CONFLICTELE/OPERAȚIILE INFORMAȚIONALE ALE FEDERAȚIEI RUSE ÎN CONTEXTUL *SARS-CoV-2*

Maior Petre SCÎRLET

Universitatea Națională de Apărare „Carol I", București

Lect. univ. dr. Cristian ICHIMESCU

Universitatea Națională de Apărare „Carol I", București

Evenimentele de mare impact global, precum pandemia Covid-19, apar foarte rar – probabil de câteva ori în decursul unui secol – și produc, printre altele, schimbări majore la nivel geopolitic, vizând alianțe, blocuri politice, regiuni, state și zone de influență.

Pandemia Covid-19 a afectat într-un timp scurt întreaga lume, iar libertatea personală a miliarde de oameni a fost îngrădită într-un mod fără precedent. Cu toate acestea, pandemia nu a înghețat diferendele existente între diverse state ale lumii.

Deși este nevoie de un răspuns global împotriva crizei coronavirusului SARS-CoV-2, Federația Rusă nu consideră că este în interesul său să contribuie în acest demers – și, de fapt, Kremlinul se folosește de criză pentru a destabiliza și mai mult lumea.

Astfel, concomitent cu virusul, cu aceeași repeziciune, se extinde în întreaga lume și o cantitate enormă de date și informații, multe dintre acestea fiind parte a unei ample campanii de influențare a opiniei publice prin conflicte/operații informaționale planificate și executate de autoritățile ruse.

Cadrul global creat prin extinderea pandemiei a reprezentat momentul operativ identificat de Kremlin pentru a pune în aplicare, din nou, mașinăria complexă reprezentată de conflictele informaționale/operațiile informaționale, care au devenit, astfel, cea mai complexă formă de confruntare modernă.

Cuvinte-cheie: activități informaționale, Covid-19, dezinformare, infodemie, operații cibernetice.

CE SUNT CONFLICTELE/OPERAȚIILE INFORMAȚIONALE CONTEMPORANE?

Doctrina operațiilor informaționale – S.M.G.-66 – din anul 2017 definește noțiunea de *operații informaționale* ca reprezentând *„o funcție de stat major destinată analizei, planificării, evaluării și integrării tuturor activităților informaționale în vederea obținerii efectelor dorite asupra voinței, capacității de înțelegere, percepției și capabilităților adversarilor, potențialilor adversari și a audiențelor țintă aprobate de Consiliul Suprem de Apărare a Țării, în sprijinul îndeplinirii obiectivelor militare”*[1].

În anul 2009, NATO, în cadrul doctrinei AJP-3.10, *Allied Joint Doctrine for Information Operations*, a definit *operaţiile informaţionale* ca fiind *„o funcţie a statului major de a analiza, a planifica, a evalua şi a integra activităţi informaţionale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor adversarilor, potenţialilor adversari şi audienţelor aprobate de NAC în sprijinul obiectivelor misiunii Alianţei”*[2].

Analizând definițiile prezentate, putem remarca o serie de similitudini. În viziunea celor două doctrine, operațiile informaționale se identifică prin *efectele* produse asupra a trei categorii distincte: voința; capacitatea de înțelegere și percepția; capabilități. În plus, din studierea doctrinelor menționate[3], operațiile informaționale se pun în practică prin executarea unor tipuri de activități, respectiv activități de influențare, activități împotriva conducerii și capabilităților de comandă și activități de protecție informațională.

În viziunea unor autori, pentru Federația Rusă, conceptul de conflict informațional implică *„operații în rețelele de calculatoare împreună cu operațiile psihologice, comunicare strategică, influențare”*[4]

NATO, în cadrul doctrinei Allied Joint Doctrine for Information Operations, a definit operaţiile informaţionale ca fiind „o funcţie a statului major de a analiza, a planifica, a evalua şi a integra activităţi informaţionale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor adversarilor, potenţialilor adversari şi audienţelor aprobate de NAC în sprijinul obiectivelor misiunii Alianţei”.

[1] S.M.G.-66, *Doctrina operațiilor informaționale,* București, 2017, p. 15.

