IDR
Romanian Diplomatic Institute

Ministerul Afacerilor Externe

POLICY BRIEF nr. 93/2026

SANCȚIUNILE UE PENTRU OPERAȚIUNI CIBERNETICE

Cazul Turla și atacurile cibernetice împotriva Poloniei

Claudiu Codreanu

Sancțiunile UE pentru operațiuni cibernetice: Cazul Turla și atacurile cibernetice împotriva Poloniei [1]

Claudiu Codreanu [2]

Analist, Institutul Diplomatic Român

Policy Brief Series no. 93 / 2026

Published by: Romanian Diplomatic Institute

ISSN: 2066-5989

Abstract

În iulie 2026, Uniunea Europeană și Regatul Unit au impus sancțiuni mai multor indivizi și entități pentru o serie de operațiuni cibernetice care au vizat statele europene. În cele două comunicate publicate, grupul Turla a fost atribuit Federației Ruse, mai exact FSB-ului. În plus, ambele comunicate atribuie Rusiei atacul cibernetic asupra infrastructurii energetice poloneze din decembrie 2025. În decembrie 2025, rețeaua electrică a Poloniei a fost vizată de mai multe atacuri cibernetice care puteau provoca întreruperi de curent pentru sute de mii de persoane. Grupul de hackeri guvernamentali cunoscut drept „Turla" are un istoric bogat de operațiuni, fiind în principal asociat cu spionajul cibernetic, iar atacul asupra Poloniei a reprezentat o escaladare în direcția operațiunilor cu obiective de perturbare sau sabotaj. Articolul examinează sancțiunile recente impuse de Uniunea Europeană și Regatul Unit, punându-le în contextul altor măsuri similare adoptate de UE sau de Statele Unite. Totodată, este evidențiată importanța atacului cibernetic asupra Poloniei, luând în considerare alte incidente similare, precum operațiunile cibernetice rusești împotriva Ucrainei din 2015 și 2016. În final, articolul propune o serie de recomandări, precum nevoia statelor euro-atlantice de a merge mai departe de sancțiuni, dezvoltarea propriilor capabilități de atribuire publică în cadrul UE și necesitatea de a evidenția în mod particular incidente majore precum cel din Polonia.

Cuvinte cheie: sancțiuni, Uniunea Europeană, operațiuni cibernetice, atribuire publică, Polonia, Turla.

[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

Pe 13 iulie 2026, Uniunea Europeană, împreună cu Regatul Unit, au impus o serie de sancțiuni în urma unor operațiuni cibernetice ale Federației Ruse (Council of the EU, 2026; GOV.UK, 2026). Sancțiunile au vizat nouă indivizi și a patru entități: ofițeri de informații ruși, infractori cibernetici și companii private care au contribuit la eforturile ofensive cibernetice ale Moscovei. De asemenea, comunicatul britanic menționează că a fost sancționată compania IMPULS (GOV.UK, 2026).

Comunicatele publice publicate de UE și Regatul Unit au **atribuit public** o serie semnificativă de operațiuni și campanii cibernetice Federației Ruse (Council of the EU, 2026). Mai exact, activitățile grupului Turla au fost atribuite Centrului 16 al FSB (Serviciul Federal de Securitate) și unor agenți ai GRU (Direcția Principală a Statului Major a Forțelor Armate). FSB a fost acuzat de infiltrări cibernetice în cel puțin nouă state europene, printre care Franța, Germania și România. Totodată, FSB-ul a fost acuzat și de operațiuni de sabotaj împotriva infrastructurii critice din sectorul energetic (Council of the EU, 2026).

Una dintre cele mai semnificative operațiuni cibernetice atribuită grupului Turla (și, deci, Rusiei) este cea care a vizat Polonia la finalul anului trecut. **Pe 29-30 decembrie 2025, infrastructura energetică a Poloniei a fost vizată de un atac cibernetic major**, autoritățile precizând că obiectivul a fost unul distructiv (CERT.PL, 2026). Operațiunea a vizat mai multe parcuri fotovoltaice și eoliene, dar și două centrale de cogenerare (care produc combinat energie electrică și termică). Comunicatul britanic precizează că atacul ar fi putut duce la o pană de curent pentru 500.000 cetățeni în mijlocul iernii (GOV.UK, 2026).

De notat este că UE nu adoptă aceeași retorică cu privire la atacul cibernetic, Regatul Unit evidențiind mai clar incidentul. Polonia este menționată vag în comunicatul UE, fiind adăugată în listă laolaltă cu Germania, Slovacia, Austria ș.a.m.d. Atacul cibernetic din decembrie este menționat foarte succint: „Recent, în Polonia, Centrul 16 a desfășurat operațiuni disruptive de sabotaj împotriva infrastructurii critice, inclusiv împotriva unor centrale de cogenerare” (Council of the EU, 2026).

