Parlamento europeo
2019-2024

Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione

2020/2268(INI)

18.10.2021

PROGETTO DI RELAZIONE

sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione
(2020/2268(INI))

Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione

Relatrice: Sandra Kalniete

INDICE

Pagina

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO

sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione
(2020/2268(INI))

Il Parlamento europeo,

– vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 7, 8, 11, 12, 39, 40, 47 e 52,

– visti la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, in particolare gli articoli 8, 9, 10, 11, 13, 16 e 17, e il protocollo addizionale della suddetta Convenzione, in particolare l'articolo 3,

– viste le comunicazioni congiunte della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 5 dicembre 2018, dal titolo "Piano d'azione contro la disinformazione" (JOIN(2018)0036) e del 14 giugno 2019 dal titolo "Relazione sull'attuazione del piano d'azione contro la disinformazione" (JOIN(2019)0012),

– visto il piano d'azione per la democrazia europea (COM(2020)0790),

– visto il pacchetto relativo alla legge sui servizi digitali,

– visti il codice di buone pratiche sulla disinformazione del 2018 e gli orientamenti sul rafforzamento del codice di buone pratiche sulla disinformazione del 2021 (COM(2021)0262),

– vista la relazione speciale n. 09/2021 della Corte dei conti europea dal titolo "La disinformazione nell'UE: combattuta ma non vinta",

– visti la proposta della Commissione del 16 dicembre 2020 di direttiva del Parlamento europeo e del Consiglio sulla resilienza dei soggetti critici (COM(2020)0829) e il proposto allegato alla suddetta direttiva,

– visti il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione[1] e gli orientamenti relativi al regolamento sul controllo degli investimenti esteri diretti del marzo 2020 (C(2020)1981),

– vista la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 16 dicembre 2020, sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale (JOIN(2020)0018),

– vista la proposta di direttiva del Parlamento europeo e del Consiglio, presentata dalla Commissione il 16 dicembre 2020, relativa a misure per un livello comune elevato di

[1] GU L 79 I del 21.3.2019, pag. 1.

cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020)0823),

– visto il pacchetto di strumenti dell'UE comprendente misure di attenuazione dei rischi per la cibersicurezza delle reti 5G del marzo 2021,

– visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013[2],

– vista la sua decisione del 18 giugno 2020 sulla costituzione, le attribuzioni, la composizione numerica e la durata del mandato della commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione[3], adottata a norma dell'articolo 207 del suo regolamento,

– visto l'articolo 54 del suo regolamento,

– vista la relazione della commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione (A9-0000/2021),

A. considerando che le ingerenze straniere costituiscono una grave violazione dei valori e principi universali su cui si fonda l'Unione, quali la dignità umana, la libertà, l'uguaglianza, la solidarietà, il rispetto dei diritti umani e delle libertà fondamentali, la democrazia e lo Stato di diritto;

B. considerando che le ingerenze straniere, la manipolazione delle informazioni e la disinformazione rappresentano una violazione delle libertà fondamentali di espressione e informazione sancite dall'articolo 11 della Carta dei diritti fondamentali dell'Unione europea e costituiscono una minaccia per dette libertà nonché per i processi democratici nell'UE e negli Stati membri, quali l'indizione di elezioni libere e regolari;

C. considerando che qualunque azione contro le ingerenze straniere e la manipolazione delle informazioni deve a sua volta rispettare le libertà fondamentali di espressione e informazione;

D. considerando che esistono prove a conferma del fatto che soggetti stranieri malintenzionati ricorrono alla manipolazione delle informazioni e ad altre tattiche di ingerenza per interferire nei processi democratici dell'UE; che tali attacchi sono fuorvianti e ingannano i cittadini, inaspriscono la polarizzazione e dividono la società, aggravano le condizioni dei gruppi vulnerabili, alterano l'integrità delle elezioni democratiche e dei referendum e seminano sfiducia nei confronti delle autorità pubbliche e della democrazia;

E. considerando che le tattiche di ingerenza straniera assumono la forma di disinformazione e soppressione delle informazioni, nonché di manipolazione delle piattaforme dei social media e dei sistemi pubblicitari, di attacchi informatici, operazioni di "hack-and-leak", minacce e molestie nei confronti di giornalisti, ricercatori, politici e membri delle organizzazioni della società civile, donazioni e

[2] GU L 151 del 7.6.2019, pag. 15.
[3] Testi approvati, P9_TA(2020)0161.

prestiti occulti a partiti politici, campagne, organizzazioni e organi d'informazione, organi d'informazione e organizzazioni falsi o mandatari, elite capture e cooptazione, false persone, pressioni all'autocensura, sfruttamento manipolatorio di narrazioni storiche, religiose e culturali, pressioni nei confronti degli istituti di istruzione e culturali, controllo delle infrastrutture critiche, pressioni nei confronti di cittadini stranieri residenti nell'UE e spionaggio;

F. considerando che le ingerenze straniere rappresentano un modello di comportamento che minaccia i valori, le procedure e i processi politici o può incidere negativamente su di essi; che tali ingerenze hanno carattere manipolatorio e sono attuate in modo intenzionale e coordinato; che i responsabili di tali ingerenze, compresi i loro mandatari all'interno e all'esterno del loro territorio, possono essere attori statali o non statali; che l'utilizzo di mandatari nazionali da parte di attori stranieri e la cooperazione con alleati nazionali rende difficilmente distinguibile il confine tra ingerenza straniera e interna;

G. considerando che è necessario trovare un accordo tra partner che condividono i medesimi princìpi su definizioni comuni delle ingerenze straniere al fine di introdurre norme e criteri validi a livello internazionale;

Necessità di una strategia coordinata dell'UE contro le ingerenze straniere

H. considerando che i tentativi di ingerenza straniera sono sempre più numerosi e sofisticati;

I. considerando che l'UE e gli Stati membri hanno il dovere di difendere tutti i cittadini dai tentativi di ingerenza straniera; che, tuttavia, l'UE e gli Stati membri non sembrano avere strumenti appropriati e sufficienti per prevenire, individuare e respingere al meglio tali minacce;

J. considerando che tra molti esponenti politici e tra i cittadini in generale c'è una scarsa consapevolezza in merito alla realtà di tali problematiche, il che potrebbe involontariamente contribuire a creare ulteriori vulnerabilità;

K. considerando che il monitoraggio delle ingerenze straniere in tempo reale da parte degli organi istituzionali e di verificatori di fatti indipendenti è fondamentale affinché possano essere adottate le misure appropriate, non soltanto per fornire informazioni in merito ad attacchi malevoli in corso ma anche per contrastarli;

L. considerando che la resilienza dei cittadini dell'Unione nei confronti delle ingerenze straniere e della manipolazione delle informazioni richiede un approccio a lungo termine che coinvolga la società nel suo insieme;

M. considerando che per individuare le vulnerabilità, identificare gli attacchi e porvi rimedio sono necessari la cooperazione e il coordinamento tra i diversi livelli e settori amministrativi;

Rafforzare la resilienza dell'UE attraverso la consapevolezza della situazione, l'alfabetizzazione mediatica e l'istruzione

N. considerando che la consapevolezza della situazione rappresenta il primo passo per contrastare la manipolazione delle informazioni e le ingerenze;

O. considerando che organi d'informazione di elevata qualità, finanziati in modo sostenibile e indipendenti e il giornalismo professionale sono fondamentali per la libertà e il pluralismo dei media e per lo Stato di diritto e rappresentano pertanto un pilastro della democrazia; che i mezzi di comunicazione professionali e il giornalismo tradizionale, in quanto fonti d'informazione di qualità, stanno affrontando difficoltà nell'era digitale; che, nonostante tutti i progressi compiuti nel sensibilizzare in merito alla situazione, molte persone, compresi i responsabili politici e i dipendenti pubblici che lavorano in ambiti potenzialmente oggetto di attacchi, sono ancora inconsapevoli dei rischi associati alle ingerenze straniere e non sanno come evitarli;

P. considerando che i diversi portatori di interessi e le diverse istituzioni utilizzano metodologie e definizioni differenti per analizzare le ingerenze straniere, tutte caratterizzate da vari livelli di comprensibilità, e che tali differenze possono impedire un monitoraggio, un'analisi e una valutazione del livello di minaccia comparabili, rendendo più difficile un'azione congiunta;

Q. considerando che è necessario integrare la terminologia riguardante i contenuti, come le notizie false e la disinformazione, con termini incentrati sul comportamento, in modo da descrivere adeguatamente il problema;

R. considerando che l'alfabetizzazione mediatica e digitale e la sensibilizzazione sono strumenti importanti per rafforzare la resilienza dei cittadini ai tentativi di ingerenza nel settore dell'informazione;

S. considerando che la manipolazione delle informazioni può assumere varie forme, quali la diffusione della disinformazione, la distorsione dei fatti e delle rappresentazioni delle opinioni, la soppressione di talune informazioni o opinioni, l'estrapolazione delle informazioni dal contesto, il sostegno a talune opinioni a danno di altre e le molestie ai danni delle persone per metterle a tacere;

T. considerando che ogni fascia della società e ogni persona possono offrire un importante contributo per contrastare la diffusione della disinformazione e mettere in guardia le persone a rischio nel proprio ambiente;

U. considerando che è importante avere facile accesso a informazioni fondate su fatti concreti nel momento in cui la disinformazione inizia a diffondersi;

V. considerando che è necessario individuare rapidamente i tentativi di manipolare la sfera dell'informazione per potervi rispondere;

W. considerando che la disinformazione trova terreno fertile nei dibattiti caratterizzati da polarizzazione ed emotività, poiché sfrutta le debolezze e i pregiudizi delle persone e all'interno della società e che la disinformazione distorce il dibattito pubblico riguardante le elezioni e altri processi democratici, il che rende difficile ai cittadini prendere decisioni informate;

X. considerando che le piattaforme online possono rappresentare strumenti economici e di facile utilizzo per i soggetti dediti alla manipolazione delle informazioni e ad altri tipi di ingerenza, come l'odio e le molestie, la riduzione al silenzio degli oppositori, lo spionaggio o la diffusione della disinformazione;

Ingerenze straniere per mezzo delle piattaforme online

Y. considerando che abbiamo assistito a continue ingerenze e a campagne di manipolazione delle informazioni riguardanti tutte le misure adottate per contenere la diffusione della COVID-19, comprese le vaccinazioni nell'UE, e che le piattaforme online hanno ottenuto scarsi risultati nel contrastarle;

Z. considerando che le piattaforme online controllano il flusso di informazioni e la pubblicità online, che esse elaborano e utilizzano algoritmi per controllare tali flussi e che non condividono o condividono in minima parte le informazioni riguardanti l'elaborazione, l'utilizzo e l'impatto di detti algoritmi;

AA. considerando che numerosi fornitori aventi sede nell'UE vendono like, commenti e condivisioni falsi a qualunque soggetto desideroso di aumentare artificiosamente la propria visibilità online; che è quasi impossibile individuare gli usi legittimi di tali servizi, a fronte di utilizzi dannosi comprendenti la manipolazione delle elezioni, la promozione delle truffe, le recensioni negative dei prodotti della concorrenza e le truffe ai danni degli inserzionisti;

AB. considerando che le piattaforme sociali, i dispositivi e le applicazioni digitali raccolgono e conservano moli immense di dati personali molto dettagliati e spesso sensibili di ciascun utente; che tali dati sono venduti sul mercato dei dati; che si verificano ripetutamente fughe di dati; che tali banche dati potrebbero essere miniere d'oro per gli attori malintenzionati che desiderano colpire persone o gruppi specifici;

AC. considerando che la scelta di non condividere i dati è generalmente complicata e dispendiosa in termini di tempo rispetto alla scelta di condividerli;

AD. considerando che le piattaforme online sono parte integrante della maggior parte delle nostre vite e possono avere un impatto enorme sul nostro modo di pensare e di agire, ad esempio quando si tratta di preferenze o comportamenti di voto;

AE. considerando che i meccanismi di gestione algoritmica, studiati per massimizzare il coinvolgimento, sono ripetutamente segnalati come promotori di contenuti polarizzanti e radicalizzanti;

AF. considerando che la diffusione di materiali audiovisivi falsi (deepfake) può diventare un problema sempre più grave;

AG. considerando che i sistemi di autoregolamentazione, come il codice di buone pratiche sulla disinformazione del 2018, hanno portato a miglioramenti ma consentono alle piattaforme di fare poco o nulla per impedire le ingerenze nei propri sistemi;