[2] AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009, p. 1-3. (în original: *„is a staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives”*).

[3] AJP-3.10, *op. cit.*, p. 1-7, și S.M.G.-66, *op. cit.*, p. 21.

[4] Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, p. 7.

și *„informații, contrainformații, măsuri active, dezinformare, război electronic”*[5].

Putem sesiza, astfel, diferența dintre cele două accepțiuni (NATO/România vs. Federația Rusă) în sensul complexității conceptului abordat de către Kremlin, care reprezintă un concept extins, ce acoperă o gamă amplă și diversă de acțiuni. Astfel, observăm că, pentru Federația Rusă, toate domeniile formează o unitate sub conceptul de *information warfare (conflictul informațional)*, în timp ce NATO abordează conceptul *information operations (operații informaționale)*. Pe parcursul acestui articol, vom utiliza conceptul *conflictele/operațiile informaționale* pentru a caracteriza acțiunile informaționale ale Federației Ruse.

Pe tot parcursul Războiului Rece, strategia sovietică a apelat la o serie de așa-zise „măsuri active”, care descriu acțiuni și strategii menite să influențeze deciziile unui stat, populația acestuia și evenimentele politice, militare și sociale importante din statul respectiv.

O trăsătură a conflictelor/operațiilor informaționale derulate de Federația Rusă este caracterul ofensiv, care s-a regăsit în toate campaniile informaționale derulate de acest stat de-a lungul timpului împotriva diverșilor actori statali. În continuare, vom prezenta o scurtă istorie a conflictelor/operațiilor informaționale puse în practică de Federația Rusă prin utilizarea unor domenii importante, cum ar fi cel al dezinformării și al măsurilor active.

ISTORIA RUSEASCĂ A CONFLICTELOR/OPERAȚIILOR INFORMAȚIONALE

Ideile de bază pe care se susțin o parte din formele conflictelor/operațiilor informaționale derulate de Federația Rusă nu sunt noi, având origini încă din perioada Războiului Rece. Pe tot parcursul Războiului Rece, strategia sovietică a apelat la o serie de așa-zise *„măsuri active”*, care descriu acțiuni și strategii menite să influențeze deciziile unui stat, populația acestuia și evenimentele politice, militare și sociale importante din statul respectiv.

Afirmațiile conform cărora Statele Unite au comis atacuri cu arme biologice au fost acuzații comune din partea unor adversari precum URSS sau Cuba, prin care s-a încercat acreditarea ideii, la nivelul comunității internaționale, potrivit căreia Statele Unite au încălcat Convenția privind armele biologice.

[5] Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 martie 2011, http://www.rferl.org/articleprintview/2345202.html, accesat la 12 martie 2020, apud Keir Giles, *op. cit.*, p. 7.

În timp ce multe acuzații legate de arme biologice au pornit de la Kremlin, acestea au fost adesea amplificate de surse media din țările aliate ale URSS. Mass-media cubaneză a afirmat constant că Statele Unite au răspândit o varietate de maladii în perioada anilor 1970-1980. În paralel, autoritățile ruse au acuzat SUA de implicare în dezvoltarea pe teritoriul Pakistanului a unor specii deosebit de periculoase de țânțari, care urma să fie folosite pentru răspândirea rapidă a armelor biologice[6].

Acuzațiile aduse la adresa Statelor Unite în privința folosirii armelor biologice au fost o practică des utilizată de către adversarii din timpul Războiului Rece, însă cele mai insidioase două campanii au fost cele referitoare la Războiul din Coreea[7] și campania de dezinformare SIDA[8].

Se poate observa că, în perioada Războiului Rece, luând ca bază teoretică definiția NATO a operațiilor informaționale, URSS a utilizat preponderent *activități informaționale pentru a crea efectele dorite asupra înțelegerii şi capabilităţilor diferitelor audiențe*. De asemenea, observăm planificarea și executarea în special a activităților de influențare și a activităților de protecție informațională.

În perioada Războiului Rece, luând ca bază teoretică definiția NATO a operațiilor informaționale, URSS a utilizat preponderent activități informaționale pentru a crea efectele dorite asupra înțelegerii şi capabilităţilor diferitelor audiențe.