Așadar, articolul examinează sancțiunile impuse de UE și Regatul Unit pentru seria de operațiuni cibernetice rusești asociate grupului Turla, punând accentul pe cazul atacului

cibernetic asupra Poloniei. Totodată, sancțiunile din iulie 2026 sunt puse în contextul măsurilor mai vechi luate de actori precum UE și SUA, fiind discutate și limitele acestora, dar și nevoia clarificării procesului de atribuire publică, esențial pentru orice demers ulterior. Atacul cibernetic asupra infrastructurii energetice poloneze din decembrie 2025 este pus în context cu atacuri rusești precedente din 2015-2016 asupra rețelei electrice ucrainene. În final, articolul propune o serie de recomandări, precum nevoia de a merge mai departe de sancțiuni, dezvoltarea propriilor capabilități tehnice de atribuire publică în UE și/sau în statele membre și necesitatea de a evidenția în mod particular incidente majore precum cel din Polonia, ținând cont că în comunicatul UE atacul cibernetic rusesc este menționat foarte succint.

CONTEXT ȘI EVENIMENTE

Sancțiunile UE pentru operațiuni cibernetice

La mijlocul deceniului trecut, statele euro-atlantice au început să trateze cu mai multă seriozitate operațiunile cibernetice malițioase, odată cu intensificarea efectelor acestora. **Două dintre răspunsurile principale adoptate de către acestea au fost emiterea de comunicate privind atribuirea publică a operațiunilor către anumiți actori și impunerea de sancțiuni**. Spre exemplu, atât UE, cât și SUA, au adoptat sancțiuni împotriva grupului de hackeri guvernamentali nord-coreeni Lazarus și ai altor grupări care au desfășurat operațiuni cibernetice în spațiul euro-atlantic (Blickhan, 2026; Erausquin, 2025; Moret & Pawlak, 2017), laolaltă cu sancțiunile ONU împotriva Coreei de Nord. Statele Unite au impus primele sancțiuni cibernetice unilaterale în 2015, iar din 2017 au început să pună sub acuzare indivizi acuzați de infiltrări cibernetice desfășurate de actori statali, în cea mai mare parte ofițeri de informații și asociați ai statului rus, chinez, nord-coreean sau iranian (Blickhan, 2026; Erausquin, 2025; Moret & Pawlak, 2017).

În schimb, **cadrul Uniunii Europene pentru sancțiuni vis-a-vis de operațiuni cibernetice a fost adoptat în 2019, iar primele sancțiuni au fost introduse în iulie 2020** (Blickhan, 2026; Erausquin, 2025; Bendiek & Schulze, 2021). Regimul de sancțiuni cibernetice a fost adoptat în cadrul instrumentarului pentru diplomație cibernetică, permițând blocarea activelor și interdicții de călătorie pentru activități cibernetice malițioase care au țintit state sau

instituții UE. Începând cu 2024 și până în prezent, Uniunea Europeană a adoptat sancțiuni împotriva Rusiei, Coreei de Nord, Chinei și Iranului (Blickhan, 2026; Erausquin, 2025).

Obiectivul principal al sancțiunilor este de a încerca să constrângă actorul vizat prin **creșterea costurilor activităților** pe care le desfășoară sau prin forțarea de a își **schimba strategia** în schimbul unor pierderi (Pawlak & Biersteker, 2019). **Sancțiunile** au, totodată, un rol normativ, fiind folosite pentru a **descuraja anumite comportamente** considerate indezirabile sau iresponsabile prin transmiterea unor semnale normative – pentru a **promova norme** deja recunoscute la nivel internațional sau pentru a promova altele noi (Pawlak & Biersteker, 2019). Rolul atribuirilor publice este similar. **Atribuirea publică** are ca obiective: **stabilirea și consolidarea unor norme**, promovând un set de standarde clare pentru comportamentul adecvat al actorilor statali și non-statali în spațiul cibernetic; **coerciția**, în sensul de descurajare și constrângere al actorilor malițioși; **afectarea eficienței operațiunilor malițioase**, atât prin determinarea actorilor de a consuma resurse pentru dezvoltarea de noi capabilități după dezvăluirea celor existente, cât și prin activități de contrainformații pentru a ascunde mai bine urmele; **prevenția și apărarea**, atribuirea publică conducând la dezvoltarea mai rapidă de îmbunătățiri de securitate ale sistemelor vizate și securizarea vulnerabilităților exploatate anterior (Egloff & Smeets, 2021). Astfel, atribuirea publică se referă la „dezvăluirea publică a informațiilor cu privire la activități cibernetice malițioase", aceasta vizând fie un anumit echipament tehnic (ex. sistem, rețea, familie de malware etc.), un anumit individ sau indivizi specifici și/sau un adversar considerat responsabil (Egloff & Smeets, 2021, 3).

