica e la fiducia del pubblico.

Altri strumenti potenti nella guerra cognitiva, meritevoli di approfondimenti, sono i big data e l'analisi dei dati. Le organizzazioni possono raccogliere e analizzare enormi quantità di dati sui comportamenti e le preferenze degli individui, utilizzando queste informazioni per creare campagne di disinformazione altamente mirate. Le campagne possono essere progettate per influenzare specifici gruppi di persone, manipolare le elezioni o creare divisioni all'interno della società. Ad esempio, durante le elezioni presidenziali degli Stati Uniti del 2016, è emerso che attori stranieri hanno utilizzato i social media per diffondere disinformazione e influenzare il risultato elettorale.[9]

Un altro esempio di utilizzo della tecnologia nella guerra cognitiva è rappresentato dalla manipolazione degli algoritmi di ricerca. Gli algoritmi che determinano quali informazioni vengono visualizzate per prime nei risultati di ricerca possono essere progettati per promuovere determinate narrative o per sopprimere informazioni sfavorevoli.

Tale forma di manipolazione può influenzare in modo significativo la percezione pubblica e il dibattito politico, in quanto la maggior parte delle persone tende a fidarsi dei risultati del motore di ricerca e a non approfondire oltre le prime pagine[10].

La guerra cognitiva rappresenta una minaccia crescente per la sicurezza nazionale e internazionale. Gli attacchi informatici possono essere utilizzati per compromettere infrastrutture critiche come reti elettriche, sistemi di trasporto e impianti di approvvigionamento idrico, causando danni economici e mettendo a rischio vite umane.

---

from the 2016 presidential campaign. Unpublished manuscript. https://5harad. com/papers/selecfive-exposure. pdf

7. E. Gartzke, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security*, 38(2), 41-73, 2013; T. Rid, *Cyber War Will Not Take Place. Journal of Strategic Studies*, 35(1), 5-32, 2012.

8. I. Kalpokas, J. Kalpokiene, *Deepfakes: A Realistic Assessment of Potentials, Risks, and Policy Regulation.* Cham, Switzerland, Springer, 2022.

9. Il Report On The Investigation Into Russian Interference In The 2016 Presidential Election, pubblicato nel 2019, è il rapporto ufficiale che documenta i risultati e le conclusioni dell'indagine dell'ex consigliere speciale Robert Mueller sugli sforzi russi di interferire nelle elezioni presidenziali degli Stati Uniti del 2016, sulle accuse di cospirazione o coordinamento tra la campagna presidenziale di Donald Trump e la Russia e sulle accuse di ostruzione della giustizia.

10. V. Krebs, *Credibility warfare: Diplomatic, information, and cyber challenges. Journal of Strategic Studies*, 41(1-2), 181-209, 2018; B. Nimmo, S. Bradshaw, *The False Information Ecosystem.* Oxford University, Project on Computational Propaganda, 2019

Gli attacchi informatici possono essere utilizzati per rubare informazioni sensibili, come segreti industriali o dati personali, con gravi implicazioni per la sicurezza e la privacy[11].

Un esempio di attacco informatico particolarmente dannoso è quello che ha colpito la rete elettrica ucraina nel dicembre 2015, attribuito ad hacker russi, che ha provocato un blackout lasciando senza elettricità centinaia di migliaia di persone[12]. L'incidente ha dimostrato come gli attacchi informatici possano avere conseguenze reali e devastanti, mettendo in evidenza la necessità di una maggiore protezione delle infrastrutture critiche contro le minacce cibernetiche.

3 TikTok e la guerra cognitiva

Un esempio evidente di come le piattaforme digitali possano essere utilizzate nella guerra cognitiva è il caso della piattaforma TikTok. TikTok è un social network che consente agli utenti di creare e condividere brevi video. È particolarmente popolare tra le generazioni Y e Z, che lo vedono come una piattaforma per esprimere sé stessi e raggiungere la celebrità digitale. TikTok è stato accusato di essere progettato per inebetire l'utenza e accelerare processi di disfacimento sociale[13].