Acuzațiile privind armele biologice din jurul actualei pandemii cu virusul SARS-CoV-2 continuă linia specifică a conflictelor/operațiilor informaționale desfășurate de Uniunea Sovietică în timpul Războiului Rece, însă capacitățile de confruntare și obiectivele urmărite sunt mult mai complexe.

Federația Rusă conduce, în prezent, poate unele dintre cele mai ample și complexe conflicte informaționale din ultimii ani, care integrează secvențe de operații mass-media, manipulare, dezinformare, propagandă – albă, neagră și gri, operații în rețele sociale, operații cibernetice și cu implicarea întregului arsenal

---

[6] Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, ianuarie 2012, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618, accesat la 11 aprilie 2020.

[7] Pentru mai multe detalii, Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 aprilie 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/, accesat la 11 aprilie 2020.

[8] Vezi Douglas Selvage, Christopher Nehring, *Operation „Denver": KGB and Stasi Disinformation regarding AIDS*, 22 iulie 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids, accesat la 11 aprilie 2020, și Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*,19 noiembrie 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/, accesat la 11 aprilie 2020.

de instrumente specifice conflictului informațional, dintre care am aminti: acuzarea adversarului pentru săvârșirea unor atrocități, propaganda sau discreditarea propagandei adversarului, amplificarea exagerată a anumitor mize, invocarea protecției etc.

Toate capacităţile de confruntare enumerate sunt utilizate, dar dimensiunea dezinformării, alături de cea cibernetică, se detaşează faţă de celelalte forme.

CORONAVIRUSUL DEZINFORMĂRII – NOUL CONFLICT INFORMAȚIONAL RUS –

În această perioadă, un număr mare de oameni sunt închiși în case și petrec o mare parte din timp pe social media. Potrivit datelor, la sfârșitul lunii martie a.c., existau mai mult de trei miliarde de postări și peste 100 de miliarde de interacțiuni asupra *#covid19*, *#coronavirus* și similare[9].

Organizația Mondială a Sănătății a avertizat că lumea se confruntă în paralel cu două epidemii: una generată de noul coronavirus SARS CoV-2 și o a doua referindu-se la o așa-zisă „infodemie”, descriind acest fenomen ca o supra-abundență de știri mai mult sau mai puțin exacte.

Încă din data de 2 februarie a.c., Organizația Mondială a Sănătății (OMS) a avertizat că lumea se confruntă în paralel cu două epidemii[10]: una generată de noul coronavirus SARS CoV-2 și o a doua referindu-se la o așa-zisă *„infodemie”*, descriind acest fenomen ca o supra-abundență de știri mai mult sau mai puțin exacte.

Narațiunea propusă de vectorii Federației Ruse se referă, în principal, la alterarea spațiului public al țintelor vizate prin injectarea de dezinformare și propagandă. Concomitent, un alt pilon este acela al lobby-ului prin care se urmărește influențarea publicului-țintă prin idei vehiculate în spațiul public de către purtători de mesaj legitimi și credibili.

Nu în ultimul rând, se apelează la operaţii psihologice elaborate în care contează atât informaţia răspândită, cât, mai ales, efectul creat de informaţie în cadrul publicului-ţintă, respectiv naşterea şi crearea sau accentuarea fricilor, crearea emoţiilor colective, pregătirea publicului pentru a reacţiona la viitoare evenimente într-o formulă dirijată.

Fluxurile narațiunii Federației Ruse

Narațiunile rusești pot fi împărțite în trei categorii: o așa-zisă dezinformare de bază, dezinformarea complexă și propaganda elaborată.

---

[9] Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31.03.2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381, accesat la 13 aprilie 2020.

[10] OMS a ridicat nivelul epidemiei Covid-19 la rangul de pandemie la data de 11 martie 2020.