Grupul Turla, asociat serviciilor de informații rusești

Turla are un istoric îndelungat de operațiuni cibernetice, dar în cea mai mare parte s-a concentrat pe spionaj cibernetic împotriva ministerelor afacerilor externe și de apărare din țările euro-atlantice în cadrul unor operațiuni deosebit de sofisticate și inovative (Jones, 2026; Insikt Group, 2026). **O serie vastă de campanii cibernetice au fost asociate Turla, cele mai vechi fiind identificate încă din sfârșitul anilor 2000**, Turla fiind numele dat de cercetătorii din domeniul securității cibernetice malware-ului utilizat în infiltrări (Apps & Finkle, 2026). Spre exemplu, un raport din 2023 al agenției americane pentru securitate cibernetică (CISA – *Cybersecurity and Infrastructure Security Agency*) arăta că Centrul 16 al FSB a dezvoltat malware-ul Snake încă din 2003-2004, acesta fiind utilizat în instrumentarul Turla în operațiuni

care au țintit 50 de state în ultimii 20 de ani, inclusiv SUA și chiar Rusia (CISA, 2023; Jones, 2026).

Turla este cunoscut și ca Secret Blizzard, Snake sau Venomous Bear, fiind considerat unul dintre cele mai longevive grupuri de spionaj cibernetic ale Rusiei (Greenberg, 2025**). A mai fost asociat în trecut cu FSB-ul de autorități ale mai multor state euro-atlantice, dar și de cercetători independenți sau companii private** (Antoniuk, 2026). Numele date malware-urilor sau APT-urilor (*Advanced Persistent Threats* – amenințări avansate persistente) provin, în cea mai mare parte, de la companii private din domeniul securității cibernetice sau de la cercetători independenți care se ocupă cu urmărirea lor. Dacă numele diverse asociate Turla pot provoca confuzii, Google se află acum într-un proces de redenumire a APT-urilor, folosind pentru statele din care provin amenințările cibernetice un (alt) nou sistem de denumiri, cum ar fi RELIC pentru Rusia, CASTLE pentru China sau ION pentru Coreea de Nord (Google Threat Intelligence Group, 2026).

Conform centrului de cercetare Insikt Group, țintele principale ale Turla sunt organizațiile guvernamentale (cu precădere cele legate de diplomație/afaceri internaționale, armată și sectorul energiei), mediul academic și publicațiile media. În ceea ce privește regiunile vizate de Turla, majoritatea operațiunilor au vizat statele europene și cele din spațiul ex-sovietic (Insikt Group, 2026). Cu toate acestea, grupul s-a aflat în centrul atenției pentru o operațiune fără precedent, mai ales că a vizat capabilități ale unui stat aliat – Iranul. În 2019, mai multe companii de securitate cibernetică și agenții de resort din țările euro-atlantice au dezvăluit că grupul Turla s-a infiltrat într-o rețea operațională a APT34 (un grup de hackeri guvernamentali iranieni), reușind să acapareze rețeaua și să o exploateze (Insikt Group, 2026). Operațiunea a reprezentat prima instanță când infrastructura operațională în spațiul cibernetic a unui actor statal este preluată, de fapt deturnată sau capturată, de un grup de hackeri dintr-un alt stat (Insikt Group, 2026). Chiar dacă nu este clar care a fost obiectivul acestei operațiuni, și nici nivelul de comunicare sau cooperare cu autoritățile iraniene, operațiunea a demonstrat capabilitățile hackerilor guvernamentali ruși.

Atacul cibernetic asupra rețelei electrice a Poloniei

În 29-30 decembrie, o serie de atacuri cibernetice au țintit infrastructura energetică a Poloniei, fiind vizate în mod direct două centrale de cogenerare pentru energie termică și electrică care serveau aproape 500.000 de cetățeni (The Chancellery of the Prime

Minister, 2026; CERT.PL 2026a). Totodată, atacurile au vizat și un sistem care gestiona energia produsă din surse regenerabile, fiind direcționate către 30 de parcuri eoliene și fotovoltaice (The Chancellery of the Prime Minister, 2026; CERT.PL, 2026a). În timp ce activitatea unor sisteme pentru eoliene și fotovoltaice a fost relativ afectată, atacul asupra centralei de cogenerare nu și-a îndeplinit obiectivele (CERT.PL, 2026a).

Conform CERT.PL (Centrul de Răspuns Rapid la Incidente de Securitate Cibernetică al Poloniei), **atacurile cibernetice au avut în mod clar obiective distructive, mai ales ținând cont de perioada aleasă** – în ajunul Anului Nou și în contextul unor temperaturi scăzute și furtuni de zăpadă. Atacurile cibernetice au afectat atât sistemele IT, cât și echipamentele industriale fizice, sisteme care nu au fost vizate de operațiuni cibernetice precedente (CERT.PL, 2026a). Astfel, **CERT.PL a subliniat că obiectivul atacurilor cibernetice asupra centralei de cogenerare a fost unul de sabotaj**, țintind distrugerea ireversibilă a datelor din rețeaua internă printr-un malware tip *wiper* (un tip de program malițios care șterge datele din sistemele în care este desfășurat). Conform rapoartelor, hackerii guvernamentali ruși au avut acces în rețeaua centralei de cogenerare timp de cel puțin cinci luni (Zetter 2026b).

În august 2026, CERT.PL a publicat un nou raport cu privire la incident. În noul raport, centrul polonez a dezvăluit că a descoperit un alt atac cibernetic care a vizat o a altă centrală de cogenerare (care furniza căldură pentru 50.000 de rezidenți), un incident care rămăsese neobservat inițial (CERT.PL 2026b). Atacul a condus la oprirea temporară a unei turbine de aburi și a sistemului de tratare a apei, întrerupând procesul de cogenerare, dar problemele cauzate au fost depistate și rezolvate rapid de operatorii centralei (CERT.PL 2026b).