AH. considerando che le attuali sanzioni per quanti utilizzano le piattaforme a scopi illeciti non sono sufficientemente severe da avere un effetto deterrente;

AI. considerando che le piattaforme dedicano molte meno risorse ai contenuti nelle lingue meno parlate e persino nelle lingue di ampia diffusione diverse dall'inglese rispetto ai contenuti in lingua inglese;

AJ. considerando che le organizzazioni o i soggetti interessati non possono ricorrere contro

le azioni o l'inazione delle piattaforme;

AK. considerando che negli ultimi mesi diversi importanti attori si sono piegati alla censura, ad esempio in occasione delle elezioni parlamentari russe del settembre 2021, quando Google e Apple hanno rimosso l'applicazione di voto intelligente "Smart Voting" dai propri store in Russia;

AL. considerando che la mancanza di trasparenza in relazione alle scelte algoritmiche delle piattaforme rende quasi impossibile confermare le loro dichiarazioni in merito alle azioni intraprese per contrastare la manipolazione delle informazioni e le ingerenze;

AM. considerando che una notevole mole di pubblicità online di marchi noti finisce su siti web che ospitano discorsi di incitamento all'odio e disinformazione, senza che gli inserzionisti ne siano a conoscenza o diano l'autorizzazione;

Infrastrutture critiche e settori strategici

AN. considerando che la gestione delle minacce alle infrastrutture critiche, soprattutto se parte di una strategia ibrida malevola e sincronizzata, richiede interventi congiunti e coordinati tra i diversi settori, a livelli differenti (UE, nazionale, regionale e locale) e in momenti diversi;

AO. considerando che la Commissione ha proposto una nuova direttiva per rafforzare la resilienza dei soggetti critici che forniscono servizi essenziali nell'UE, che include un elenco di nuovi tipi di infrastrutture critiche; che l'elenco dei servizi sarà definito nell'allegato alla direttiva;

AP. considerando che la crescente globalizzazione della divisione del lavoro e delle catene di produzione si è tradotta in carenze in termini di capacità produttiva e di competenze in settori di fondamentale importanza nell'Unione; che di conseguenza l'UE è fortemente dipendente dalle importazioni per molti prodotti essenziali e beni primari provenienti dall'estero;

AQ. considerando che gli investimenti esteri diretti, ossia gli investimenti provenienti da paesi terzi, nei settori strategici dell'UE sono stati motivo di crescente preoccupazione negli ultimi anni;

Finanziamento occulto di attività politiche da parte di donatori stranieri

AR. considerando che solidi elementi di prova dimostrano che soggetti stranieri hanno interferito attivamente con il funzionamento democratico dell'UE e degli Stati membri, in particolare durante i periodi elettorali e referendari, attraverso operazioni di finanziamento occulto;

AS. considerando che, a titolo esemplificativo, Russia, Cina e altri regimi autoritari hanno distribuito più di 300 milioni di dollari in 33 paesi per interferire con i processi democratici e che tale tendenza sta chiaramente accelerando; che metà dei casi riguarda interventi russi in Europa;

AT. considerando che tali operazioni sono volte a finanziare i partiti politici o movimenti europei con l'intenzione di aggravare la frammentazione sociale e minare la legittimità

delle autorità pubbliche europee e nazionali;

AU. considerando che le leggi elettorali, in particolare le disposizioni sul finanziamento delle attività politiche, non sono armonizzate a livello dell'UE e che di conseguenza danno adito a metodi di finanziamento opachi da parte di attori stranieri, attraverso diverse norme e pratiche che generano numerose scappatoie e pratiche legali o illegali all'interno dell'UE;

AV. considerando che la pubblicità politica online non è soggetta alle norme della pubblicità politica offline;

AW. considerando che il regolamento (UE, Euratom) n. 1141/2014, del 22 ottobre 2014, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee[4] è in fase di revisione allo scopo di garantire un livello maggiore di trasparenza in relazione al finanziamento delle attività politiche;

Cibersicurezza e resilienza contro gli attacchi informatici

AX. considerando che l'incidenza degli attacchi informatici è aumentata negli ultimi anni; che diversi attacchi informatici, come le campagne di e-mail spear phishing indirizzate contro le strutture strategiche di conservazione dei vaccini e gli attacchi informatici contro l'Agenzia europea per i medicinali (EMA) e il parlamento norvegese, sono stati ricondotti a gruppi di hacker sostenuti dallo Stato, principalmente affiliati ai governi russo e cinese;

AY. considerando che attualmente la capacità di fronteggiare le minacce informatiche è limitata a causa della scarsità di risorse umane e finanziarie;

AZ. considerando che le capacità e le strategie frammentate dell'Unione nel settore informatico stanno diventando un problema sempre più grave;

BA. considerando che attori statali stranieri hanno utilizzato programmi di sorveglianza illegali e su vasta scala per controllare giornalisti, attivisti per i diritti umani ed esponenti politici, compresi i capi di Stato europei;

Protezione delle istituzioni europee

BB. considerando che il carattere decentralizzato e multinazionale delle istituzioni dell'UE può essere sfruttato da soggetti stranieri malevoli per seminare discordia nell'UE;

BC. considerando che è necessario porre in atto procedure appropriate per la gestione delle crisi prima che queste si manifestino;

BD. considerando che diverse istituzioni dell'UE sono state di recente oggetto di attacchi informatici, il che dimostra la necessità di promuovere una forte cooperazione interistituzionale per la rilevazione, il monitoraggio e la condivisione delle informazioni durante gli attacchi informatici e/o per prevenirli;

Ingerenze attraverso l'elite capture, le diaspore nazionali e le università

[4] GU L 317 del 4.11.2014, pag. 1.

BE. considerando che diversi ex politici e dipendenti pubblici europei di alto livello sono assunti o cooptati da imprese straniere controllate dagli Stati che perpetrano ingerenze dolose nell'UE, in cambio delle loro conoscenze a discapito degli interessi dell'UE e degli Stati membri;

BF. considerando che due paesi sono particolarmente attivi nel campo dell'elite capture e della cooptazione, ossia Russia e Cina; che, a titolo esemplificativo, l'ex cancelliere tedesco Gerhard Schröder e l'ex primo ministro finlandese Paavo Lipponen hanno lavorato entrambi per la Gazprom per accelerare il processo di candidatura del Nord Stream 1 e 2, l'ex ministra austriaca degli Affari esteri Karin Kneissl è stata nominata membro del consiglio di amministrazione di Rosneft, l'ex primo ministro francese François Fillon è stato nominato membro del consiglio di amministrazione di Zaroubejneft, l'ex primo ministro francese Jean-Pierre Raffarin è impegnato attivamente nella promozione degli interessi cinesi in Francia e l'ex commissario ceco Štefan Füle ha lavorato per la CEFC China Energy;

BG. considerando che alle strategie di lobbying economica si possono accompagnare obiettivi di ingerenza straniera;

BH. considerando che il controllo delle diaspore nazionali residenti nel territorio dell'UE rappresenta un importante elemento delle strategie di ingerenza straniera;

BI. considerando che diversi attori statali, come il governo russo e il partito comunista cinese, cercano di aumentare la propria influenza per mezzo di istituzioni culturali, d'istruzione (ad esempio mediante sovvenzioni e borse di studio) e religiose;

BJ. considerando che vi sono prove dell'ingerenza russa e della manipolazione delle informazioni online ai danni di numerose democrazie liberali in tutto il mondo, fra l'altro in occasione del referendum sulla Brexit nel Regno Unito e delle elezioni presidenziali in Francia e negli Stati Uniti, nonché del sostegno pratico a forze e attori di estrema destra e radicali in tutta Europa, come in Francia, Germania, Italia e Austria, per citare soltanto alcuni esempi; che le recenti scoperte riguardanti contatti stretti e regolari tra funzionari russi e i rappresentanti di un gruppo di secessionisti catalani in Spagna richiedono un'indagine approfondita, visti i continui tentativi da parte della Russia di sfruttare qualunque occasione per favorire la destabilizzazione interna e le divisioni nell'UE;

BK. considerando che sono stati aperti oltre 500 centri Confucio nel mondo, di cui circa 200 in Europa, e che gli Istituti Confucio e le Classi Confucio sono utilizzati dalla Cina come strumento di ingerenza nell'UE;

Deterrenza e sanzioni collettive

BL. considerando che l'UE e gli Stati membri non dispongono attualmente di un regime specifico di sanzioni relative alle ingerenze straniere e alle campagne di disinformazione orchestrate da attori statali stranieri, il che significa che detti attori possono supporre con una certa sicurezza che non subiranno conseguenze per le loro campagne di destabilizzazione nei confronti dell'UE;

BM. considerando che l'UE dovrebbe rafforzare i propri strumenti di deterrenza in modo che gli attori malevoli stranieri paghino per le loro decisioni e ne subiscano le conseguenze;

Cooperazione mondiale e multilateralismo

BN. considerando che le azioni malevole orchestrate da regimi autoritari stranieri colpiscono numerosi paesi democratici in tutto il mondo;

BO. considerando che fra i partner che condividono gli stessi princìpi non esistono ancora una comprensione comune e definizioni comuni per quanto riguarda la natura delle minacce in questione;

BP. considerando che è necessaria una cooperazione a livello mondiale tra partner che condividono gli stessi princìpi per far fronte alle ingerenze straniere malevole;

Necessità di una strategia coordinata dell'UE contro le ingerenze straniere

1. esprime grave preoccupazione per la crescente incidenza e la natura sempre più sofisticata dei tentativi di ingerenza straniera e manipolazione delle informazioni rivolti a tutti gli aspetti del funzionamento democratico dell'Unione europea e degli Stati membri;

2. invita la Commissione a proporre, e i colegislatori e gli Stati membri a sostenere, una strategia multilivello e intersettoriale e a stanziare risorse finanziarie adeguate, al fine di dotare l'UE e gli Stati membri di politiche di resilienza e strumenti di deterrenza adeguati, che consentano loro di far fronte a tutte le minacce ibride e agli attacchi orchestrati da paesi stranieri; ritiene che detta strategia debba fondarsi su: 1 – definizioni comuni, valutazioni d'impatto critiche ed ex post delle legislazioni finora adottate, nonché sulla comprensione e consapevolezza della situazione in merito alle questioni in gioco, 2 – politiche concrete per rafforzare la resilienza tra i cittadini dell'UE in linea con i valori democratici, 3 – capacità di "rottura" appropriate e 4 – risposte diplomatiche e deterrenti in un contesto globale;

3. sottolinea che tutti i provvedimenti tesi a prevenire, individuare e contrastare le ingerenze straniere devono essere elaborati in modo da rispettare e promuovere i diritti fondamentali, compreso il rispetto della vita privata e della libertà di pensiero, espressione e informazione;

4. ritiene che tale strategia dovrebbe fondarsi su un approccio basato sui rischi, che coinvolga la società e i governi nel loro insieme e riguardi in particolare i seguenti aspetti:

   a) rafforzamento della resilienza dell'UE attraverso la consapevolezza della situazione, l'alfabetizzazione mediatica e l'istruzione,

   b) ingerenze straniere per mezzo delle piattaforme online,

   c) infrastrutture critiche e settori strategici,

   d) finanziamento occulto di attività politiche da parte di donatori stranieri,

   e) cibersicurezza e resilienza agli attacchi informatici,

   f) protezione delle istituzioni europee,

g) ingerenze attraverso l'elite capture, le diaspore nazionali e le università,

h) deterrenza e sanzioni collettive,

i) cooperazione mondiale e multilateralismo;

5. invita, in particolare, l'UE a fornire maggiori risorse e mezzi agli organi e alle organizzazioni responsabili del monitoraggio delle minacce e della sensibilizzazione in merito alla loro gravità, compresa la disinformazione, in modo da rafforzare la protezione degli interessi strategici e delle infrastrutture dell'UE e degli Stati membri e da promuovere la cooperazione internazionale con partner che condividono gli stessi princìpi e devono affrontare sfide analoghe;

6. esprime preoccupazione per la diffusa mancanza di consapevolezza riguardo alla gravità delle minacce attualmente poste da regimi autoritari stranieri a tutti i livelli e in tutti i settori della società europea, minacce che mirano a indebolire la legittimità delle autorità pubbliche e ad aggravare la frammentazione politica e sociale;

7. è preoccupato per la mancanza di misure adeguate e sufficienti a prevenire, individuare e contrastare tali tentativi di ingerenza, il che fa dell'ingerenza una tattica allettante per gli attori malintenzionati, visto che il rischio di incorrere in sanzioni, o persino di essere scoperti, è estremamente basso;