Dezinformarea de bază constă în cele mai puțin sofisticate tipuri de dezinformare. Aceste abordări vizează publicul cel mai puțin informat din masele rusești și nu numai, printre care sentimentul anti-american este puternic din punct de vedere istoric și ușor de inflamat. Instrumentele utilizate includ platforme de dezinformare, bloggeri, precum și conturi utilizate de către rușii care trăiesc în SUA, Canada și UE. Pentru acest public-țintă, propagandiștii ruși folosesc în mod deliberat un limbaj nesofisticat și argumente primitive, dar convingătoare, simple[11].

Dezinformarea complexă promulgă idei similare, dar îmbrăcate diferit. Această abordare se bazează pe teorii ale conspirației elaborate, care au ca scop crearea așa-numitei realități alternative și încercarea de a promova neîncrederea în rândul publicului străin. Platformele de informare din Rusia folosesc *„dovezi"* pseudoștiințifice că virusul a fost creat într-un laborator american pentru a opri creșterea economică a Chinei[12].

Dezinformarea complexă promulgă idei similare, dar îmbrăcate diferit. Această abordare se bazează pe teorii ale conspirației elaborate, care au ca scop crearea așa-numitei realități alternative și încercarea de a promova neîncrederea în rândul publicului străin.

Iar cea de-a treia categorie prezintă un exemplu de *propagandă elaborată*, concepută pentru cercuri foarte înguste din afara Federației Ruse. În acest caz, statul rus se bazează pe oameni de știință proeminenți proprii și, uneori, apelează și la surse străine (în principal, chineze). Potrivit teoriilor acestora, *„coronavirusul ... a devenit sfârșitul lumii moderne"*[13]. Se susține faptul că ordinea mondială stabilită după Războiul Rece se prăbușește acum și face loc unei noi perioade, în care vor apărea noi lideri.

„Dezinformarea se joacă cu viețile oamenilor. Dezinformarea poate să ucidă" – susținea, într-o conferință de presă, în a doua decadă a lunii martie a.c., Josep Borrell, directorul Serviciului European de Acțiune Externă. Acest joc periculos a debutat la începutul anului curent și s-a dezvoltat gradual.

---

[11] *NATO uses COVID-19 to mobilise Western military forces against Russia*, 19.03.2020, Interviu cu Alexander Artamonov, realizat de Agenția de știri Novorossia, https://novorosinform.org/808651, accesat la 13 aprilie 2020.

[12] Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13.02.2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/, accesat la 14 aprilie 2020.

[13] Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 05.04.2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship, accesat la 14 aprilie 2020 (în original, *„Coronavirus... has become the end of the modern world").*

Prima dezinformare înregistrată pe tema Covid-19 a apărut în *Sputnik News*, pe 22 ianuarie[14], când a fost publicat un articol potrivit căruia virusul a fost creat de om, o armă creată de NATO[15].

Potrivit unui studiu efectuat de EUvsDisinf[16], analizând articolele publicate în mass-media străine între 22 ianuarie și 25 martie a.c. pe tema Covid-19, ținta predilectă rămân SUA, 39 de articole fiind îndreptate către acestea, articole în care se susține că SUA au creat virusul SARS-CoV-2. A doua cea mai comună narațiune, cu 26 de articole publicate, este că UE nu reușește să facă față crizei și, ca urmare, se dezintegrează, împreună cu spațiul Schengen. În special, această narațiune a eșecului și a lipsei de solidaritate a UE este în trend după acordarea ajutorului rusesc în Italia. Narațiunea că virusul este folosit ca o armă împotriva Chinei și economia sa vine pe locul al treilea, cu 24 de articole. Pe locul patru este narațiunea că întreaga criză coronavirus este un plan secret al elitei globale, cu 17 articole[17].

În domeniul militar, dezinformarea a vizat exercițiul multinațional „Defender Europe 2020". Conducerea rusă a criticat exercițiul ca fiind un „scenariu anti-rus" ofensiv, dar apoi a folosit propaganda pentru a răspândi teoria potrivit căreia, prin desfășurarea exercițiului, s-ar putea facilita răspândirea virusului SARS-CoV-2 în Europa din cauza sosirii și mișcării unui număr mare de trupe.

