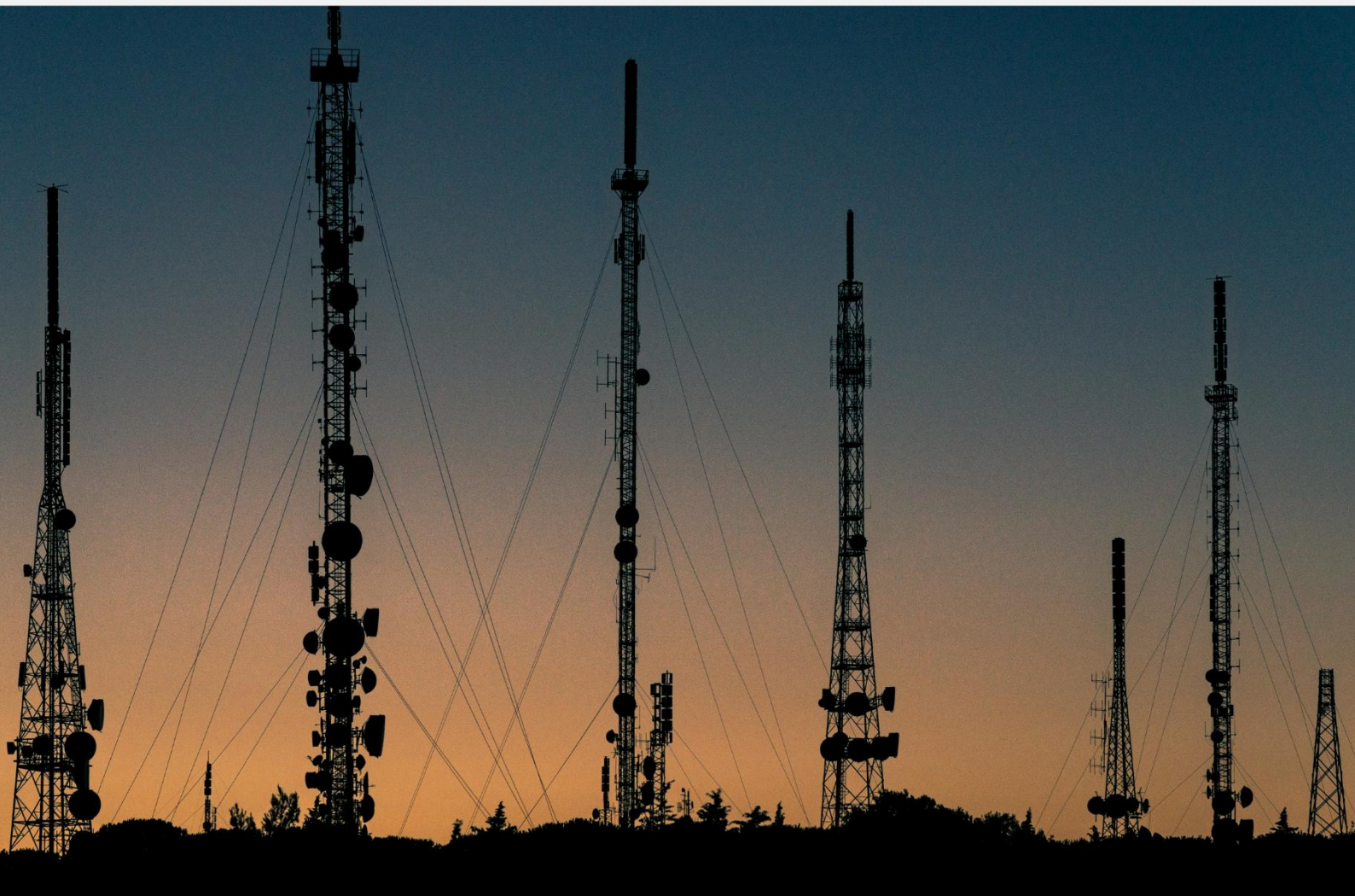


IDR

Romanian Diplomatic Institute



POLICY PAPER

nr. 43/2025

TAIFUNURI, URȘI ȘI PANDA. ULTIMELE CAMPANII MAJORE DE SPIONAJ CIBERNETIC

Claudiu Codreanu



MINISTERUL AFACERILOR EXTERNE



Taifunuri, urși și panda. Ultimele campanii majore de spionaj cibernetic¹

Claudiu Codreanu²

Analist

Institutul Diplomatic Român

ABSTRACT: Spionajul cibernetic rămâne printre cele mai comune forme de operațiuni cibernetică interstatale la nivel global. Majoritatea statelor se spionează reciproc, această practică nefiind una neobișnuită în afacerile internaționale. Totuși, exploatarea spațiului cibernetic pentru spionaj amplifică potențialul de colectare a datelor sensibile și implică riscul generării unor breșe de securitate care pot fi ulterior exploatare de alți actori. China și Rusia reprezintă principalii actori care desfășoară astfel de acțiuni împotriva statelor euro-atlantice, însă obiectivele și metodele de operare rămân în mare parte distincte. Acest studiu analizează două campanii cibernetică majore desfășurate de China – Volt Typhoon și Salt Typhoon – evidențiind tranziția Beijingului de la spionajul convențional la infiltrarea strategică a infrastructurii critice occidentale. În paralel, cercetarea examinează și activitățile de spionaj cibernetic ale Rusiei, punând accentul pe campaniile legate de războiul de agresiune împotriva Ucrainei. De asemenea, este examinat rolul *spyware*-urilor comerciale, precum Pegasus, utilizate în scopuri represive împotriva jurnaliștilor, activiștilor și opoziției politice. În final, studiul propune o serie de recomandări de politici publice, precum atribuirea publică a campaniilor, impunerea de sancțiuni, dar și consolidarea securității cibernetică și reglementarea exportului și utilizării *spyware*-urilor comerciale.

CUVINTE CHEIE: spionaj cibernetic, Volt Typhoon, Salt Typhoon, Rusia, *spyware* comercial.

¹ Această publicație se bazează exclusiv pe surse deschise. Opiniile exprimate aparțin în întregime autorului și nu reflectă neapărat poziția instituției.

² claudiu.codreanu@idr.ro



INTRODUCERE

Spionajul, un set de activități prin care se încearcă înțelegerea lumii, nu poate să asigure sau să obțină controlul unui actor, dar poate reprezenta un factor care să permită controlul prin acumularea de informații (Zilincik, Myklin & Kovanda 2019). **China, Iran, Rusia, Statele Unite și majoritatea statelor lumii întreprind diferite activități legate de spionaj cibernetic.** În mod similar, Coreea de Nord derulează campanii de spionaj cibernetic, în ciuda faptului că hackerii guvernamentali de la Pyongyang sunt mai cunoscuți pentru campaniile ransomware și extragerea de fonduri (Iyengar 2023). Mai mult, și poate mai îngrijorător față de activitățile tradiționale de spionaj, în ultimii ani a devenit vizibil rolul jucat de spyware-urile comerciale, unelte digitale prin care guvernele și alți actori pot spiona împotriva altor oficiali guvernamentali, dar și împotriva jurnaliștilor și activiștilor anti-guvernamentali sau a opoziției politice.

Grupuri de hackeri cunoscute sub pseudonime date de companii de securitate cibernetică, de la cele rusești precum Fancy Bear sau Cozy Bear, sau Evasive Panda (și Salt/Volt Typhoon în cazul Chinei), identificate mai apoi ca unități ale serviciilor de informații sau al armatelor celor două țări, sunt principalii actori în operațiunile întreprinse împotriva statelor euro-atlantice. **Dacă Rusia utilizează un amestec de spionaj cibernetic pentru colectarea de informații preponderent militare și de securitate, influență politică și apoi dublarea cu atacuri cibernetic sau campanii de dezinformare, Beijingul a pus de-a lungul timpului accentul pe spionaj comercial.** China este, cel mai probabil, principalul actor internațional în ceea ce privește acțiunile majore de spionaj cibernetic (Gilli & Gilli 2019). Campaniile de spionaj cibernetic ale Chinei din 2007-2011 au reușit să obțină cantități substanțiale și importante de date de la Pentagon, inclusiv design-ul pentru avioanele de luptă F-22 și F-35 (Gilli & Gilli 2019, 180). În decembrie 2024, China a fost acuzată de SUA de că a desfășurat o intruziune împotriva Departamentului pentru Trezorerie într-o campanie de spionaj cibernetic (Agence France-Presse 2024). Cu trei luni înainte, Departamentul pentru Justiție al SUA a anunțat că a neutralizat o rețea de 200.000 de dispozitive la nivel global, acuzând că era utilizată de hackeri susținuți de guvernul chinez pentru atacuri cibernetic (Agence France-Presse 2024).

