

IDR

Institutul Diplomatic Român

Policy Paper Nr. 34/2023



**Provocările ofensivei autoritarismului digital.
Modelele Rusiei și Chinei. Modalități de
combateră**

Claudiu Codreanu



MINISTERUL AFACERILOR EXTERNE

**Provocările ofensivei autoritarismului digital.
Modelele Rusiei și Chinei. Modalități de combatere**

Claudiu Codreanu
Referent relații II, Direcția pentru Furnizare Expertiză
Institutul Diplomatic Român

EXECUTIVE SUMMARY

- **The rise of digital authoritarianism affects the global Internet and democracy.** Moreover, digital authoritarianism has become offensive, as cyber operations play an important role.
- **China and Russia developed similar models of digital authoritarianism, but there are still relevant differences between their approaches.** China's model relies on a massive filtering of web traffic and on encoding the official ideology in policies regarding digital technologies. Russia's model is repressive, but the level of control is far less tight than China's. Russian Internet is censored, but citizens can still access most parts of the global Internet.
- **The global export of digital authoritarianism erodes democracy and strengthens authoritarian and repressive regimes.** Most states with a highly-developed tech industry, including Western democracies, export digital technologies that can be abused. However, public policy and scholarly attention is rather focused on China, which exports digital technologies for mass surveillance and an entire model of digital authoritarianism to like-minded regimes, strengthening authoritarianism in those states.
- **Cyber operations against democratic states are part of coordinated campaigns to undermine democracies.** Cyber operations used by authoritarian states have become an important element of digital authoritarianism, as they are used for undermining democracies and eroding democratic institutions.
- **Democracies should develop a democratic model of Internet governance and promote it at an international level.** Digital technologies should be used responsibly and Internet traffic should be filtered as low as possible. In this regard, the priority should be setting limits for the use of mass surveillance digital tools and AI tools. Moreover, the model should also include punishments for digital authoritarians – public condemnations, attributions and international sanctions should be key elements of a strategy to counter digital authoritarianism.

- **A democratic model of Internet governance should be grounded in liberal democratic values and maintaining a free and open Internet.** Promoting digital rights, privacy rights or encryption should be a priority in the age of mass data collection and surveillance. However, digital authoritarian practices are used in democratic countries as well. Thus, democracies should firstly show that an alternative democratic model can provide a platform for upholding national security and interests without undermining democratic values.

REZUMAT

- **Ascensiunea autoritarismului digital afectează Internetul global și democrațiile.** În plus, autoritarismul digital a devenit ofensiv, iar operațiunile cibernetice joacă un rol important.
- **China și Rusia au dezvoltat modele similare, dar există diferențe relevante între abordările lor.** Modelul Chinei este puternic ancorat în filtrarea masivă a traficului de Internet și în implementarea ideologiei oficiale în politicile privind tehnologiile digitale. Modelul Rusiei este represiv, dar nivelul de control este mai redus față de China. Internetul rusesc este cenzurat, dar cetățenii pot accesa cea mai mare parte din Internetul global.
- **Exportul global de autoritarism digital erodează democrația și întărește regimurile autoritare și represive.** Majoritatea statelor cu industrii tehnologice dezvoltate, inclusiv democrațiile occidentale, exportă diferite tipuri de tehnologii care pot fi abuzate. Totuși, atenția principală cade pe China, care exportă tehnologii digitale pentru supraveghere în masă și un întreg model de autoritarism digital către regimuri cu viziuni similare, întărind autoritarismul din statele respective.
- **Operațiunile cibernetice împotriva statelor democratice fac parte din campanii coordonate de subminare a democrațiilor.** Operațiunile cibernetice ofensive ale statelor autoritare au devenit un element important al autoritarismului digital, acestea fiind utilizate pentru subminarea democrațiilor și erodarea instituțiilor democratice.
- **Statele democratice trebuie să dezvolte un model democratic de guvernare al Internetului și să îl promoveze la nivel internațional.** Tehnologiile digitale ar trebui să fie utilizate responsabil iar traficul web ar trebui să fie filtrat cât mai puțin posibil. În această privință, prioritatea ar trebui să fie impunerea unor limite pentru utilizarea uneltelor digitale pentru supraveghere în masă și a uneltelor AI. Mai mult, modelul ar trebui să includă și pedepsele pentru statele care practică autoritarismul digital – condamnările publice, atribuirile și sancțiunile internaționale pot fi elemente cheie ale unei strategii de combatere a autoritarismului digital.
- **Modelul democratic de guvernare a Internetului trebuie să fie puternic ancorat în principiile democrației liberale, inclusiv ideea de Internet deschis și liber.** Promovarea drepturilor digitale, a drepturilor la intimitate online și criptarea datelor ar trebui să reprezinte o prioritate în era colectării masive de date și a supravegherii în

masă. Totuși, există practici de autoritarism digital și în statele democratice din spațiul occidental. Democrațiile ar trebui, mai întâi, să demonstreze că modelul democratic poate oferi o platformă pentru asigurarea securității naționale și a intereselor naționale, fără subminarea valorilor democratice.

INTRODUCERE

Ascensiunea autoritarismului digital a fost semnalată de către Freedom House încă din 2018.¹ Conform Freedom House, libertatea pe Internet la nivel global a scăzut pentru al 12-lea an consecutiv. Una dintre cele mai mari scăderi a fost înregistrată în Rusia, în urma invaziei Ucrainei și a încercărilor Moscovei de a reprima opoziția față de regim și război.² Abuzul tehnologiilor digitale și practicile autoritare în spațiul cibernetic au început să fie din ce în ce mai răspândite și accentuate în ultimii ani. În prezent, guvernele secționează Internetul global pentru a crea spații online mult mai controlabile la nivel național.³ Fragmentarea Internetului la nivel național face parte dintr-o luptă globală pentru controlul spațiului cibernetic.⁴ Spre exemplu, internetul Chinei și cel global au devenit aproape complet separate în ultimii ani, rămânând foarte puțină comunicare directă care trece de așa-numitul „Mare Firewall al Chinei” (*the Great Firewall of China*).

În același timp, dezvoltarea accelerată a tehnologiilor bazate pe învățare automată (*machine learning*) și inteligență artificială (*artificial intelligence* – AI), împreună cu tehnologiile digitale pentru supraveghere în masă, provoacă noi îngrijorări pentru situația privind drepturile omului și intimitatea persoanelor.⁵ Astfel, **alegerile din 2024, mai ales cele americane, ar putea să aducă incidente fără precedent, fiind descrise de site-ul specializat *Wired* drept primele „alegeri deepfake”.**⁶

În ultimii ani, atitudinile și politicile legate de China și Rusia au fost înăsprite în spațiul occidental odată cu întărirea regimurilor autoritare din cele două țări și dezvoltarea unor politici externe din ce în ce mai agresive.⁷ În plus, coordonarea operațiunilor cibernetică ale Rusiei și Chinei în cadrul unor campanii de influențare hibridă indică faptul că acestea fac parte din practicile autoritarismului digital. Așadar, competiția tehnologică dintre statele occidentale și

¹ Adrian Shahbaz, „The Rise of Digital Authoritarianism”, *Freedom House*, 2018,

<https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>, accesat la 30 mai 2023.

² „Freedom of the Net 2022. Countering an Authoritarian Overhaul of the Internet”, *Freedom House* 2022, <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>, accesat la 30 mai 2023.

³ „Freedom of the Net 2022”, 1.

⁴ *Ibid.*, 16.

⁵ Dahlia Peterson și Samantha Hoffman, „Geopolitical implications of AI and digital surveillance adoption”, *Brookings*, iunie 2022, https://www.brookings.edu/wp-content/uploads/2022/06/FP_20220621_surveillance_exports_peterson_hoffman_v2.pdf, accesat la 30 mai 2023.

⁶ Thor Benson, „Brace Yourself for the 2024 Deepfake Election”, *Wired*, 27 aprilie 2023, <https://www.wired.com/story/chatgpt-generative-ai-deepfake-2024-us-presidential-election/>, accesat la 30 mai 2023.

⁷ Elina Sinkkonen și Jussi Lassila, „Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints”, în *Russia-China Relations. Emerging Alliance or Eternal Rivals?*, ed. Sarah Kirchberger, Svenja Sinjen și Nils Wormer, (Cham: Springer, 2022), 165-184, <https://doi.org/10.1007/978-3-030-97012-3>.

cei doi actori s-a transformat într-o competiție între idei politice liberale și iliberale.⁸ În acest fel, autoritarismul digital remodelează balanța de putere dintre democrații și autocrații.⁹ Spațiul cibernetic, din care face parte și social media, se întrepătrunde cu realitatea fizică, determinând unele opinii și comportamente ale indivizilor și comunităților. Interacțiunile din spațiul cibernetic pot determina evenimente din spațiul fizic, cum ar fi rezultatul unor alegeri politice, ceea ce evidențiază rolul pe care îl au anumite acțiuni de influență în online.