Gli algoritmi di TikTok promuovono contenuti che possono essere dannosi per la salute mentale, come video che incitano al suicidio o promuovono comportamenti rischiosi. Questo ha portato a un aumento dei disturbi del sonno e della depressione tra gli adolescenti[14].

La versione cinese di TikTok, Douyin, adotta un approccio diverso. Douyin promuove contenuti educativi e moralmente positivi mentre frena o nasconde quelli collegati ad azioni criminali, temi LGBT o semplicemente frivoli; questo dimostra come gli algoritmi possono essere programmati per promuovere determinati valori e comportamenti[15].

TikTok è visto come un'arma psico-digitale innovativa utilizzata per influenzare le percezioni e i comportamenti delle persone. Il caso di Taiwan è particolarmente significativo: è l'unico paese che ha vietato ai propri dipendenti pubblici di scaricare TikTok citando esplicitamente il concetto di guerra cognitiva[16].

L'impatto di TikTok sulla salute mentale dei giovani è stato ampiamente documentato[17]. Studi hanno mostrato che l'uso prolungato della piattaforma può portare a un aumento dei livelli di ansia, depressione e disturbi del sonno. Tale fenomeno è particolarmente preoccupante data la popolarità della piattaforma tra gli adolescenti, un gruppo particolarmente vulnerabile alle influenze esterne.

La stessa piattaforma è stata criticata per la sua mancanza di trasparenza[18] riguardo alla raccolta e all'uso dei dati degli utenti. TikTok raccoglie una vasta gamma di dati personali, che possono essere utilizzati per creare profili dettagliati degli utenti, sollevando gravi preoccupazioni sulla privacy e la sicurezza dei dati[19],

11. M.D. Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Routledge, 2007; G.S. Corn, H.H. Wilson, (Eds.), *Cyber Warfare: A Reference Handbook.* ABC-CLIO, 2014; M. Fisher, S. Kelly, J.J. Albright, *Toward a doctrine of collective cyber defense.* The Brookings Institution, 2018.

12. Russia-Ucraina: è guerra informatica, in ictsecuritymagazine al link: https://www.ictsecuritymagazine.com/articoli/russia-ucraina-e-guerra-informatica/

13. P. Mauri, E. Pietrobon, *Un'arma chiamata TikTok*, «InsideOver», 16 marzo 2023; J. Quinn, New Report Reveals TikTok Parent's Extensive Links to Chinese Military-Surveillance Complex, «National Review», 20 marzo 2023

14. TikTok Statistics – Updated Mar , «Wallaroo», 21 marzo 2023

15. K. Paul, What TikTok does to your mental health: 'It's embarrassing we know so little', «The Guardian» 30 ottobre 2022

16. C. Stokel-Walker. *TikTok Boom: China's Dynamite App and the Superpower Race for Social Media. Kingston upon Thames,* England: Canbury Press, 2021; Sul tema vedi anche: T. Walz, N. Niklas, T. Dobbelstein, *TikTok und Instagram: Erfolgsfaktoren zur Markenführung für Konsumgüter in der Generation Z.* 1st ed. Göttingen: Cuvillier Verlag, Print, 2021.

17. L. McVay, TikTok and Your Child's Brain, «OurPact» 17 ottobre 2022

18. K. Paul, What TikTok does to your mental health: 'It's embarrassing we know so little', «The Guardian» 30 ottobre 2022

19. L. Chung, Is time up for TikTok on Taiwan? Island weighs ban over 'cognitive warfare' fears, «South China Morning Post», 10 dicembre 2022

soprattutto considerando la possibilità che questi possano essere utilizzati per manipolare le percezioni e i comportamenti degli utenti.