Alte două campanii de hacking ale Chinei au fost dezvăluite de SUA în 2023-2024. Operațiunea **Salt Typhoon** a presupus intruziuni cibernetice în zeci de companii telecomunicații într-o campanie de spionaj cibernetic a Chinei, iar rețeaua de hacking **Volt Typhoon** a exploatat vulnerabilități în infrastructura Statelor Unite (Davidson 2024; Montgomery 2024). Evoluția la Volt Typhoon a arătat o tranziție de la spionaj obișnuit la semnale privind pregătirea unor potențiale atacuri cibernetice substanțiale în cazul escaladării tensiunilor internaționale. Astfel, China urmărește să se pre-poziționeze în rețele informatice critice pentru potențiale atacuri cibernetice distructive sau de perturbare împotriva infrastructurii critice a SUA în contextul unor potențiale crize majore sau a unui conflict cu Statele Unite (Davidson 2024).

În paralel, în aprilie 2024, șase persoane au fost arestate în Regatul Unit și Germania sub acuzația de spionaj pentru China, în contextul unei opoziții din ce în ce mai mari față de campaniile chineze de influență în politica și comerțul din Europa (Higgins & Schuetze 2024). Autoritățile de la Berlin și Londra au acuzat că statul chinez utilizează spioni pentru a încerca să influențeze procesele democratice din Germania și Regatul Unit, ceea ce reprezintă o intensificare a acțiunilor de spionaj de la obiective economice la cele politice, similar cu spionajul desfășurat de Rusia (Higgins & Schuetze 2024). Pe de o parte, evenimentul evidențiază o schimbare a obiectivelor Chinei legate de spionaj, dar și o toleranță mai redusă din partea statelor europene cu privire la acțiunile de influență chineze.

Așadar, studiul explorează principalele evoluții legate de cele mai recente campanii majore de spionaj cibernetic interstatal, punând accentul pe două campanii chineze, Volt Typhoon și Salt Typhoon, dar și pe acțiunile similare ale Rusiei. Totodată, cercetarea include și evoluțiile legate de chestiunea spyware-urilor comerciale și spionajul cibernetic împotriva disidenților. Pentru început, studiul aduce clarificări conceptuale cu privire la spionajul cibernetic și un scurt istoric, iar apoi discută operațiunile Chinei și ale Rusiei, precum și chestiunea spyware-ului Pegasus. În final, studiul analizează aceste campanii de spionaj cibernetic și le pune în context, oferind în final și o serie de recomandări.



SPIONAJUL CIBERNETIC – DEFINIȚII ȘI CONTEXT

Conceptul de spionaj cibernetic

Spionajul cibernetic este definit de Brandon Valeriano și Ryan C. Maness drept „utilizarea de acțiuni ofensive periculoase de intelligence pentru a fura, altera sau șterge informații în sfera cibernetică de interacțiuni” (2015, 49). Acesta se referă la **sustragerea de date guvernamentale sau comerciale secrete, furtul de drepturi de proprietate intelectuală sau informații sensibile din domenii strategice** (ENISA, 2020).

Spionajul cibernetic se încadrează în ceea ce literatura de specialitate descrie acțiunile subversive sau de sabotaj (Maschmeyer, 2023). Astfel de activități rămân la o intensitate scăzută, mult sub pragul războiului, dar pot avea efecte care să depășească scopul inițial al acțiunii. Spionajul cibernetic interstatal reprezintă unul dintre cele mai comune tipuri de operațiuni cibernetică la nivel global (Valeriano & Maness 2015, 9). Obiectivul principal al activităților de spionaj este de a acumula informații, reprezentând încercări de a extrage informații sensibile din sistemele altor actori (Rid, 2012). Astfel, **rolul spionajului este mai degrabă de a facilita o mai bună înțelegere asupra lumii, și nu de a încerca să o modeleze** (Zilincik, Myklin & Kovanda 2019, 5; Rid 2012).

De cele mai multe ori, actorii guvernamentali sau non-statali care întreprind campanii frecvente, extinse și sofisticate de spionaj cibernetic sunt identificate drept APT-uri. **Amenințările persistente avansate (APT – *advanced persistent threats*) se referă la actori cu capacități deosebite care utilizează operațiuni cibernetică pentru a îndeplini obiective specifice pentru o perioadă lungă de timp** (Dunn Cavelty & Egloff 2019, 44). Serviciile de informații se încadrează între cei mai importanți actori în utilizarea strategică a spațiului cibernetic (Dunn Cavelty & Egloff 2019, 47). Acestea exploatează vulnerabilități de securitate în software-uri utilizate pe scară largă pentru a putea să se poziționeze în diferite puncte ale infrastructurii de internet sau să acceseze anumite sisteme (Dunn Cavelty & Egloff 2019, 47). Statele se abțin de la a-și desfășura întregul set de capacități cibernetică în activitățile de spionaj, alegând acțiuni concentrate și precise (Valeriano & Maness 2015, 49). **Majoritatea operațiunilor de spionaj cibernetic sunt desfășurate la o intensitate redusă, sub pragul de război, obiectivul fiind extragerea de date, hărțuirea altor actori statali sau promovarea capacităților de a penetra rețelele respective** (Valeriano & Maness 2015, 68).



Scurt istoric

Una dintre cele mai importante evoluții prin care au fost dezvăluite modul de operare al serviciilor de informații în spațiul cibernetic a fost scurgerea de date făcută de **Edward Snowden**, fost agent contractual al NSA (*National Security Agency* – Agenția Națională pentru Securitate). Edward Snowden a extras și publicat o serie substanțială de fișiere din activitatea NSA, din poziția de colaborator al agenției americane, informațiile făcând referire la activitățile de cyber intelligence ale NSA (Devanny, Martin & Stevens 2021, 434). **Dezvăluirile făcute de Snowden au arătat magnitudinea campaniei globale de colectare de intelligence a SUA, dar și metodele, tehnicile și unele software-uri utilizate** (Devanny, Martin & Stevens 2021, 435).

Totuși, China reprezintă statul cel mai implicat în activități de spionaj cibernetic interstatal (Gilli & Gilli, 2019). **China are un istoric bogat de spionaj cibernetic împotriva țintelor guvernamentale din Europa și SUA.** În perioada 2007-2011, hackerii guvernamentali chinezi au reușit să se infiltreze în serverele Pentagonului și să obțină accesul la cantități semnificative de date care conțineau design-uri și proiecte pentru avioane de luptă americane de tip *stealth* (Gilli & Gilli, 2019). Totodată, la aproape zece ani distanță de la incident, CISA (*Cybersecurity and Infrastructure Security Agency* – Agenția pentru Securitatea Cibernetică și Securitatea Infrastructurii) și FBI (*Federal Bureau of Investigation* – Biroul Federal pentru Investigații) au emis un comunicat în care au acuzat China că a penetrat rețelele unor conducte de gaze și petrol din SUA în perioada 2011-2013 (Greenberg & Newman 2023).

În 2014, hackerii guvernamentali chinezi au reușit să extragă cantități fără precedent de informații confidențiale de la Biroul SUA pentru Managementul Personalului (OPM – *Office for Personnel Management*), în urma unei intruziuni cibernetice (Devanny, Martin & Stevens 2021, 436). Au fost extrase datele a peste 22 de milioane de persoane, ceea ce a putut ajuta guvernul chinez să își îmbunătățească înțelegerea cu privire la forța de muncă federală a Statelor Unite, dar și să permită selectarea unor anumiți angajați pentru viitoare atacuri cibernetice țintite, șantajări sau înșelăciuni online (Devanny, Martin & Stevens 2021, 437). China și Statele Unite au semnat ulterior acestui eveniment un acord bilateral pentru securitatea cibernetică care a vizat în principal reducerea operațiunilor de spionaj cibernetic comercial, reușind să amelioreze intensitatea campaniile chineze (Martin 2025).