În domeniul militar, dezinformarea a vizat exercițiul multinațional *Defender Europe 2020*. Conducerea rusă a criticat exercițiul ca fiind un *„scenariu anti-rus"* ofensiv[18], dar apoi a folosit propaganda pentru a răspândi teoria potrivit căreia, prin desfășurarea exercițiului, s-ar putea facilita răspândirea virusului SARS-CoV-2 în Europa din cauza sosirii și mișcării unui număr mare de trupe.

Canale utilizate

Pentru atingerea obiectivelor, Moscova dispune de o serie de vectori de propagare a mesajelor, care pot fi împărțiți astfel:

1. Mass-media tradițională (trustul *Russia Today*, care deține și postul de televiziune *Russia Today* și proiectul *Sputnik*, *Pervy Kanal*);

---

[14] *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/, accesat la 14 aprilie 2020.

[15] *A new Chinese coronavirus was likely elaborated in NATO biolabs*, https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/, accesat la 14 aprilie 2020.

[16] *EuvsDisinfo*, din cadrul East StratCom Task Force, este proiectul Serviciului European de Acțiune Externă. Aceasta a fost înființată în 2015, pentru a răspunde campaniilor de dezinformare ale Federației Ruse care afectează Uniunea Europeană. Pentru mai multe informații, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en, accesat la 14 aprilie 2020.

[17] *Ibidem.*

[18] *The US Defender 2020 military manoeuvre is explicitly directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia, după Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen*, https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title, accesat la 14 aprilie 2020.

2. Mediul virtual (armata de troli a Kremlinului) – structuri specializate în activități pe platforme de blog, producție de știri, crearea de imagini și conținut denigrator pentru subminarea unei anumite ținte, producția de conținut video și redactarea de comentarii pro-Kremlin postate în medii virtuale. Conform unui raport pregătit pentru Global Engagement Center[19] din cadrul Departamentului de Stat al SUA, s-a observat utilizarea unor conturi controlate de statul rus și utilizate inițial pentru influențarea evenimentelor specifice conflictului din Siria și grevelor extinse din Franța, pentru a posta, în prezent, mesaje legate de pandemia coronavirus.
   Potrivit Departamentului de Stat, în momentul în care mass-media rusă a început să difuzeze articole și interviuri antioccidentale despre originile virusului SARS-CoV-2, conturile ruse au început să le promoveze pe plan mondial, acoperind peste 20 de limbi – de la engleză la rusă și de la sârbă la arabă.
3. Implicarea unor personaje influente din Federația Rusă, formatori de opinie aserviți Kremlinului. Evident, în acest tablou nu putea lipsi unul dintre cei mai influenți gânditori geopolitici ai Federației Ruse, Alexander Dughin, un naționalist rus și un susținător foarte activ al Bisericii Ortodoxe, care a avansat ideea că, atunci când virusul își va termina marșul victoriei pe întreaga planetă, va fi distrusă ordinea mondială existentă. Este de notorietate faptul că mesajele acestuia se înscriu în agenda propagandei ruse, intens promovată în ultimii ani, fiind unul dintre principalele instrumente pe care aceasta construiește, promovează și dezvoltă elementele constitutive ale unei imagini de marcă a Federației Ruse.
4. ONG-uri, think-tank-uri și alte platforme de discuții al căror scop este de a disemina propaganda rusă.
5. Și, nu în ultimul rând, am aminti implicarea serviciilor de informații ruse în promovarea de mesaje în sprijinul politicii externe ruse la nivelul țărilor membre ale UE. Acestea folosesc jurnaliști independenți, ziariști, ONG-uri și institute de cercetare.

Conform unui raport pregătit pentru Global Engagement Center din cadrul Departamentului de Stat al SUA, s-a observat utilizarea unor conturi controlate de statul rus și utilizate inițial pentru influențarea evenimentelor specifice conflictului din Siria și grevelor extinse din Franța, pentru a posta, în prezent, mesaje legate de pandemia coronavirus.

[19] Lea Gabrielle, *Briefing on Disinformation and Propaganda Related to COVID-19*, https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19, accesat la 14 aprilie 2020.