8. esorta la Commissione a includere una prospettiva di manipolazione delle informazioni e di ingerenza straniera nella valutazione d'impatto ex ante condotta prima di presentare nuove proposte; invita altresì la Commissione a eseguire verifiche periodiche della resilienza, con le quali valuti lo sviluppo delle minacce e il loro effetto sulle attuali legislazioni e politiche;

9. invita la Commissione ad analizzare gli organismi nazionali istituiti recentemente, quali il coordinatore nazionale australiano per le azioni di contrasto alle ingerenze straniere, il comitato per la sicurezza della Finlandia a supporto del governo e dei ministeri, l'agenzia per la protezione civile svedese, la nuova agenzia per la difesa psicologica, il Centro nazionale cinese e la nuova agenzia nazionale Viginum in Francia, allo scopo di valutare quali pratiche di eccellenza possano essere attuate a livello dell'Unione;

10. esprime preoccupazione per le numerose lacune e scappatoie delle attuali normative e politiche a livello europeo e nazionale volte a individuare, prevenire e contrastare le ingerenze;

11. invita la Commissione a istituire un meccanismo dell'UE per l'esame delle normative e politiche vigenti al fine di individuare le lacune che potrebbero essere sfruttate da soggetti malevoli e a suggerire rapidamente possibili soluzioni per colmarle; sottolinea che tale struttura dovrebbe cooperare con le altre istituzioni dell'UE e con gli Stati membri a livello nazionale, regionale e locale e favorire lo scambio di migliori pratiche;

12. invita a creare sistemi a tutti i livelli e settori della società europea tesi a rafforzare la resilienza delle organizzazioni e dei cittadini nei confronti delle ingerenze straniere, che consentano loro di individuare tempestivamente gli attacchi e di contrastarli nel modo più efficiente possibile;

Rafforzare la resilienza dell'UE attraverso la consapevolezza della situazione, l'alfabetizzazione mediatica e l'istruzione

13. sottolinea che le istituzioni e gli Stati membri dell'UE necessitano di sistemi solidi ed efficaci per individuare, analizzare, registrare e mappare i casi in cui attori statali e non statali stranieri cercano di interferire con i processi democratici, al fine di favorire la consapevolezza della situazione e la chiara comprensione del tipo di comportamento che l'UE e gli Stati membri devono scoraggiare e affrontare;

14. osserva che è ugualmente importante che le informazioni ottenute mediante detta analisi non siano utilizzate soltanto da gruppi di specialisti in ingerenze straniere, ma siano condivise anche con il grande pubblico, in particolare con le persone che svolgono funzioni sensibili, in modo che tutti siano consapevoli delle forme di minaccia e possano evitare i rischi;

15. sottolinea che è necessario elaborare una metodologia comune per promuovere la consapevolezza della situazione, raccogliere prove sistematiche e individuare la manipolazione dell'ambiente di informazione, nonché norme in materia di attribuzione tecnica;

16. sottolinea l'esigenza che l'UE, in cooperazione con gli Stati membri e i partner globali, elabori una definizione concettuale della minaccia di ingerenza; osserva che tale definizione deve riflettere le tattiche, le tecniche e procedure che descrivono i modelli di comportamento attualmente posti in essere dagli attori responsabili delle minacce;

17. invita le istituzioni dell'UE a sviluppare ulteriormente l'importante lavoro della divisione StratCom del Servizio europeo per l'azione esterna (SEAE), con le sue task force, il Centro UE di situazione e di intelligence (EU INTCEN) e la cellula dell'UE per l'analisi delle minacce ibride, il sistema di allarme rapido, la consolidata cooperazione a livello amministrativo tra il SEAE, la Commissione e il Parlamento, la rete contro la disinformazione guidata dalla Commissione, la task force amministrativa contro la disinformazione del Parlamento e la cooperazione in corso con la NATO, il G7, la società civile e l'industria privata, per promuovere la collaborazione in materia di intelligence, analisi, condivisione delle migliori pratiche e sensibilizzazione in merito alla manipolazione delle informazioni e alle ingerenze straniere;

18. sottolinea l'esigenza di rafforzare le attività di monitoraggio ben prima delle elezioni o di altri importanti processi politici;

19. invita gli Stati membri a sfruttare appieno tali risorse condividendo le informazioni pertinenti e partecipando attivamente al sistema di allarme rapido; è del parere che l'analisi e la cooperazione nell'ambito dell'intelligence debbano essere ulteriormente rafforzate;

20. accoglie con favore l'idea della presidente della Commissione von der Leyen di istituire un Centro comune di consapevolezza situazionale, pur attendendo ulteriori informazioni riguardanti la sua struttura e la sua missione; sottolinea che tale centro richiederebbe la cooperazione attiva con i servizi della Commissione, il SEAE, il Consiglio e il Parlamento;

21. ribadisce l'esigenza di conferire al SEAE il mandato di monitorare e contrastare la

manipolazione delle informazioni e le ingerenze al di fuori delle regioni attualmente coperte dalle tre task force, attraverso un approccio basato sui rischi, e di dotarlo delle risorse necessarie; chiede con urgenza di garantire che il SEAE disponga di capacità adeguate per far fronte alla manipolazione delle informazioni e alle ingerenze da parte della Cina; sottolinea altresì l'esigenza di promuovere in modo significativo le competenze e le conoscenze linguistiche per quanto riguarda la Cina e altre regioni strategicamente importanti, sia all'interno del SEAE che delle istituzioni dell'UE in generale;

22. sottolinea l'importanza dei giornalisti, dei verificatori di fatti e dei ricercatori indipendenti per un dibattito democratico vivace e libero; accoglie con favore le iniziative volte a riunire, formare e sostenere in altro modo le organizzazioni di giornalisti, verificatori di fatti e ricercatori indipendenti in tutta Europa e in particolare nelle regioni più a rischio, quali ad esempio l'Osservatorio europeo dei media digitali;

23. esprime apprezzamento per l'indispensabile attività di ricerca e le numerose iniziative di sensibilizzazione e alfabetizzazione mediatica e digitale creative e di successo promosse da singole persone, scuole, università, organizzazioni operanti nel settore dei media, istituzioni pubbliche e organizzazioni della società civile;

24. chiede fonti di finanziamento pubblico affidabili e sostenibili per i verificatori di fatti, i ricercatori, i mezzi di comunicazione di qualità e i giornalisti indipendenti, e per le ONG che indagano sui casi di manipolazione delle informazioni e ingerenze, promuovono l'alfabetizzazione mediatica e altri strumenti per la responsabilizzazione dei cittadini e conducono ricerche su come misurare concretamente l'efficacia dell'alfabetizzazione mediatica, delle campagne di sensibilizzazione, delle attività di confutazione della disinformazione e della comunicazione strategica; sottolinea che numerosi paesi nel mondo intraprendono azioni volte a garantire che i mezzi di comunicazione abbiano risorse finanziarie adeguate; accoglie con favore, a tale proposito, le nuove possibilità di finanziamento per l'alfabetizzazione mediatica previste nel quadro del programma Europa creativa 2021-2027;

25. sottolinea l'esigenza di rendere pubblici le analisi, le segnalazioni di incidenti e i dati riguardanti la manipolazione delle informazioni e le ingerenze; suggerisce pertanto di creare un archivio pubblico, contenente le informazioni più importanti in tutte le lingue dell'UE;

26. invita tutti gli Stati membri a includere l'alfabetizzazione mediatica e digitale, nonché la riflessione critica e la partecipazione pubblica, nei propri programmi scolastici, dall'istruzione per l'infanzia all'apprendimento degli adulti, compresa la formazione di insegnanti e ricercatori;

27. invita le istituzioni dell'UE e gli Stati membri, a tutti i livelli amministrativi, a individuare i settori a rischio di tentativi di ingerenza e a fornire al personale che lavora in tali settori una formazione ed esercitazioni regolari su come rilevare ed evitare i tentativi di ingerenza e sottolinea che tali sforzi trarrebbero giovamento da un formato standardizzato stabilito dall'UE; raccomanda di offrire una formazione di base anche a tutti i dipendenti pubblici; accoglie in tal senso con favore le opportunità di formazione offerte dall'amministrazione del Parlamento ai deputati e al personale; invita a sviluppare ulteriormente tale formazione;

28. sottolinea l'esigenza di sensibilizzare in merito al fenomeno della manipolazione delle informazioni e dell'ingerenza, accoglie con favore le iniziative intraprese dal SEAE, dalla Commissione e dall'amministrazione del Parlamento, quali gli eventi di formazione e sensibilizzazione per giornalisti, insegnanti, influencer, studenti e visitatori, sia online che offline, a Bruxelles e in altre capitali dell'UE, e raccomanda di svilupparle ulteriormente;

29. invita gli Stati membri, l'amministrazione UE e le organizzazioni della società civile a condividere le migliori pratiche per la formazione in materia di alfabetizzazione mediatica e sensibilizzazione, come previsto dalla direttiva sui servizi di media audiovisivi; esorta la Commissione a organizzare tali scambi in cooperazione con il gruppo di esperti sull'educazione ai media;

30. invita l'UE e gli Stati membri ad attuare programmi mirati di sensibilizzazione e alfabetizzazione mediatica rivolti alle diaspore e alle minoranze ed esorta la Commissione a istituire un sistema per la condivisione semplice di materiali nelle lingue minoritarie, al fine di ridurre i costi per la traduzione e raggiungere il maggior numero possibile di persone;

31. invita la Commissione a presentare una strategia per l'alfabetizzazione mediatica che dedichi un'attenzione particolare alla lotta contro la manipolazione delle informazioni;

32. sottolinea l'importanza della comunicazione strategica per contrastare le narrazioni antidemocratiche più comuni; evidenzia che tutte le organizzazioni democratiche devono difendere la democrazia e hanno la responsabilità comune di coinvolgere i cittadini, utilizzando le lingue e le piattaforme da essi preferite;

33. esprime preoccupazione per la diffusione della propaganda di Stato straniera, proveniente da Mosca e Pechino, che viene tradotta nelle lingue locali, ad esempio attraverso contenuti mediatici finanziati da RT, Sputnik o dal partito comunista cinese e spacciati per giornalismo, e distribuita attraverso i quotidiani; è preoccupato per il modo in cui tali narrazioni si sono diffuse nei prodotti giornalistici reali;

34. esprime grave preoccupazione per le molestie e le minacce nei confronti dei giornalisti e invita la Commissione a presentare tempestivamente proposte concrete e ambiziose per la sicurezza di giornalisti e professionisti dei mezzi di comunicazione, come previsto dal piano d'azione per la democrazia europea;

35. sottolinea l'esigenza di coinvolgere i decisori politici a livello locale e regionale responsabili delle decisioni strategiche negli ambiti di loro competenza, quali le infrastrutture, la cibersicurezza, la cultura e l'istruzione; evidenzia che i politici e le autorità locali e regionali possono spesso individuare con tempestività eventuali sviluppi preoccupanti e sottolinea che è spesso necessaria una conoscenza della situazione locale per individuare e attuare le contromisure adeguate;

36. raccomanda agli Stati membri di creare dei canali di comunicazione ai quali le imprese, le ONG e i cittadini possano rivolgersi qualora siano vittime di manipolazione delle informazioni o di ingerenze; invita gli Stati membri a sostenere le vittime di attacchi o quanti sono sottoposti a pressioni;

Ingerenze straniere per mezzo delle piattaforme online

37. sottolinea che la libertà di espressione non deve essere erroneamente interpretata come libertà di dedicarsi ad attività online che sono illegali offline, quali le molestie, lo spionaggio e le minacce; evidenzia che le piattaforme non devono soltanto rispettare la legge ma anche soddisfare i termini di utilizzo dichiarati agli utenti;

38. pone innanzi tutto in risalto l'esigenza di una maggiore trasparenza per quanto concerne le operazioni condotte dalle piattaforme online;

39. chiede l'adozione di una regolamentazione che obblighi le piattaforme a fare la propria parte per limitare la manipolazione delle informazioni e le ingerenze, ad esempio utilizzando indicazioni in riferimento ai reali autori dietro agli account, limitando gli account utilizzati regolarmente per diffondere la disinformazione o che violano ripetutamente i termini di utilizzo della piattaforma, sospendendo gli account non autentici utilizzati per campagne di ingerenza coordinate o demonetizzando i siti che diffondono la disinformazione;