Mai recent, în 2020-2021, Statele Unite au dezvăluit o altă campanie majoră de spionaj cibernetic desfășurată de hackeri guvernamentali chinezi, care a vizat agenții federale americane, dar și companii private (Devanny, Martin & Stevens 2021, 439). Un aspect notabil este legat de neglijența campaniei chineze în comparație cu meticulozitatea celei rusești din aceeași perioadă. Hackerii chinezi au exploatat o vulnerabilitate din software-ul Microsoft Exchange printr-o intruziune cibernetică care lăsa victimele vulnerabile în fața unor atacuri cibernetic care puteau proveni de la alți actori, cu obiective de perturbare, nu doar de spionaj (Devanny, Martin & Stevens 2021, 441).

În 2023, oficiali americani au susținut că China are în plan instalarea în Cuba a unor facilități de spionaj asupra comunicațiilor electronice din sud-estul SUA (Reuters 2023). În schimb, ministerul afacerilor externe chinez acuza că Statele Unite reprezintă „cel mai mare imperiu de hackeri din lume”, respingând acuzațiile că Beijingul ar încerca să dezvolte instalații de spionaj împotriva SUA pe teritoriul Cubei (Reuters 2023). Cu toate acestea, hackerii Ministerului pentru Securitate de Stat al Chinei au mers mai departe față de simple acte de spionaj în zona Asiei de Sud-Est, lansând atacuri cibernetic care au distrus date, inclusiv împotriva companiei de stat pentru petrol din Taiwan (Greenberg & Newman, 2023).

Pe de altă parte, **hackerii guvernamentali ruși și cei afiliați guvernului au o listă lungă de campanii de spionaj cibernetic, de la infiltrări în sisteme guvernamentale cu scopul de spionaj comercial sau pentru susținerea de operațiuni de influență în alegeri, până la operațiuni mai sofisticate precum deturnarea legăturilor de internet prin satelit** (Mueller et al. 2023; Maschmeyer & Dunn Cavelty 2022). Operațiunile rusești utilizează un amestec de campanii avansate de spionaj și utilizarea de *malware*-uri (Mueller et al. 2023). În 2018, Washingtonul a acuzat Rusia de infiltrarea în mai multe zone ale infrastructurii critice, de la sectorul nuclear, la energie, aviație, și până la sectorul furnizării apei potabile (Lonergan & Poznansky 2025). Cu toate acestea, Rusia nu a exploatat astfel de infiltrări prin lansarea de atacuri cibernetic împotriva SUA până în prezent, riscul cel mai mare apărând după războiul de agresiune împotriva Ucrainei (Lonergan & Poznansky 2025).

Totodată, în cadrul campaniei de spionaj cibernetic **SolarWinds**, Rusia a reușit să infecteze mii de organizații publice și private din SUA prin compromiterea unui software larg utilizat de zeci de agenții și departamente federale americane (Devanny, Martin & Stevens 2021, 438). Grupul de hackeri Cozy Bear (APT29), identificat ca fiind parte a serviciului militar de informații rusesc (GRU) a exploatat o vulnerabilitate în software-ul companiei

SolarWinds pentru a extrage date (Mueller et al. 2023). Agenții de informații ruși au injectat un cod malițios în software-ul Orion al companiei SolarWinds în 2021, ceea ce a permis accesul în rețelele guvernului federal și în mai multe companii majore (Sanger & Barnes 2024). În paralel, a devenit vizibilă și potențiala utilizare a grupurilor de hackeri independenți pentru țintirea unor state occidentale. Un grup de criminalitate cibernetică suspect de sprijin din partea guvernului rus a derulat în 2021 o operațiune cibernetică de tip *ransomware* împotriva celui mai mare distribuitor de combustibil și gaze din estul SUA, Colonial Pipeline, perturbând furnizarea de combustibil în 2021 (Sanger & Barnes 2024; Mueller et al. 2023).

ULTIMELE CAMPANII MAJORE DE SPIONAJ INTERSTATAL

China – Salt Typhoon

În noiembrie-decembrie 2024, Statele Unite au dezvăluit o campanie extinsă de spionaj cibernetic a Chinei, denumită de către Microsoft drept **Salt Typhoon**. Grupul de hackeri a mai fost acuzat de operațiuni împotriva unor ținte guvernamentale din Arabia Saudită, Brazilia, Burkina Faso, Canada, Israel și Guatemala (Montgomery 2024). Nouă companii americane majore de telefonie mobilă au fost victime ale intruziunii cibernetică chineze, permițând accesul la datele apelurilor și mesajelor text în timp real (Greenberg 2025a). În ansamblu, **operațiunea a presupus penetrarea sistemelor a peste 80 de companii americane, furnizori de internet, dar și mai multe companii importante de telecomunicații, precum Verizon, AT&T sau T-Mobile** (Tait 2024). Hackerii au obținut accesul atât la detalii privind registrul de apeluri și mesaje text, și inclusiv la conținutul mesajelor (Montgomery 2024).

Chiar dacă au fost interceptate comunicații ale unor oficiali guvernamentali din Washington DC, țintele au fost diverse, accesul obținut fiind unul extins (Montgomery 2024). Hackerii chinezi, parte ai Ministerului pentru Securitatea de Stat, au reușit să penetreze rețelele companiilor de telecomunicații pentru a spiona convorbirile prin voce și text ale mai multor oficiali guvernamentali și politicieni importanți, precum Donald Trump, JD Vance sau campania candidatei democrate Kamala Harris (Volz 2025; Sanger & Barnes 2024). Mai mult, **inclusiv programul de interceptări telefonice al guvernului american a fost accesat de hackeri, fiind extrase înregistrări telefonice** (Montgomery 2024).

Totuși, hackerii nu puteau să asculte sau să citească conversațiile din aplicații care criptează datele, precum WhatsApp sau Signal, dar puteau să citească mesaje text (SMS) clasice, dar și să asculte convorbiri telefonice obișnuite – ceea ce guvernul poate să facă doar în baza unui mandat judecătoresc (Sanger & Barnes 2024). Autoritățile americane au făcut un apel pentru angajații din sectorul public să nu utilizeze aplicațiile tradiționale de mesaje text, ci să folosească aplicațiile care criptează mesajele, precum Signal sau WhatsApp (Montgomery 2024).

Conform unor oficiali americani anonimi citați de *The Wall Street Journal*, reprezentanți ai guvernului chinez ar fi recunoscut indirect că Beijingul s-a aflat în spatele operațiunii Salt Typhoon în timpul unei întâlniri secrete SUA-China la Geneva în decembrie 2024 (Volz 2025). Oricum, în decembrie 2024, *The Guardian* susținea că oficialii americani considerau că motivația pentru Salt Typhoon a fost colectarea de informații și nu pregătirea pentru un atac asupra infrastructurii (Tait 2024).

Aparent, în urma dezvăluirii operațiunii Salt Typhoon, hackerii par să își fi suspendat intruziunea pentru a nu putea fi identificat întreg mecanismul care a permis hack-ul, dar acest lucru nu înseamnă neapărat că nu mai au acces la rețelele americane (Sanger & Barnes 2024). Compania de securitate cibernetică Recorded Future a arătat în februarie 2025 că operațiunea Salt Typhoon a continuat intruziunile și în perioada decembrie 2024 – ianuarie 2025, identificând prezența hackerilor în alte cinci companii de telefonie mobilă și internet din lume, dar și în mai mult de zece universități din SUA, Vietnam, și alte zone (Greenberg 2025a).

Cazul Volt Typhoon – mai mult decât simplu spionaj

Volt Typhoon este numele dat unei operațiuni cibernetice a Chinei prin care au fost compromise mii de dispozitive conectate la internet (Davidson 2024). Autoritățile americane au precizat că operațiunea face parte dintr-o campanie mai largă a Chinei de a se infiltra în rețelele infrastructurii critice ale statelor din spațiul occidental, inclusiv în cele ale sectorului energetic, al telecomunicațiilor, în rețelele furnizorilor de internet sau al porturilor navale (Davidson 2024).