Dacă, în privința americanilor, conflictele informaționale derulate de Federația Rusă urmăresc destabilizarea și discreditarea Statelor Unite pe plan european, profitând de incapacitatea SUA de a-și ajuta aliații, pentru Uniunea Europeană agenda este una mai complexă, vizând subminarea coeziunii prin cultivarea unor concentrări a activităților informaționale asupra unor țări membre ale UE.

În acest context, Moscova a încercat anihilarea mișcărilor de imagine ale Chinei de a trimite ajutor Italiei și Spaniei și a acționat pentru a revendica toată publicitatea și beneficiile.

Din Rusia, cu dragoste...

Ajutorul Moscovei pentru Italia în legătură cu coronavirusul a fost acoperit pe scară largă, atât în presa internațională[20], cât și în cea rusă. Italia a salutat cu recunoștință sosirea unui avion chinez – în prezența președintelui italian și a ambasadorului chinez –, care a transportat medici și echipamente. Mass-media de stat rusă a prezentat situația din Italia în contextul luptei pe care această țară o poartă pentru limitarea răspândirii coronavirusului, în moduri diferite.

La Radio Vesti FM, controlat de Kremlin, publicului i s-a spus că epidemia coronavirusului va forța Italia să părăsească UE. Anterior, Sputnik, controlat tot de Kremlin, a promovat teoria conspirației conform căreia coronavirusul ar fi putut fi creat pentru a limita povara economică a cetățenilor pensionați din bugetul Italiei.

La *Radio Vesti FM*, controlat de Kremlin, publicului i s-a spus că epidemia coronavirusului va forța Italia să părăsească UE[21]. Anterior, *Sputnik*, controlat tot de Kremlin, a promovat teoria conspirației conform căreia coronavirusul ar fi putut fi creat pentru a limita povara economică a cetățenilor pensionați din bugetul Italiei[22].

Sputnik i-a acuzat, de asemenea, pe membrii Parlamentului European că doresc să lanseze o campanie împotriva ajutorului rusesc pentru Italia, când, în realitate, au cerut să analizeze campaniile de dezinformare și utilizarea geopolitică a ajutorului.

Totodată, în mass-media rusă a fost intens promovat un videoclip în care un cetățean italian a înlocuit steagul Uniunii Europene cu cel al Rusiei, vehiculând, în mod fals, ideea că acest curent este unul

[20] Potrivit unei analize efectuate de cotidianul italian *La Stampa*, aproximativ 80% din proviziile trimise de Rusia sunt *„inutile”*, Jacopo Iacoboni, *La Stampa*, 25 martie 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: „Più che aiuti arrivano militari russi in Italia”*, https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327, accesat la 15 aprilie 2020.

[21] *Coronavirus: BBC Challenges Pro-Kremlin Reporting from Italy*, 1 aprilie 2020, https://euvsdisinfo.eu/coronavirus-bbc-challenges-pro-kremlin-reporting-from-italy/, accesat la 15 aprilie 2020.

[22] *Ibidem*.

generalizat. Un reporter al televiziunii britanice *BBC* a contactat respectivul cetățean italian pentru solicitarea unui punct de vedere în care a precizat că a decis ridicarea mai multor steaguri ale Federației Ruse în afara magazinului pe care îl deține pentru a-și exprima recunoștința față de Rusia!

Un alt videoclip care a fost distribuit în presa pro-Kremlin arată imnul Federației Ruse intonat în Italia. Printre publicațiile rusești care au transmis videoclipul s-au numărat rețeaua controlată de stat *Rossiya 1* și canalul de televiziune pro-Kremlin *REN TV*, a cărui poveste a fost prezentată online sub titlul: *„Imnul Rusiei a sunat pe străzile Italiei"*[23].

Mass-media rusă nu a explicat nici că muzica din videoclip apare din interiorul biroului unei organizații pe care articolul *BBC* o descrie ca *„neofascistă"* și nici că persoana din spatele videoclipului este un activist care are legături cu Rusia.

În articolul său, *BBC* a demonstrat că două videoclipuri diferite cu imnul Rusiei, care au circulat în mass-media rusă, sunt, de fapt, înregistrări ale aceluiași eveniment, dar din unghiuri diferite.