În ceea ce privește **atribuirea**, Centrul de Răspuns Rapid la Incidente de Securitate Cibernetică al Poloniei arată că, analizând infrastructura utilizată în atacul cibernetic (serverele compromise, router-ele, tiparele traficului ș.a.m.d.), este remarcată, cu un nivel ridicat de încredere, o suprapunere considerabilă cu infrastructura utilizată de cluster-ul descris de Microsoft ca *Ghost Blizard* sau de Cisco ca *Static Tundra*, acestea fiind asociate statului rus (CERT.PL, 2026a). Inițial, companiile de securitate cibernetică ESET și Dragos au atribuit atacul grupului Sandworm (asociat GRU), ținând cont că atacurile asupra sectorului energetic au fost frecvent asociate acestui malware (Antoniuk & Martin, 2026; Zetter, 2026a). Sandworm, numele unui grup de hackeri operat de GRU, a fost în spatele atacurilor cibernetice asupra rețelei electrice ucrainene din 2015 și 2016 (Zetter, 2026a). Totuși, CERT-ul polonez a urmărit infrastructura atacului și a reușit să o lege de FSB.

În urma unei ședințe de guvern din 14 ianuarie, premierul polonez Donald Tusk a afirmat că atacul cibernetic **nu a produs efecte negative sau întreruperi de curent**, adăugând, totuși, că securitatea sistemului energetic trebuie consolidată în continuare (The Chancellery of the Prime Minister, 2026). Polonia reprezintă una dintre țintele principale ale operațiunilor cibernetice malițioase ale Rusiei și Iranului împotriva statelor europene. Spre exemplu, în martie 2026, autoritățile poloneze au comunicat că Centrul Național pentru Cercetare Nucleară a fost vizat de un atac cibernetic, acesta fiind respins (Clark, 2026). Ministrul Digitalizării, Krzysztof Gawkowski, a afirmat atunci că, cel mai probabil, Iranul s-ar fi aflat în spatele operațiunii (Clark, 2026).

ATACUL CIBERNETIC ÎMPOTRIVA POLONIEI ȘI NEVOIA DE A MERGE MAI DEPARTE DE SANCȚIUNI

Semnificația și impactul atacului cibernetic rusesc asupra Poloniei

Atacurile asupra infrastructurilor critice civile sunt din ce în ce mai puțin rare sau izolate. **În ultimii ani, actori precum Iran sau Rusia au început să vizeze din ce în ce mai mult rețelele infrastructurii alimentării cu apă potabilă sau cele din energie** – atât în mod direct pentru a provoca pagube care pot afecta populația, cât și pentru că multe din sisteme sunt învechite sau au vulnerabilități majore și permit atacuri oportuniste. Spre exemplu, în luna august a acestui an, mai multe **stații de filtrare a apei** din Statele Unite au fost țintite de o serie de atacuri cibernetice (Robins-Early & Kerr, 2026). Au fost detectate intruziuni cibernetice în 11 state americane, printre care Georgia, Michigan sau Minnesota, unde furnizarea cu apă potabilă a fost afectată după afectarea a 30 de sisteme de alimentare (Sherman, 2026). Conform investigațiilor *The New York Times* și *Washington Post*, mai mulți oficiali anonimi au guvernului american au susținut că, cel mai probabil, **Iranul** a lansat atacurile cibernetice (Robins-Early & Kerr, 2026; Sherman, 2026).

Compania de securitate cibernetică Dragos a precizat că hackerii din spatele atacului asupra Poloniei din 2025 au avut potențialul de a cauza mai multe daune, dar atacul nu a fost unul țintit și bine-pregătit, ci a fost mai degrabă unul oportunist (Zetter, 2026a). Metode similare au fost utilizate în atacul cibernetic rusesc împotriva Ucrainei din decembrie 2015. Atunci, hackerii guvernamentali ruși s-au infiltrat în rețelele unor stații de distribuție a energiei

electrice din vestul Ucrainei, reușind să provoace o pană de curent și să șteargă toate datele din sistemele IT pentru a perturba munca operatorilor de a restabili furnizarea energiei (Zetter, 2026a). În cazul Poloniei, **țintirea concomitentă a mai multor stații de distribuție a energiei electrice sau a mai multor parcuri fotovoltaice/eoliene într-un atac cibernetic coordonat putea conduce la un impact major și la o pană de curent extinsă** (Zetter, 2026a). Chiar dacă nu a fost cauzată de operațiuni cibernetice, pana de curent din Spania și Portugalia din 2025 a arătat care pot fi efectele asupra rețelei energetice atunci când apar fluctuații de frecvență în sistemele de energie regenerabilă (Zetter, 2026a).