4 Il Caso Cambridge Analytica e la manipolazione dell'informazione

Cambridge Analytica è un altro esempio di come i dati raccolti dai social media possano essere utilizzati per influenzare il comportamento delle persone. Fondata nel 2013 da Robert Mercer, Cambridge Analytica è specializzata nell'analisi dei dati psicometrici degli utenti dei social network. La società raccoglieva dati da Facebook e altri social network, analizzando i "mi piace", i commenti e le condivisioni degli utenti per creare profili psicometrici dettagliati.

I profili permettevano a Cambridge Analytica di sviluppare campagne di microtargeting comportamentale personalizzate su misura per influenzare le emozioni e le decisioni degli utenti. Il modello sviluppato da Cambridge Analytica poteva prevedere e anticipare le risposte degli individui, permettendo di veicolare il messaggio più efficace nel momento e nel contesto giusti, impattando significativamente su diverse elezioni e referendum, inclusa la campagna per il referendum sulla Brexit nel Regno Unito.

L'uso dei dati psicometrici solleva importanti questioni etiche e legali, poiché si tratta di una forma di manipolazione altamente[20] sofisticata che può compromettere la democrazia e la privacy degli individui. La capacità di prevedere e influenzare il comportamento degli elettori rappresenta una potente arma politica, in grado di alterare i risultati elettorali e influenzare il corso delle politiche pubbliche[21].

La vicenda di Cambridge Analytica ha anche evidenziato le vulnerabilità delle piattaforme di social media e la necessità di una maggiore regolamentazione per proteggere i dati personali degli utenti. Le rivelazioni sulla raccolta e l'uso dei dati da parte di Cambridge Analytica hanno portato a un'indagine approfondita da parte delle autorità di regolamentazione[22] e hanno sollevato domande sulla responsabilità delle piattaforme di social media nella protezione della privacy degli utenti.

Infine, il caso di Cambridge Analytica ha mostrato come le tecniche di manipolazione dell'informazione possano essere utilizzate per creare divisioni all'interno della società. La campagna per il referendum sulla Brexit, ad esempio, è stata caratterizzata da un alto livello di polarizzazione e conflitto sociale, alimentato in parte dalle campagne di disinformazione e manipolazione psicologica orchestrate da Cambridge Analytica[23].

5 Strategie di difesa, resilienza e normative europee

Il dominio dell'informazione rappresenta una sfida multidimensionale per la sicurezza nazionale che richiede risposte innovative e coordinate da parte delle istituzioni pubbliche. Le strategie di difesa devono integrare la sicurezza informatica con la resilienza sociale, promuovendo la consapevolezza critica e la capacità di discernimento del pubblico.

La sicurezza informatica è fondamentale per proteggere le infrastrutture critiche e i dati dagli attacchi informatici; ciò richiede investimenti in tecnologie avanzate, la formazione di personale specializzato e la cooperazione tra settore pubblico e privato.

La resilienza sociale si riferisce alla capacità della società di resistere e recuperare dagli attacchi di disinformazione e propaganda, richiedendo la promozione dell'alfabetizzazione mediatica e digitale, la trasparenza nell'uso dei dati e la responsabilizzazione delle piattaforme digitali.

La cooperazione internazionale è essenziale per contrastare le minacce transnazionali e promuovere norme globali per la gestione responsabile dell'informazione in ambito digitale. Le istituzioni internazionali devono

20. C. Wylie, *Il mercato del consenso: come ho creato e poi distrutto Cambridge Analytica,* Milano, Longanesi, 2020

21. B. Kaiser, *La dittatura dei dati,* Harper Collins Italia, 2019.

22. N. Tirino, Cambridge Analytica. Il potere segreto, la gestione del consenso e la fine della propaganda, Libellula Edizioni, 2019,

23. S. Zuboff et al., *Surveillance Capitalism: An Interview with Shoshana Zuboff." Surveillance & society.* 17.1/2: 257–266, 2019.

lavorare insieme per sviluppare politiche e strategie comuni che possano affrontare efficacemente le sfide della guerra cognitiva[24].