40. accoglie con favore la proposta di revisione del codice di buone pratiche sulla disinformazione e le proposte riguardanti la legge sui servizi digitali, la legge sui mercati digitali e altre misure legate al piano d'azione per la democrazia europea; raccomanda di tenere conto degli aspetti illustrati nella presente sezione durante la lettura definitiva di tali testi;

41. chiede l'adozione di norme europee vincolanti per limitare la quantità di dati che le piattaforme possono conservare sugli utenti e la durata di utilizzo di tali dati, soprattutto per le piattaforme e le applicazioni che utilizzano dati particolarmente riservati e/o sensibili, quali le applicazioni di messaggistica, di servizi sanitari, finanziari e di appuntamenti e i piccoli gruppi di discussione, nonché per separare le diverse funzioni delle piattaforme al fine di limitare le informazioni disponibili su ciascun utente e garantire che il rifiuto alla conservazione e alla condivisione dei dati sia agevole quanto il consenso; chiede un divieto a livello di UE del microtargeting per gli annunci politici o basati su questioni specifiche;

42. chiede l'adozione di norme europee vincolanti che impongano alle piattaforme di individuare, valutare e mitigare regolarmente i rischi di manipolazione delle informazioni e di ingerenza associati all'uso dei loro servizi, obblighino le piattaforme a istituire dei sistemi di monitoraggio dell'utilizzo dei loro servizi, almeno in tutte le lingue nazionali e regionali ufficiali, al fine di rilevare la manipolazione delle informazioni e le ingerenze e di segnalare le sospette ingerenze alle autorità competenti, nonché di aumentare i costi sostenuti dai soggetti che consentono di chiudere un occhio su azioni di questo tipo favorite dai loro sistemi;

43. chiede di regolamentare i servizi che offrono strumenti e servizi di manipolazione dei social media; sottolinea che tale regolamento deve basarsi su una valutazione approfondita delle attuali pratiche e dei rischi associati;

44. sottolinea la generale necessità di trasparenza per quanto riguarda la persona fisica o giuridica dietro ai contenuti online e agli account; invita le piattaforme a introdurre meccanismi per individuare e sospendere gli account falsi connessi a operazioni di influenza coordinata; sottolinea che le richieste di prove devono consentire di proteggere l'anonimato per le persone in posizioni vulnerabili (ad esempio informatori o dissidenti e oppositori politici di regimi autocratici) e lascino spazio agli account satirici

e umoristici;

45. sottolinea che una maggiore responsabilità rispetto alla rimozione di contenuti illegali e pericolosi non deve causare l'eliminazione arbitraria di contenuti leciti; invita a essere cauti nel sospendere completamente gli account di persone reali;

46. chiede l'adozione di norme vincolanti che obblighino le piattaforme a creare canali di comunicazione facilmente disponibili per le persone o le organizzazioni che desiderano segnalare abusi o sospette ingerenze e manipolazioni, e a introdurre procedure di ricorso, sia per le vittime dei contenuti pubblicati online che per le persone o le organizzazioni interessate dalla decisione di segnalare gli account, limitarne la visibilità, disabilitarne l'accesso o sospenderli, o di limitare l'accesso ai proventi pubblicitari;

47. invita ad adottare norme volte a rendere trasparenti i procedimenti online, ad esempio obbligando le piattaforme a creare archivi pubblici facilmente consultabili di annunci pubblicitari online e a garantire un accesso significativo alle informazioni sull'elaborazione, l'uso e l'impatto degli algoritmi e dei dati a livello individuale a ricercatori verificati affiliati a istituzioni accademiche, ai giornalisti, alle organizzazioni della società civile e alle organizzazioni internazionali che operano nell'interesse pubblico;

48. invita le piattaforme a correggere l'equilibrio tra la necessità, motivata da esigenze commerciali, di indurre le persone a rimanere più a lungo sulle piattaforme fornendo loro contenuti coinvolgenti e la responsabilità di promuovere contenuti di qualità; esorta le piattaforme a garantire che i loro algoritmi non promuovano contenuti illegali, estremisti o radicalizzanti, ma offrano invece agli utenti una pluralità di prospettive;

49. chiede che gli algoritmi siano modificati al fine di eliminare i contenuti provenienti da account non autentici e canali che favoriscono artificiosamente la diffusione della manipolazione dolosa straniera delle informazioni;

50. sottolinea l'esigenza di valutare sistematicamente le conseguenze degli algoritmi; sottolinea che tale esame dovrebbe verificare anche se le piattaforme possono mantenere le garanzie promesse nei rispettivi termini di utilizzo e se consentono un comportamento coordinato e non autentico su larga scala per manipolare i contenuti mostrati sulle loro piattaforme;

51. è allarmato dal numero elevato di annunci pubblicitari online di marchi noti che appaiono su siti web malevoli che promuovono l'incitamento all'odio e la disinformazione senza che i marchi interessati abbiano dato l'autorizzazione o ne siano a conoscenza e che finiscono con il finanziarli involontariamente; è del parere che i servizi di pubblicità programmatica, come Google Ads e altri servizi di scambi di inserzioni pubblicitarie, dovrebbero essere responsabili della selezione di siti web degli editori elencati nel proprio archivio, onde impedire che i siti che diffondono la disinformazione siano finanziati dai loro servizi pubblicitari; si congratula con le organizzazioni dedite all'opera di sensibilizzazione in merito a tale questione preoccupante; sottolinea che gli inserzionisti dovrebbero avere il diritto di sapere e decidere dove vengono posizionati i loro annunci e quale intermediario ha trattato i loro dati;

52. sottolinea che il codice di buone pratiche sulla disinformazione aggiornato, la legge sui

servizi digitali, la legge sui mercati digitali e altre misure legate al piano d'azione per la democrazia europea richiederanno un meccanismo efficace di controllo e valutazione una volta adottati, al fine di valutarne periodicamente l'attuazione a livello nazionale e dell'UE e di individuare eventuali lacune e porvi rimedio tempestivamente;

Infrastrutture critiche e settori strategici

53. ritiene che, data la loro natura interconnessa e transfrontaliera, le infrastrutture critiche sono sempre più vulnerabili nei confronti della manipolazione esterna ed è del parere che il quadro attualmente in vigore debba essere rivisto; accoglie pertanto con favore la proposta della Commissione riguardante una nuova direttiva per migliorare la resilienza dei soggetti critici che forniscono servizi essenziali nell'Unione europea;

54. raccomanda che, nel considerare detta proposta, si compiano sforzi tesi a rafforzare i canali di collegamento e comunicazione già ben coordinati utilizzati da attori multipli, a sostenere le autorità competenti degli Stati membri attraverso il gruppo per la resilienza dei soggetti critici e lo scambio delle pratiche migliori non soltanto tra gli Stati membri ma anche tra titolari e gestori delle infrastrutture critiche, a livello regionale e locale, anche attraverso la comunicazione interagenzia, al fine di individuare con tempestività eventuali sviluppi preoccupanti ed elaborare le contromisure adeguate;

55. è del parere che l'elenco delle infrastrutture critiche potrebbe essere esteso ai mezzi di comunicazione e alle infrastrutture per le elezioni, vista la loro importanza fondamentale nel garantire il funzionamento dell'UE e degli Stati membri e che andrebbe assicurata una certa flessibilità in relazione all'aggiunta nell'elenco di nuovi settori strategici da proteggere;

56. chiede un approccio globale dell'UE per affrontare il problema delle minacce ibride ai processi elettorali e per migliorare il coordinamento e la cooperazione tra gli Stati membri; invita la Commissione a valutare criticamente la dipendenza dalle piattaforme e dalle infrastrutture di dati nel contesto delle elezioni; ritiene che vi sia una mancanza di sorveglianza democratica sul settore privato;

57. raccomanda di adottare un approccio estremamente flessibile che consenta di aggiornare e modificare rapidamente la direttiva proposta, sulla base delle valutazioni delle minacce, dei rischi e delle vulnerabilità condotte dal Centro comune di ricerca in collaborazione con l'INTCEN del SEAE; sottolinea l'esigenza di elaborare un metodo modulare per garantire una rapida adattabilità e flessibilità;

58. ritiene che l'UE e gli Stati membri debbano fornire alternative di finanziamento in modo da impedire che ampie parti delle loro infrastrutture critiche finiscano nelle mani di paesi terzi, come avvenuto nel caso del porto del Pireo in Grecia e come sta avvenendo con gli investimenti cinesi nella posa in opera di cavi sottomarini nel Mar Baltico, nel Mediterraneo e nel Mar Artico; accoglie pertanto con favore il regolamento sul controllo degli investimenti esteri diretti quale importante strumento per coordinare le azioni degli Stati membri in relazione agli investimenti stranieri nelle infrastrutture critiche, e invita a elaborare un quadro normativo più rigoroso al fine di garantire un maggiore trasferimento di competenze alle istituzioni europee in materia di controllo degli investimenti esteri diretti; è del parere che il quadro dovrebbe essere anche correlato meglio con analisi indipendenti, svolte da istituti nazionali e dell'UE o da gruppi di riflessione pertinenti; ritiene che potrebbe essere appropriato includere anche

altri settori strategici nel quadro, come le reti 5G, in modo da limitare la dipendenza da fornitori ad alto rischio;

59. è inoltre del parere che l'UE debba affrontare più sfide a causa della sua dipendenza da fornitori esteri di tecnologia; ritiene che il tentativo dell'UE di procedere verso una maggiore autonomia strategica e una sovranità digitale sia molto importante e rappresenti la giusta strada da percorrere; reputa che la legge europea sui semiconduttori, annunciata dalla Commissione per garantire che le parti essenziali per la produzione dei semiconduttori siano prodotte in Europa, sia un passo importante per limitare la dipendenza da paesi terzi quali la Cina e gli Stati Uniti; ritiene che gli investimenti nella produzione di semiconduttori debbano essere fatti in maniera coordinata in tutto il blocco, onde evitare una corsa a sovvenzioni pubbliche nazionali e la frammentazione del mercato unico; invita pertanto la Commissione a istituire un fondo europeo specifico per i semiconduttori;

60. accoglie con favore lo sviluppo, da parte dell'Unione europea, di GAIA-X, una rete europea di infrastrutture di dati e fornitori di servizi disciplinata da norme di sicurezza europee, in quanto passo importante per contrastare il dominio dei fornitori di servizi cloud statunitensi;

61. invita la Commissione a proporre azioni tese a garantire l'approvvigionamento sicuro e sostenibile di materie prime per la produzione di batterie e apparecchiature per le energie rinnovabili;

Finanziamento occulto di attività politiche da parte di donatori stranieri

62. sottolinea che i finanziamenti stranieri delle attività politiche attraverso operazioni occulte rappresentano una grave compromissione dell'integrità del funzionamento democratico dell'UE e degli Stati membri, in particolare durante i periodi elettorali, e violano pertanto il principio di elezioni libere e regolari, e che dovrebbe quindi essere ritenuto illegale nell'UE perseguire qualunque attività occulta finanziata da una potenza straniera che intende influenzare i processi politici europei;

63. evidenzia che una parte considerevole dei finanziamenti occulti da parte di attori stranieri non è illegale in senso stretto poiché sono consentiti da numerose lacune derivanti dalle diverse disposizioni relative al finanziamento delle attività politiche previste dalle legislazioni nazionali degli Stati membri in materia elettorale;

64. sottolinea che tali lacune includono:

a) contributi in natura da parte di attori stranieri a favore di partiti polittici, compresi prestiti finanziari da parte di persone fisiche o giuridiche con sede all'estero, che dovrebbero essere proibiti;

b) donatori prestanome con cittadinanza nazionale[5]: la trasparenza relativa ai donatori fisici e giuridici deve essere imposta tramite dichiarazioni di conformità da parte dei donatori per attestare il loro status e conferendo maggiori poteri di

[5] Persona che dona a proprio nome denaro di altri a un partito politico o a un candidato.