Spațiul cibernetic a început să devină din ce în ce mai puțin occidental și din ce în ce mai puțin liberal. O parte din cele mai mari companii de tehnologie sunt în Asia, iar multe state din afara Occidentului încep să devină puteri cibernetic emergente. Mai mult, Asia are cei mai mulți utilizatori de Internet din lume, iar dezvoltarea tehnologică are loc într-un ritm crescut în regiune.¹⁰

Cercetarea de față pornește de la două întrebări principale: 1) Cum se desfășoară autoritarismul digital după modelul Chinei și, respectiv, cel al Rusiei?; 2) Cum pot statele democratice din spațiul occidental să gestioneze și să amelioreze efectele autoritarismului digital?

Ca răspuns la cele două întrebări de cercetare, studiul propune două ipoteze: 1) Autoritarismul digital a devenit ofensiv, China și Rusia utilizând operațiuni cibernetic împotriva statelor democratice; 2) Statele democratice din spațiul occidental trebuie să respingă ofensiva autoritarismului digital, promovând la nivel global un model democratic de guvernare a Internetului.

Studiul va fi împărțit în două părți. Prima va discuta caracteristicile autoritarismului digital, diferențiind între modelul Chinei și cel al Rusiei, și rolul operațiunilor cibernetic ofensive. Totodată, va explora modalitățile prin care cei doi actori își exportă la nivel global modelul autoritar digital și tehnologii digitale. În cea de-a doua parte, studiul va discuta modalitățile prin care democrațiile ar putea să răspundă ascensiunii autoritarismului digital, notând și practicile autoritar digitale ale unor state democratice. Răspunsul principal care ar trebui adoptat este dezvoltarea și promovarea unui model democratic de guvernare a Internetului și a activității statelor în spațiul cibernetic.

CONTEXT ȘI CONCEPTE

Autoritarismul digital se referă la utilizarea Internetului și a tehnologiilor digitale de către regimuri autoritare pentru a **controla și modela comportamentul populației interne sau a unor populații străine prin supraveghere în masă, represiune, manipulare și cenzură**.¹¹ Obiectivul autoritarismului digital, care poate fi implementat și de către lideri individuali cu

⁸ Sinkkonen și Lassila, „Digital Authoritarianism”, 166.

⁹ Alina Polyakova și Chris Meserole, „Exporting digital authoritarianism. The Russian and Chinese models”, *Brookings*, august 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf, accesat la 30 mai 2023.

¹⁰ Andre Barrinha și Thomas Renard, „Power and diplomacy in the post-liberal cyberspace”, *International Affairs* 96, nr. 3 (2020): 176-198, <https://doi.org/10.1080/23340460.2017.1414924>.

¹¹ Polyakova și Meserole, „Exporting digital authoritarianism”, 1; Lydia Khalil, „Digital Authoritarianism, China and COVID”, *Lowy Institute Analysis*, 2 noiembrie 2020, <https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid>, accesat la 30 mai 2023.

tendințe autoritare (nu doar de regimuri autoritare), este scăderea încrederii populației în instituțiile publice, creșterea controlului politic și social, și subminarea libertăților civile.¹²

Autoritarismul digital include supravegherea în masă a populației prin camere cu recunoaștere facială, drone sau monitorizarea locației prin GPS. Aceste practici normalizează supravegherea publică constantă și elimină toate așteptările pentru intimitate personală. În plus, autoritarismul digital presupune consolidarea unui control central asupra guvernării Internetului și a infrastructurii, dar și sprijinirea sau cooptarea industriei tehnologice naționale pentru a servi eforturilor regimurilor autoritare de a menține controlul social.¹³

Steven Feldstein notează șase tehnici ale **represiunii digitale**: supraveghere publică; cenzură; manipulare socială și hărțuire (inclusiv atacuri cibernetice); blocarea conexiunilor la Internet; și persecutarea țintită a utilizatorilor online.¹⁴ Oprirea temporară a Internetului dintr-o țară (*Internet shutdowns*) este practică cel mai des de state ca Iran. Metoda nu presupune neapărat tăierea completă a Internetului de fiecare dată, uneori referindu-se doar la blocarea temporară a anumitor platforme sau scăderea intenționată a vitezei de conectare.¹⁵

Viteza cu care companiile dezvoltă tehnologii de supraveghere pe baza AI și ritmul cu care statele adoptă astfel de tehnologii nu permit un timp adecvat pentru o dezbatere publică serioasă cu privire la implicațiile și limitele utilizării acestora.¹⁶ Din ce în ce mai multe state utilizează instrumente de supraveghere avansate pe baza AI pentru a monitoriza cetățenii, o parte din aceste activități încălcând drepturile omului.¹⁷ Pentru regimurile autoritare, tehnologiile de supraveghere pe baza AI pot contribui la consolidarea capacității statului de a exercita putere coercitivă. În schimb, pentru democrațiile liberale și regimurile hibride, acestea pot ajuta la reducerea sarcinilor forțelor de ordine prin automatizarea anumitor operațiuni, dar există riscul abuzării sistemelor.¹⁸

Autoritarismul digital afectează drepturile omului și libertățile civile, mai ales cea de exprimare, dar și dreptul la intimitate online și offline.¹⁹ **Guvernele autoritare pun în practică strategii sofisticate de cenzură, dublate de campanii de dezinformare, pentru a putea submina opoziția și societatea civilă.**²⁰ Iar, atunci când aceste campanii nu au succesul așteptat, autoritățile sunt pregătite să taie accesul la Internet pentru o perioadă de timp.²¹ Autoritarismul digital include utilizarea operațiunilor cibernetice ofensive împotriva statelor democratice sau cu aspirații democratice.

¹² Erol Yayboke și Sam Brannen, „Promote and Build. A Strategic Approach to Digital Authoritarianism”, *CSIS Briefs*, 15 octombrie 2020, <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism>, accesat la 30 mai 2023.

¹³ Khalil, „Digital Authoritarianism”, 6.

¹⁴ Steven Feldstein, „When it comes to digital authoritarianism, China is a challenge – but not the only challenge”, 12 februarie 2020, <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>, accesat la 30 mai 2023.

¹⁵ Steven Feldstein, „Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?”, *Carnegie*, 31 martie 2022, <https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond-pub-86687>, accesat la 30 mai 2023.

¹⁶ Peterson și Hoffman, „Geopolitical implications”, 3.

¹⁷ Steven Feldstein, „The Global Expansion of AI Surveillance”, *Carnegie*, 20 aprilie 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf, accesat la 30 mai 2023.

¹⁸ Peterson și Hoffman, „Geopolitical implications”, 3.

¹⁹ Yayboke și Brannen, „Promote and Build”, 2.

²⁰ Khalil, „Digital Authoritarianism”, 6.

²¹ Feldstein, „When it comes to”.

Autoritarismul digital este într-un proces de extindere în țările autoritare, precum China, Rusia, Iran sau Arabia Saudită. Dar, totodată, regimurile autoritare își extind utilizarea uneltelor digitale și în afara granițelor, consolidând supravegherea propriilor cetățeni din diaspora, dar și a cetățenilor altor state. În acest proces, uneltele autoritarismului digital sunt exportate către regimuri cu viziuni similare. **O parte din uneltele, practicile și modelele de autoritarism digital sunt adoptate și în cadrul statelor democratice**, fie de unele guverne, fie de anumite partide politice, grupuri neguvernamentale sau companii private.²²

AUTORITARISMUL DIGITAL ÎN RUSIA ȘI CHINA

Statele autoritare își promovează modelul de control digital la nivel internațional.²³ Rusia și China împărtășesc politici și viziuni similare în ceea ce privește chestiunile cibernetice. Principalul aspect asupra căruia pot cădea de acord cele două țări este neîncrederea față de „ordinea liberală” occidentală, percepută ca o hegemonie americană.²⁴ În plus, parteneriatul strategic dintre China și Rusia a fost consolidat în ultimii ani,²⁵ mai ales în condițiile „prieteniei fără limite” asumate în urma comunicatului comun adoptat în februarie 2022, înainte de invazia rusă a Ucrainei.²⁶

Cele două state se raportează la spațiul cibernetic ca la extinderea spațiului real, fizic, referindu-se la securitatea acestuia drept „securitatea informațiilor”, în comparație cu termenul occidental de „securitate cibernetică”.²⁷ **Ambele state percep informația online drept risc principal de securitate.** Astfel, China și Rusia au format un bloc de state cu viziuni similare care acum își promovează propria viziune asupra Internetului în cadrul ONU.²⁸ La nivel internațional, ambele state au promovat ideea suveranității cibernetice. Conceptul prevede ca guvernele naționale să aibă o putere exclusivă asupra jurisdicției propriului spațiu cibernetic național, atât în privința conținutului, cât și în privința infrastructurii.²⁹

Există și **diferențe** destul de semnificative în abordarea Rusiei și Chinei privind spațiul cibernetic, inclusiv cu privire la poziția față de normele internaționale. Aspectele militare și de *intelligence* sunt mult mai importante pentru Rusia decât pentru China. În plus, China are o concepție mult mai pozitivă față de spațiul cibernetic global, punând accentul pe cooperare internațională la nivel global.³⁰

²² Yayboke și Brannen, „Promote and Build”, 2.