Concomitent cu ajutorul acordat, Italia a fost și ținta unor atacuri cibernetice, ca, de altfel, întreaga Europă.

Infractorii cibernetici profită de timpul tot mai mare pe care oamenii îl petrec online din cauza noilor măsuri luate de statele membre pentru a opri răspândirea virusului.

Operațiile cibernetice ruse

Operațiile cibernetice reprezintă unul dintre cele mai importante domenii din cadrul conflictului informațional pe care Federația Rusă îl desfășoară pe fondul pandemiei cu virusul *SARS-CoV-2*.

Președintele Comisiei Europene, Ursula von der Leyen, a avertizat, în data de 24 martie a.c., despre creșterea semnificativă a criminalității informatice din UE, în contextul extinderii pandemiei *Covid-19*[24]. Infractorii cibernetici profită de timpul tot mai mare pe care oamenii îl petrec online din cauza noilor măsuri luate de statele membre pentru a opri răspândirea virusului.

Primul grup de hackeri sponsorizat de Kremlin care a fost angajat pe acest front a fost grupul *Hades*[25], despre care există indicii

[23] *На улицах итальянских городов прозвучал гимн России*, 26 martie 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii, accesat la 15 aprilie 2020.

[24] *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis*, VOA News, 24 martie 2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus, accesat la 15 aprilie 2020.

[25] Cătălin Cîmpanu, *State-sponsored hackers are now using coronavirus lures to infect their targets*, 13 martie 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/, accesat la 16 aprilie 2020.

că funcționează în afara Federației Ruse, și o legătură cu gruparea APT28, unul dintre cele mai renumite grupări de spionaj cibernetic ale Federației Ruse. Potrivit companiei chineze de securitate cibernetică QiAnXin, hackerii Hades au desfășurat o campanie la jumătatea lunii februarie, când au ascuns un virus troian în documente care conțineau cele mai noi știri despre *Covid-19*. Documentele au fost trimise către ținte din Ucraina, deghizate în e-mailuri provenite de la Centrul de Sănătate Publică al Ministerului Sănătății din Ucraina[26].

În perioada pandemiei cu virusul SARS-CoV-2, luând ca bază teoretică definiția NATO a operațiilor informaționale, Federația Rusă a utilizat preponderent activități informaționale pentru a crea efectele dorite asupra voinței, înțelegerii şi capabilităților diferitelor audiențe. De asemenea, observăm planificarea și executarea activităților de influențare, a activităților împotriva conducerii și capabilităților de comandă, precum și a activităților de protecție informațională.

Și un raport al Europol[27] din cursul lunii martie confirmă cele deja enumerate, evidențiind faptul că, în această perioadă, infracțiunile cibernetice au crescut semnificativ. Europol monitorizează încă de la început impactul pandemiei *Covid-19* asupra peisajului criminalității informatice și a publicat o evaluare actualizată a amenințărilor cu privire la potențialele evoluții ulterioare în acest domeniu al criminalității.

Principalele constatări din această evaluare sunt: impactul pandemiei cu virusul *SARS-CoV-2* asupra criminalității informatice a fost cel mai vizibil în comparație cu alte activități infracționale; infractorii activi în domeniul criminalității informatice au fost capabili să se adapteze rapid și să valorifice anxietățile și temerile victimelor lor; campaniile de *phishing* și *ransomware* sunt lansate pentru a exploata criza actuală și se preconizează că vor continua să crească în domeniul de aplicare și la scară largă; atât organizațiile criminale, statele, cât și actorii susținuți de stat încearcă să exploateze criza sănătății publice pentru a promova interesele geopolitice[28].

Se poate observa că, în perioada pandemiei cu virusul *SARS-CoV-2*, luând ca bază teoretică definiția NATO a operațiilor informaționale, Federația Rusă a utilizat preponderent *activități informaționale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor* diferitelor audiențe. De asemenea, observăm planificarea și executarea activităților de influențare, a activităților împotriva conducerii și capabilităților de comandă, precum și a activităților de protecție informațională.

---

[26] *Ibidem.*

[27] *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*, 3 aprilie 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, accesat la 16 aprilie 2020.