applicazione alle commissioni elettorali;

c) società di comodo e società controllate nazionali appartenenti a società madri straniere[6]: le società di comodo dovrebbero essere vietate e dovrebbero essere introdotte prescrizioni più solide per rivelare l'origine di un finanziamento attraverso le società madri;

d) organizzazioni senza scopo di lucro e terze parti[7], coordinate da attori stranieri e create allo scopo di influenzare i processi elettorali: andrebbero considerate norme più uniformi e una maggiore trasparenza nell'UE per le organizzazioni che intendono finanziare le attività politiche laddove cerchino di influenzare direttamente i processi elettorali come le campagne elettorali e referendarie;

e) pubblicità politica online, che non è soggetta alle norme applicate alla pubblicità televisiva, radiofonica e a mezzo stampa e che in genere non è regolamentata in alcun modo: è pertanto necessario garantire la totale trasparenza degli afflussi e dei deflussi di denaro legati alla pubblicità politica online e una responsabilità ben maggiore sull'uso degli algoritmi, in linea con il principio della conoscenza del proprio cliente; la Commissione dovrebbe presentare quanto prima una proposta legislativa sulla trasparenza dei contenuti politici sponsorizzati, come richiesto dal piano d'azione per la democrazia europea, che garantirà l'effettivo diritto dei partiti dell'UE di fare campagna elettorale online in vista delle elezioni europee;

65. invita pertanto la Commissione a presentare proposte concrete per colmare tutte le lacune che danno adito a metodi di finanziamento opachi dei partiti politici da parte di fonti di paesi terzi e a proporre norme comuni a livello dell'UE che si applicherebbero alle leggi elettorali nazionali in tutti gli Stati membri; ritiene che gli Stati membri dovrebbero puntare a introdurre un divieto sulle donazioni ai partiti politici da fonti esterne all'UE e allo Spazio economico europeo (SEE), fatta eccezione per gli elettori che vivono al di fuori dell'UE e del SEE;

66. accoglie con favore la revisione in corso del regolamento (UE, Euratom) n. 1141/2014 relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee; sostiene tutti gli sforzi tesi a ottenere un livello maggiore di trasparenza nel finanziamento delle attività dei partiti politici europei e delle fondazioni politiche europee, in particolare in vista delle elezioni europee del 2024, compreso un divieto su tutte le donazioni da fonti esterne all'UE e da fonti anonime;

Cibersicurezza e resilienza contro gli attacchi informatici

67. esorta le istituzioni europee ad aumentare rapidamente gli investimenti nelle capacità e competenze digitali strategiche dell'Unione, quali l'intelligenza artificiale, la comunicazione sicura e le infrastrutture di dati e cloud, al fine di migliorare la cibersicurezza dell'Unione; invita inoltre la Commissione a investire di più nel miglioramento delle conoscenze digitali e della competenza tecnica dell'Unione in

[6] Questa lacuna riguarda due diverse realtà: le società di comodo, che non conducono reali attività commerciali e che non sono nient'altro che canali di occultamento finanziario e le società controllate nazionali appartenenti a società madri straniere usate per convogliare denaro in politica.
[7] Le organizzazioni senza scopo di lucro e le terze parti non sono tenute a rivelare l'identità dei donatori ma sono autorizzate a finanziare i partiti politici e i candidati in diversi Stati membri dell'UE.

modo da comprendere meglio i sistemi digitali utilizzati nell'UE; invita la Commissione a stanziare ulteriori risorse, sia umane che finanziarie, per la cibersicurezza delle istituzioni europee e degli Stati membri;

68. accoglie con favore le proposte della Commissione riguardanti una nuova strategia per la cibersicurezza e una nuova direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148[8] (NIS2); raccomanda che l'esito finale del lavoro in corso sulla proposta colmi le lacune della direttiva NIS del 2018, in particolare inasprendo i requisiti di sicurezza, introducendo obblighi di esecuzione più severi, come le sanzioni armonizzate, e proponendo regolamenti orizzontali e un'adeguata cooperazione tra il settore pubblico e quello privato a livello operativo; sottolinea l'importanza di raggiungere un livello comune elevato di cibersicurezza negli Stati membri, in modo da limitare le vulnerabilità della cibersicurezza comune dell'UE;

69. invita la Commissione a elaborare un pacchetto di strumenti dell'UE comprendente misure di attenuazione dei rischi per la nuova generazione di tecnologie, come le reti 5G e 6G, in modo da tenere meglio conto dei rischi associati all'utilizzo di software e hardware prodotti da imprese controllate da Stati stranieri autoritari, e a introdurre norme globali e regole in materia di concorrenza per queste nuove tecnologie, nel rispetto dei valori democratici; esorta la Commissione a promuovere gli scambi tra le istituzioni dell'UE e le autorità nazionali in merito alle sfide, alle migliori pratiche e alle soluzioni associate alle misure previste dal pacchetto; ritiene che l'UE dovrebbe investire di più nelle proprie capacità nel settore delle tecnologie 5G e post 5G, al fine di ridurre la dipendenza da fornitori stranieri;

70. sostiene l'idea della Commissione di elaborare una legge sulla resilienza informatica che vada a integrare la politica europea in materia di difesa informatica, poiché l'informatica e la difesa sono interconnesse; chiede di destinare maggiori risorse alle capacità europee di difesa informatica e al loro coordinamento;

71. condanna l'uso massiccio e illecito del software di sorveglianza Pegasus da parte di soggetti statali nei confronti di giornalisti, difensori dei diritti umani e politici; rammenta che Pegasus è soltanto uno di numerosi esempi di programmi di sorveglianza illeciti utilizzati da soggetti statali ai danni di cittadini innocenti;

72. è preoccupato che i giornalisti e gli attivisti democratici possano essere oggetto di sorveglianza illegale e molestie da parte dei regimi autoritari da cui cercano di scappare, persino sul territorio dell'UE, e ritiene che ciò rappresenti una grave violazione dei valori fondamentali dell'Unione e dei diritti fondamentali degli individui, come sancito dalla Carta dei diritti fondamentali, dalla Convenzione europea dei diritti dell'uomo (CEDU) e dal Patto internazionale relativo ai diritti civili e politici; deplora la mancanza di assistenza legale fornita alle vittime di tale software di spionaggio;

73. sottolinea la necessità urgente di rafforzare il quadro legislativo in modo da considerare responsabili quanti distribuiscono e usano detto software e ne abusano per finalità illecite e non autorizzate; fa, in particolare, riferimento alle sanzioni imposte il 21 giugno 2021 ad Alexander Shatrov, amministratore delegato di un'impresa bielorussa

[8] Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020)0823).

che produce un software di riconoscimento facciale utilizzato da un regime autoritario;

74. chiede un'ambiziosa revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche, al fine di rafforzare la riservatezza delle comunicazioni e dei dati personali quando si utilizzano dispositivi elettronici, senza abbassare il livello di protezione garantito dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie; chiede che l'UE e gli Stati membri coordinino ulteriormente le loro azioni sulla base della direttiva relativa agli attacchi contro i sistemi di informazione al fine di garantire che l'accesso illegale a sistemi di informazione e l'intercettazione illegale siano considerati reati; rammenta che qualunque violazione della riservatezza per ragioni di sicurezza nazionale deve avvenire in modo lecito e per finalità legittime ed esplicite in una società democratica, sulla base di rigorose condizioni di necessità e proporzionalità, come previsto dalla CEDU e dalla Corte di giustizia dell'Unione europea;

Protezione delle istituzioni europee

75. sottolinea che le reti, gli edifici e il personale delle istituzioni europee rappresentano un bersaglio per tutti i tipi di minacce ibride e di attacchi compiuti da attori statali stranieri e dovrebbero, pertanto, essere adeguatamente protetti; prende atto del costante aumento di attacchi finanziati da Stati stranieri contro le istituzioni, gli organi e le agenzie dell'UE, compresa l'Agenzia europea per i medicinali (EMA), e nei confronti delle istituzioni e delle autorità pubbliche degli Stati membri;

76. invita a eseguire un controllo approfondito dei servizi, delle reti, delle apparecchiature e dell'hardware delle istituzioni, degli organi e delle agenzie dell'UE utilizzati per garantire la cibersicurezza; esorta le istituzioni europee e gli Stati membri a fornire orientamenti adeguati e strumenti sicuri al personale; sottolinea la necessità di sensibilizzare in merito all'uso di servizi e reti sicuri all'interno delle istituzioni e amministrazioni;

77. sottolinea l'importanza del coordinamento tra le diverse istituzioni, gli organi e le agenzie dell'UE specializzati in cibersicurezza, quali la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (CERT-UE), unitamente al pieno sviluppo delle relative capacità operative, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e la futura unità congiunta per il ciberspazio che garantiranno una risposta coordinata alle minacce per la cibersicurezza su vasta scala nell'UE; accoglie con favore l'attuale cooperazione strutturata tra la CERT-UE e l'ENISA; apprezza le recenti iniziative intraprese dai segretari generali delle istituzioni europee volte a elaborare norme comuni in materia di informazione e cibersicurezza;

78. attende con interesse le due proposte di regolamento della Commissione per l'istituzione di un quadro normativo per la sicurezza dell'informazione e la cibersicurezza in tutte le istituzioni, gli organi e le agenzie dell'UE e ritiene che tali regolamenti dovrebbero includere il rafforzamento delle capacità; invita la Commissione e gli Stati membri a destinare ulteriori fondi e risorse alla cibersicurezza delle istituzioni europee, al fine di rispondere alle sfide in un contesto di minacce in costante evoluzione;

79. attende con interesse la relazione speciale di audit della Corte dei conti europea sulla cibersicurezza, prevista per l'inizio del 2022;

80. invita tutte le istituzioni dell'UE a promuovere la sensibilizzazione tra il personale mediante una formazione e orientamenti adeguati, al fine di attenuare i rischi per la sicurezza di natura informatica e non informatica e di rispondere ad essi; chiede che sia prevista una formazione obbligatoria e periodica in materia di sicurezza per tutto il personale e i deputati al Parlamento europeo;

81. sottolinea l'esigenza di procedure adeguate per la gestione delle crisi in caso di manipolazione delle informazioni, compresi sistemi di allarme tra i diversi livelli e settori amministrativi, onde garantire la fornitura reciproca di informazioni e prevenire la diffusione della manipolazione delle informazioni; accoglie in tal senso con favore il sistema di allarme rapido (RAS) e la procedura di allarme rapido istituiti prima delle elezioni europee del 2019 e le procedure poste in atto nelle amministrazioni della Commissione e del Parlamento per segnalare possibili casi riguardanti le istituzioni o i processi democratici dell'UE; chiede all'amministrazione dell'UE di valutare ulteriormente la possibile elaborazione di un pacchetto di strumenti condivisi da attivare in caso di allarme del RAS;

Ingerenze attraverso l'elite capture, le diaspore nazionali e le università

82. condanna tutti i tipi di elite capture e la tecnica della cooptazione di funzionari pubblici di alto livello e di ex politici europei utilizzata dalle imprese straniere collegate ai governi impegnati attivamente in azioni di ingerenza contro l'UE e deplora la mancanza degli strumenti e delle azioni di contrasto necessari per prevenire tali pratiche; ritiene che la divulgazione delle informazioni riservate acquisite durante mandati pubblici o nell'esercizio di funzioni pubbliche, a discapito degli interessi strategici dell'UE e degli Stati membri, dovrebbe essere rigorosamente vietata;

83. invita la Commissione a incoraggiare e coordinare le azioni contro l'elite capture, ad esempio integrando i periodi di incompatibilità ("cooling-off") per i commissari dell'UE con un obbligo di resoconto una volta trascorso detto periodo, e a elaborare norme strutturate per contrastare l'elite capture a livello dell'UE;

84. esprime preoccupazione per le strategie di lobbying integrate che combinano gli interessi industriali e gli obiettivi di politica estera, in particolare se favoriscono gli interessi di uno Stato autoritario; invita pertanto le istituzioni dell'UE a riformare il registro per la trasparenza, introducendo fra l'altro norme più rigorose in materia di trasparenza, mappando i finanziamenti stranieri per le attività di lobbying associate all'UE e garantendo un sistema di inserimento che consenta di identificare i finanziamenti provenienti da governi stranieri; ritiene che il regime di trasparenza delle influenze straniere introdotto dall'Australia sia un buon esempio da seguire;

85. invita gli Stati membri a prendere in considerazione l'istituzione di un regime di registrazione delle influenze straniere e la creazione di un registro gestito dal governo delle attività dichiarate intraprese per conto di uno Stato estero o a suo nome, seguendo le buone pratiche di altre democrazie che condividono gli stessi princìpi;

86. è preoccupato per i tentativi di controllo ad opera di Stati autoritari stranieri sulle diaspore che vivono nel territorio dell'UE; pone l'accento sul ruolo fondamentale svolto dal Fronte unito cinese, un dipartimento che fa capo direttamente al Comitato centrale del partito comunista cinese e incaricato di coordinare la strategia di ingerenza esterna della Cina attraverso il rigoroso controllo dei cittadini e delle imprese cinesi all'estero;

richiama l'attenzione sulle esperienze di Australia e Nuova Zelanda nel trattare con il Fronte unito;