²³ „Freedom of the Net 2022”, 2.

²⁴ Dennis Broeders, Liisi Adamson și Rogier Creemers, „A coalition of the unwilling? Chinese & Russian perspectives on cyberspace”, *The Hague Program for Cyber Norms*, octombrie 2019, <https://www.thehagueprogram.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace>, accesat la 30 mai 2023.

²⁵ Liliana Popescu, și Răzvan Tudose, „The Dragonbear and the Grey Rhinos. The European Union Faced with the Rise of the China-Russia Partnership”, *Romanian Journal of European Affairs* 21, nr. 2 (2021): 130-147.

²⁶ Monique Taylor, *China's Digital Authoritarianism. A Governance Perspective*, (Cham: Palgrave Macmillan), <https://doi.org/10.1007/978-3-031-11252-2>.

²⁷ Broeders, Adamson și Creemers, „A coalition of the unwilling?”, 2.

²⁸ Robert K. Knake, „Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity”, *Council on Foreign Relations*, septembrie 2020, https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digital-trade_csr_combined_final.pdf, accesat la 30 mai 2023.

²⁹ Broeders, Adamson și Creemers, „A coalition of the unwilling?”, 3.

³⁰ *Ibid.*

Succesul Chinei în dezvoltarea de companii tehnologice majore la nivel intern și internațional are și efecte negative pentru Beijing. Operatori globali precum Huawei, ZTE sau Alibaba sunt mult mai vulnerabili față de măsurile politice internaționale luate ca ripostă față de practicile companiilor chineze. Astfel, **în comparație cu Rusia, China este mult mai interesată în menținerea unei stabilități cu privire la aspectele economice.**³¹

Rusia a desfășurat campanii active de destabilizare politică și subminare a statelor occidentale, cum ar fi în cazul interferenței în alegerile prezidențiale americane din 2016. În schimb, *hacker*-ii chinezi s-au concentrat pe spionaj cibernetic asupra unor ținte economice, politice sau militare, căutând în principal informații și nu provocarea unor pagube. Rusia are interese economice mult mai limitate față de China, dar și o influență mai mare a agențiilor de *intelligence* și a celor militare. Astfel, Moscova utilizează mult mai vizibil autoritarismul digital împotriva unor ținte străine pentru a provoca pagube, subminare și destabilizare.³²

Modelul chinezesc

Pentru al optulea an consecutiv, China este statul care înregistrează cel mai mic nivel de libertate pe Internet din lume. China a experimentat majoritatea tehnologiilor represive de supraveghere în provincia Xinjiang, utilizând un nivel fără precedent de represiune pe baza unor tehnologii avansate împotriva populației uigure.³³ Răspunsul guvernului chinez la pandemia de COVID-19 a permis Chinei să își extindă utilizarea mecanismelor autoritare digitale în toată țara.³⁴

Guvernul chinez a continuat înăsprirea controlului asupra sectorului tehnologic, inclusiv prin reguli noi care impun platformelor să utilizeze sisteme algoritmice pentru a promova ideologia partidului.³⁵ Reglementările chineze cer companiilor să promoveze linia oficială a Partidului Comunist Chinez. În ceea ce privește moderarea conținutului, materialele care se concentrează pe povești pozitive, alinate cu valorile partidului, și pe conținut patriotic sunt promovate de algoritmi.³⁶ Beijingul a instituit politici noi pentru a consolida controlul asupra companiilor chineze din industria tehnologică. Principala agenție de reglementare a Internetului a emis un ghid prin care le cere platformelor să alinieze sistemele de moderare și recomandare a conținutului cu „Gândirea lui Xi Jinping”, ideologia oficială a actualului lider.³⁷

Partidul Comunist Chinez și companiile legate de statul chinez au dezvoltat **cel mai sofisticat model de izolare cibernetică, supranumit „Marele Firewall al Chinei”**. Traficul de Internet din afara țării trece prin filtre controlate de stat, facilitând blocarea în masă a site-

³¹ *Ibid.*, 4.

³² *Ibid.*

³³ Polyakova și Meserole, „Exporting digital authoritarianism”, 1-4.

³⁴ Khalil, „Digital Authoritarianism”, 14.

³⁵ „Freedom of the Net 2022”, 2.

³⁶ Benjamin Cedric Larsen, „The geopolitics of AI and the rise of digital sovereignty”, 8 decembrie 2022, <https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>, accesat la 30 mai 2023.

³⁷ „Freedom of the Net 2022”, 9; Pentru o analiză IDR a „Gândirii lui Xi Jinping”, vezi Sinziana Dumitrescu, „Campania de educare «Gândirea lui Xi Jinping asupra socialismului cu caracteristici chineze pentru noua eră» implicații pentru politica chineză internă și externă”, Institutul Diplomatic Român, iunie 2023, https://www.idr.ro/publicatii/Xi_Jinping_thought.pdf, accesat la 12 iunie 2023.

urilor și monitorizarea datelor. Adoptând modelul Chinei, guvernul iranian a impus bariere asemănătoare între infrastructura locală și traficul global.³⁸

Diplomația cibernetică a Chinei este ghidată de eforturile pentru îndeplinirea obiectivului de a deveni „o superputere cibernetică” în toate domeniile (economic, comercial, normativ sau militar). Conceptul de *superputere cibernetică* integrează obiective strategice și militare cu interese comerciale. Ținta finală constă în dezvoltarea unei economii moderne și competitive la nivel global. Astfel, unul dintre elementele cheie ale devenirii unei superputeri cibernetice este promovarea viziunii normative a Chinei și puterea de a stabili agenda în dezbaterile internaționale privind spațiul cibernetic.³⁹

Modelul rusesc

Rusia se bazează mai puțin pe filtrarea informației și mai mult pe dezvoltarea unui regim legal represiv și pe intimidarea companiilor cheie și a societății civile. Modelul rus presupune costuri mai scăzute și poate fi transferat mai ușor în alte state.⁴⁰ Conform legislației rusești, furnizorii de Internet și de telecomunicații sunt obligați să instaleze echipamente de monitorizare a traficului. Acestea permit Serviciul Federal de Informații (FSB) să acceseze toate datele online fără niciun control din partea companiilor.⁴¹

Rusia a introdus sistemul SORM (*Sistema Operativno-Rozisknih Meropriati* – Sistemul pentru Activități de Investigare Operativă) în anii 1990. Acesta prevedea specificațiile tehnice pentru toate interceptările legale de telecomunicații și rețele telefonice. SORM obligă toți operatorii de telecomunicații să instaleze *hardware*-uri specificate de FSB, permițând monitorizarea comunicațiilor. SORM a întâmpinat o serie de dificultăți financiare și tehnologice, o parte din operatorii independenți reușind să ocolească măsurile impuse de sistem (cel puțin pentru o perioadă).⁴²

Frontiera digitală dintre Internetul global și cel rusesc a început să crească după februarie 2022, odată cu războiul de agresiune al Rusiei împotriva Ucrainei. O parte dintre companiile occidentale și media și-au oprit operațiunile din Rusia în urma sancțiunilor internaționale impuse. În paralel, autoritățile rusești au interzis o serie de site-uri și platforme occidentale, înăsprind și legile privind controlul informației pe Internet. Spre exemplu, în 2023 chiar și ordinele de mobilizare pentru cetățenii ruși au fost digitalizate, acest lucru ducând și la dezvoltarea unei baze naționale de date. În plus, prima fază a pandemiei a contribuit la digitalizarea autorităților locale, de la înregistrarea online a vaccinării împotriva SARS-CoV-2, la monitorizarea carantinei prin camere și aplicații mobile.⁴³

³⁸ Freedom of the Net 2022”, 16; Polyakova și Meserole, „Exporting digital authoritarianism”, 1.

³⁹ Nikolay Bozhkov, „China’s Cyber Diplomacy: A primer”, *EU Cyber Direct*, martie 2020, 18, <https://eucyberdirect.eu/research/chinas-cyber-diplomacy-a-primer>, accesat la 30 mai 2023.

⁴⁰ Polyakova și Meserole, „Exporting digital authoritarianism”, 1.

⁴¹ *Ibid.*, 8.

⁴² Sinkkonen și Lassila, „Digital Authoritarianism”, 168-169.

⁴³ Adam Satariano și Valerie Hopkins, „Russia, Blocked From the Global Internet, Plunges Into Digital Isolation”, *New York Times*, 7 martie 2022, <https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html>, accesat la 30 mai 2023; Tatiana Stanovaya, „Russia’s New Conscription Law Brings the Digital Gulag Much, Much Closer”, *Carnegie*, 17 aprilie 2023, <https://carnegieendowment.org/politika/89553>, accesat la 30 mai 2023.