Până la operațiunile împotriva Poloniei din decembrie 2025, activitățile cibernetice ale Turla erau orientate în principal în aria spionajului cibernetic. Spionajul reprezintă una dintre formele principale de operațiuni cibernetice la nivel internațional, în special la nivel interstatal, dar și una dintre cele mai agreate și obișnuite forme de activități cibernetice malițioase. Problemele cele mai mari pe care le creează spionajul cibernetic apar, mai degrabă, din exploatarea unor vulnerabilități sau provocarea unor breșe care lasă apoi „ușa" deschisă pentru alți actori care pot avea obiective distructive. Astfel, **atacul cibernetic asupra Poloniei ar fi trebuit să fie încadrat într-un alt comunicat**. Comunicatele UE și ale Regatului Unit prin care sunt atribuite publice campaniile cibernetice ale APT-ului Turla doar menționează succint atacul asupra infrastructurii energetice poloneze, cu toate că acesta reprezintă cel mai grav incident. Atacul cibernetic asupra rețelei electrice a Poloniei reprezintă una dintre cele mai periculoase și serioase operațiuni rusești împotriva statelor europene din ultimii ani. Rusia a desfășurat constant, la fel ca Iranul, operațiuni care să testeze vulnerabilități în rețele critice, sau chiar să încerce să exploateze anumite breșe cu scopuri de a perturba infrastructurile. Totuși, un atac care țintește direct elemente critice ale infrastructurii energetice dintr-un stat UE reprezintă o escaladare.

Într-o măsură considerabilă, **atacurile cibernetice împotriva rețelei electrice poloneze pot fi comparate cu cele care au vizat rețeaua ucraineană în 2015 și 2016**, mai ales că și atacul asupra Poloniei a avut loc tot în luna decembrie. În 2015, atacurile cibernetice rusești au reușit să provoace întreruperi de curent în mai multe regiuni ucrainene pentru sute de mii de persoane pentru mai multe ore în perioada sărbătorilor de iarnă și în contextul unor temperaturi scăzute. Totuși, operațiunile împotriva Ucrainei au fost bine pregătite și țintite, având obiective strategice clare de a perturba infrastructura energetică ucraineană pentru a afecta populația civilă și pentru a scădea încrederea cetățenilor în instituțiile ucrainene. Scopul

final al operațiunilor cibernetice rusești din 2014-2022 a fost ca Ucraina **să renunțe la aspirațiile euro-atlantice**. În schimb, atacurile cibernetice împotriva Poloniei au fost mai degrabă **oportuniste**, ținând cont că nu au fost identificate semne că ar fi existat un plan bine stabilit de a afecta în mod specific acea parte a infrastructurii sau un obiectiv clar de a provoca o pană de curent cu un anumit scop. Orișicât, **chiar dacă atacul cibernetic a fost unul oportunist, acțiunea se încadrează tot în categoria sabotajului, având intenții distructive**.

Cu toate acestea, în ambele cazuri poate fi observată **importanța unei apărări cibernetice bine pusă la punct** – atacurile rusești asupra Ucrainei din decembrie 2016, chiar dacă au fost sofisticate, au fost gestionate mai bine de autorități și de operatorii rețelei, fiind restabilită alimentarea energiei electrice mult mai repede, similar cu o pană obișnuită. Mai mult decât atât, atacul cibernetic asupra Poloniei nici nu a reușit să provoace o întrerupere de curent datorită contramăsurilor de securitate cibernetică și a răspunsului prompt al operatorilor centralelor.

Limitele sancțiunilor

Există multiple critici cu privire la sancțiunile cibernetice ale UE. Pe de o parte, există un oarecare consens că **sancțiunile pot perturba infrastructura largă utilizată de hackerii guvernamentali**, precum nevoia de a schimba o parte din rețele sau companiile utilizate drept paravan din cauza numirii lor publice sau mutarea unor activități în rețele clandestine (Erausquin, 2025). Totuși, pe de altă parte, **sancțiunile nu au un impact direct prea ridicat deoarece, deseori, indivizii vizați nu au active în Europa și nu circulă des în afara țării lor** (Erausquin, 2025). Spre exemplu, două companii care au vizate de sancțiuni UE pentru sprijinirea operațiunilor cibernetice ale Federației Ruse au reușit să își continue activitățile doar prin transferarea resurselor într-o altă entitate legală, menținându-și infrastructura doar prin înregistrarea unor noi firme în alte țări (Stowe, 2025). Chiar și așa, sancțiunile reprezintă un pas în direcția potrivită. Până în iulie 2026, singurele răspunsuri adoptate de UE în contextul activităților Turla au fost emiterea unor recomandări la nivel național cu privire la gestionarea riscurilor (Blickhan, 2026).