În 2023, Microsoft și autoritățile americane au depistat coduri malițioase în sistemele de telecomunicații din Guam, insulă care este teritoriu al SUA din Micronezia, dar și în alte zone ale Statelor Unite (Sanger 2023). Microsoft a precizat că un grup de hackeri

guvernamentali chinezi a injectat codul, generând îngrijorări deoarece insula din Pacific găzduiește mai multe porturi și o bază aeriană americană semnificativă, esențială în cazul unui răspuns militar american la o posibilă escaladare chineză împotriva Taiwanului (Sanger 2023).

Operațiunea a fost desfășurată foarte meticulos și în secret, uneori prin intermediul unor routere de rețea casnice și altor dispozitive conectate la internet, pentru a putea evita detectarea și urmărirea acțiunilor hackerilor (Sanger 2023). NSA, împreună cu agenții similare din Regatul Unit, Canada, Australia și Noua Zeelandă, au publicat un document care face referire la dezvoltările Microsoft și la activitățile Chinei (Sanger 2023).

În mai 2023, Microsoft anunța că a reușit să identifice un grup de hackeri pe care îl consideră asociat statului chinez (Greenberg & Newman, 2023). **Grupul de hackeri, denumit Volt Typhoon, a derulat o campanie amplă de intruziuni cibernetice în sistemele infrastructurii critice din SUA și Guam, inclusiv din sectorul comunicațiilor.** Pre-poziționându-se în aceste rețele, grupul de hackeri ar putea să exploateze breșele de securitate pentru atacuri cibernetice disruptive în cazul unor conflicte militare sau diplomatice între Washington și Beijing. Conform investigației Microsoft, Volt Typhoon a fost activă începând cu jumătatea anului 2021, compania susținând că, prin țintirea infrastructurii americane din Guam și alte zone, operațiunea viza obținerea unor capacități pentru a putea perturba comunicațiile între SUA și Asia în contextul unor potențiale viitoare crize (Davidson 2024). Operațiunea cibernetică Volt Typhoon a fost desfășurată prin exploatarea unor vulnerabilități și breșe în routere și alte dispozitive învechite, care nu mai primeau actualizări de securitate (Davidson 2024).

NSA, CISA și Departamentul de Justiție au publicat în mai 2023 un comunicat comun pentru a dezvălui operațiunea, laolaltă cu principalele agenții de intelligence din Canada, Regatul Unit și Australia (Greenberg & Newman 2023). Încă de la sfârșitul anilor 2000, China a fost acuzată că s-a infiltrat în rețelele informatice ale infrastructurii energetice americane, cu scopul de a exploata intruziunile în cazul unui conflict (Greenberg & Newman 2023). Washingtonul a precizat că modul în care a fost derulată operațiunea și țintele alese nu se încadrează în tiparul unei campanii de spionaj cibernetic tradiționale (Davidson 2024). Autoritățile americane au avertizat că *malware*-urile găsite în infrastructura Statelor Unite par a fi pregătite pentru utilizare în cazul în care SUA ar veni în ajutorul Taiwanului în contextul unei potențiale escaladări (Sanger & Landler 2024). **Față de alte operațiuni ale Chinei, Statele Unite și aliații au argumentat că scopul nu a fost extragerea de date pentru spionaj**

obișnuit, ci pre-poziționarea în anumite puncte strategice din interiorul infrastructurii critice pentru a pregăti potențiale acte de sabotaj în viitor (Davidson 2024). Lin Jian, purtător de cuvânt al MAE chinez, a respins acuzațiile, catalogându-le drept dezinformări (Sanger & Landler 2024).

Toată atenția pe războiul de agresiune împotriva Ucrainei. Ultimele campanii ale Rusiei

Pe 21 mai 2025, CISA a emis un comunicat comun cu mai multe agenții similare din SUA și alte state euro-atlantice prin care a dezvăluit o campanie de spionaj cibernetic a Rusiei împotriva unor companii tehnologice și a unor entități din zona logistică din spațiul occidental (CISA 2025). Comunicatul a fost emis în comun cu agenții similare din Australia, Canada, Cehia, Danemarca, Estonia, Franța, Germania, Olanda, Polonia, Regatul Unit. Entitățile vizate de compania rusă au fost cele implicate în coordonarea, livrarea și transportul de asistență către Ucraina, fiind țintite sistemele de camere de supraveghere de la frontiera mai multor state din spațiul euro-atlantic (CISA 2025). Încercări de a obține accesul la sistemele de camere au avut loc în Bulgaria, Cehia, Franța, Germania, Grecia, Italia, Olanda, Polonia, Slovacia, Statele Unite, Ucraina, dar și România și Republica Moldova (CISA 2025). Comunicatul publicat de CISA a atribuit campania cibernetică grupului APT28, sau Fancy Bear, identificat anterior ca fiind unitatea militară 26165 din cadrul GRU.

Începând cu 2022, odată cu invazia totală a Ucrainei, hackerii guvernamentali ruși au început să vizeze țările care furnizează asistență de securitate Ucrainei, concentrându-se pe ținte din sectoarele guvernamentale, financiare, energetice, sanitare și de transporturi (CISA 2024). Campaniile cibernetice ale acestora au inclus atacuri prin care au fost vandalizate website-uri, extragerea de date, scanarea de vulnerabilități și alte elemente ale infrastructurii, dar și operațiuni de scurgere a datelor extrase (CISA 2024). În plus, pe lângă publicarea online a datelor sustrase, hackerii GRU vând pe piața neagră datele obținute prin operațiunile cibernetice (CISA 2024).

Conform unor oficiali guvernamentali citați de media americană, CISA a emis pe 4 aprilie 2024 o directivă de urgență privind intruziunea cibernetică a unui grup de hackeri afiliat SVR în rețelele Microsoft (Heilweil et al. 2024). Grupul, cunoscut de APT29 (sau Cozy Bear) este responsabil și pentru *hack*-urile din 2015-2016 împotriva Comitetului Național al Partidului Democrat, cât și de campania de spionaj SolarWinds din 2020. Microsoft a anunțat



în martie 2024 că hackerii ruși au reușit să acceseze codul sursă al unor software-uri ale companiei (Heilweil et al. 2024).

În septembrie 2024, FBI, CISA și NSA au emis un comunicat în care au atribuit public o serie de operațiuni cibernetice unei unități a agenției militare rusești de informații (GRU), fiind găsită responsabilă de operațiuni împotriva mai multor ținte de pe glob cu obiective legate de sabotaj, spionaj sau afectarea reputației (CISA 2024). Obiectivele operațiunilor cibernetice ale Unității GRU 29155 includ colectarea de informații pentru spionaj, încercarea de a afecta reputația țintelor vizate prin furtul și scurgerea în media de informații sensibile (acțiune cunoscută drept *kompromat*) și sabotaj sistematic prin distrugerea de date (CISA 2024). **Unitatea 29155 a vizat atât ținte din Ucraina, prin malware-ul WhisperGate, cât și ținte din statele membre NATO și alte țări din Europa, America Latină și Asia Centrală (CISA 2024).**

Totodată, în februarie 2025, Microsoft a dezvăluit o campanie de intruziuni cibernetice a grupului **Sandworm** (identificat de autoritățile SUA drept parte a GRU) împotriva unor ținte din SUA, Regatul Unit, Australia și Canada (Greenberg 2025b). Mai exact, cercetătorii Microsoft au identificat un nou grup, numit **BadPilot**, care execută intruziunile inițiale pentru a putea obține un avanpost în rețelele vizate înainte ca hackerii Sandworm să preia operațiunea (Greenberg 2025b). Dacă în 2022 se axa numai pe Ucraina, din 2023 a început să desfășoare operațiuni cibernetice asupra diferitor rețele la nivel global (Greenberg 2025b). Conform Microsoft, țintele vizate de intruziunile cibernetice au inclus rețele guvernamentale, dar și din sectorul energiei, telecomunicațiilor, transportului maritim și industria de armament (Greenberg 2025b).