In questo contesto, la Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi (NIS 2) dell'Unione Europea[25] rappresenta un importante strumento normativo per garantire la sicurezza e la resilienza delle infrastrutture digitali contro le minacce informatiche. La NIS 2 stabilisce requisiti di sicurezza e di notifica degli incidenti per gli operatori di servizi essenziali ed i fornitori di servizi digitali, promuovendo la cooperazione tra Stati membri e il settore privato per mitigare i rischi cibernetici e proteggere l'integrità dell'informazione[26].

La Direttiva NIS 2 è stata sviluppata per migliorare la sicurezza delle reti e dei sistemi informativi nell'UE. Essa impone obblighi di sicurezza agli operatori di servizi essenziali e ai fornitori di servizi digitali, richiedendo loro di adottare misure di sicurezza adeguate e di notificare gli incidenti significativi alle autorità competenti.

Il quadro normativo descritto, rappresenta un passo importante verso la costruzione di un'infrastruttura digitale sicura e resiliente, capace di resistere agli attacchi informatici e proteggere l'integrità dell'informazione.

Il Cybersecurity Act[27] dell'Unione Europea altra normativa rilevante sul tema, mira a rafforzare la cooperazione e la capacità di risposta dell'UE nel campo della sicurezza informatica, istituendo un'Agenzia dell'Unione Europea per la cibersicurezza e un quadro comune per la certificazione dei prodotti e dei servizi digitali, rappresentando un passo importante verso la costruzione di un'infrastruttura digitale sicura e resiliente[28].

Un altro elemento essenziale nella strategia di difesa contro la guerra cognitiva è la promozione dell'alfabetizzazione mediatica e digitale. Le persone devono essere in grado di identificare e valutare criticamente le informazioni che ricevono; questo richiede educazione e formazione continua, non solo nelle scuole ma anche attraverso programmi di educazione degli adulti e campagne di sensibilizzazione pubblica.

La promozione dell'alfabetizzazione mediatica può aiutare le persone a riconoscere le tecniche di manipolazione dell'informazione e sviluppare una maggiore resilienza contro la disinformazione.

La trasparenza nell'uso dei dati e la responsabilizzazione delle piattaforme digitali sono anche componenti essenziali di una strategia di difesa efficace. Le piattaforme digitali devono essere trasparenti riguardo a come raccolgono e utilizzano i dati degli utenti, e devono essere responsabili per il contenuto che ospitano; ciò dovrebbe comportare la possibilità di includere l'implementazione di misure per ridurre la diffusione della disinformazione, come la verifica dei fatti, la rimozione di contenuti falsi o fuorvianti e la promozione di contenuti di qualità e affidabili.

La collaborazione tra governi, settore privato e organizzazioni internazionali è fondamentale per sviluppare strategie efficaci di difesa e resilienza. Le istituzioni devono lavorare insieme per creare un ambiente sicuro e trasparente per l'informazione digitale, implementando regolamentazioni che garantiscano la protezione dei

24. A. Calder, *Cyber Resilience: Defence-In-Depth Principles*, Ely : IT Governance Ltd, 2023; R. Sadeghi, A. Azadegan, O. Divesh, *A Path to Build Supply Chain Cyber-Resilience through Absorptive Capacity and Visibility: Two Empirical Studies.* Industrial marketing management the international journal for industrial and high-tech firms, 111: 202–215, 2023; K. Sūda, B. Balamurugan, S. Grima, *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management.* First edition. Leeds, England: Emerald Publishing Limited, 2023.

25. Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

26. M. Maggiore, *Il commercio elettronico: digital markets act, digital services act e altre dimensioni giuridiche,* Torino, Giappichelli, 2024.

27. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

28. M. Iaselli, G.B. Caria, *Cybersecurity e Cyberwarfare. Diritto, tecnologia e sicurezza,* EPC Editore, 2022. Sul tema vedi anche: B. Ponti, *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in Rivista italiana di informatica e diritto n. 2/2024, 2024; F. Resta, *Cybersicurezza e protezione dati: un rapporto ambivalente,* in Rivista italiana di informatica e diritto n. 2/2024, 2024

dati e la responsabilità delle piattaforme digitali. In futuro, sarà fondamentale monitorare e adattarsi ai cambiamenti nelle tecnologie di informazione e comunicazione.