Astfel, un aspect remarcat de literatura de specialitate este nevoia unei abordări integrate, care să meargă **mai departe de sancțiuni** (Erausquin, 2025; Moret & Pawlak, 2017). Spre exemplu, în urma atribuirilor publice emise în ultimii ani, **Statele Unite au emis**

recomandări tehnice publice privind operațiunile cibernetice, anchete penale și puneri sub acuzare, dar și demersuri diplomatice (Erausquin, 2025). Polonia a convocat Ambasadorul rus de la Varșovia pentru discuții în urma repetatelor intruziuni și căderi de drone pe teritoriul Poloniei (Reuters 2026), dar nu a fost chemat la consultări în urma atacurilor cibernetice din decembrie 2025. În mod cert, dronele rusești care au planat și căzut pe teritoriul polonez reprezintă o amenințare mult mai mare la adresa cetățenilor din toate punctele de vedere, dar acest lucru nu înseamnă că o operațiune cibernetică țintită asupra rețelei energetice nu intră în aceeași zonă a încălcării suveranității statului și a punerii în pericol a populației civile. Spre exemplu, însărcinatul cu afaceri al Ambasadei Rusiei la Paris a fost convocat la Ministerul Afacerilor Externe în urma atribuirii publice a operațiunilor cibernetice Moscovei (Marzolf et al., 2026). Totodată, până în prezent nicio țară nu a mers atât de departe precum Albania în această privință. **În urma operațiunile cibernetice ale Iranului împotriva Albaniei din 2022, Tirana a luat decizia de a rupe legăturile diplomatice cu Teheranul pentru o perioadă nedeterminată**, acestea nefiind restabilite nici până în prezent (Gritten, 2022).

CONCLUZII ȘI RECOMANDĂRI

În contextul internațional actual, **este de așteptat ca incidența unor astfel de operațiuni să crească, crescând riscul unor atacuri distructive reușite**. Spre exemplu, în contextul campaniilor hibride rusești, hackerii guvernamentali ai Moscovei au desfășurat constant operațiuni cibernetice care au țintit infrastructura energetică a statelor euro-atlantice, fie cu obiective de destabilizare, fie cu obiective de spionaj. Totodată, incidente de acest fel nu sunt izolate doar la nivelul unor state ca Rusia și Iran, fiind utilizate în anumite contexte conflictuale și de state occidentale. Conform relatărilor din media americană, SUA au utilizat atacuri cibernetice împotriva rețelei de energie electrică a Venezuelei pentru a provoca pene de curent cu scopul de a perturba apărarea antiaeriană și comunicațiile militare în timpul intervenției militare din ianuarie 2026 (Barnes & Kurmanaev, 2026).

Există un risc crescut ca nu numai Rusia, ci și Iranul să încerce atacuri cibernetice asupra infrastructurilor critice europene și nord-americane, mai ales în zona energetică (ex. rețeaua electrică) și în cea a furnizării apei potabile sau a gestionării barajelor sau hidrocentralelor. CISA a emis încă din aprilie 2026 un avertisment cu privire la riscurile unor

atacuri cibernetice iraniene asupra infrastructurilor critice (Robins-Early & Kerr, 2026). În plus, pe lângă actori statali care pot avea obiective strategice clare de a perturba guvernele și de a crea instabilitate în societățile vizate, există și grupări de criminalitate cibernetică care se pot infiltra în diferite infrastructuri prin intermediul unor atacuri oportuniste cu scopul de a încerca obținerea unor răscumpărări financiare (ex. ransomware) sau pentru a-și demonstra capabilitățile.

Așadar, **statele membre UE ar trebui să depună mai multe eforturi pentru a consolida cooperarea pentru a publica propriile lor atribuiri publice cu privire la atacurile cibernetice care le-au vizat în mod direct**. Foarte puține state europene au publicat rapoarte privind atribuirea unor operațiuni cibernetice, neavând capabilitățile și rețelele de intelligence necesare pentru a investiga infrastructurile utilizate de actorii cibernetici sau de a merge chiar până la identificarea unor agenți specifici, firme sau unități militare (Soesanto, 2025). Determinarea originii unei operațiuni cibernetice, atribuirea publică, și mai ales, tehnică și politică (sau de intelligence) a atacului este o **precondiție esențială pentru a putea impune sancțiuni într-un mod cât mai legitim la nivel internațional** (Bendiek & Schulze, 2021). Cel puțin pentru procesul de atribuire publică, coordonarea în materie de intelligence cu Regatul Unit și Statele Unite rămâne esențială (Soesanto, 2025). Multe din criticile asupra instrumentarului de sancțiuni pe operațiuni cibernetice al Uniunii Europene vizau coordonarea insuficientă între UE cu Regatul Unit și SUA în adoptarea de sancțiuni și atribuiri publice (Martin 2024; Stowe, 2025; Blickhan, 2026; Soesanto, 2025).

Totuși, acest lucru nu înseamnă că UE nu ar trebui să își dezvolte propriile mecanisme interne de coordonare între statele membre, ci din contră. Capacitatea UE de atribuire este încă dependentă de schimbul de informații cu Statele Unite și Regatul Unit (Bendiek & Schulze, 2021). Spre exemplu, în septembrie 2024, **Estonia** a atribuit public atacurile cibernetice din 2020 Federației Ruse, numind trei membri ai unității GRU 29155, fiind prima dată în istorie când guvernul estonian a atribuit o campanie cibernetică unui actor statal străin (Soesanto, 2025). În mod similar, **Franța** a atribuit GRU o serie de operațiuni cibernetice în aprilie 2025, iar o lună mai târziu **Cehia** a atribuit o campanie de spionaj cibernetic grupului APT31, asociat serviciilor de intelligence ale Chinei (Erausquin, 2025). Atribuirea unei operațiuni la nivel național poate să fie un stimulent și o precondiție pentru a propune includerea actorilor respectivi pe lista de sancțiuni cibernetice ale UE. Până în prezent, Cehia, Estonia, Franța, Germania și Olanda au reușit să propună și să ducă până la adoptare

propriile pachete de sancțiuni pentru operațiuni cibernetice care le-au vizat în mod direct (Soesanto, 2025; Erausquin, 2025).