SPIONAJ GUVERNAMENTAL ÎMPOTRIVA DISIDENȚEI. CHESTIUNEA SPYWARE-ULUI COMERCIAL

În 2021, o serie de publicații media precum *The Guardian*, *Haaretz* sau *The Washington Post*, au publicat o investigație asupra modului în care a fost utilizat abuziv un *spyware* dezvoltat o companie israeliană, NSO Group. **Pegasus a fost utilizat pentru infiltrarea cibernetică în telefoanele celor vizați printr-o vulnerabilitate în aplicația WhatsApp, fiind extrase date precum mesaje text, locații, informații privind utilizarea anumitor aplicații și interceptarea convorbirilor telefonice (European Parliament 2023).** Pegasus se încadrează

în categoria *spyware*-urilor comerciale – software-uri de monitorizare dezvoltate de companii private și vândute în principal către guverne. Grecia, Polonia și Ungaria au fost implicate în scandaluri privind folosirea abuzivă a *spyware*-ului împotriva unor jurnaliști și al unor personalități din cadrul opoziției (Deibert 2022). Conform unui raport al *AccessNow*, citat de *The Guardian*, cel puțin șapte jurnaliști și activiști vocali împotriva Kremlinului au fost vizați de un actor statal care folosea *spyware*-ul Pegasus în timp ce se aflau pe teritoriul UE (Kirchgaessner 2024).

În mai 2025, un tribunal federal american a decis ca NSO Group să plătească aproape 170 de milioane de dolari către WhatsApp și Meta drept compensanții din cauza intruziunilor cibernetice care au permis compromiterea a cel puțin 1.400 de conturi în 2019 prin exploatarea sistemului de apeluri video pentru infectarea cu *malware* a telefoanelor (Miller 2025).

Totodată, Parlamentul European a înființat un comitet pentru investigarea utilizării *spyware*-ului în țările membre UE (Miller 2025). Comitetul a adoptat un raport privind Pegasus în martie 2023 și a pregătit un draft de recomandare care condamnă utilizarea abuzivă a *spyware*-ului de către guvernele statelor membre (European Parliament 2023). Lista celor vizați de Pegasus include jurnaliști, activiști, membri ai societății civile, politicieni, diplomați, oameni de afaceri și așa mai departe (European Parliament 2023).

În 2024, după schimbarea guvernului în Polonia în urma alegerilor legislative, autoritățile au dezvăluit că peste 600 de persoane au fost spionate de către fostul guvern conservator utilizând Pegasus (Smalley 2024b). După o anchetă de 18 luni a Senatului polonez pe această chestiune, una dintre concluzii a fost că alegerile din 2019 au fost afectate din cauza unor intruziuni cibernetice împotriva liderului opoziției de atunci (Smalley 2024b). Polonia nu este un caz izolat în Europa, scandaluri similare privind abuzul Pegasus având loc și în Grecia, Spania și Ungaria (Smalley 2024b). **Dezvăluirile jurnaliștilor de investigație au arătat că Grecia, Spania, Polonia și Ungaria au utilizat *spyware*-ul Pegasus, fiind vizați în Europa jurnaliști, politicieni de opoziție și lideri ai societății civile** (Smalley 2024a). Spre exemplu, inclusiv Președinta Parlamentului European, Roberta Metsola, a fost țintită de *spyware*-ul Predator în 2023 (Smalley 2024a). În mod similar, în Spania, Înalta Curte a deschis o anchetă privind potențialul spionaj asupra premierului Pedro Sanchez și ai altor politicieni, existând, oricum, și o investigație cu privire la potențiala urmărire a unor activiști catalani pentru independență (Smalley 2024b). Conform investigațiilor jurnalistice, țintele Pegasus în Spania

au inclus fiecare membru catalan al Parlamentului European care a susținut independența Cataloniei și fiecare președinte catalan din 2010-2020 (Deibert 2022).

Totodată, Pegasus a fost utilizat împotriva unor critici guvernamentali în Emiratele Arabe Unite, Thailanda și Arabia Saudită (Deibert 2022). Atât state autoritare, cât și democrații precum SUA, Spania, Mexicul sau Ungaria au utilizat spyware-ul Pegasus în moduri care încalcă responsabilitatea publică și respectarea normelor privind drepturile omului (Deibert 2022). Compania NSO Group a precizat în mai multe rânduri că software-ul era destinat doar pentru a fi utilizat în anchetele poliției și în investigațiile de *intelligence*, susținând că Pegasus a fost folosit pentru prinderea unor infractori importanți, precum traficantul de droguri Joaquin Guzman Loera (El Chapo) (Smalley 2024b).

În 2024, Administrația Biden a susținut un angajament împreună cu alte țări pentru a utiliza *spyware*-urile responsabil, și inclusiv Administrația Trump a sprijinit în 2025 un efort internațional pentru a stabili un cod de conduită pentru utilizarea acestor software-uri (Miller 2025). În 2023, Statele Unite, Regatul Unit, și alte nouă state au semnat un comunicat privind pericolul generat de proliferarea și abuzarea la nivel global a *spyware*-urilor comerciale (GOV.UK 2024). Ulterior, s-au mai alăturat alte șase state, lista completă incluzând și Australia, Franța, Japonia, Polonia sau Coreea de Sud, printre altele (GOV.UK 2024). **NSO Group a fost adăugat în 2021 de Departamentul american pentru Comerț pe lista de entități responsabile de activități cibernetice malițioase**, restricționând dreptul companiei de a desfășura afaceri cu firme americane și îngreunând capabilitățile de a-și vinde software-urile la nivel global (Miller 2025).

ANALIZĂ. SPIONAJUL CIBERNETIC INTERSTATAL ȘI OPERAȚIUNILE CIBERNETICE OFENSIVE

Faptul că statele se spionează reciproc nu reprezintă un element remarcabil în afacerile internaționale. De exemplu, în urma unor operațiuni de HUMINT (*human intelligence* – informații din surse umane), statele impun costuri care să afecteze reputația celui alt actor și să îi perturbe operațiunile, precum declararea unor membri ai personalului ambasadei drept *personae non gratae* și expulzarea acestora – însă acțiunile tind să fie provizorii și proporționale (Devanny, Martin & Stevens 2021, 431). Cu toate acestea, un studiu recent a arătat că **operațiunile cibernetice distructive sau disruptive produc mai multe știri și**

conținut în presă față de activitățile de spionaj cibernetic, generând astfel o atenție mai mare a societății (Makridis, Maschmeyer & Smeets, 2024).

Cu toate acestea, cercetări recente au arătat că operațiunile ciberneticе sunt ori prea slabe, încete sau volatile pentru a putea deveni instrumente în operațiunile militare, oferind o valoare strategică limitată chiar și în condiții hibride (Maschmeyer & Dunn Caveltу, 2022). În plus, **spionajul cibernetic ar putea chiar să consolideze stabilitatea strategică, atâta vreme cât statele afectate recunosc acest lucru și se abțin de la escaladarea situațiilor** (Devanny, Martin & Stevens, 2021). Spionajul cibernetic, inclusiv cel rusesc sau chinez, reprezintă ceva comun și obișnuit în afacerile internaționale. Așadar, trebuie luate măsuri pentru a pune piedici operațiunilor altor state, dar acest lucru nu înseamnă că reprezintă noutăți sau evoluții care să genereze răspunsuri deosebit de severe. Excepția în acest caz o fac campaniile de spionaj cibernetic neglijente, care produc breșe exploatabile și de alți actori, sau care afectează serios buna-funcționare a sistemelor vizate.

Dacă Salt Typhoon reprezintă o campanie de spionaj tradițională (chiar dacă una grandioasă), în cazul Volt Typhoon scopul inițial de colectare de informații a fost depășit, fiind vorba de intruziuni care au avut obiectivul de a obține pre-poziționări strategice în infrastructura critică. Volt Typhoon se aseamănă mai mult cu campaniile ciberneticе rusești, prin care hackerii încearcă să scaneze sau să testeze vulnerabilități și breșe în rețelele informatice ale diferitelor sectoare critice. Obiectivul final al acestor acțiuni de **pre-
poziționare**, sau al obținerii unor implanturi în rețele, este activarea acestora (sau „detonarea”) în contextul unor escaladări substanțiale în relațiile dintre cele două state, fie că vorbim de un conflict în Taiwan sau o escaladare a războiului ruso-ucrainean.