[28] *Ibidem.*

CONCLUZII

Deși amenințarea generată de amploarea acestei pandemii este una reală și deloc de neglijat, Federația Rusă vede în această catastrofă o oportunitate de a promova și dezvolta planurile de executare a unor conflicte/operații informaționale împotriva Occidentului pe fondul pandemiei *Covid-19*.

Răspândirea virusului *SARS-CoV-2* a oferit un nou câmp de luptă, în care conflictele/operațiile informațiile constituie cea mai avansată armă, în prezent acestea beneficiind de o viteză de propagare mult mai rapidă, precum și de o rază de acțiune mare, contribuind decisiv la modelarea și influențarea rapidă atât a opiniilor, cât și a acțiunilor audiențelor țintă.

Răspândirea virusului SARS-CoV-2 a oferit un nou câmp de luptă, în care conflictele/ operațiile informațiile constituie cea mai avansată armă, în prezent acestea beneficiind de o viteză de propagare mult mai rapidă, precum și de o rază de acțiune mare, contribuind decisiv la modelarea și influențarea rapidă atât a opiniilor, cât și a acțiunilor audiențelor țintă.

O miză pentru Federația Rusă în acest context o reprezintă relaționarea cu Italia, care vine într-un moment în care această țară este vulnerabilă. Interesul tot mai mare al Federației Ruse în UE și oferirea ajutorului către Italia reprezintă elemente concrete de punere în practică a unor conflicte/operații informaționale împotriva UE și a țărilor membre.

Din analiza comparată a modului de punere în practică a domeniilor conflictelor/operațiilor informaționale din perioada Războiului Rece cu perioada specifică pandemiei cu virusul *SARS-CoV-2* se poate observa trecerea de la utilizarea parțială a unor activități informaționale specifice Războiului Rece la folosirea tuturor activităților informaționale *pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor* diferitelor audiențe. Tipologia mesajelor utilizate nu este una nouă, însă, ce este diferit acum este executarea conflictelor/operațiilor informaționale din ce în ce mai intruzive și utilizarea acestora nu doar pentru destabilizarea SUA, ci și a Uniunii Europene.

De asemenea, considerăm că este probabil ca acțiunile subsumate conflictelor/operațiilor informaționale, derulate de Federația Rusă, *să se intensifice și să se dezvolte*, căutând să identifice noi vulnerabilități, având în vedere măsurile de contracarare deja întreprinse de autoritățile Uniunii Europene, precum și de către SUA.

În contextul în care Federația Rusă investește masiv în programe de cercetare privind inteligența artificială, specialiștii în securitate descriu deja noul concept de *știri false*, care va fi inițiat de capacitatea tehnologică a inteligenței artificiale de a reproduce fidel vocea individului, ca ființă umană, ca fiind un nou domeniu al conflictelor/ operațiilor informaționale ale viitorului.

BIBLIOGRAFIE:

1. ***, AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
2. ***, S.M.G.-66, *Doctrina operațiilor informaționale*, București, 2017.
3. Cătălin Cîmpanu, *State-sponsored hackers are now using coronavirus lures to infect their targets*, 13 martie 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/
4. Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 5 aprilie 2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship
5. Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 aprilie 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/
6. Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016.
7. Jacopo Iacoboni, *La Stampa*, 25 martie 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327
8. Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*, 19 noiembrie 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/
9. Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618
10. Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 martie 2011, http://www.rferl.org/articleprintview/2345202.html
11. Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13 februarie 2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/
12. Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 iulie 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids
13. Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31 martie 2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381

14. *A new Chinese coronavirus was likely elaborated in NATO biolabs,* https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/
15. *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*, 3 aprilie 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
16. *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/
17. *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis,* VOA News, 24 martie 2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus
18. *На улицах итальянских городов прозвучал гимн России*, 26 martie 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii
19. *NATO uses COVID-19 to mobilise Western military forces against Russia*, 19 martie 2020, Interviu cu Alexander Artamonov, realizat de Agenția de știri Novorossia, https://novorosinform.org/808651
20. *The US Defender 2020 military manoeuvre is explicitly directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia după Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen,* https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title.