87. sottolinea che gli sforzi del Cremlino tesi ad attuare le cosiddette politiche di protezione dei compatrioti, in particolare nelle repubbliche baltiche e nei paesi del vicinato orientale, sono parte della strategia geopolitica del regime di Putin volta a creare divisioni nelle società dell'UE, unitamente all'attuazione del concetto di "mondo russo" per giustificare le azioni espansionistiche del regime;

88. è allarmato dall'applicazione extraterritoriale delle misure coercitive previste dalla nuova legge sulla sicurezza nazionale cinese, in combinazione con gli accordi in materia di estradizione stipulati dalla Cina con altri paesi, che consentono a quest'ultima di attuare misure deterrenti su vasta scala contro cittadini non cinesi critici, come avvenuto ad esempio recentemente nei confronti di due parlamentari danesi;

89. è preoccupato per il numero di università, scuole e centri culturali europei impegnati in partenariati con soggetti cinesi, compresi gli Istituti Confucio, che consentono il furto di conoscenze scientifiche e l'esercizio di un rigido controllo su tutti gli aspetti relativi alla Cina nel settore della ricerca e dell'insegnamento, il che costituisce una violazione della protezione della libertà e autonomia accademica prevista dalla Costituzione, e sulle scelte delle attività culturali riguardanti la Cina; deplora, in particolare, la decisione del museo di Nantes di cancellare la mostra su Genghis Kahn nel 2020, a seguito delle forti pressioni esercitate dalla Cina contro la sua organizzazione[9];

90. condanna la decisione del governo ungherese di aprire una sede dell'università cinese Fudan, chiudendo nel contempo l'Università dell'Europa centrale a Budapest; esprime preoccupazione per la crescente dipendenza finanziaria delle università europee dalla Cina e invita la Commissione e gli Stati membri ad assicurare lo stanziamento di risorse finanziarie adeguate alle università europee; esorta la Commissione a proporre misure legislative volte a rafforzare la trasparenza dei finanziamenti delle università, ad esempio mediante dichiarazioni obbligatorie delle donazioni;

91. è preoccupato per il crescente numero di Istituti Confucio istituiti nel mondo, e in particolare in Europa, molto vicini allo Stato cinese; osserva che gli Istituti Confucio hanno cambiato nome nel 2020 e sono ora noti come "Centri per l'istruzione linguistica e la cooperazione"; sottolinea che gli Istituti Confucio sono privi di status giuridico; invita gli Stati membri e la Commissione a sostenere corsi di lingua cinese indipendenti che non prevedano il coinvolgimento del partito comunista cinese e dello Stato cinese; è del parere che il Centro nazionale cinese istituito recentemente in Svezia potrebbe essere una risorsa importante nell'offrire un contesto alle azioni e comunicazioni degli Istituti Confucio;

92. ritiene altresì che gli Istituti Confucio fungano da piattaforma per azioni di lobbying a favore degli interessi economici della Cina e per i servizi di intelligence cinesi e il reclutamento di spie; rammenta che numerose università hanno deciso di porre fine alla cooperazione con gli Istituti Confucio a causa dei rischi di spionaggio e ingerenza cinese, come nel caso delle università di Düsseldorf nel 2016, di Bruxelles (VUB e ULB) nel 2019 e di Amburgo nel 2020, e di tutte le università svedesi;

[9] https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/

93. osserva che le ingerenze straniere possono assumere anche la forma di influenza esercitata negli istituti religiosi, come nel caso dell'ingerenza russa nelle chiese ortodosse, in particolare in Serbia e Montenegro, al fine di generare divisioni tra le popolazioni locali, promuovere una ricostruzione storica distorta e un'agenda anti-UE, e dell'ingerenza turca attraverso le moschee in Francia e Germania; invita la Commissione e gli Stati membri a garantire un coordinamento migliore per proteggere gli istituti religiosi dalle ingerenze straniere;

Deterrenza e sanzioni collettive

94. ritiene che i regimi sanzionatori istituiti di recente dall'UE, come le misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri[10] e il regime globale di sanzioni dell'UE in materia di diritti umani[11], adottati rispettivamente il 17 maggio 2019 e il 7 dicembre 2020, abbiano dimostrato un valore aggiunto nel fornire all'UE preziosi strumenti di deterrenza; rammenta che i regimi sanzionatori contro gli attacchi informatici e le violazioni dei diritti umani sono stati utilizzati due volte, rispettivamente nel 2020 e nel 2021;

95. invita l'UE e i suoi Stati membri a intraprendere ulteriori misure contro la disinformazione e le minacce ibride, nel pieno rispetto della libertà di espressione e di informazione, anche introducendo un regime sanzionatorio a norma dell'articolo 29 del trattato sull'Unione europea (TUE) e dell'articolo 215 del trattato sul funzionamento dell'Unione europea (misure restrittive) in materia di ingerenze straniere, compresa la disinformazione, che dovrebbe essere destinato per quanto possibile ai decisori politici e agli organi responsabili di azioni aggressive; è del parere che i paesi dediti alle ingerenze straniere e alla manipolazione delle informazioni allo scopo di destabilizzare la situazione nell'UE dovrebbero pagare i costi delle loro decisioni e sostenerne le conseguenze a livello economico e/o di reputazione e/o diplomatico; invita la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza a presentare proposte concrete a tale riguardo;

96. insiste che, pur cercando di preservare i processi democratici, i diritti umani e le libertà sanciti dai trattati, un regime sanzionatorio debba prestare particolare attenzione agli effetti sui diritti e sulle libertà fondamentali delle eventuali sanzioni irrogate, al fine di garantire il rispetto della Carta dei diritti fondamentali;

97. ritiene che sebbene la natura degli attacchi ibridi vari, i rischi per i valori, gli interessi fondamentali, la sicurezza, l'indipendenza e l'integrità dell'Unione europea e per il consolidamento e il sostegno della democrazia, dello Stato di diritto, dei diritti umani e dei principi del diritto internazionale possono essere considerevoli in termini di portata degli attacchi, della loro natura o degli effetti cumulativi; reputa necessario condurre un'analisi più approfondita della natura e degli effetti della disinformazione individuale, delle minacce ibride e delle azioni che non rientrano nel summenzionato regime sanzionatorio già in vigore per gli attacchi informatici, al fine di classificare gli attacchi e definire quelli che non richiedono una risposta da parte dell'UE;

98. sottolinea che la consapevolezza che talune azioni di ingerenza straniera stanno incidendo gravemente sui processi democratici e sull'esercizio dei diritti o dei doveri si

[10] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC
[11] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L:2020:410I:TOC

sta diffondendo a livello internazionale; richiama in tal senso le modifiche adottate nel 2018 con l'emendamento della legislazione sulla sicurezza nazionale australiana (spionaggio e ingerenze straniere), volte a criminalizzare le attività occulte e ingannevoli di attori stranieri allo scopo di interferire con i processi politici o di governo, influire sui diritti e i doveri, o sostenere le attività di intelligence di un governo straniero, introducendo nuovi reati come l'"ingerenza straniera dolosa";

99. è consapevole che a norma dell'articolo 21, paragrafo 3, TUE l'Unione deve garantire la coerenza tra i diversi ambiti della sua azione esterna e tra questi e altre politiche, come previsto dai trattati; sottolinea, a tale proposito, che le ingerenze straniere, come le minacce poste dai combattenti terroristi stranieri e dai gruppi che influenzano le persone rimaste nell'UE, sono state considerate anche nella direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo[12];

100. evidenzia che, al fine di rafforzarne l'impatto, le sanzioni dovrebbero essere irrogate collettivamente, coordinandosi con partner che condividono gli stessi princìpi, anche in relazione ad altri tipi di reazione agli attacchi, coinvolgendo possibilmente le organizzazioni internazionali e mediante la formalizzazione in un accordo internazionale; richiama, in particolare, il comunicato della riunione NATO del 14 giugno 2021, in cui si affermava che una decisione riguardante il ricorso all'articolo 5 del trattato NATO in caso di attacco informatico viene presa dal Consiglio del Nord Atlantico sulla base di un esame caso per caso, e che l'impatto di attività informatiche cumulative dolose potrebbe, in talune circostanze, essere considerato equivalente a un attacco armato[13];

Cooperazione mondiale e multilateralismo

101. riconosce che molti paesi democratici in tutto il mondo si trovano ad affrontare operazioni di destabilizzazione simili condotte da Stati stranieri autoritari;

102. sottolinea l'esigenza di una cooperazione mondiale tra paesi che condividono gli stessi princìpi su tali questioni di importanza fondamentale, sotto forma di partenariato basato su una visione comune e definizioni condivise, al fine di istituire norme e princìpi internazionali;

103. ritiene che, sulla base di una consapevolezza comune della situazione, i partner che condividono gli stessi princìpi dovrebbero promuovere lo scambio di migliori pratiche e individuare soluzioni comuni, ivi comprese le sanzioni collettive;

104. invita l'UE e gli Stati membri a considerare i formati internazionali giusti che consentirebbero la realizzazione di un siffatto partenariato e la cooperazione tra partner che condividono posizioni simili;

105. accoglie con favore la dichiarazione NATO del 14 giugno 2021, che riconosce le crescenti sfide poste dalle minacce informatiche, ibride e asimmetriche di altra natura, comprese le campagne di disinformazione, e dall'utilizzo malevolo di tecnologie

[12] GU L 88 del 31.3.2017, pag. 6.
[13] https://www.nato.int/cps/en/natohq/news_185000.htm

emergenti e innovative sempre più sofisticate;

106. plaude alle iniziative già intraprese, in particolare a livello amministrativo, per condividere, in tempo reale, le conoscenze sullo stato degli attacchi ibridi, comprese le operazioni di disinformazione, come il sistema di allarme rapido istituito dal SEAE in parte aperto a paesi terzi che condividono i medesimi princìpi, il meccanismo di risposta rapida istituito dal G7 e la Divisione congiunta di intelligence e sicurezza della NATO;

107. sottolinea che la cooperazione mondiale dovrebbe fondarsi su progetti comuni, che coinvolgano le organizzazioni internazionali come l'Organizzazione per la cooperazione e lo sviluppo economici e l'UNESCO e rafforzino le capacità democratiche nei paesi chiamati ad affrontare minacce ibride straniere analoghe; chiede all'UE di istituire un fondo europeo per i mezzi di comunicazione democratici a sostegno del giornalismo indipendente nei paesi del vicinato europeo;

108. sottolinea l'importanza dei paesi strategici come quelli del vicinato orientale e meridionale dell'UE e dei Balcani occidentali, poiché la Russia cerca di utilizzarli come laboratorio di manipolazione delle informazioni e per la guerra ibrida; è del parere che le azioni dell'UE possano assumere la forma di finanziamenti di progetti volti a garantire la libertà dei mezzi di comunicazione e la cooperazione per l'alfabetizzazione mediatica; richiama l'attenzione sull'esigenza di rafforzare le capacità del SEAE in tale ambito;

109. invita il Parlamento a svolgere un ruolo di guida nella promozione dello scambio delle informazioni e a discutere delle pratiche migliori con i parlamenti partner in tutto il mondo, utilizzando la sua vasta rete di delegazioni interparlamentari, nonché le iniziative democratiche e le attività di sostegno coordinate dal suo Gruppo per il sostegno alla democrazia e il coordinamento elettorale;

110. chiede al SEAE di rafforzare il ruolo delle delegazioni dell'UE nei paesi terzi al fine di migliorare la loro capacità di confutazione delle campagne di disinformazione che minacciano i valori democratici orchestrate da attori statali stranieri;

111. chiede che la questione delle ingerenze straniere malevole sia affrontata nel quadro dell'imminente nuova bussola strategica dell'UE;

°

° °

112. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio, alla Commissione, al vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza nonché ai governi e ai parlamenti degli Stati membri.

MOTIVAZIONE

Contesto

Quando il Parlamento europeo ha deciso di istituire la Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione, il 18 giugno 2020, le ha conferito l'incarico di elaborare un approccio a lungo termine inteso a far fronte alle prove di ingerenze straniere nelle istituzioni e nei processi democratici dell'UE e dei suoi Stati membri.