Totodată, dezvoltarea unor astfel de capabilități ar veni, totodată, în sprijinul eforturilor de a consolida **suveranitatea digitală și tehnologică a Uniunii Europene** – capabilități tehnice și de intelligence și o mai bună coordonare între statele membre pentru a realiza atribuirea publică fără a menține dependența crescută în această privință față de țările din grupul Five Eyes (mai ales SUA și Regatul Unit). Totuși, **această chestiune nu se referă la renunțarea sau diminuarea cooperării cu Washington sau Londra, ci chiar să aducă o contribuție netă la eforturile de atribuire proprii ale celor două state euroatlantice**, nu doar o reducere a dependenței.

De asemenea, devine din ce în ce mai importantă nevoia atragerii de susținere pentru sancțiuni din state terțe UE. Spre exemplu, un articol din jurnalul *European Security* din 2023 arată că, în cea mai mare parte, sancțiunile impuse de Uniunea Europeană au parte de legitimitate și în statele non-membre, fiind mai multe instanțe în care state non-UE s-au aliniat sancțiunilor (Cardwell & Moret, 2023). Acest lucru a putut fi observat și în cazul sancțiunilor impuse în iulie 2026 împotriva Turla, aliniindu-se la comunicatul public opt state non-UE. Comunicatul UE a fost semnat și de mai multe state non-UE, printre care Albania, Bosnia și Herțegovina, Macedonia de Nord, Muntenegru, Republica Moldova și Ucraina (Council of the EU, 2026).

Totodată, **operațiunile cibernetice majore care puteau provoca consecințe extinse, precum cea a Rusiei împotriva Poloniei din 2025, ar trebui să fie subiectul unor sancțiuni și comunicate separate**. Astfel de incidente nu ar trebui să fie trecute doar într-o listă lungă, laolaltă cu un istoric vag de operațiuni care au avut loc în ultimii 10-15 ani, ci să fie descrise pe larg. Sancțiunile adoptate de UE au menționat, în general, întreaga serie de campanii cibernetice ale Turla, și nu vizează nu vizează în mod specific atacurile din Polonia. Comunicatul UE ar fi trebuit să pună mai mult accentul pe atacul cibernetic împotriva Poloniei, fiind cel mai recentă operațiune majoră din ultimii ani, și poate chiar cea mai gravă – atacul fiind menționat mult mai clar în comunicatul Regatului Unit.

BIBLIOGRAFIE

Antoniuk, D. (2026, June 26). *Turla group adds more malware to Russia's espionage efforts against Ukraine*. The Record. https://therecord.media/russia-turla-espionage-ukraine-stockstay-malware

Antoniuk, D., & Martin, A. (2026, July 13). *Russia's FSB blamed for Poland grid attack as UK and EU impose first joint cyber sanctions*. The Record. https://therecord.media/russia-blamed-for-poland-grid-cyberattack-in-joint-uk-eu-sanctions-package

Apps, P., & Finkle, J. (2014, March 7). *Suspected Russian spyware Turla targets Europe, United States*. Reuters. https://www.reuters.com/article/technology/suspected-russian-spyware-turla-targets-europe-united-states-idUSBREA260YI/

Barnes, J. E., & Kurmanaev, A. (2026, January 15). Cyberattack in Venezuela Demonstrated Precision of U.S. Capabilities—The New York Times. *The New York Times*. https://www.nytimes.com/2026/01/15/us/politics/cyberattack-venezuela-military.html

Bendiek, A., & Schulze, M. (2021). Attribution: A major challenge for EU cyber sanctions: an analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW. In *SWP Research Paper 11/2021* (Version 1). Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs. https://doi.org/10.18449/2021RP11

Blickhan, A. (2026, June 16). *Can Europe's APT response keep up?* Binding Hook. https://bindinghook.com/can-europes-apt-response-keep-up/

Cardwell, P. J., & Moret, E. (2023). The EU, sanctions and regional leadership. *European Security*, *32*(1), 1–21. https://doi.org/10.1080/09662839.2022.2085997

CERT.PL. (2026a, January 30). *Energy Sector Incident Report—29 December 2025*. CERT Polska. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

CERT.PL. (2026b, August 8). *Follow-Up Report of the December 2025 Energy Sector Incident*. CERT Polska. https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/

CISA. (2023, May 9). *Hunting Russian Intelligence "Snake" Malware*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

Clark, S. (2026, March 12). *Poland investigates Iran links behind cyberattack on nuclear facility*. POLITICO. https://www.politico.eu/article/poland-investigates-iran-links-as-hackers-target-nuclear-facility/