Modelul rusesc a fost dezvăluit și în scurgerile de informații făcute de un avertizor de integritate rus. *Vulkan leaks*, denumite după compania de securitate cibernetică *Vulkan*, din Moscova, au arătat modul de operare al Rusiei în spațiul cibernetic pentru a accentua represiunea internă și pentru a submina alte state. În plus, acestea au indicat o cooperare strânsă între serviciului de informații al armatei ruse (GRU), Serviciul de Informații Externe (SVR) și companii private de securitate cibernetică. Scurgerile de informații au evidențiat și o parte din armele cibernetică utilizate de Rusia, unele împotriva propriilor cetățeni.⁴⁴

Exportul internațional de autoritarism digital

Modelul chinezesc de „suveranitate” asupra Internetului, conform căruia statul își delimitează și controlează Internetul de pe teritoriul de suveranitate, a reprezentat o sursă de inspirație pentru multe guverne autoritare, de la Egipt la Tailanda.⁴⁵ În plus, modelul chinezesc de relaționare față de AI și supraveghere digitală este promovat la nivel internațional, fiind propuse standarde globale pe baza celor interne din China.⁴⁶ Pentru Președintele Xi Jinping au devenit o prioritate dezvoltarea și promovarea globală a standardelor naționale chineze.⁴⁷ Acest obiectiv implică atât consolidarea lor în interiorul Chinei, exportul acestora către alte țări, dar și adoptarea lor ca standarde internaționale. **Promovarea standardelor tehnice chineze reprezintă o extindere a strategiei Partidului Comunist Chinez de a spori puterea economică și militară a țării la nivel global.**⁴⁸

China a exportat tehnologii digitale în Angola, Etiopia, Zimbabwe, Ecuador, Venezuela, Dubai, Malaiezia etc. Acestea au implicat sisteme de supraveghere publică bazate pe camere cu tehnologii de recunoaștere facială sau dezvoltarea de echipamente de telecomunicații pentru monitorizarea și supravegherea jurnaliștilor și a activiștilor de opoziție.⁴⁹ Companiile chineze **au instalat sisteme de supraveghere bazate pe camere cu recunoaștere facială în țări din Africa, precum Uganda, dar și în state europene ca Serbia.**⁵⁰

China este cel mai mare exportator de sisteme complexe de supraveghere pe baza AI, problema principală fiind că tehnologiile sunt concepute pentru a satisface nevoile și politicile Partidului Comunist Chinez.⁵¹ Cel puțin 18 state utilizau sisteme de monitorizare și supraveghere chinezești în 2019, iar peste 36 de guverne au participat la sesiuni de instruire și seminare ținute de China privind media și informațiile.⁵² Steve Feldstein estima în 2019 că numărul țărilor care utilizează tehnologii de supraveghere pe baza Inteligenței Artificiale produse de companii chineze ar fi de peste 60.⁵³

⁴⁴ Andrei Soldatov, „Cyberwarfare leaks show Russian army is adopting mindset of secret police”, *The Guardian*, 30 martie 2023, <https://www.theguardian.com/technology/2023/mar/30/cyberwarfare-leaks-show-russian-army-is-adopting-mindset-of-secret-police>, accesat la 30 mai 2023.

⁴⁵ Maya Wang, „China’s Techno-Authoritarianism Has Gone Global”, *Foreign Affairs*, 8 aprilie 2021, <https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global>, accesat la 30 mai 2023.

⁴⁶ Peterson și Hoffman, „Geopolitical implications”, 8.

⁴⁷ Taylor, *China’s Digital Authoritarianism*, 117.

⁴⁸ *Ibid.*, 126.

⁴⁹ Polyakova și Meserole, „Exporting digital authoritarianism”, 6.

⁵⁰ Feldstein, „When it comes to”.

⁵¹ Peterson și Hoffman, „Geopolitical implications”, 3.

⁵² Polyakova și Meserole, „Exporting digital authoritarianism”, 6.

⁵³ Feldstein, „The Global Expansion”, 1.

Unele dintre companiile din industria tehnologică sunt deținute direct de guvernul chinez, iar altele sunt influențate de sau vulnerabile la presiunile autorităților.⁵⁴ În 2021, compania chineză Xiaomi a ajuns să controleze peste 40% din piața de *smartphone*-uri cu tehnologie 5G din Europa Centrală și de Est.⁵⁵ Mai mult de jumătate din dispozitivele cu tehnologie 4G din Europa sunt de origine chineză, inclusiv cele specifice rețelelor informatice (ex. *router*-e, *bridge*-uri etc.).⁵⁶ Mai mult, Belgia, Cipru, Lituania și Malta s-au bazat exclusiv pe infrastructura *wireless* a Huawei pentru rețelele 4G.⁵⁷ În plus, compania chineză Huawei a ajuns cel mai mare furnizor de tehnologii informatice și de comunicații din Africa.⁵⁸ Printre altele, Huawei furnizează la nivel global platforme de „safe city”, oferind sisteme de supraveghere inteligentă, recunoaștere facială și capacități analitice avansate regimurilor autoritare.⁵⁹ Peste 80 de state din America Latină, Africa și Asia au implementat soluții *Safe City* de la Huawei și de la alte companii tehnologice chineze.⁶⁰

Principalele state din Orientul Mijlociu care au adoptat politici de autoritarism digital sunt Arabia Saudită și Emiratele Arabe Unite. În 2018-2021, ambele și-au intensificat cooperarea cu China pentru a obține accesul la tehnologii avansate, dar și cu Israelul.⁶¹ Companii chineze precum Dahua, Huawei și ZTE au sprijinit dezvoltarea de platforme de supraveghere și proiecte pentru poliție în Ecuador, Peru sau Venezuela în 2012-2016.⁶² În Africa, Kenya, Uganda, Zambia și Zimbabwe au importat tehnologii de supraveghere din China, contribuind la formarea unui spațiu cibernetic mult mai autoritar, după modelul chinez.⁶³ Mai mult decât atât, experți tehnici ai companiei Huawei a ajutat autoritățile din Uganda și Zambia să își spioneze opoziția în 2017-2018.⁶⁴ Activitățile au presupus interceptarea comunicațiilor, infiltrări cibernetice și utilizarea de aplicații pentru monitorizare locației.

Totuși, colaborarea dintre țările africane și China în domeniul cibernetic a scăzut după 2018, după descoperirea faptului că spioni chinezi au pus microfoane în sediul Uniunii Africane din Etiopia. Înainte de incident, Uniunea Africană își exprimase intenția să colaboreze cu China în domeniul securității cibernetice, dar inițiativa nu s-a mai materializat.⁶⁵

În schimb, modelul rusesc reprezintă o alternativă cu costuri mai mici și cu tehnologii mai puțin avansate față de modelul Chinei. Modelul Rusiei nu se bazează pe tehnologii cu capacități avansate de filtrare a informațiilor și poate fi implementat fără existența în prealabil

⁵⁴ Wang, „China’s Techno-Authoritarianism”.

⁵⁵ Marta Makowska, „China’s Digital Authoritarianism vs. EU Technological Sovereignty: The Impact on Central and Eastern Europe”, *Council on Foreign Relations*, 19 mai 2022, <https://www.cfr.org/blog/chinas-digital-authoritarianism-vs-eu-technological-sovereignty-impact-central-and-eastern>, accesat la 30 mai 2023.

⁵⁶ Makowska, „China’s Digital Authoritarianism”, 6.

⁵⁷ *Ibid.*

⁵⁸ Nathalie Van Raemdonck, „Africa as a Cyber Player”, *EU Cyber Direct*, ianuarie 2021, <https://eucyberdirect.eu/research/africa-as-a-cyber-player>, accesat la 30 mai 2023.

⁵⁹ Feldstein, „When it comes to”.

⁶⁰ Khalil, „Digital Authoritarianism”, 26.

⁶¹ Jane Lynch, „Iron Net: Digital Repression in the Middle East and North Africa”, *European Council on Foreign Relations*, iunie 2022, <https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/>, accesat la 30 mai 2023.

⁶² Peterson și Hoffman, „Geopolitical implications”, 6.

⁶³ Van Raemdonck, „Africa as a Cyber Player”, 39.

⁶⁴ Feldstein, „When it comes to”.

