

# România, în prima linie a războiului cu dezinformările Kremlinului

Marius Bâtcă

Observatorul Militar Nr.17/2020



Autoritățile de la București au avertizat Bruxellesul asupra necesității unei coordonări eficiente și rapide între statele membre și în relația acestora cu instituțiile europene, precum și a unei comunicări publice adecvate care să permită combaterea acțiunilor de dezinformare și informarea corectă a cetățenilor și a mediului de afaceri, în plină criză provocată de pandemia Covid-19. În România, mai multe publicații electronice au fost suspendate, din cauza răspândirii de fakenews de proveniență rusească. În același timp, Serviciul Român de Informații trage un semnal de alarmă legat de siguranța datelor bancare. Secretarul de stat pentru Afaceri Europene, Iulia Matei, a participat, în cursul săptămânii trecute, la reuniunea informală a miniștrilor și secretarilor de stat pentru afaceri europene din statele membre ale Uniunii Europene, care s-a desfășurat prin sistem video-conferință,

informează Ministerul Afacerilor Externe. Oficialul român a subliniat necesitatea comunicării eficiente a măsurilor adoptate la nivel UE și asupra competențelor care revin instituțiilor europene în gestionarea crizei actuale, provocate de noul coronavirus. De asemenea, secretarul de stat român a arătat că respectarea valorilor și drepturilor fundamentale, precum și solidaritatea între statele membre, contribuie, cu atât mai mult în contextul unei situații de criză, la menținerea relevanței și valorii-adăugate a Uniunii Europene. Potrivit MAE, reuniunea a fost dedicată discutării măsurilor adoptate la nivelul Uniunii Europene și de statele membre pentru gestionarea crizei generate de pandemia Covid-19, inclusiv sub aspectul schimbului de bune practici între statele membre în gestionarea crizei.

Avertismentul României vine în contextul în care, la nivel comunitar și aliat transatlantic, se amplifică eforturile de combatere a dezinformărilor care au scopul de a panica populația și de a slăbi încrederea în măsurile adoptate de autoritățile competente, prin intermediul bombardării cu știri cu tentă conspiraționistă, lipsite de orice fundament științific și, de cele mai multe ori, în afara logicii bunului-simț.

### **Amplificarea teoriilor conspiraționiste**

Uniunea Europeană a identificat multiplicarea în manieră coordonată și o convergență trilaterală a narativelor de dezinformare promovate de China, Iran și Federația Rusă privind pandemia de coronavirus. Potrivit unui document intern comunitar, citat de *Radio Europa Liberă* și datat 20 aprilie, Rusia și, într-o mai mică măsură, China continuă să amplifice teorii conspiraționiste țintite pe publicul european, dar și pe cel din vecinătatea apropiată, cum ar fi Republica Moldova, Ucraina și Georgia. Surse oficiale ruse și media de stat desfășoară, în continuare, o campanie coordonată menită să afecteze Uniunea Europeană și răspunsul în situații de criză și să împrăștie confuzie privind implicațiile SARS-CoV2 asupra sănătății. Cea mai mare parte a conținutului identificat ca fiind fals și puternic înșelător persistă pe rețelele sociale, cum ar fi *Facebook* sau *Twitter*, indiferent de limbile folosite, căpătând aspect *viral*, chiar dacă, deja, fusese demontat de autorități și marcat ca atare de instituțiile de avertizare locale. Documentul a fost redactat de divizia de comunicare strategică a Serviciului European de Acțiune Externă, reprezentând o continuare a raportului precedent din luna aprilie.

Site-uri pline de *fakenews*, suspendate de ANCOM Mai multe site-uri din România au fost închise de Agenția Națională pentru Reglementare în Comunicații (ANCOM), ca urmare a faptului că, prin publicarea unor serii de articole, au răspândit informații false cu privire la pandemia de Covid-19. Măsura a fost luată în conformitate cu prevederile Decretului de prelungire a stării de urgență pe teritoriul României nr. 240/2020, care menționează, printre altele, că: *Furnizorii de servicii de găzduire și furnizorii de conținut sunt obligați ca, la decizia motivată a Autorității Naționale pentru Administrare și Reglementare în Comunicații, să întrerupă imediat, cu informarea utilizatorilor, transmiterea într-o rețea de comunicații electronice ori stocarea conținutului, prin eliminarea acestuia la sursă, dacă prin conținutul respectiv se promovează știri false cu privire la evoluția Covid-19 și la măsurile de protecție și prevenire.*

Printre site-urile închise pentru răspândirea de *fakenews* se numără: *stiridemoment.ro*; *breackingnews.xyz*; *romania-veche.ro*; *bpnews.ro*; *justitiarul.ro* și *ortodoxinfo.ro*. Cel din urmă nu are nicio legătură cu Biserica Ortodoxă Română și s-a făcut remarcant, chiar și înainte de pandemie, prin răspândirea dezinformărilor dictate de la Moscova. După cum se poate observa, chiar și numai din seria de titluri, site-urile menționate au selectat și preluat trunchiat declarații și informații pe care, potrivit Grupului de Comunicare Strategică și ANCOM, *le-au titrat în formulări și exprimări alarmiste, menite să genereze panica în rândul cetățenilor*. Astfel, au fost diseminate următoarele titluri false: *Se închid de luni Kaufland, Auchan, Metro, Carrefour și Lidl*; *ATENȚIE: TRUC & ÎNȘELĂCIUNE SAU ANTENELE 5G ȘI COVID?*; *Europe Defender 20 sau începuturile unui nou război mondial?*; *Adevărul din spatele virusului: Armata americană și Defender Europe 20* etc.