A un anno di distanza dalla riunione istitutiva della commissione del 23 settembre 2020 e sulla base di una lunga serie di testimonianze di vari esperti e soggetti operativi, la relatrice è già in grado di delineare un quadro della situazione, della portata e dell'estrema complessità della miriade di forme assunte dalle operazioni di ingerenza aggressive concepite e finanziate da attori stranieri nei confronti dell'UE; la relatrice prende altresì atto, con una certa preoccupazione, della rapida capacità di adattamento, della volatilità e dell'accelerazione di tale fenomeno, attraverso nuovi attori, nuove narrazioni e nuovi strumenti emersi nell'arco di un solo anno.

Dalle campagne di disinformazione su nuova scala legate alla COVID-19 agli attacchi informatici contro le autorità pubbliche, comprese le infrastrutture di sanità pubblica, dalle strategie di ingerenza che prevedono l'elite capture e le attività di lobbying industriale al finanziamento occulto delle attività politiche, dal controllo dei centri accademici e culturali alla strumentalizzazione delle diaspore nazionali, la nostra commissione ha analizzato la natura eterogenea e dinamica di questo nuovo tipo di guerra, volta a minare la coesione sociale e la fiducia reciproca delle nostre società democratiche europee allo scopo di indebolirle.

La commissione ha fortunatamente assistito anche alla diffusione di una maggiore consapevolezza in merito a tali aspetti di fondamentale importanza, compreso il comune riconoscimento del fatto che l'UE e gli Stati membri dovrebbero rapidamente introdurre vere e proprie politiche per la resilienza e strumenti di deterrenza, sulla base di un approccio che coinvolga la società nel suo insieme, che consenta loro di affrontare tutti i tipi di minacce ibride e di attacchi, tutelando in tal modo il funzionamento sostenibile della democrazia.

Rafforzare la resilienza dell'UE attraverso la consapevolezza della situazione, l'alfabetizzazione mediatica e l'istruzione

È evidente che la base per una difesa efficace contro le ingerenze straniere è rappresentata dalla consapevolezza della situazione. Per ottenerla, si deve procedere in due direzioni: è innanzi tutto necessario monitorare, mappare e analizzare i differenti tentativi di ingerenza, in modo da comprendere pienamente la minaccia; in secondo luogo, dobbiamo assicurarci che chi di dovere sia a conoscenza di detta analisi.

Molti ricercatori, organizzazioni della società civile, giornalisti e membri del personale delle istituzioni nazionali o europee stanno svolgendo un eccellente lavoro d'indagine sulle minacce di questo tipo. La commissione INGE ha incontrato molti di loro. A livello europeo, la relatrice apprezza in particolare il lavoro condotto dalle task force della StratCom del SEAE. È tuttavia necessario intensificare ulteriormente gli sforzi in tal senso. È inaccettabile che non vi sia ancora una task force preposta al monitoraggio delle ingerenze della Cina.

Dobbiamo inoltre accertarci che le informazioni siano divulgate a un pubblico più ampio. Sia le campagne di formazione mirata per il personale con funzioni sensibili alle ingerenze straniere sia le campagne di sensibilizzazione generali sono importanti. In tale contesto, l'alfabetizzazione mediatica e digitale è fondamentale per fornire ai cittadini gli strumenti necessari per meglio interpretare e valutare le informazioni a cui hanno accesso.

I giornalisti svolgono un ruolo cruciale nel garantire un clima favorevole al dibattito. Sfortunatamente, essi hanno subito gli effetti finanziari negativi della digitalizzazione, soprattutto laddove i sistemi pubblicitari sembrano privilegiare i contenuti emotivi, comprese le opinioni e la disinformazione, rispetto al giornalismo di qualità. I singoli giornalisti sono inoltre vittime frequenti di molestie e minacce organizzate quando si occupano di tematiche sensibili. Se da un lato è importante difendere l'indipendenza di mezzi di comunicazione di qualità, lo è altrettanto individuare modalità per sostenere nuovi canali di informazione e i giornalisti, sia dal punto di vista finanziario che contro le molestie.

Ingerenze straniere per mezzo delle piattaforme online

È chiaro che l'attuale sistema di divulgazione delle informazioni per mezzo delle piattaforme crea un clima online contorto, in cui la disinformazione e altri tipi di manipolazione delle informazioni possono prosperare. I rapporti riguardanti la fuga e la vendita di dati sensibili, gli algoritmi che promuovono contenuti radicalizzanti e le piattaforme che chiudono un occhio su evidenti violazioni della legge o dei loro termini di utilizzo sono talmente comuni che rischiamo di abituarci ad essi e di non esserne più sconvolti. È necessario porre un freno a tutto ciò.

Alla luce delle numerose discussioni avute con gli esperti, la relatrice è giunta alla conclusione che l'attuale metodo di autoregolamentazione non funziona e deve essere sostituito da norme vincolanti. Non possiamo accettare che attori stranieri possano manipolare liberamente i contenuti che riceviamo online attraverso le piattaforme o utilizzino in maniera impropria i sistemi pubblicitari in modo che gli inserzionisti finiscano con finanziarli involontariamente. È altresì inaccettabile che le piattaforme possano continuare a non fare nulla senza pagarne le conseguenze.

Va riconosciuto che sono stati compiuti numerosi progressi, sia su iniziativa delle piattaforme stesse che grazie a misure pubbliche come il codice di buone pratiche. Senza una trasparenza adeguata è tuttavia impossibile avere un quadro preciso dell'impatto di tali azioni. È inoltre fondamentale che il codice di buone pratiche, volontario per natura, sia dotato di un meccanismo di attuazione efficace e sia integrato da normative rigorose. Colpisce peraltro il fatto che molte politiche contro le ingerenze riguardino unicamente i contenuti in lingua inglese o i contenuti in un numero estremamente limitato di lingue. Non possiamo accettare che i cittadini di lingua lettone, bulgara, greca, o persino francese e tedesca siano molto meno tutelati contro la manipolazione rispetto agli anglofoni, soltanto perché le piattaforme danno la priorità ai contenuti in inglese.

Infrastrutture critiche e settori strategici

Le infrastrutture critiche sono essenziali per il funzionamento dell'economia e della società. Al fine di garantire una migliore protezione dei settori critici, è necessario intraprendere sforzi congiunti e coordinati in tutti i settori e a diversi livelli: dell'UE, nazionale, regionale e locale. La nuova direttiva della Commissione per il rafforzamento della resilienza dei soggetti critici costituisce un importante punto di partenza. La relatrice ritiene tuttavia che l'elenco delle

infrastrutture critiche potrebbe essere esteso anche ai mezzi di comunicazione e alle infrastrutture per le elezioni, vista la loro importanza fondamentale nel garantire il funzionamento dell'UE e degli Stati membri, e che andrebbe assicurata una certa flessibilità in relazione all'aggiunta nell'elenco di nuovi settori strategici in futuro. È della massima importanza che la direttiva mantenga un approccio estremamente flessibile che permetta di procedere rapidamente ad aggiornamenti e modifiche.

Inoltre, la dipendenza da investimenti stranieri e da fornitori stranieri di tecnologie per le infrastrutture critiche pone numerose minacce per il funzionamento autonomo delle infrastrutture. La spinta dell'UE verso l'autonomia strategica e la sovranità digitale è pertanto essenziale per contrastare tali minacce.

Finanziamento occulto di attività politiche da parte di donatori stranieri

Prove concrete dimostrano che gli attori stranieri hanno interferito attivamente con le elezioni democratiche e i referendum dei paesi europei, attraverso operazioni di finanziamento occulto durante le campagne elettorali.

Tali operazioni dolose mettono a repentaglio l'integrità delle elezioni indette nell'UE, poiché favoriscono una concorrenza sleale tra i partiti e i candidati, stanziando ulteriori risorse a taluni partiti – generalmente quelli antieuropeisti – non conteggiate nelle dichiarazioni ufficiali delle campagne elettorali.

Secondo la relazione della Alliance for Securing Democracy sui finanziamenti stranieri occulti del 2020[1], negli ultimi dieci anni la Russia, la Cina e altri regimi autoritari hanno distribuito più di 300 milioni di dollari in 33 paesi per interferire con i processi democratici più di 100 volte e la metà dei casi riguarda azioni della Russia in Europa.

Alcune di queste operazioni non sono neppure illegali: sfruttano i numerosi vuoti normativi esistenti tra gli Stati membri le cui disposizioni in materia elettorale riguardanti il finanziamento delle attività politiche non sono armonizzate a livello dell'UE.

Cibersicurezza e resilienza contro gli attacchi informatici

La crescente digitalizzazione dei servizi ha comportato una maggiore dipendenza delle infrastrutture critiche dai sistemi online, fattore che ne ha accresciuto la vulnerabilità ad attacchi informatici e al rischio di esposizione dei dati. Negli ultimi anni sono aumentati gli attacchi informatici, indirizzati a settori strategici come l'Agenzia europea per i medicinali (EMA) e il parlamento norvegese.

La frammentazione delle capacità e competenze e la scarsità di risorse umane e finanziarie evidenziano la vulnerabilità dell'UE agli attacchi informatici. Gli attacchi informatici non conoscono confini. È pertanto imperativo che l'UE investa rapidamente nelle sue capacità e competenze digitali strategiche, stanziando ulteriori risorse, sia umane che finanziarie, per la cibersicurezza, garantendo nel contempo un livello comune elevato di cibersicurezza in tutti gli Stati membri. La strategia dell'UE in materia di cibersicurezza del 2020 e la direttiva NIS2 sono proposte importanti per il miglioramento della cibersicurezza dell'UE, che sarà rafforzata in futuro dalla legge sulla resilienza informatica e la politica in materia di difesa informatica.

[1] https://securingdemocracy.gmfus.org/covert-foreign-money/

Sarebbe inoltre opportuno affrontare rapidamente la questione dei software di spionaggio, come Pegasus, rafforzando il quadro legislativo in modo da chiamare i distributori, gli utilizzatori e quanti abusano di tali software a rispondere del proprio operato.

Protezione delle istituzioni europee

La cibersicurezza non dovrebbe essere migliorata soltanto a livello di Stati membri ma anche nelle istituzioni dell'UE. I recenti attacchi informatici indirizzati contro le istituzioni europee hanno evidenziato l'esigenza di una forte cooperazione interistituzionale per l'individuazione, il monitoraggio e la condivisione delle informazioni durante gli attacchi informatici e/o per prevenirli. Le istituzioni europee hanno già adottato misure per rafforzare la cibersicurezza e introdotto strumenti per il coordinamento e la rilevazione degli attacchi informatici, quali ad esempio CERT-EU, ENISA e la futura unità congiunta per il ciberspazio.

Occorre tuttavia fare di più. Innanzi tutto si dovrebbero aumentare le risorse umane e finanziarie per rispondere alle sfide in un contesto di minacce in costante evoluzione. In secondo luogo, le istituzioni europee dovrebbero condurre un'analisi approfondita dei propri servizi e delle proprie reti, al fine di attenuare i rischi per la sicurezza e garantire che le istituzioni non dipendano da tecnologie straniere per la propria sicurezza. È infine necessario provvedere ad attività di sensibilizzazione, nonché a formazione e orientamento adeguati, per tutto il personale, onde mitigare e affrontare i rischi per la sicurezza di natura informatica e non informatica.

Ingerenze attraverso l'elite capture, le diaspore nazionali e le università

Un'altra serie di strumenti a disposizione dei paesi stranieri che mirano a interferire con il funzionamento dell'UE è rappresentata dall'ingerenza attraverso le persone.

L'"elite capture" o cooptazione è purtroppo un fenomeno diffuso e la sua forma più nota è l'assunzione di ex politici e dipendenti pubblici europei di alto livello da parte di imprese controllate da Stati stranieri in cambio delle loro conoscenze acquisite nello svolgimento dei loro incarichi pubblici o delle loro funzioni. Le loro conoscenze, spesso basate su informazioni e contatti riservati, vengono quindi utilizzate a discapito degli interessi strategici dell'UE e degli Stati membri. Tali operazioni sono spesso associate a strategie di lobbying industriale, in cui gli obiettivi economici e politici si fondono.

Un'altra forma di ingerenza attraverso le persone avviene con la crescente influenza, e infine con il controllo, nei confronti delle università, delle scuole e dei centri culturali e religiosi da parte di agenti di Stati stranieri, in relazione ad aspetti rilevanti per un determinato paese straniero. Il modo in cui gli Istituti Confucio, ora chiamati "Centri per l'istruzione linguistica e la cooperazione", cercano di controllare tutti i tipi di ricerca, di insegnamento o persino di eventi culturali riguardanti la Cina all'interno di numerose università e musei europei è un chiaro esempio di tale pratica. Anche altri paesi sono molto attivi in tale ambito, ad esempio la Russia attraverso le chiese ortodosse.