⁶⁵ Van Raemdonck, „Africa as a Cyber Player”, 39-40.

a unui *firewall* guvernamental.⁶⁶ China și-a exportat practicile și politicile către Rusia, care depune eforturi de mai mulți ani pentru formarea *Runet*, un Internet național prin care va tăia traficul cu restul lumii.⁶⁷

În martie 2023, Rusia și-a depus propria viziune privind securitatea informațiilor în cadrul Grupului Deschis de Lucru (OEWG) din cadrul ONU. Documentul reprezintă un nou exemplu al modelului de autoritarism digital rusesc, prevederile având posibilitatea să submineze responsabilitatea statelor pentru acțiunile din spațiul cibernetic. Acesta pune accentul pe stabilitate economică și socială, fără să menționeze drepturile omului și dreptul la intimitate, iar importanța libertății de exprimare este minimizată.⁶⁸

Chiar dacă majoritatea exporturilor rusești de autoritarism digital a fost efectuată către statele post-sovietice, sisteme de tehnologii de supraveghere rusești au fost vândute și către țările din sudul global. Modelul rusesc este mai atrăgător pentru statele post-sovietice, care au cadre legale similare cu cele ale Rusiei. Compania rusească *Protei* (care a dezvoltat tehnologia SORM) a exportat sisteme de filtrare a Internetului către Belarus, Kârgâzstan, Uzbekistan și alte state post-sovietice. În plus, *Protei* a exportat diferite produse și servicii și către Bahrain, Iordania, Irak, Palestina, Qatar, Sudan, Tunisia, Yemen, Cuba, Mexic și Venezuela. O altă companie, *Peter-Service*, a exportat tehnologie care permite filtrarea și supravegherea Internetului către Georgia și Ucraina, cel puțin până la invazia rusă din 2014. În Africa, influența Rusiei privind politicile de securitate cibernetică s-a limitat mai mult la Africa de Sud, cele două semnând în 2017 un acord de cooperare în domeniu.⁶⁹

Ofensiva autoritarismului digital implică și operațiuni cibernetice

China conduce inovarea în tehnologiile avansate pentru control social, în timp ce Rusia a fost mult mai dispusă să instrumentalizeze tehnologiile informaționale ca parte a unor operațiuni de influență țintite.⁷⁰ **Rusia urmărește destabilizarea statelor occidentale și polarizarea societăților pentru a le slăbi din interior.** În schimb, **China se concentrează pe promovarea unei viziuni pozitive asupra Chinei** sau reprimarea opiniilor negative prin tehnici de intimidare sau influențare.⁷¹

Rusia a țintit infrastructura energetică a Ucrainei și înainte de războiul de agresiune început în 2022, dar cu instrumente cibernetice. În decembrie 2015, Rusia a desfășurat un atac cibernetic sofisticat împotriva rețelei electrice ucrainene, lăsând fără energie electrică peste 230.000 de persoane. Atacul a reprezentat un precedent periculos, fiind pentru prima dată când

⁶⁶ Polyakova și Meserole, „Exporting digital authoritarianism”, 7.

⁶⁷ Knake, „Weaponizing Digital Trade”, 5.

⁶⁸ Valentin Weber, „The Dangers of a New Russian Proposal for a UN Convention on International Information Security”, *Council on Foreign Relations*, 21 martie 2023, <https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security>, accesat la 30 mai 2023.

⁶⁹ Robert Morgus, „The Spread of Russia’s Digital Authoritarianism”, în *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Maxwell: Air University Press, 2019), 89-97, <http://www.jstor.com/stable/resrep19585.17>; Van Raemdonck, „Africa as a Cyber Player”, 40; Polyakova și Meserole, „Exporting digital authoritarianism”, 7.

⁷⁰ Polyakova și Meserole, „Exporting digital authoritarianism”, 9.

⁷¹ *Ibid.*, 11.

un atac cibernetic (reușit) a avut ca țintă infrastructura civilă și obiectivul de a afecta direct populația civilă.⁷²

În timpul alegerilor prezidențiale americane din 2016, Rusia a combinat atacurile cibernetice cu campanii de dezinformare, exploatând rețelele sociale pentru a crește tensiunile sociale.⁷³ Totodată, în 2016, Parlamentul german a fost ținta unei campanii cibernetice rusești, fiind vizată inclusiv Cancelara Angela Merkel.⁷⁴ Un an mai târziu, Rusia a desfășurat campanii informaționale și cibernetice de tip *kompromat* și împotriva candidatului Emmanuel Macron în timpul alegerilor prezidențiale franceze din 2017.⁷⁵ În 2020-2021, Rusia a fost responsabilă de o campanie de spionaj cibernetic agresivă împotriva Statelor Unite, având o magnitudine aproape fără precedent.⁷⁶

China a fost responsabilă aproape exclusiv doar de campanii de spionaj cibernetic, dar intensitatea intruziunilor și pagubelor provocate pentru a se infiltra în sisteme a fost amplificată în ultimii ani. În 2021, Statele Unite au acuzat Ministerul pentru Securitatea Statului din China pentru o campanie masivă de spionaj cibernetic care a utilizat o vulnerabilitate din *software*-ul *Microsoft Exchange Server*. Atacul cibernetic a compromis mii de organizații din întreaga lume, fiind unul dintre cele mai complexe și extinse atacuri de până acum.⁷⁷

Cel mai recent, **agresiunea militară a Rusiei în Ucraina a subminat și libertățile online din teritoriile ucrainene aflate sub ocupație rusească.** În regiunea Herson și orașul omonim, cât timp au fost sub ocupație, autoritățile Rusiei au forțat furnizorii de Internet să redirecționeze traficul către rețelele rusești. În acest fel, cetățenii ucraineni au rămas fără acces la majoritatea platformelor de social media și la majoritatea site-urilor media internaționale sau ucrainene.⁷⁸

În decursul războiului, Rusia a atacat infrastructura de Internet a Ucrainei atât prin atacuri cibernetice, cât și prin atacuri fizice. Armata rusă a lansat serii recurente de rachete balistice și de croazieră asupra infrastructurii critice ucrainene, afectând-o și pe cea informatică. Totuși, guvernul și societatea ucraineană au dat dovadă de reziliență. Autoritățile și companiile de telecomunicații au lucrat împreună pentru a repara infrastructura și pentru a asigura accesul la resurse online și informații.⁷⁹

Rusia a utilizat frecvent atacuri cibernetice masive și cu efecte serioase în Ucraina, iar acest lucru ridică așteptarea ca armata rusă să utilizeze, înaintea sau în timpul invaziei, atacuri cibernetice devastatoare.⁸⁰ Totuși, Rusia a preferat să lanseze rachete de croazieră și de alte tipuri asupra clădirilor rezidențiale și asupra infrastructurii energetice ucrainene, ținând cont că

⁷² Alina Polyakova și Spencer P. Boyer, „The future of political warfare: Russian, the West, and the coming age of global digital competition”, Brookings, martie 2018, <https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/>, accesat la 30 mai 2023.

⁷³ Polyakova și Boyer, „The future of political warfare”, 2.

⁷⁴ *Ibid.*, 10.

⁷⁵ *Ibid.*, 3.

⁷⁶ Lucas Kello, „Cyber legalism: why it fails and what to do about it”, *Journal of Cybersecurity* 7, nr. 1 (2021): 1-15, <https://doi.org/10.1093/cybsec/tyab014>.

⁷⁷ Andy Greenberg, „How China’s Hacking Entered a Reckless New Phase”, *Wired*, 19 iulie 2021, <https://www.wired.com/story/china-hacking-reckless-new-phase/>, accesat la 30 mai.

⁷⁸ „Freedom of the Net 2022”, 5.

⁷⁹ *Ibid.*, 6.

⁸⁰ Mihai Cocoru, „Rolul domeniului operațional cibernetic în războiul din Ucraina”, *România occidentală* 1, nr. 2 (2022): 46-52, https://www.idr.ro/publicatii/Romania_Occidentala_nr_2.pdf.

o rachetă ajunge mult mai repede la țintă și are efecte mult mai puternice și vizibile, dar și șanse mai mari de reușită față de un atac cibernetic. Faptul că Rusia a supus Ucraina la o serie considerabilă de atacuri cibernetice majore a determinat Kievul să își întărească apărarea și securitatea cibernetică (așa cum a fost și în cazul Estoniei, prima victimă a unui atac cibernetic rusesc major, în 2007). Totodată, așa cum demonstrează și Lennart Maschmeyer⁸¹, operațiunile cibernetice desfășurate de Rusia în Ucraina nu au influențat cu nimic războiul din Donbas sau invazia Crimeii, începute în 2014, și nici nu au fost utilizate în tandem cu operațiunile militare rusești din Ucraina.