Însă, una dintre cele mai grave dezinformări a venit prin intermediul site-ului *ortodoxinfo.ro*, care a titrat: *Se pregătește omorârea pensionarilor în lagăre de concentrare și exterminare*. În mod evident, astfel de titluri sunt false și nici nu au legătură cu deciziile anunțate oficial de entitățile la care fac referire. Iar potrivit Grupului de Comunicare Strategică, diseminarea unor astfel de *fakenews* poate genera comportamente sociale neadecvate și disproporționate cu situația reală.

### Recomandările specialiștilor

*Recomandăm verificarea conturilor bancare pentru a depista eventualele accesări neautorizate. În cazul în care aveți suspiciuni de infectare a dispozitivului mobil, sunt indicate următoarele măsuri: resetarea dispozitivului prin revenire la setările din fabrică și schimbarea credențialelor pentru autentificarea în dispozitiv și în aplicații. Preventiv, pentru a asigura securitatea dispozitivelor mobile, este recomandată evitarea accesării link-urilor sau a atașamentelor provenite din surse necunoscute, se precizează în avertismentul Serviciului Român de Informații.*

### Capacitatea de apărare a NATO, neafectată

În ciuda încercărilor Moscovei de a transforma criza coronavirusului într-o criză de securitate, pandemia provocată de Covid-19 nu a diminuat capacitățile Alianței Nord-Atlantice de a se apăra.

Concluzia aparține secretarului general al NATO, Jens Stoltenberg, și președintelui polonez, Andrzej Duda, care au discutat săptămâna trecută, într-o videoconferință. *Pandemia nu are niciun efect asupra capacităților noastre de apărare și descurajare. (...) Polonia și celelalte țări din NATO se pot simți deplin protejate de sistemul aliat*, a declarat, ulterior, Krzysztof Szczerski, șeful de cabinet al președintelui polonez. Potrivit sursei oficiale citate, Andrzej Duda și Jens Stoltenberg au dezbătut și chestiuni legate de *fakenews*, în această criză, cei doi afirmând că *una dintre sarcinile actuale ale NATO este combaterea dezinformării despre pandemie*. Potrivit părții poloneze, *în afară de amenințarea epidemiologică, asistăm astăzi și la*

*tentative de a trage avantaje de pe urma situației actuale pentru a răspândi informații false ce subminează Alianța, securitatea țărilor individuale, în scopul reducerii moralului NATO.*

De asemenea, tot în cursul săptămânii trecute, ministrul apărării din Lituania, Raimundas Karoblis, a anunțat că a primit un e-mail *fake*, în care se anunța retragerea forțelor Alianței Nord-Atlantice din țara sa, transmite Agerpres. Mesajul, trimis în numele secretarului general al NATO, Jens Stoltenberg, a fost expediat și la unele publicații și televiziuni lituaniene, precum și unor oficiali de la sediul Alianței din Bruxelles. *Este o nouă încercare de a transforma criza coronavirusului într-o criză de securitate*, a afirmat oficialul lituanian. *Această informație falsă urmărește discreditarea aliaților NATO și organizația însăși*, a adăugat Raimundas Karoblis.

O unitate multinațională, formată din circa 450 de militari și condusă de Germania, este staționată la baza militară Rukla din centrul Lituaniei, în cadrul eforturilor vizând asigurarea flancului estic al NATO. Armata lituaniană a menționat că au fost constatate, în ultimele luni, *o serie de tentative consecvente de a răspândi informații false legate de pandemia de Covid-19, generată de noul coronavirus SARS-CoV-2*. De altfel, focarul de coronavirus din rândul trupelor NATO din Lituania a fost lichidat complet, a declarat, la 24 aprilie, ministrul apărării Raimundas Karoblis. Peste 20 de militari de la baza Rukla din centrul Lituaniei au fost infectați cu noul coronavirus. Printre cei testați pozitiv s-au aflat și militari germani. Anterior, în cursul acestei luni, șase soldați germani infectați cu noul coronavirus au fost repatriați pe cale aeriană, din Lituania. Anterior, Germania și Croația au trimis personal medical suplimentar în Lituania, în cadrul eforturilor aliate de luptă cu pandemia.

### ***SRI: În plină pandemie Covid-19, campanie de furt de date bancare***

În contextul asociat pandemiei de SARS-CoV-2 a fost identificată o campanie de distribuire de malware care vizează furtul de credențiale bancare de pe terminalele mobile ale utilizatorilor, anunță Serviciul Român de Informații. Din punct de vedere tehnic, acțiunea ilicită are la bază distribuirea unui mesaj tip text care conține o versiune nouă a troianului *Cerberus Android Banker*. Mesajul este redactat în limba română și invită utilizatorii să acceseze un link pentru descărcarea de informații privind SARS-CoV2. Sintagma utilizată în conținutul mesajului este *Detalii secrete! (Covid-19)*.

Link-ul inițiază descărcarea unui fișier denumit *File.apk*) care infectează cu respectivul troian dispozitivele mobile cu sisteme de operare *Android*, versiunile cuprinse între 4.0 și 10. Funcționalitățile *Cerberus Android Banker* împiedică atât detectarea acestuia de serviciul *Play Protect* specific *Android*, cât și dezinstalarea ulterioară a aplicației de utilizator. Principalul pericol este acela că troianul oferă acces ilicit la date din aplicațiile bancare. De asemenea, *Cerberus Android Banker* poate extrage date despre aplicațiile de mesagerie și poștă electronică instalate pe dispozitivul vizat (spre exemplu, *Telegram*, *WhatsApp* sau *Gmail*), precum și jurnalizarea apăsărilor de taste și exfiltrarea datelor astfel obținute. Acesta permite de asemenea colectarea și redirecționarea SMS-urilor și a poștei electronice, efectuarea sau redirecționarea de apeluri, colectarea listei de contacte și a istoricului apelurilor, precum și monitorizarea locației dispozitivului.