L'evoluzione costante delle tecniche di manipolazione dell'informazione richiede una vigilanza continua e una capacità di risposta rapida ed efficace. Inoltre, l'adozione di norme internazionali per la gestione responsabile dell'informazione sarà un passo importante per affrontare le sfide globali della guerra cognitiva.

Un esempio di progresso in questa direzione è rappresentato dagli sforzi per regolamentare l'uso dei dati e la trasparenza delle piattaforme digitali. Ad esempio, il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea stabilisce norme rigorose sulla raccolta, l'uso e la protezione dei dati personali.

Tale regolamentazione può aiutare a proteggere gli utenti dalla manipolazione dell'informazione e dalla disinformazione, garantendo al contempo la trasparenza e la responsabilità delle piattaforme digitali; ciò avviene grazie ai principi fondamentali del GDPR (General Data Protection Regulation), che impongono alle piattaforme digitali obblighi stringenti in materia di gestione dei dati personali e sicurezza degli stessi[29].

6 Conclusione e prospettive future

Il dominio dell'informazione rappresenta un fronte fondamentale nella guerra cognitiva del XXI secolo. Il suo impatto sulla sicurezza nazionale e sulla stabilità geopolitica è profondo e pervasivo, richiedendo una risposta strategica e coordinata da parte della comunità internazionale. Solo attraverso la collaborazione e l'innovazione possiamo affrontare le sfide emergenti e proteggere l'integrità dell'informazione come pilastro fondamentale della democrazia e della sicurezza globale.

Per affrontare efficacemente le sfide poste dalla guerra cognitiva, è essenziale sviluppare una comprensione approfondita delle dinamiche della disinformazione e delle tecniche di manipolazione dell'informazione.

Per realizzare ciò, è necessario solo effettuare investimenti in tecnologie di sicurezza avanzate, ma anche promuovere un impegno verso l'alfabetizzazione mediatica e digitale tra il pubblico. La collaborazione tra governi, settore privato e organizzazioni internazionali è essenziale per sviluppare strategie efficaci di difesa e resilienza. Le istituzioni devono lavorare insieme per creare un ambiente sicuro e trasparente per l'informazione digitale, implementando regolamentazioni che garantiscano la protezione dei dati e la responsabilità delle piattaforme digitali[30].

In futuro, sarà fondamentale monitorare e adattarsi ai cambiamenti nelle tecnologie di informazione e comunicazione. L'evoluzione costante delle tecniche di manipolazione dell'informazione richiede una vigilanza continua e una capacità di risposta rapida ed efficace. Inoltre, l'adozione di norme internazionali per la gestione responsabile dell'informazione sarà un passo importante per affrontare le sfide globali della guerra cognitiva.

La protezione del dominio dell'informazione è una componente essenziale della sicurezza nazionale e internazionale nel XXI secolo. Solo attraverso una cooperazione globale, l'innovazione tecnologica e l'alfabetizzazione mediatica possiamo sperare di affrontare efficacemente le minacce della guerra cognitiva e proteggere l'integrità dell'informazione come pilastro della democrazia e della sicurezza globale.

Infine, è importante riconoscere che la guerra cognitiva non è solo una questione di tecnologia e sicurezza informatica, ma anche di etica e valori. La difesa contro la manipolazione dell'informazione richiede un impegno a promuovere la verità, l'integrità e la trasparenza. Questo significa non solo combattere la disinformazione,

29. S. Slokenberga, *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe. Ed. by Santa. Slokenberga, Olga. Tzortzatou, and Jane. Reichel.* 1st ed. 2021. Cham: Springer Nature. Sul tema vedere anche: G. Cassano, G. Cerrina Feroni, M. Barbarossa, *Il processo di adeguamento al GDPR. Seconda edizione.* Milano: Giuffrè Francis Lefebvre, 2022; K. Mariusz, *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union,* Alphen aan den Rijn: Wolters Kluwer, 2018