Ținând cont de aceste aspecte, o parte din acțiunile cibernetice ofensive ale autoritarismului digital pot fi încadrate și în ceea ce Mikael Wigell a descris ca „**interferență hibridă**”, o strategie de a manipula interesele strategice ale altor state prin subminarea coeziunii interne.⁸² Astfel, starea care este creată și întreținută de practicile ofensive și defensive din spațiul cibernetic și din sfera autoritarismului digital poate fi descrisă ca una de „nepace”, așa cum o numește Lucas Kello. Rivalitatea interstatală din prezent nu se încadrează nici în sfera războiului și nici în limitele păcii.⁸³

Lucas Kello descrie activitățile de spionaj cibernetic sau fraudă financiară ca încadrându-se în zona păcii. Atacurile cibernetice asupra sistemelor de transport sau sanitare, sau cele care au ca obiectiv perturbarea operațiunilor tactice pe timpul războiului, se încadrează în zona utilizării forței. În schimb, atacurile cibernetice care au ca scop distrugerea infrastructurii fizice (ex. *Stuxnet*, 2010), perturbarea infrastructurii energetice (ex. Ucraina, 2015) sau perturbarea sistemelor de sănătate publică (ex. *WannaCry*, 2017) se încadrează într-o situație de „nepace”. În aceeași categorie intră și spionajul cibernetic și *kompromatul* (ex. *Macron Leaks*, 2017), infiltrarea pe scară largă și monitorizarea rețelelor guvernamentale (ex. *SolarWinds*, 2020) sau perturbarea industrială și comercială nediscriminatorie (ex. *NotPetya*, 2017).⁸⁴

Astfel, autoritarismul digital are și această componentă importantă a operațiunilor cibernetice ofensive îndreptate împotriva statelor democratice din spațiul occidental, confirmând prima ipoteză a acestui studiu (autoritarismul digital a devenit ofensiv, China și Rusia utilizând operațiuni cibernetice împotriva statelor democratice). Coordonarea operațiunilor cibernetice cu alte tipuri de activități (ex. campanii de dezinformare, campanii de influență, corupție și finanțări ilicite, sabotaj etc.) are ca obiectiv subminarea democrațiilor. Erodarea democrațiilor, scăderea încrederii în procesele și instituțiile democratice și provocarea de pagube guvernelor sau societății (inclusiv a afacerilor) reprezintă firul roșu care leagă operațiunile cibernetice ofensive ale actorilor care practică autoritarismul digital. **Atacurile cibernetice nu reprezintă incidente izolate, ci sunt legate și coordonate și au obiective politice.** Acestea promovează direct și indirect autoritarismul digital. În mod direct, deoarece atacă democrațiile și încearcă slăbirea lor și provocarea de pagube. În mod indirect, deoarece provoacă un grad de urgență pentru asigurarea securității cibernetice, iar urgența atrage unele

⁸¹ Lennart Maschmeyer, „The subversive trilemma: Why cyber operations fall short of expectations”, *International Security* 46, nr. 2 (2021): 51-90, <https://doi.org/10.1177/13540661221117051>.

⁸² Mikael Wigell, „Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy”, *International Affairs* 95, nr. 2 (2019): 7-26, <https://doi.org/10.1093/ia/iiz018>.

⁸³ Kello, „Cyber legalism”, 3.

⁸⁴ Kello, „Cyber legalism”, 9.

măsuri pripite. Guvernele democratice aleg de multe ori soluții care afectează libertățile digitale și drepturile omului, modificarea ulterioară a politicilor necesitând o implicare serioasă din partea societății civile.

SITUAȚIA ÎN DEMOCRAȚIILE DIN SPAȚIUL OCCIDENTAL

Practici de autoritarism digital în democrațiile din spațiul occidental

Există și companii semnificative din state democratice care au exportat instrumente de supraveghere digitală către regimuri iliberale. Companii precum *Amesys* (Franța), *Trovicor* (Germania) sau *NSO Group* (Israel) au vândut astfel de instrumente către Libia, Bahrain și diferite state autoritare din Africa și Orientul Mijlociu.⁸⁵ Spre exemplu, Arabia Saudită nu achiziționează astfel de tehnologii doar din China, ci și din SUA, Regatul Unit sau Japonia.⁸⁶ Arabia Saudită a colaborat cu Huawei pentru a implementa platforme de tip *safe city*, dar pentru operarea serverelor pentru platforme cloud a colaborat cu Google și Microsoft.⁸⁷ În plus, compania britanică BAE a furnizat sisteme de supraveghere în masă, iar compania japoneză NEC a vândut camere cu recunoaștere facială.⁸⁸

Companii din Franța, Germania, Israel, Japonia, Regatul Unit sau Statele Unite furnizează tehnologii avansate către regimuri autoritare. Instrumentele variază de la *spyware*-uri care monitorizează locația, supraveghere video avansată, *software*-uri pentru *hacking* sau instrumente pentru filtrarea traficului web și pentru cenzură. Companii americane semnificative furnizează astfel de tehnologii AI de supraveghere în peste 32 de state, cele mai importante fiind IBM, *Palantir* și *Cisco*.⁸⁹

Conform lui Steven Feldstein, mai mult de jumătate din democrațiile liberale utilizează sisteme de supraveghere pe baza AI, de la platforme tip *safe city*, la camere cu recunoaștere facială. Totuși, simpla utilizare a tehnologiilor de supraveghere nu înseamnă că acestea sunt și abuzate.⁹⁰ Există și situații în care statele democratice din spațiul occidental au abuzat sisteme de supraveghere și instrumente cibernetice.⁹¹ *Pegasus*, *spyware*-ul creat și distribuit de compania israeliană NSO Group, a fost abuzat de mai multe guverne autoritare și/sau iliberale din lume pentru a spiona activiști pentru drepturile omului, jurnaliști sau avocați. Instrumentul cibernetice a fost utilizat și de Ungaria, un stat membru NATO și UE.⁹²

În acest context, Președintele american Joe Biden a semnat în martie 2023 un ordin executiv prin care a restricționat utilizarea de către guvernul american a unei categorii de

⁸⁵ Peterson și Hoffman, „Geopolitical implications”, 7.

⁸⁶ Jessica Chen Weiss, „Understanding and rolling back digital authoritarianism”, *War on the Rocks*, 17 februarie 2020, <https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/>, accesat la 30 mai 2023.

⁸⁷ Feldstein, „When it comes to”.

⁸⁸ *Ibid.*

⁸⁹ Feldstein, „The Global Expansion”, 1; Feldstein, „When it comes to”.

⁹⁰ Feldstein, „The Global Expansion”, 2.

⁹¹ Aici se pot încadra și dezvăluirile făcute de Edward Snowden cu privire la practicile agenției americane NSA sau ultimele dezbateri UE privind criptarea datelor.

⁹² Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani și Michael Safi, „Revealed: leak uncovers global abuse of cyber-surveillance weapon”, *The Guardian*, 18 iulie 2021, <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>, accesat la 30 mai 2023.

instrumente cibernetice tip *spyware*. Ordinul se referă la *spyware*-urile care au fost abuzate de guverne străine, care ar putea viza cetățeni americani din afara țării, sau care ar putea prezenta riscuri de securitate după instalarea în rețelele federale. Ulterior, SUA a semnat un comunicat comun împreună cu o serie de state, printre care Canada, Franța, Suedia sau Regatul Unit, făcând un apel pentru controlul intern și internațional asupra proliferării *spyware*-urilor comerciale. Comunicatul evidențiază că aceste instrumente cibernetice au fost utilizate de anumite guverne împotriva opoziției și pentru a restricționa libertatea de exprimare și pentru a permite încălcări ale drepturilor omului.⁹³

Respingerea și combaterea autoritarismului digital la nivel intern și global

Statele Unite și statele partenere ar trebui să desemneze o serie de regimuri drept „autoritare digital”, dacă acestea utilizează în mod curent și intenționat supravegherea în masă fără protecțiile necesare.⁹⁴ Statele care au fost victime ale unor agresiuni cibernetice sau hibride ar trebui să le trateze și să le pedepsească nu ca acțiuni individuale, ci drept campanii strategice.⁹⁵ Riscul de a deveni ținta unor sancțiuni internaționale coordonate ar putea reprezenta un mecanism suficient de puternic pentru schimbarea comportamentului statelor care nu fac parte concret din niciunul dintre blocuri.⁹⁶ Spre exemplu, atacurile cibernetice rusești asupra Estoniei din 2007, atacurile din 2008 împotriva Georgiei sau cele din 2014 împotriva Ucrainei sunt strâns legate. Acestea fac parte din campania Rusiei de a submina încrederea publică în coeziunea și securitatea NATO și UE sau de a crește costul aderării la cele două organizații.⁹⁷ Totodată, SUA și alte democrații partenere au instituit sancțiuni, controlul asupra exporturilor și interdicții pentru investiții pentru a încetini propagarea necontrolată a tehnologiilor de monitorizare.⁹⁸

Spre exemplu, atacurile cibernetice *WannaCry* și *NotPetya* din mai 2017 și iunie 2017 au fost atribuite Rusiei de către Statele Unite și alte câteva state partenere în decembrie 2017 și februarie 2018. În februarie 2018, Departamentul pentru Justiție al SUA a pus sub acuzare 13 oficiali ruși și 3 companii pentru interferarea în alegerile prezidențiale din 2016. Șase ofițeri GRU ai Rusiei au fost puși sub acuzare de SUA în 2020 pentru atacurile cibernetice asupra Ucrainei, Georgiei, asupra alegerilor prezidențiale franceze din 2017 și cele împotriva Jocurilor Olimpice de Iarnă din PyeongChang.⁹⁹

Spațiul cibernetic nu trebuie văzut neapărat ca un domeniu care favorizează ofensiva în detrimentul defensivei, dar nici ca o zonă unde apărarea poate fi vreodată impenetrabilă. Atâta vreme cât întrebarea este când va avea loc un următor atac cibernetic (și nu dacă), actorii statali trebuie să lucreze activ pentru a spori reziliența. Totodată, o parte din

⁹³ Mark Mazzetti, „Biden Acts to Restrict U.S. Government Use of Spyware”, *New York Times*, 27 martie 2023, <https://www.nytimes.com/2023/03/27/us/politics/biden-spyware-executive-order.html>, accesat la 30 mai 2023; „Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware”, *The White House*, 30 martie 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/>, accesat la 30 mai 2023.