Council of the EU. (2026, July 13). *Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners—Consilium*. European Council. Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies*, *46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117

Erausquin, G. S. (2025). *RUSI Cyber Sanctions Taskforce: Countering State-Backed Cyber Threats*. https://www.rusi.org/explore-our-research/publications/insights-papers/rusi-cyber-sanctions-taskforce-countering-state-backed-cyber-threats

Google Threat Intelligence Group. (2026, July 25). *Updated Cyber Threat Actor Naming System*. Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/updated-cyber-threat-actor-naming-system

GOV.UK. (2026, July 13). *UK and EU strike Russian cyber networks with new sanctions*. GOV.UK. Foreign, Commonwealth & Development Office. https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

Greenberg, A. (2025, July 31). *The Kremlin's Most Devious Hacking Group Is Using Russian ISPs to Plant Spyware*. Wired. https://www.wired.com/story/russia-fsb-turla-secret-blizzard-apolloshadow-isp-cyberespionage/

Gritten, D. (2022, September 7). Albania severs diplomatic ties with Iran over cyber-attack. https://www.bbc.com/news/world-europe-62821757

Insikt Group. (2026). *Swallowing the Snake's Tail: Tracking Turla Infrastructure*. https://www.recordedfuture.com/research/turla-apt-infrastructure

Jones, J. (2026, June 26). *The Latest Addition to Turla's Intelligence Gathering Apparatus*. Google Threat Intelligence Group. https://cloud.google.com/blog/topics/threat-intelligence/stockstay-turla-intelligence-gathering

Martin, A. (2024, December 14). EU issues first-ever sanctions over 'Russian hybrid threats'. *The Record*. https://therecord.media/eu-issues-sanctions-over-russia-hybrid-threats

Marzolf, É., Roussi, A., Loesel, J., & Clark, S. (2026, July 13). *EU sanctions Russian cyber spies for years-long hacking*. POLITICO. https://www.politico.eu/article/eu-sanctions-russian-cyber-spies-for-years-long-hacking/

Moret, E., & Pawlak, P. (2017). *The EU Cyber Diplomacy Toolbox: Towards a cyber sanctions regime?* (No. 24; Brief Issue). European Union Institute for Security Studies. https://data.europa.eu/doi/10.2815/399444

Pawlak, P., & Biersteker, T. (Eds). (2019). *Guardian of the galaxy: EU cyber sanctions and norms in cyberspace*. EU Institute for Security Studies, Publications Office of the European Union. https://doi.org/10.2815/04457

Reuters. (2026, July 31). *Poland summons Russian ambassador after missile incident*. Reuters. https://www.reuters.com/world/poland-summons-russian-ambassador-after-missile-incident-2026-07-31/

Robins-Early, N., & Kerr, D. (2026, August 4). US water facilities targeted by 'malicious cyber actors' – who's to blame? *The Guardian*. https://www.theguardian.com/technology/2026/aug/04/us-cyber-attacks-water-minnesota-iran

Sherman, J. (2026, August 12). *Why hackers targeting America's water systems have the upper hand—Bulletin of the Atomic Scientists*. Bulletin of the Atomic Scientists. https://thebulletin.org/2026/08/why-hackers-targeting-americas-water-systems-have-the-upper-

hand/?utm_source=LinkedIn&utm_medium=SocialMedia&utm_campaign=LinkedInPost082026&utm_content=DisruptiveTechnologies_Hackers_08122026

Soesanto, S. (2025, March 25). Inside the Fourth EU Cyber Sanctions Package. *Lawfare*. https://www.lawfaremedia.org/article/inside-the-fourth-eu-cyber-sanctions-package

Stowe, L. (2025). *'Neutral' internet governance enables sanctions evasion*. Binding Hook. https://bindinghook.com/neutral-internet-governance-enables-sanctions-evasion/

The Chancellery of the Prime Minister. (2026, January 15). *Poland Stops Cyberattacks on Energy Infrastructure—The Chancellery of the Prime Minister—Gov.pl website*. GOV.PL. https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure

Zetter, K. (2026a, January 28). Attack Against Poland's Grid Disrupted Communication Devices at About 30 Sites. *Zero Day*. https://www.zetter-zeroday.com/attack-against-polands-grid-disrupted-communication-devices-at-about-30-sites/

Zetter, K. (2026b, January 30). *Polish Grid Systems Targeted in Cyberattack Had Little Security, Per New Report*. Zero Day. https://www.zetter-zeroday.com/polish-grid-systems-targeted-in-cyberattack-had-little-security-per-new-report/

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 problematici 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 Brief IDR
ISSN 2066-5989
ISSN-L 2066-5989

Editare, formatare și grafică: Claudiu Codreanu

Imagine copertă: https://unsplash.com/photos/three-european-flags-flying-in-front-of-a-building-dxQ6ISn7_tQ

Institutul Diplomatic Român - IDR
https://www.idr.ro/en/ | secretariat@idr.ro
Primăverii 17, sector 1, București, 011972