Conform unei analize a lui Ciaran Martin (2025) pentru *think tank*-ul RUSI, China s-a aflat în ultimii doi ani într-un proces de tranziție a capabilităților și obiectivelor în spațiul cibernetic – de la obiective economice la cele politice, de la acțiuni oportuniste la operațiuni strategice, și de la o abordare pasivă la una activă. Astfel, **China a trecut de la simple campanii de spionaj cibernetic și furt de date la operațiuni care pot pune bazele unor atacuri ciberneticе masive împotriva infrastructurii critice ale statelor din spațiul occidental** (Martin 2025).

Salt Typhoon reprezintă o operațiune tradițională de spionaj cibernetic, chiar dacă a avut o magnitudine semnificativă (Lonergan & Poznansky 2025). Salt Typhoon reprezintă o operațiune de spionaj cibernetic derulată de Ministerul pentru Securitatea de Stat din China

(principalul serviciu de informații), prin care au fost reușite infiltrări în sistemul de telecomunicații al Statelor Unite (Martin 2025). În schimb, Volt Typhoon reprezintă o operațiune cibernetică cu obiective strategice politice și, potențial, militare, desfășurată de unitatea cibernetică a armatei chineze, prin care au fost inserate *malware*-uri în infrastructură critică americană (Martin 2025). Zonele vizate de Volt Typhoon au inclus, conform Administrației Biden, energia transporturile, construcțiile, educația, guvernul, dar și sectorul IT (Martin 2025).

Chiar dacă uneori este folosit pentru pregătirea unor atacuri cibernetice și implică anumite operațiuni ofensive, spionajul nu este în esență ofensiv, ci urmărește o înțelegere mai bună a afacerilor internaționale. Atât operațiunile cibernetice cu obiective de perturbare, cât și campaniile de spionaj cibernetic, implică acțiuni ofensive (precum intruziuni, accesări ilegale a unor date sau rețele), important este scopul final al activităților respective. Totuși, devine din ce în ce mai dificilă identificarea distincției dintre simplele acte de spionaj și intruziunile cu scopuri ofensive, precum pre-poziționarea pentru atacuri ulterioare.

Volt Typhoon reprezintă o acțiune de pre-poziționare pentru potențiale atacuri cibernetice viitoare, obiectivul fiind obținerea accesului și infiltrarea în diferite puncte ale rețelelor pentru a le putea exploata în cazul unui conflict (Lonergan & Poznansky 2025). **În cazul unui conflict, China ar putea lansa atacuri cibernetice distructive sau perturbatoare asupra infrastructurii critice a SUA sau a partenerilor pentru descuraja implicarea în conflict sau pentru a îngreuna capacitățile militare și civile în cazul unei crize sau conflict (Lonergan & Poznansky 2025).** Comunicatul comun emis de statele care fac parte din grupul Five Eyes (Statele Unite, Regatul Unit, Australia, Canada, Noua Zeelandă) precizează că implanturile de *malware* reprezintă resurse strategice care pot fi activate în cazul unei crize sau conflict major între China și Occident (Martin 2025). Totodată, Erica Lonergan și Michael Poznansky (2025) argumentează că Volt Typhoon face parte dintr-un set mai larg de instrumente ale Chinei pregătite pentru un potențial conflict cu SUA și partenerii săi, iar astfel Washingtonul va trebui să descurajeze un război cu China pentru a putea descuraja a activarea implanturilor inserate.

China nu are un istoric deloc bogat în lansarea de atacuri cibernetice distructive (Martin 2025). Față de capacitățile cibernetice ale Chinei, dezvoltate pentru a urmări obiective economice, cele ale Rusiei au fost dintotdeauna dezvoltate pentru obiective politice (Martin 2025). În ultimii ani, grupuri de criminalitate cibernetică originare din Rusia (și tolerate sau

sprijinite probabil de guvernul rus) au provocat perturbări semnificative în sectoare critice, precum energia sau sănătatea, prin operațiuni cibernetice de tip *ransomware* (Martin 2025). În schimb, actorii statali nu au mai desfășurat atacuri cibernetice substanțiale. **Rusia nu a reușit să provoace perturbări semnificative sau să obțină victorii strategice nici măcar în operațiunile cibernetice lansate împotriva Ucrainei și aliaților după invazia totală din 2022 (Martin 2025).**

Pe lângă simple campanii de spionaj, Rusia s-a concentrat și pe operațiuni cibernetice de perturbare a statului, societății și economiei, precum și subminarea încrederii cetățenilor în instituții publice. **Pre-poziționări ale hackerilor guvernamentali ruși în sectoare sensibile ale infrastructurii critice americane, precum campania Volt Typhoon, au fost deja identificate în ultimii 7 ani, dar nu au fost (încă) exploatate.** Motivele pentru care nu s-a întâmplat acest lucru variază de la simpla reținere a Rusiei sau Chinei de la escaladarea tensiunilor și atacurilor cibernetice, teama de o ripostă cibernetică sau de alt tip, consolidarea apărării cibernetice în statele euroatlantice, dar și faptul că tensiunile între cele două grupuri de state nu au depășit anumite linii roșii luate în considerare de acestea. În ultimii ani, majoritatea operațiunilor cibernetice și informaționale ale Rusiei în spațiul occidental au avut obiective legate de războiul de agresiune împotriva Ucrainei.

În plus, cercetătoarea Myriam Dunn Cavelty argumentează că acțiunile întreprinse de diferiți actori statali pentru a crește nivelul de securitate reușesc să scadă, de fapt, nivelul de securitate atât în spațiul cibernetic, cât și în lumea fizică (Dunn Cavelty 2014, 702). Astfel, **serviciile de informații pot determina un spațiu cibernetic mai nesigur, în încercarea de a obține accesul la cât mai multe date** (Dunn Cavelty 2014, 710). Spre exemplu, dezvăluirile făcute de Edward Snowden au arătat că agenția americană NSA a identificat și exploatat vulnerabilități ultra-recente (*zero-day*), injectând totodată *malware*-uri proprii în diferite puncte ale infrastructurii de internet (Dunn Cavelty 2014, 710). În acest fel, au fost create puncte de acces sub acoperire (*backdoors*) care pot fi activate oricând pentru diferite tipuri de activități, de la monitorizare, spionaj sau atacuri distructive (Dunn Cavelty 2014, 710). Totuși, aceste vulnerabilități pot fi exploatate și de grupuri de criminalitate cibernetică sau de hackerii altor actori statali – provocând, așadar, amenințări inclusiv pentru statul care le întreține (Dunn Cavelty 2014, 710).

Pe lângă evoluțiile îngrijorătoare cu privire la spionajul cibernetic interstatal, *spyware*-urile comerciale reprezintă un alt element poate la fel de periculos pentru democrații, prin

spionarea opoziției, societății civile și a jurnaliștilor. **Ultimele incidente au arătat nevoia unor reglementări internaționale substanțiale, dar și a impunerii unor sancțiuni** atunci când anumite companii sau state permit ca software-urile lor să fie abuzate de alte state, sau când aleg să exporte astfel de programe către state autoritate recunoscute pentru represiunea opoziției democratice și cu un istoric de abuzuri ale unor astfel de software-uri. Cu toate acestea, luarea unor măsuri serioase în acest caz reprezintă un efort dificil, ținând cont că exportul de *spyware* comercial aduce avantaje strategice pentru statele care livrează aceste instrumente. Spre exemplu, o investigație a *New York Times* a dezvăluit că vânzările făcute de NSO au ajutat guvernul israelian condus de Benjamin Netanyahu să încheie Acordurile de la Abraham cu Bahrain, Maroc și Emiratele Arabe Unite, ținând cont că Israelul aprobă licențele de export pentru vânzările companiei (Deibert 2022).