⁹⁴ Polyakova și Meserole, „Exporting digital authoritarianism”, 11.

⁹⁵ Kello, „Cyber legalism”, 11.

⁹⁶ Knake, „Weaponizing Digital Trade”, 14.

⁹⁷ Kello, „Cyber legalism”, 11.

⁹⁸ Peterson și Hoffman, „Geopolitical implications”, 1.

⁹⁹ Monica Kaminska, „Restraint under conditions of uncertainty: why the United States tolerates cyberattacks”, *Journal of Cybersecurity* 7, nr. 1 (2021): 1-15, <https://10.1093/cybsec/tyab008>.

apărarea cibernetică include și dezafectarea sistemelor și rețelelor actorilor statali sau non-statali care lansează atacuri cibernetice. Astfel de atacuri cibernetice nu trebuie lansate ca represalii (spre ex. ca un actor statal să lanseze un atac asupra infrastructurii energetice a unui stat care a desfășurat atacuri cibernetice asupra rețelei de telecomunicații), ci doar pentru a ținti precis și limitat sistemele utilizate de atacatori. Până acum, doar Statele Unite și Regatul Unit au discutat relativ deschis despre operațiunile cibernetice ofensive pentru apărare, în timp ce Londra chiar a publicat un document important în aprilie 2023 prin care este explicată destul de detaliat modalitatea de acțiune și principiile care stau la baza operațiunilor cibernetice ofensive ale *National Cyber Force*.¹⁰⁰

Totuși, chestiunea atribuirii rămâne una complicată, iar eforturile pot (și trebuie) să fie dublate de credibilitatea internațională a statelor care atribuie operațiunea cibernetică. Cel mai complicat aspect rămâne atribuirea tehnică a unei operațiuni cibernetice, ținând cont de toate eforturile pe care atacatorul le desfășoară pentru a ascunde cât mai mult originea atacului. În această direcție devin foarte importante activitățile serviciilor de informații și ale altor instituții care se ocupă de colectarea și analiza de date și informații – dificultățile tehnice pot fi depășite prin analizarea aspectelor politice, a tiparelor, strategiilor, intențiilor sau a motivațiilor actorilor. Pentru aceste demersuri, ar putea avea un rol foarte important inclusiv societatea civilă, media (mai ales jurnalismul de investigație, fiind destul de evidentă importanța grupului *Bellingcat*).

Totodată, Statele Unite și statele partenere trebuie să sprijine eforturile de a implementa restricții pentru furnizorii de tehnologii pentru infrastructura 5G care să acopere Huawei și alte companii din China.¹⁰¹ În 2019 și 2020, SUA, România, Bulgaria, Polonia, Cehia, Slovacia și țările baltice au semnat declarații privind securitatea rețelelor 5G, angajându-se să utilizeze doar furnizori de încredere pentru construirea rețelelor.¹⁰² Totuși, Ungaria a decis să coopereze tot cu Huawei pentru dezvoltarea sistemului de rețele 5G din țară.¹⁰³ În același context, UE a adoptat în 2022 Acordul European pentru Cipuri, după ce în 2021 anunțase strategia Global Gateway, având ca scop creșterea rezilienței lanțurilor de aprovizionare UE și reducerea decalajelor din infrastructură la nivel global.¹⁰⁴

Companiile care furnizează tehnologii care pot fi abuzate de regimurile care practică autoritarismul digital trebuie sancționate, și nu doar cele din Rusia sau China, ci și cele din Europa, SUA sau Israel.¹⁰⁵ Un astfel de pas poate fi și comunicatul comun adoptat de Statele Unite împreună cu Regatul Unit, Franța, Canada, Suedia și alte state pentru a atrage atenția asupra proliferării *spyware*-urilor comerciale.¹⁰⁶ Statele semnatare au afirmat că interesul lor este de a proteja indivizii și organizațiile care se confruntă cu riscul de a deveni victimele abuzului de *spyware* din întreaga lume, cu precădere jurnaliștii, activiștii și dizidenții. Astfel, statele democratice ar trebui să restricționeze exportul instrumentelor de supraveghere

¹⁰⁰ „The National Cyber Force: Responsible Cyber Power in Practice”, *National Cyber Force*, martie 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf, accesat la 30 mai 2023.

¹⁰¹ Bozhkov, „China’s Cyber Diplomacy”, 49.

¹⁰² Makowska, „China’s Digital Authoritarianism”, 9.

¹⁰³ *Ibid.*, 10.

¹⁰⁴ *Ibid.*, 11.

¹⁰⁵ Polyakova și Meserole, „Exporting digital authoritarianism”, 11.

¹⁰⁶ „Joint Statement on Efforts to”, 104.

către state autoritare, dar și să le ceară companiilor care exportă tehnologii cu utilizare duală să efectueze rapoarte privind impactul acelor produse asupra drepturilor omului.¹⁰⁷

Există și state care au adoptat practici de autoritarism digital la care au renunțat ulterior, ceea ce indică faptul că astfel de măsuri de combatere ar putea funcționa în viitor. Un exemplu este Ecuador, care a implementat un sistem de monitorizare chinezesc în 2011. În 2017, când a fost aleasă altă administrație prezidențială, a fost începută o anchetă cu privire la abuzul sistemului, permițând și accesul *The New York Times* la documente. Relatăriile au evidențiat exportul Chinei de autoritarism digital, dar și faptul că statele pot să dea înapoi de la alunecările către autoritarism.¹⁰⁸

Mai mult decât atât, statele democratice pot să pună presiune substanțială împotriva guvernelor care blochează Internetul și să sprijine cetățenii să ocolească controlul online și filtrele impuse de state autoritare. Metode de ocolire a cenzurii online sau a opririi conexiunilor la anumite platforme sunt în mare parte de natură tehnică. Acestea includ utilizarea de rețele personale virtuale (*Virtual Private Networks* – VPN) sau crearea unei rețele independente de dispozitive care pot transmite semnal de Internet prin Wi-Fi. În plus, statele democratice, împreună cu societatea civilă și companiile din sectorul tehnologiei, ar trebui să sprijine populația din țările unde există riscul opririi Internetului. Pe de o parte, statele democratice ar putea să asigure public că vor impune măsuri punitive (ex. condamnări publice, sancțiuni internaționale etc.). Pe de altă parte, democrațiile ar putea oferi stimulente financiare statelor care mențin accesul deschis la Internet, sau susținerea cetățenilor prin oferirea de ghiduri și instrumente tehnice.¹⁰⁹

Nevoia unui model alternativ de guvernare democratică a Internetului

Cel mai important, statele din spațiul democratic occidental trebuie să dezvolte un model democratic de guvernare digitală care să aibă potențialul de a deveni mai atractiv față de cele autoritare. Statele occidentale trebuie să ofere modele convingătoare de supraveghere digitală care consolidează nivelul de securitate fără să afecteze protecția libertăților civile și a drepturilor omului.¹¹⁰ Statele democratice trebuie să depună eforturi pentru a dezvolta și promova internațional un model alternativ de supraveghere publică, demonstrând că recunoașterea facială și alte instrumente pe baza AI pot fi utilizate responsabil. Odată demonstrat că acestea pot funcționa și democratic, statele ar trebui să propună standarde alternative de recunoaștere facială în cadrul Uniunii Internaționale pentru Telecomunicații (*International Telecommunication Union* – ITU).¹¹¹

Așadar, confirmând a doua ipoteză a studiului (statele democratice din spațiul occidental trebuie să respingă ofensiva autoritarismului digital, promovând la nivel global un model democratic de guvernare a Internetului), devine din ce în ce mai imperativ ca statele democratice din spațiul occidental să respingă la nivel intern și internațional ofensiva autoritarismului digital. Obiectivul principal trebuie să fie promovarea unui model alternativ

¹⁰⁷ Yayboke și Brannen, „Promote and Build”, 9.

¹⁰⁸ Weiss, „Understanding and rolling back”.

¹⁰⁹ Feldstein, „Government Internet Shutdowns”, 2-4.

¹¹⁰ Polyakova și Meserole, „Exporting digital authoritarianism”, 11.

¹¹¹ Peterson și Hoffman, „Geopolitical implications”, 1-2.

democratic și enunțarea și respectarea unor politici clare și recunoscute internațional pentru pedepsirea regimurilor autoritare digitale.