30. E. Gartzke, J. R. Lindsay, *Weaving tangled webs: Offense, defense, and deception in cyberspace,* Security Studies, 27(2), 235-268, 2018; U. Gori (a Cura di), *Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato,* FrancoAngeli, 2023; B. Nimmo, S. Bradshaw, *The False Information Ecosystem.* Oxford University, Project on Computational Propaganda, 2019; V. Krebs, *Credibility warfare: Diplomatic, information, and cyber challenges,* Journal of Strategic Studies, 41(1-2), 181-209, 2018.

ma anche promuovere un'informazione di qualità, sostenere il giornalismo indipendente e proteggere la libertà di espressione. Solo attraverso un impegno collettivo per questi valori fondamentali possiamo sperare di costruire una società resiliente e informata, capace di affrontare le sfide della guerra cognitiva e proteggere la democrazia nel XXI secolo[31].

Pertanto, il dominio dell'informazione è un fronte complesso e vitale nella guerra cognitiva moderna. La sua importanza non può essere sottovalutata, poiché la capacità di controllare e manipolare l'informazione ha implicazioni profonde per la sicurezza nazionale, la stabilità geopolitica e il funzionamento delle democrazie. Affrontare questa sfida richiede un approccio olistico che integri tecnologie avanzate, alfabetizzazione mediatica, trasparenza e responsabilità, nonché una cooperazione internazionale rafforzata. Solo attraverso un impegno coordinato e sostenuto possiamo sperare di proteggere l'integrità dell'informazione e costruire un futuro sicuro e stabile per le generazioni a venire.

Riferimenti Bibliografici

Arquilla J., Ronfeldt D., *Cyberwar is Coming!* Comparative Strategy, 12(2), 141-165, 1993.

Calder A., *Cyber Resilience: Defence-In-Depth Principles*, Ely : IT Governance Ltd, 2023;

Cassano G., Cerrina Feroni G., Barbarossa M., *Il processo di adeguamento al GDPR. Seconda edizione.* Milano: Giuffrè Francis Lefebvre, 2022;

Cavelty M.D., *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Routledge, 2007;

Chen T., Glick M., *China's Information Campaigns: What the United States Can Learn. RAND Corporation,* 2019.

Chung L., Is time up for TikTok on Taiwan? Island weighs ban over 'cognitive warfare' fears, «South China Morning Post», 10 dicembre 2022;

Corn G.S., Wilson H.H., (Eds.), *Cyber Warfare: A Reference Handbook.* ABC-CLIO, 2014;

Dubois E., Grant B., *The Echo Chamber is overstated: The moderating effect of political interest and diverse media. Information, Communication amp*; Society 21:729–745, 2018.

Fisher M., Kelly S., Albright J.J., *Toward a doctrine of collective cyber defense.* The Brookings Institution, 2018;

Flaxman S., Sharad G., Rao J. M., *Filter bubbles, Echo Chambers, and online news consumption.* Public Opinion Quarterly 80:298–320, 2016.

Fletcher R., Craig T. R., Rasmus K. N., *How many people live in politically partisan online news echo chambers in different countries?* Journal of Quantitative Description: Digital Media 1, 2021.

Gartzke E., Lindsay J. R., *Weaving tangled webs: Offense, defense, and deception in cyberspace,* Security Studies, 27(2), 235-268, 2018;

Gartzke E., *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security*, 38(2), 41-73, 2013; T. Rid, *Cyber War Will Not Take Place. Journal of Strategic Studies*, 35(1), 5-32, 2012.

Gori U. (a Cura di), *Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato*, FrancoAngeli, 2023.

Iaselli M., Caria G.B., *Cybersecurity e Cyberwarfare. Diritto, tecnologia e sicurezza,* EPC Editore, 2022.

Jamieson K. H., Cappella J. N., *Echo chamber rush limbaugh and the Conservative Media Establishment,* Oxford University Press, 2010.