Răspunsurile luate de statele occidentale împotriva spionajului cibernetic

Devanny, Martin & Stevens (2021) argumentează că răspunsul statelor la operațiuni cibernetică care le vizează depinde substanțial de contextul strategic și bilateral în care se manifestă incidentele respective. În general, Statele Unite aduc în discuție ideea de a „impune costuri” în urma unor campanii de spionaj cibernetic împotriva lor, ceea ce implică inclusiv lansarea propriilor operațiuni cibernetică (Devanny, Martin & Stevens 2021, 431).

Spre exemplu, Statele Unite au impus sancțiuni economice în urma campaniei SolarWinds în aprilie 2021, au expulzat mai mulți membri ai misiunii diplomatice rusești de la Washington, lansând apoi inclusiv propriile operațiuni cibernetică împotriva agențiilor de *intelligence* rusești (Devanny, Martin & Stevens 2021, 439). Totuși, nu este clar dacă răspunsul american la campania SolarWinds – atribuire publică, sancțiuni economice și puneri sub acuzare – a avut un rol în descurajarea Rusiei de la operațiuni de spionaj cibernetic (Lonergan & Poznansky 2025).

În mod similar, în martie 2024, Statele Unite și Regatul Unit au anunțat impunerea de sancțiuni împotriva hackerilor acuzați de o campanie de spionaj cibernetică începută încă din anii 2010, parte a unei companii paravan a grupului APT31 (Zirconium sau Judgement Panda), asociat cu guvernul Chinez (Robins-Early 2024). Washingtonul și Londra au acuzat Ministerul pentru Securitatea de Stat al Chinei că au derulat campania timp de 14 ani, într-un efort de a injecta *malware*-uri în infrastructura critică americană (Sanger & Landler 2024). Campania

cibernetică a durat în jur de 14 ani și a țintit inclusiv companii, oficiali publici, critici ai Beijingului, vizând și intruziuni împotriva unor sectoare ale infrastructurii critice americane, precum apărarea sau energia (Robins-Early 2024). Totodată, autoritățile de la Londra au acuzat că una dintre operațiunile cibernetice a permis accesarea datelor de la a zeci de milioane de votanți de la Comisia Electorală britanică, iar în alte cazuri au fost desfășurate campanii de spionaj cibernetic împotriva unor parlamentari cunoscuți pentru ridicarea chestiunii amenințărilor provenite din China (Robins-Early 2024).

Totodată, au fost luate și alte măsuri, precum interzicerea unor companii de la licitații (precum Huawei) sau a produselor altor firme. Spre exemplu, în iunie 2024, Washingtonul a interzis compania de securitate cibernetică rusească Kaspersky pe teritoriul SUA, atât pentru companii, cât și pentru indivizi, nemaiavând autorizație nici să își vândă produsele, dar nici să trimită actualizări pentru sistemele care au programul antivirus deja instalat (Stahie 2024). Motivul invocat de autoritățile americane este lipsa încrederii că, în cazul în care Rusia va lua decizia să instrumentalizeze datele colectate de programul antivirus, compania va rezista presiunilor de a colabora cu guvernul rus (Stahie 2024). Kaspersky a fost oricum interzis pe sistemele guvernului federal american încă din 2017, fiind acuzat de legături cu agențiile de informații rusești și acuzat că a extras ilegal date din calculatoare (Stahie 2024). În 2022, Germania, Italia și România au interzis utilizarea Kaspersky în sectorul public (Stahie 2024).

CONCLUZII ȘI RECOMANDĂRI

Momentul în care spionajul cibernetic devine o problemă semnificativă este atunci când sunt depășite anumite limite, precum campaniile în urma cărora sunt extrase date foarte sensibile. La fel este și cazul campaniilor când sunt create breșe de securitate, vulnerabilități care pot fi apoi utilizate de alți actori malițioși, care pun în pericol utilizatorii finali, și care afectează utilizatorii casnici. **Evoluții îngrijorătoare nu au fost generate doar de spionajul cibernetic inter-statal, ci și de spionajul guvernelor împotriva cetățenilor țării lor, altor țări, ONG-uri, companii, alte guverne etc., prin utilizarea de *spyware*-uri comerciale.** Față de ceea ce se întâmplă pe piața neagră, unde aceste software-uri sunt scoase la licitație, companiile respective respectă, sau trebuie să respecte, reglementările naționale și internaționale (Perlroth 2021).

Oricum, indiferent de măsurile care pot fi luate, operațiuni disruptive de intensitate mică vor continua să afecteze statele occidentale, precum atacurile *ransomware* (Maschmeyer & Dunn Cavelty, 2022). Campanii precum Salt Typhoon vor mai avea loc în perioada următoare, dar riscul cel mai ridicat este continuarea unor campanii de tipul Volt Typhoon și potențialul utilizării unor atacuri distructive sau care să perturbe serios activitățile economice sau guvernamentale ale unui stat. Mai mult, intruziunile cibernetice și accesul obținut pentru scopuri de spionaj cibernetic pot fi la fel de ușor exploatare pentru a lansa operațiuni disruptive sau distructive (Devanny, Martin & Stevens, 2021). Totodată, operațiunile de influențare cibernetică, lansate pentru a crește polarizările din societate, dar și cele de spionaj cibernetic ar putea să fie intensificate în anii următori, ținând cont de tensiunile dintre principalii actori internaționali (Maschmeyer & Dunn Cavelty, 2022).

Spionajul cibernetic reprezintă o activitate normală atâta vreme cât nu afectează negativ infrastructura critică. În cazul Rusiei, statele euroatlantice au deja experiență și pot anticipa că operațiunile de spionaj cibernetic ale Moscovei sunt deseori urmate de campanii de dezinformare și scurgeri de date sau maschează, de fapt, pre-poziționări sau atacuri cibernetice de ștergere a datelor. Totuși, China s-a axat în ultimii 20 de ani pe operațiuni de spionaj, și nu pe acțiuni perturbatoare sau distructive. Astfel, o campanie de tipul Volt Typhoon poate să ia prin surprindere decidenții.

Recomandări

Principalele măsuri pentru a gestiona impactul unei operațiuni ca Salt Typhoon sunt: identificarea magnitudinii operațiunii, oprirea extinderii acesteia, eliminarea intruziunilor din rețele și actualizarea sau înlocuirea echipamentelor de telecomunicații pentru a le face mai puțin vulnerabile la alte operațiuni viitoare (Lonergan & Poznansky 2025).

Statele occidentale trebuie să continue politica de *naming and shaming* ca răspuns la astfel de campanii cibernetice – **atribuirea publică a statului care a lansat operațiunea și emiterea de comunicate comune cu cât mai multe state.** Un alt aspect în acest caz este și **punerea sub acuzare a celor găsiți responsabili și descrierea metodelor exacte de operare ale hackerilor** – element care poate ajuta la identificarea unor tipare în viitor și care poate descuraja operațiuni similare ulterioare împotriva altor state. Totodată, **inițiativele internaționale pentru ameliorarea tensiunilor interstatale în spațiul cibernetic** ar trebui să

include și țări care nu sunt neapărat în sfera de *like-minded states* pentru democrațiile occidentale, pentru cât mai multă legitimitate la nivel internațional.

Comunicarea publică a faptului că un stat afectat de astfel de operațiuni este dispus să aleagă orice măsuri pentru a se apăra reprezintă tot o formă de descurajare. Statele Unite și aliații trebuie să continue politica de a transmite public și răspicat Chinei că perturbarea serviciilor critice americane sau din alte state aliante este inacceptabilă și va genera consecințe serioase (Martin 2025).

În plus, **spionajul tradițional poate fi contracarat printr-o mai bună securizare a datelor din serverele infrastructurilor critice și a rețelelor strâns legate de securitatea națională.** Totodată, reducerea intensității operațiunilor cibernetice străine și diminuarea riscului ca anumite state să lanseze atacuri distructive poate fi obținută și prin **îmbunătățirea relațiilor diplomatice și comerciale și prin ameliorarea tensiunilor internaționale.**

Totuși, **acțiunile contracarare și pedepsire a spionajului cibernetic interstatal trebuie dublate și de măsuri precise pentru a limita utilizarea spyware-urilor comerciale,** disponibile pentru o serie largă de actori, chiar dacă cele mai sofisticate rămân disponibile doar pentru guverne. Aceste măsuri includ **controlul exporturilor, sancțiuni pentru companii și statele** care permit abuzul acestor software-uri, dar și a statelor care le utilizează abuziv.

