

SERVIZIO DI INFORMAZIONE ESTERNO
N. 1956 del 4 dicembre 2024NESECRET
Copia n. 1

Analisi di alcuni rischi per la sicurezza razionale causati dalle azioni di attori informatici statali e non statali su alcune infrastrutture IT&C, a supporto del processo elettorale.

- Estratto non classificato della nota n. 0654 del 28 novembre 2024 -

- La Russia ha una storia di interferenze nei processi elettorali di altri Paesi. Mentre nell'ex spazio sovietico la Russia è stata ed è tuttora quasi pervasiva attraverso azioni di influenza apparente, in Occidente il coinvolgimento è diventato molto più evidente dopo le elezioni presidenziali del 2016/USA.

L'interesse della Russia per queste azioni ostili contro l'Occidente è cresciuto d'intensità, con un modus operandi sempre più complesso, di cui un'altissima percentuale è online, perché: a) è difficile identificare i legami tra le operazioni stesse e gli individui; b) i servizi russi hanno dovuto adattarsi e sono passati dalle classiche azioni di influenza (gestione delle fonti umane con metodi tradizionali) alle azioni online.

- Quest'anno si sono svolti diversi scrutini in Occidente, tra cui le elezioni del Parlamento europeo del 2024, con la Russia che ha esercitato diversi gradi di influenza. Sono emerse le seguenti conclusioni preliminari sull'interferenza russa:

Su richiesta del Cremlino, sono state condotte ricerche sociologiche dettagliate sugli Stati target (in riferimento all'opinione pubblica, prospettive politiche di alcuni partiti/candidati, misure adottate dalle autorità contro le interferenze elettorali straniere) ed è stato studiato il quadro legislativo degli Stati target per identificare le lacune/vulnerabilità e la capacità di risposta;

L'attenzione si è concentrata sull'aggressione informativa, compresa la propaganda, e sull'uso dell'intelligenza artificiale per la creazione rapida di contenuti;

Nello spazio online occidentale, la Russia ha costantemente cercato di accedere al pubblico più ampio possibile espandendo la propria infrastruttura online (un portafoglio variegato di canali di diffusione: vettori ufficiali, formatori locali e reti di troll) e diversificando le tecniche di diffusione delle narrazioni (pro)russe, con particolare attenzione alla loro distribuzione locale (ad es. coordinamento dei messaggi; aumento della capacità e della qualità dei contenuti multimediali, anche attraverso software di intelligenza artificiale/IA; deumarchizzazione e creazione di hashtag, prevalentemente sulla rete X);

Continua l'interesse di Mosca ad aumentare le chance dei candidati filorussi, di estrema destra, antisistema, "pacifisti" e nazionalisti. Secondo il Cremlino, l'estrema destra europea è ricettiva nei confronti di Mosca e ha un trend di popolarità in crescita.

La Russia ha inondato lo spazio informativo con narrazioni divisive e vettori di sostegno (persone o partiti politici) con visioni vicine al Cremlino (estremisti, nazionalisti, populistici, figure politiche anti-sistema, ecc.)

Tattiche, tecniche e procedure: Creazione e consolidamento di vaste reti di piattaforme online e canali/gruppi di social media; sviluppo di reti di sostegno pro-Cremlino, che agiscono poi come vettori per promuovere le narrazioni russe, con particolare attenzione agli opinionisti locali con visibilità/visioni euroscettiche; diversificazione dei metodi per aggirare le misure occidentali; organizzazione di eventi culturali dedicati ai valori/politiche russe; estrapolazione dal contesto di dichiarazioni di funzionari europei; alimentazione di teorie cospirative; creazione di contenuti deepfake per diffamare candidati scomodi.

Lo schema di diffusione/amplificazione degli ammassi arabi decentralizzati: satelliti locali pro-russi, cloni di siti web affidabili, account/canali e reti di troll su piattaforme di social media;

Obiettivo: amplificare i timori della popolazione sul deterioramento della situazione della sicurezza; minare la fiducia nell'autorità screditando i leader europei, i funzionari/partiti al governo e vittimizzando l'opposizione (tesi dell'"Europa totalitaria"); evidenziare l'impatto negativo dei politici/delle decisioni sulla situazione socio-economica; rafforzare la posizione dei leader/forme euroscettiche ed estremiste; erodere il sostegno politico e sociale all'Ucraina; amplificare il malcontento sociale;

- sfruttando la passività delle autorità per creare breccie nell'opinione pubblica.

- Nelle elezioni moldave sono state osservate tecniche di manipolazione dell'informazione su misura per gruppi demografici (ad esempio nazionalisti, comunità religiose, popolazione rurale, cittadini vulnerabili), con l'utilizzo di videoclip virali e immagini emotive per provocare forti reazioni negative. I narafive si alternano in base agli sviluppi politici, garantendo la pertinenza, e i messaggi inviati su Telegram, Facebook, Instagram, TikTok e VKontakte sono coordinati e uniformi.
- La Romania è percepita dai centri decisionali di Mosca come uno stato nemico ("neprieten"), e la Secondo i nostri dati, Mosca sta attivamente scoraggiando la Romania.