O coaliție de state democratice a început deja să pună accentul mai mult pe promovarea drepturilor omului în online în cadrul mai multor forumuri multilaterale. Totuși, progresul în această chestiune este afectat de practicile problematice privind libertatea online din propriile țări.¹¹² Înainte de a promova în mod credibil un nou model de guvernare democratică a Internetului, statele occidentale trebuie să își revizuiască propriile practici și politici. În special SUA, dar și alte state, vor trebui să depună eforturi pentru a reglementa legile privind supravegherea în masă și colectarea și analizarea datelor personale.¹¹³ În orice caz, **democrațiile liberale trebuie să respecte și să promoveze aceleași principii și în offline, și în online**, și trebuie să se rețină de la practici și politici care afectează intimitatea online a populației, securitatea cibernetică a cetățenilor și a grupurilor media și ale societății civile. În acest sens, trebuie puse în practică principiile asumate în strategiile de securitate cibernetică adoptate după 2020 în diferite democrații occidentale sau în cadrul rapoartelor grupurilor de lucru ale ONU în sfera spațiului cibernetic.

Statele democratice trebuie să integreze o abordare consistentă de a combate autoritarismul digital în eforturile legate de promovare democrației, a statului de drept, a drepturilor omului sau a bunei guvernări. Totodată, statele democratice ar trebui să reglementeze sau să sprijine dezvoltarea unor algoritmi AI și mecanisme de învățare automată care să conserve intimitatea personală și a datelor. Politicile privind criptarea datelor ar trebui să se axeze pe promovarea criptării în cât mai multe medii (spre ex. platforme de tip *cloud*, mesagerie etc.). În acest fel, se va reduce volumul de date accesibil agențiilor guvernamentale sau grupurilor de criminalitate cibernetică, contribuind inclusiv la protejarea libertăților digitale a cetățenilor din statele aflate într-un declin autoritar.¹¹⁴

Modelul trebuie să rămână puternic ancorat în principiile democrației liberale și în ideea de Internet deschis, liber și care ține cont de libertățile digitale. Promovarea internațională necesită, în primul rând, demonstrarea faptului că modelul funcționează la nivel național în statele democratice. Așadar, concomitent cu promovarea internațională a modelului, trebuie demonstrat succesul acestuia la nivel intern.

În această privință, Uniunea Europeană poate fi un promotor foarte important și poate genera așa-numitul „efect Bruxelles”, similar cu cazul legislației GDPR. Totuși, și Statele Unite pot să reprezinte un model atrăgător la nivel internațional, în special din punct de vedere al abordării mai puțin stricte cu privire la Internet și la companiile din domeniul tehnologiei. Totodată, revenirea la optimismul din anii 1990 și 2000 cu privire la rolul Internetului pentru consolidarea democrațiilor poate fi o altă cale pentru dezvoltarea unei alternative democratice.

Internetul și tehnologiile digitale, cu toate vulnerabilitățile și riscurile pe care le prezintă, încă au potențialul de a dezvolta democrațiile, dar un Internet din ce în ce mai restrictiv și periculos va descuraja o astfel de implicare din partea societății. În al doilea rând, **devine necesară și formarea efectivă a unui bloc concret de state democratice care să adopte modelul** (ex. statele UE, Regatul Unit, SUA, Canada, Israel, Australia, Noua Zeelandă, Japonia,

¹¹² „Freedom of the Net 2022”, 2.

¹¹³ Wang, „China’s Techno-Authoritarianism”.

¹¹⁴ Yayboke și Brannen, „Promote and Build”, 8-9.

Coreea de Sud etc.). Actorii respectivi trebuie să treacă mai întâi peste propriile neînțelegeri cu privire la guvernarea Internetului și să ajungă la un consens împotriva unui adversar comun – autoritarismul digital.

Una din provocările cele mai mari pentru diplomația cibernetică a statelor democratice este de a atrage sprijinul Braziliei, Indiei sau Indoneziei, state considerate neutre, pentru promovarea unui model democratic de guvernare a Internetului la nivel global. Cele trei state ar putea sprijini un astfel de model la nivel internațional și să aplice practici de autoritarism digital la nivel național, fără să adopte modelul normativ susținut de China la ONU.¹¹⁵

CONCLUZII

Consolidarea relațiilor dintre Rusia și China din 2022 până în prezent, în contextul războiului Moscovei împotriva Ucrainei, ar putea influența și activitățile din spațiul cibernetic. Pe de o parte, Federația Rusă a înăsprit autoritarismul în interior pentru a ameliora opoziția față de război, iar represiunea internă într-o eră digitală este bazată pe tehnologii digitale. Totuși, Rusia era cunoscută pentru tehnologii mai accesibile, dar funcționale în domeniul autoritarismului digital, sistemul de filtrare SORM (mult mai permisiv față de Marele Firewall al Chinei) fiind cel mai important în această privință. Întărirea parteneriatului cu Beijingul ar putea aduce o modernizare a sistemelor digitale represive ale Rusiei, China având deja investiții serioase în țară, în ciuda ezitării inițiale ale guvernului rus. Totodată, rămâne de urmărit cum vor evolua și operațiunile cibernetiche ale celor două state, și dacă va începe să se vadă o convergență mai mare în acțiunile celor doi actori împotriva statelor euro-atlantice.

Încă din anii 2000, China s-a axat preponderent (aproape exclusiv) pe operațiuni de spionaj cibernetic, sesizându-se doar o creștere a complexității și magnitudinii atacurilor. În schimb, Rusia a desfășurat activități de spionaj cibernetic, dar și o serie vastă de atacuri cibernetiche împotriva statelor euro-atlantice. Cele mai notabile sunt cele împotriva Ucrainei sau cele care au vizat alegerile din mai multe state din Europa și America de Nord.

În ceea ce privește invazia rusă a Ucrainei, începută în februarie 2022, cercetătorii din zona securității cibernetiche par să fie de acord că războiul Rusiei nu a schimbat mult dinamica *cyberwarfare*-ului.¹¹⁶ Era deja recunoscut că operațiunile cibernetiche se derulează la un nivel redus între actorii statali, dar continuu. Riscul unor atacuri cibernetiche majore lansate de Federația Rusă asupra unor ținte militare sau civile din spațiul euro-atlantic (în special infrastructura critică, energetică sau sistemele de sănătate) rămâne major, dar nu este clară intenția Moscovei de a lansa astfel de atacuri. Până acum, strategia statelor euro-atlantice a fost de a condamna și atribui public operațiunile cibernetiche cele mai importante lansate de Rusia, și în cele mai substanțiale dintre acestea chiar să impună sancțiuni internaționale în cadrul unor

¹¹⁵ Knake, „Weaponizing Digital Trade”, 2.

¹¹⁶ Lucas Kello și Monica Kaminska, „Cyberspace and War in Ukraine: Prepare for Worse”, *Lawfare*, 14 aprilie 2022, <https://www.lawfareblog.com/cyberspace-and-war-ukraine-prepare-worse>, accesat la 30 mai 2023; Brandon Valeriano, Erica D. Lonergan, Shawn W. Lonergan și Benjamin Jensen, „Putin’s Invasion of Ukraine Didn’t Rely on Cyberwarfare. Here’s Why”, *CATO Institute*, 7 martie 2022, <https://www.cato.org/commentary/putins-invasion-ukraine-didnt-rely-cyberwarfare-heres-why>, accesat 30 mai 2023; Lennart Maschmeyer și Myriam Dunn Cavelti, „Goodbye Cyberwar: Ukraine as Reality Check”, *Policy Perspectives* 10, nr. 3: 1-4, https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

coaliții ad-hoc, a unor grupuri internaționale (ex. *Five Eyes*, aprilie 2022) sau în cadrul Uniunii Europene. Mai mult, **un alt aspect care ar descuraja Rusia să lanseze un astfel de atac, în ciuda dificultății de atribuire tehnică a atacului, ar fi posibilitatea ca NATO să activeze Articolul 5 în acest context.**

Oricum, în niciun caz nu ar putea fi provocată sau influențată o schimbare majoră a politicilor interne ale Chinei și Rusiei, dar statele care nu fac neapărat parte din vreun bloc digital mai au încă o șansă (ex. Serbia, Turcia, India, Brazilia, Mexic etc.). Chiar și în regimuri iliberale, Internetul ar putea rămâne relativ liber, iar supravegherea în masă ar putea fi responsabilă. Dar, înainte de promovarea unui model democratic de guvernare a Internetului, trebuie rezolvate problemele interne dintr-un potențial bloc democratic. Trebuie combătute practicile SUA, Regatului Unit, Israelului și ale altor țări democratice care au un istoric de a abuza tehnologiile digitale pentru îndeplinirea unor obiective din sfera securității naționale. Totodată, trebuie prevenit și declinul democratic al unor state precum Ungaria sau Polonia. Credibilitatea internațională a modelului democratic de guvernare a spațiului cibernetic va juca un rol important în promovarea acesteia la nivel internațional.