Tale forma di ingerenza sfrutta principalmente i tentativi di controllare le diaspore nazionali residenti nell'UE, che rappresentano uno strumento potenzialmente molto efficace per esercitare pressioni ai vari livelli delle società europee. Tali sforzi mirano inoltre a ridurre al silenzio gli oppositori politici residenti all'estero.

Deterrenza e sanzioni collettive

L'UE e gli Stati membri devono adottare strumenti di deterrenza credibili. In effetti, l'UE e gli Stati membri non dispongono attualmente di un regime specifico di sanzioni riguardanti le ingerenze straniere e le campagne di disinformazione orchestrate da attori statali stranieri.

La relatrice è consapevole delle problematiche giuridiche che possono emergere istituendo un siffatto regime sanzionatorio, inclusa la necessità di definire con precisione le fattispecie di reato e i loro possibili effetti cumulativi conformemente alle legislazioni dell'UE e internazionali.

La relatrice ritiene tuttavia che l'UE possa trarre un'utile ispirazione dalle esperienze di altri partner a tale riguardo, come ad esempio l'Australia, che ha definito in modo specifico che cosa sia un'"ingerenza straniera dolosa" e ha equiparato a reato le attività occulte e ingannevoli di attori stranieri.

La relatrice è inoltre del parere che sia possibile partire da quanto già fatto a livello dell'UE, in particolare dal regime di misure restrittive riguardanti gli attacchi informatici che minacciano l'Unione e i suoi Stati membri, utilizzato due volte lo scorso anno.

Infine, ma non per questo meno importante, è necessaria una stretta cooperazione con i nostri partner internazionali che condividono i medesimi princìpi in materia di sanzioni, allo scopo di irrogare collettivamente sanzioni per rafforzarne l'efficacia e l'effetto deterrente.

I soggetti stranieri responsabili di operazioni di ingerenza aggressive contro le democrazie non dovrebbero poter credere che non pagheranno le conseguenze delle loro campagne di destabilizzazione.

Cooperazione mondiale e multilateralismo

L'UE non è assolutamente l'unica area democratica al mondo interessata da azioni di ingerenza straniera sempre più aggressive. Molti altri paesi, sia sviluppati che in via di sviluppo, sono oggetto di tali operazioni da parte di Cina, Russia o altri regimi autoritari, che perseguono lo stesso obiettivo: minare il funzionamento democratico per rafforzare la propria influenza.

È necessario riunire partner che condividono gli stessi princìpi per affrontare tali problematiche in modo coordinato, sulla base di un partenariato di democrazie.

Deve innanzi tutto essere trovato un accordo su definizioni comuni e su una visione condivisa di quanto è attualmente in gioco, al fine di concordare norme e standard internazionali.

È necessario porsi le seguenti domande specifiche e individuare risposte collettive: che cosa sono le ingerenze straniere aggressive? In che modo si devono classificare, dal punto di vista giuridico, le operazioni di disinformazione e manipolazione orchestrate da un paese straniero? Come possiamo inquadrare tali minacce e attacchi come reati? Quale regime sanzionatorio collettivo si potrebbe introdurre?

La cooperazione mondiale dovrebbe quindi basarsi sullo scambio delle migliori pratiche e sulla gestione di progetti concreti. In virtù della sua vasta rete di forum interparlamentari, il Parlamento europeo potrebbe svolgere un importante ruolo in tal senso, insieme alle delegazioni dell'UE nei paesi terzi.

Metodi di lavoro

Indipendentemente dalle nostre opinioni politiche su diversi atti legislativi e dalla nostra posizione nello spettro politico, in qualità di membri della commissione INGE siamo accomunati dalla convinzione che la nostra democrazia debba opporsi con risolutezza ai tentativi di ingerenza straniera. Per tale ragione, il lavoro della commissione si fonda su una stretta cooperazione tra i gruppi politici. I coordinatori hanno deciso di comune accordo con il presidente quali esperti invitare e quali studi commissionare. La relatrice ha regolarmente consultato i relatori ombra durante l'elaborazione del documento.

Dal punto di vista tematico, è possibile operare una distinzione tra la fase di diagnosi e la fase di individuazione delle soluzioni. Durante la prima fase, sono stati invitati esperti che ci hanno aiutato a comprendere le minacce e i metodi utilizzati in tutte le diverse sfumature. Sulla base del mandato, sono state organizzate diverse audizioni sulle ingerenze nella sfera pubblica e privata e sono stati analizzati i metodi utilizzati dai diversi attori stranieri. Nella fase dedicata all'individuazione delle soluzioni, la commissione INGE si è adoperata per individuare possibili strumenti e strategie per prevenire e contrastare i problemi rilevati.

La commissione INGE ha inoltre commissionato sei studi e invitato gli autori a presentarne i risultati. La situazione sanitaria legata alla pandemia di COVID-19 ci ha impedito di organizzare missioni durante i primi due semestri di attività dell'INGE. Al momento della stesura del presente documento, tuttavia, i membri della commissione INGE erano appena rientrati dalla prima missione, conclusa con successo, presso l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ad Atene, Grecia. Sono previste altre tre missioni: a Taipei, Parigi e Washington.

Per la formulazione delle raccomandazioni sono state inoltre presentate due interrogazioni con richiesta di risposta orale. Nel luglio 2021 è stato chiesto al VP/AR Josep Borrell come intendeva porre rimedio alla mancanza di risorse e di mandato per le task force della StratCom del SEAE e alla mancanza di sanzioni adeguate nei confronti di attori stranieri che commettono ingerenze. Nell'ottobre 2021 abbiamo chiesto alla vicepresidente della Commissione Věra Jourová come intende garantire che la mancanza di coordinamento tra i diversi settori e livelli politici non aumenti l'esposizione alle ingerenze straniere e come intende migliorare la trasparenza degli algoritmi e sostenere l'alfabetizzazione mediatica.

Una delle principali conclusioni riguardava l'importanza della cooperazione e della condivisione delle informazioni, sia a livello globale che tra i livelli di governance e i diversi settori all'interno dell'UE. Alle nostre riunioni sono state pertanto invitate, fin dall'inizio, altre commissioni e delegazioni con competenze associate alle ingerenze straniere. Le competenze di questi organismi hanno offerto un contributo prezioso ai dibattiti con gli invitati e hanno fatto sì che le informazioni raccolte durante le audizioni venissero trasmesse alle commissioni ordinarie che si occupano delle proposte legislative corrispondenti.

Un evento importante sarà la riunione interparlamentare prevista a novembre 2021. Tale riunione tra i parlamentari dei paesi dell'UE e un gruppo selezionato di partner globali che condividono gli stessi princìpi offrirà l'importante opportunità di trarre insegnamenti dalle esperienze altrui e di discutere di sfide e soluzioni comuni.

Per redigere la presente relazione, la relatrice ha approntato quattro documenti di lavoro: sullo stato delle ingerenze straniere nell'Unione europea, inclusa la disinformazione, sul finanziamento occulto di attività politiche da parte di donatori stranieri, sulle ingerenze

straniere per mezzo delle piattaforme online e sul rafforzamento della resilienza dell'UE contro le minacce ibride.

Oltre a tutte le riunioni formali menzionate, la relatrice ha raccolto informazioni attraverso incontri, la partecipazione a conferenze e la lettura di numerosi studi e articoli di giornale.

Cooperazione con altri organismi del Parlamento europeo e dell'UE

Alla luce della natura intersettoriale del mandato, la commissione INGE ha invitato cinque commissari per discutere di aspetti diversi delle ingerenze straniere:

- Věra Jourová, vicepresidente della Commissione per i Valori e la trasparenza,
- Margaritis Schinas, vicepresidente per la Promozione dello stile di vita europeo,
- Josep Borrell, vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,
- Thierry Breton, commissario per il Mercato interno e
- Margrethe Vestager, vicepresidente esecutiva dell'UE per Un'Europa pronta per l'era digitale e commissaria per la Concorrenza

Sono state inoltre condotte diverse discussioni con il personale della Commissione e del Servizio europeo per l'azione esterna ed è stata indetta una riunione speciale, insieme alla commissione CONT, con la Corte dei conti europea in merito alla sua relazione speciale n. 09/2021: "La disinformazione nell'UE: combattuta ma non vinta".

La commissione speciale INGE ha inoltre stabilito un piano di cooperazione con diverse commissioni del PE con cui condivide alcune competenze. La commissione INGE conta attualmente undici commissioni e undici delegazioni.

Consulenza esterna

La commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione, ha richiesto la consulenza esterna sui seguenti temi, importanti per il lavoro che la commissione sta portando avanti:

- Disinformazione - mappatura e soluzioni, compresa la regolamentazione delle piattaforme
- Finanziamento - mappatura e soluzioni
- Infrastrutture
- Migliori pratiche per l'approccio della società nel suo insieme al contrasto alle minacce ibride
- Impatto delle campagne di disinformazione sui migranti, le persone LGBTI e le minoranze
- Lezioni apprese dagli abusi perpetrati dai regimi autoritari

Panoramica delle audizioni con esperti esterni

Audizioni tematiche

- **Minacce ibride, disinformazione e polarizzazione – panoramica istituzionale**, 24 settembre 2020
- **Ingerenze elettorali, finanziamento dei partiti politici e piattaforme dei social media – panoramica**, 2 ottobre 2020
- **Come l'ingerenza straniera compromette la sovranità: l'esempio dei nostri vicini orientali**, 21 ottobre 2020
- **Ingerenze straniere nella sfera pubblica: verifica dei fatti, piattaforme dei social media e loro utilizzo nella disinformazione, nelle ingerenze straniere e nello sviluppo della resilienza**, 26 ottobre 2020 e 9 novembre 2020
- **Ingerenze straniere nella sfera politica: ingerenze straniere durante i processi elettorali, anche attraverso attacchi informatici, fughe di dati e comunicazioni maligne**, 12 novembre 2020
- **Ingerenze straniere nella sfera politica: finanziamento politico tramite forme legali o illegali di società di comodo e donatori di paesi terzi che utilizzano prestanome**, 2 dicembre 2020
- **Giornalismo vs. propaganda**, 11 dicembre 2020
- **Possibili minacce di ingerenza di paesi terzi in un contesto geopolitico**, 25 gennaio 2021 e 1° febbraio 2021
- **Comunicazione strategica per contrastare le ingerenze straniere**, 22 febbraio 2021
- **Come rendere più trasparente il finanziamento dei partiti politici e delle campagne elettorali: quali norme sono necessarie nell'UE?**, 23 febbraio 2021
- **Democrazia online: quali sono i rischi e come possiamo proteggerci?**, 17 marzo 2021
- **Interferenza straniera nel finanziamento di organizzazioni anti-scelta nell'UE**, 25 marzo 2021,
- **Sviluppi tecnologici e approcci normativi relativi alla disinformazione: ingerenze mediante la pubblicità**, 13 aprile 2021
- **Sviluppi tecnologici e approcci normativi relativi alla disinformazione**, 15 aprile 2021
- **Scambio di opinioni con Mikhail Khodorkovsky, fondatore di Dossier Center**, 10 maggio 2021
- **Audizione con Facebook, Twitter e Youtube sul ruolo delle piattaforme di social media nella diffusione e nello sviluppo della disinformazione e soluzioni per**

individuarla e contrastarla, 10 maggio 2021

- **Modalità con cui la storia, la cultura e l'istruzione possono contribuire a contrastare la disinformazione**, 15 giugno 2021

- **Disinformazione e discriminazione**, 12 luglio 2021

- **Il piano d'azione per la democrazia europea e la legge sui servizi digitali e altri strumenti dell'UE: in che modo le proposte potrebbero proteggere i processi democratici nell'UE dalle ingerenze straniere e la via da seguire**, 2 settembre 2021

- **Sanzioni e contromisure collettive**, 2 settembre 2021

Scambio di opinioni

- **Il ruolo dell'istruzione, dei media e della cultura nel contrastare la disinformazione e le ingerenze straniere**, 9 settembre 2021

- **Ingerenze straniere e spionaggio ai danni di politici europei e delle istituzioni europee**, 9 settembre 2021

- **Sicurezza delle istituzioni dell'UE: risposta all'escalation degli attacchi informatici**, 9 settembre 2021

- **Danno economico causato da ingerenze straniere/disinformazione, compreso il mercato dei dati**, 14 ottobre 2021.