Nella visione della Russia, il nostro Paese:

"sfida e minaccia" la sicurezza della Russia ospitando il potenziale militare della NATO e degli Stati Uniti;
"vuole risolvere i suoi problemi economici a spese della Russia" (questione del Tesoro); è un concorrente diretto della Moldavia.

La Romania - insieme ad altri Stati del fianco orientale della NATO - è diventata una priorità per le azioni ostili della Russia, con un crescente interesse del Cremlino a influenzare (almeno) l'umore e l'agenda della società rumena in vista delle elezioni:

Propaganda e disinformazione (anche attraverso l'uso di tecnologie emergenti in attività mirate a gruppi e comunità specifiche, ad esempio aggregando dati pubblicamente disponibili - ad esempio preferenze politiche, economiche e di consumo dei media - e impiegando moduli di intelligenza artificiale generativa in grado di fornire messaggi di propaganda su misura, in tempo reale, a livello individuale);

sostenendo candidati euroscettici e alimentando i movimenti anti-sistema, anche attraverso "il loro coinvolgimento in proteste che contribuiranno a smuovere l'agenda pubblica";

Incoraggiare il malcontento/causare reazioni emotive tra la popolazione per fare pressione sulle autorità affinché riducano/interrompano il sostegno all'Ucraina.

Riteniamo che la Romania sia un obiettivo per le azioni ibride aggressive della Russia, compresi gli attacchi informatici.

hack, fughe di notizie e sabotaggi.

Si noti che quest'anno la situazione politica in Romania è stata discussa anche nei talk-show - i giornalisti russi lanciano l'idea che le forze filorusse in Romania potrebbero ottenere più del 30% alle elezioni parlamentari.

- L'analisi del modo in cui l'apparato di propaganda russo ha preso di mira la Romania nel 2024 evidenzia un approccio:

- indirettamente, attraverso l'adesione alla NATO/UE e in relazione al sostegno all'Ucraina e alla R. Moldova, i cui riferimenti sono stati attivati dagli sviluppi di questi temi/spazi;

direttamente, attraverso operazioni informative nel contesto di una crescente "minaccia Romania".

La "minaccia dell'UE alla sicurezza della Russia" dovuta all'espansione della NATO sul fianco orientale, le violazioni dello spazio aereo nazionale da parte di droni russi e la disinformazione sui cosiddetti rifugiati ucraini che chiudono i magazzini sul territorio nazionale.

de I messaggi riguardavano: (i) la divisione della società su questioni come il controllo esercitato SUH NATO

de sulla Romania, le minacce alla sicurezza poste dall'adesione NATO și de

il sostegno dato a Kiev; (ii) screditare la capacità di risposta della NATO e della **Romania**, amplificando la sfiducia della popolazione nella capacità di difesa nazionale; (iii) erodere il sostegno della popolazione alle decisioni di politica estera della Romania; (iv) evidenziare il coinvolgimento della Romania nei conflitti e le ambizioni territoriali in relazione agli Stati vicini (ad esempio, Ucraina e Moldavia).

Il caso delle **operazioni di informazione** che hanno preso di mira direttamente la Romania, il modus operandi è stato simile ad altre azioni di propaganda lanciate nello spazio europeo dall'inizio della guerra in

stiriUcraina: la stessa **strategia** per fabbricare e convalidare i falsi (tramite il conto falso multimediali e ampi dettagli falsi), l'uso di metodi simili per divulgare e far girare **i contenuti** (stessa fonte originale; stessi account coinvolti nella divulgazione del messaggio; stesso pubblico) e il collegamento fuorviante degli eventi con vettori ucraini (rifugiati o movimento **desistenza**).

Tattiche, tecniche e procedure:

i) l'uso di materiale video di cui non si conosce la veridicità - registrazioni di presunti incidenti (che non contengono elementi di identificazione visibili, la fonte iniziale o il luogo in cui sono stati girati i video non possono essere identificati), accompagnate da esagerazioni sulla loro portata; foto tratte da vecchi articoli della stampa locale e manipolate (ad esempio, ritagliando la data di un'immagine che mostra un incendio del 31 luglio 2024 a Bragadiru);

ii) La rootolizzazione di massa di Across-Oostinin0 attraverso all'incirca gli stessi account su più social network (X, Telegram, Facebook) - sono stati impegnati: vettori di propaganda russa rivolti al pubblico russo, tra cui scienziati politici o account associati alle chiese, account (pro)russi dedicati all'insabbiamento della guerra in Ucraina e contuñ con alta visibilità nello spazio europeo (ad esempio pubblico in inglese, francese, tedesco, bulgaro, spagnolo), ma anche tra il pubblico arabo e cinese.

Tali **azioni** informative conferiscono credibilità alle notizie gravi sugli incidenti di sabotaggio (veri o falsi che siano), generano panico e sfiducia nelle autorità e manipolano la mente collettiva (soprattutto il pubblico alfabetizzato ai media) per attribuire la responsabilità al vettore ucraino fin dall'inizio.