31. V. Krebs, *Credibility warfare: Diplomatic, information, and cyber challenges,* Journal of Strategic Studies, 41(1-2), 181-209, 2018; J. Arquilla, D. Ronfeldt, *Cyberwar is Coming!* Comparative Strategy, 12(2), 141-165, 1993. Sul Tema vedi anche: M. Fisher, S. Kelly, J.J. Albright, *Toward a doctrine of collective cyber defense,* The Brookings Institution, 2018.

Kaiser B., *La dittatura dei dati,* Harper Collins Italia, 2019.

Kalpokas I., Kalpokiene J., *Deepfakes: A Realistic Assessment of Potentials, Risks, and Policy Regulation.* Cham, Switzerland, Springer, 2022.

Klimburg A., *The Darkening Web: The War for Cyberspace.* Penguin, 2017;

Krebs V., *Credibility warfare: Diplomatic, information, and cyber challenges. Journal of Strategic Studies*, 41(1-2), 181-209, 2018;

Maggiore M., *Il commercio elettronico: digital markets act, digital services act e altre dimensioni giuridiche,* Torino, Giappichelli, 2024;

Mariusz K., *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union,* Alphen aan den Rijn: Wolters Kluwer, 2018

Mauri P., Pietrobon E., *Un'arma chiamata TikTok*, «InsideOver», 16 marzo 2023;

McVay L., TikTok and Your Child's Brain, «OurPact» 17 ottobre 2022;

Nimmo B., Bradshaw S., *The False Information Ecosystem.* Oxford University, Project on Computational Propaganda, 2019.

Nimmo B., Bradshaw S., *The False Information Ecosystem.* Oxford University, Project on Computational Propaganda, 2019;

Pariser E., *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Books Ltd, 2012

Paul K., What TikTok does to your mental health: 'It's embarrassing we know so little', «The Guardian» 30 ottobre 2022;

Peterson E., Sharad G., Shanto I., *Echo chambers and partisan polarization: Evidence from the 2016 presidential campaign.* Unpublished manuscript. https://5harad. com/papers/selecfive-exposure. pdf

Ponti B., *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in Rivista italiana di informatica e diritto n. 2/2024, 2024;

Quinn J., New Report Reveals TikTok Parent's Extensive Links to Chinese Military-Surveillance Complex, «National Review», 20 marzo 2023

Resta F., *Cybersicurezza e protezione dati: un rapporto ambivalente,* in Rivista italiana di informatica e diritto n. 2/2024, 2024;

Sadeghi K., Azadegan A., Divesh O., *A Path to Build Supply Chain Cyber-Resilience through Absorptive Capacity and Visibility: Two Empirical Studies.* Industrial marketing management the international journal for industrial and high-tech firms, 111: 202–215, 2023;

Slokenberga S., *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe. Ed. by Santa. Slokenberga, Olga. Tzortzatou, and Jane. Reichel.* 1st ed. 2021. Cham: Springer Nature.

Stokel-Walker C.. *TikTok Boom: China's Dynamite App and the Superpower Race for Social Media. Kingston upon Thames,* England: Canbury Press, 2021;

Sūda K., Balamurugan B., Grima S., *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management.* First edition. Leeds, England: Emerald Publishing Limited, 2023;

Tirino N., Cambridge Analytica. Il potere segreto, la gestione del consenso e la fine della propaganda, Libellula Edizioni, 2019;

Walz T., Niklas N., Dobbelstein T., *TikTok und Instagram: Erfolgsfaktoren zur Markenführung für Konsumgüter in der Generation Z.* 1st ed. Göttingen: Cuvillier Verlag, Print, 2021;

Wylie C., *Il mercato del consenso: come ho creato e poi distrutto Cambridge Analytica,* Milano, Longanesi, 2020

Zuboff S. et al., *Surveillance Capitalism: An Interview with Shoshana Zuboff." Surveillance & society.* 17.1/2: 257–266, 2019;