BIBLIOGRAFIE

- Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, 15(1), 35–57.
- CISA. (2024, September 5). *Russian Military Cyber Actors Target US and Global Critical Infrastructure*. CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a>
- CISA. (2025, May 21). *Russian GRU Targeting Western Logistics Entities and Technology Companies*. CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a>
- Davidson, H. (2024, February 13). Explainer: What is Volt Typhoon and why is it the ‘defining threat of our generation’? *The Guardian*.

<https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer>

Deibert, R. J. (2022). The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. *Foreign Affairs*. <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert>

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, 6(3), 429–450. <https://doi.org/10.1080/23738871.2021.2000628>

Dunn Cavelt, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20(3), 701–715. <https://doi.org/10.1007/s11948-014-9551-y>

ENISA. (2020). *Cyber Espionage* (ENISA Threat Landscape). ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage>

European Parliament. (2023). *Investigation of the use of Pegasus and equivalent surveillance spyware*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA\(2023\)747923_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf)

France-Presse, A. (2024, December 31). Beijing denies involvement in US treasury cyber-attack. *The Guardian*. <https://www.theguardian.com/technology/2024/dec/31/beijing-denies-involvement-in-us-treasury-cyber-attack>

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, 43(3), 141–189. https://doi.org/10.1162/isec_a_00337

GOV.UK. (2024, March 28). *Efforts to counter the proliferation and misuse of commercial spyware: Joint statement*. GOV.UK. <https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement>

Greenberg, A. (2025a). A Hacker Group Within Russia's Notorious Sandworm Unit Is Breaching Western Networks. *Wired*. <https://www.wired.com/story/russia-sandworm-badpilot-cyberattacks-western-countries/>

- Greenberg, A. (2025b). China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers. *Wired*. <https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/>
- Greenberg, A., & Newman, L. H. (2023). China Hacks US Critical Networks in Guam, Raising Cyberwar Fears. *Wired*. <https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/>
- Heilweil, R., Starks, T., Vicens, A., & Groll, E. (2024). Federal government affected by Russian breach of Microsoft. *CyberScoop*. <https://cyberscoop.com/federal-government-russian-breach-microsoft/>
- Higgins, A., & Scheutze, C. F. (2024). Suddenly, Chinese Spies Seem to Be Popping Up All Over Europe. *The New York Times*. <https://www.nytimes.com/2024/04/27/world/europe/china-spies.html>
- Iyengar, R. (2023). North Korea's Hackers Prioritize Espionage Over Cryptocurrency. *Foreign Policy*. <https://foreignpolicy.com/2023/06/23/north-korea-cyber-espionage-cryptocurrency-theft/>
- Kirchgaessner, S. (2024, May 30). Critics of Putin and his allies targeted with spyware inside the EU. *The Guardian*. <https://www.theguardian.com/technology/article/2024/may/30/critics-of-putin-and-his-allies-targeted-with-spyware-inside-the-eu>
- Lonergan, E., & Poznansky, M. (2025, February 25). A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats. *War on the Rocks*. <https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/>
- Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, 61(1), 72–86. <https://doi.org/10.1177/00223433231220264>
- Martin, M., Ciaran. (2025). Typhoons in Cyberspace. *RUSI*. <https://www.rusi.org/explore-our-research/publications/commentary/typhoons-cyberspace>
- Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, 46(3), 570–594. <https://doi.org/10.1080/01402390.2022.2104253>

- Maschmeyer, L., & Dunn Cavelty, M. (2022). Goodbye Cyberwar: Ukraine as Reality Check. *Policy Perspectives*, 10(3). <https://doi.org/10.3929/ETHZ-B-000549252>
- Miller, M. (2025, May 6). Israeli spyware giant NSO Group ordered to pay nearly \$170M to WhatsApp for hacking accounts. *POLITICO*. <https://www.politico.com/news/2025/05/06/nso-group-pegasus-whatsapp-hack-170-million-damages-00332155>
- Montgomery, B. (2024, December 12). Why did China hack the world's phone networks? *The Guardian*. <https://www.theguardian.com/technology/2024/dec/09/why-did-china-hack-the-worlds-phone-networks>
- Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber Operations during the Russo-Ukrainian War. *CSIS*. <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>
- Perloth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury.
- Reuters. (2023, June 9). China: 'Hacker empire' US is 'spreading rumours' with talk of Cuba spy station. *Reuters*. <https://www.reuters.com/world/china-hacker-empire-us-is-spreading-rumours-with-talk-cuba-spy-station-2023-06-09/>
- Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. <https://doi.org/10.1080/01402390.2011.608939>
- Robins-Early, N. (2024, March 26). US and UK unveil sanctions against Chinese state-backed hackers over alleged 'malicious' attacks. *The Guardian*. <https://www.theguardian.com/technology/2024/mar/25/us-sanctions-chinese-hackers>
- Sanger, D. E. (2023). *Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?* <https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html>
- Sanger, D. E., & Barnes, J. E. (2024). China's Hacking Reached Deep Into U.S. Telecoms. *The New York Times*. <https://www.nytimes.com/2024/11/21/us/politics/china-hacking-telecommunications.html>
- Sanger, D. E., & Landler, M. (2024). U.S. and Britain Accuse China of Cyberespionage Campaign. *The New York Times*. <https://www.nytimes.com/2024/03/25/us/politics/china-hacking-us-sanctions.html>



- Smalley, S. (2024). *How Italy became an unexpected spyware hub*. <https://therecord.media/how-italy-became-an-unexpected-spyware-hub>
- Smalley, Suzanne. (2024). *Polish Parliament strips official of immunity, clearing path for prosecution in spyware scandal*. <https://therecord.media/polish-parliament-strips-official-of-immunity-pegasus-spyware>
- Stahie, S. (2024). *US Bans Kaspersky Software for Users and Companies; Customers Advised to Seek Trusted Alternatives*. Bitdefender. <https://www.bitdefender.com/en-us/blog/hotforsecurity/us-bans-kaspersky>
- Tait, R. (2024, December 14). Democrats and Republicans condemn espionage-driven Chinese hack. *The Guardian*. <https://www.theguardian.com/world/2024/dec/13/democrats-republicans-condemn-salt-typhoon-hack>
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.
- Volz, D. (2025). In Secret Meeting, China Acknowledged Role in U.S. Infrastructure. *The Wall Street Journal*. <https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb>
- Zilincik, S., Myklin, M., & Kovanda, P. (2019). Cyber power and control: A perspective from strategic theory. *Journal of Cyber Policy*, 4(2), 290–301. <https://doi.org/10.1080/23738871.2019.1635177>

IDR

Institutul Diplomatic Român

Misiune. Institutul Diplomatic Român (IDR) își asumă misiunea de a contribui substanțial la creșterea calității diplomației românești prin formare, educare continuă, cercetare, prin dezvoltarea gândirii critice și strategice, prin conectare internațională. O politică externă bună servește unei politici interne benefice.

Principii: valorizarea resurselor umane, profesionalismul, respectul și dialogul, responsabilitatea pentru comunitate.

Pornind de la atribuțiile legale fondatoare ale IDR, dezvoltarea în continuare a institutului se realizează, în funcție de nevoile identificate în MAE, pe următoarele patru direcții:

- Formarea și educarea continuă a diplomaților și a altor categorii de cursanți;
- Aprofundarea dimensiunii de cercetare și expertiză pe spații regionale și problematice funcționale;
- Funcționarea IDR ca *think-tank* al MAE;
- Integrarea IDR în cadrul unei rețele internaționale de institute relevante similare.

Autor: Claudiu Codreanu (PhD) este analist la Institutul Diplomatic Român – Serviciul Furnizare de Expertiză pentru MAE.

Seria Policy Paper IDR

ISSN 2285-8938

ISSN-L 2285-8938

Imagine copertă: <https://unsplash.com/photos/black-towers-during-sunset-0C9VmZUqcT8>

Institutul Diplomatic Român - IDR

<https://www.idr.ro/en/> | secretariat@idr.ro

Primăverii 17, sector 1, București, 011972