BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Considerații preliminare asupra cooperării internaționale a Chinei în domeniul securității cibernetice: legistație, instituții competente și provocări

Preliminary considerations on China's international cooperation in cyber security: legislation, competent authorities, and challenges

Drd. Andreea-Maria PIERȘINARU*
*Școala Națională de Studii Politice și Administrative (SNSPA)
e-mail: andreea_piersinaru@yahoo.com

Abstract

În acest articol s-au punctat aspecte generale privind cadrul legislativ, instituțiile competente, obiectivele strategice ale Chinei și provocările în ceea ce privește cooperarea internațională în domeniul securității cibernetice. Obiectivul principal al cercetării este identificarea actorilor implicați în asigurarea securității cibernetice a Chinei, descrierea atribuțiilor lor și corelarea acestora cu legislația chineză în materie de securitate cibernetică și cu Strategia de cooperare a Chinei în securitate cibernetică. Prin acest studiu, se trasează considerațiile preliminare pentru viitoarele analize aprofundate cu privire la impactul acțiunilor Chinei asupra securității cibernetice la nivel internațional. Printre principalele concluzii ale studiului, se regăsesc câteva aspecte legate de influențele politicilor și narativelor Partidului Comunist Chinez, prezentate în Strategia de cooperare internațională a Chinei în securitate cibernetică, precum și de faptul că, în pofida intenției Chinei de a deveni o putere cibernetică, deschisă către cooperare, reacțiile internaționale sunt destul de reticente, din cauza acuzațiilor de spionaj cibernetic și problemelor de supraveghere internă, existente la nivel național, printre altele.

This article addressed general issues regarding the Chinese legislative framework, competent authorities, China's strategic objectives and the challenges in terms of international cooperation in the field of cybersecurity. The main objective of the research is to identify the actors involved in ensuring China's cybersecurity, describe their responsibilities and correlate them with Chinese cyber-security legislation and China Cyber Security Cooperation Strategy. This study traces preliminary considerations for future in-depth analyses of the impact of China's actions in the field of international cybersecurity. Among the main findings of the study the aspects briefly identified were related to the influences of the policies and narratives of the Chinese Communist Party presented in China's International Cyber Security Cooperation Strategy, as well as to the fact that, despite China's intention to become a cyber power, open to cooperation, international reactions are quite reluctant due to allegations of cyber espionage and domestic surveillance problems existing at the national level, among others.

Cuvinte-cheie:
China; securitate cibernetică; suveranitate cibernetică; spionaj cibernetic; cooperare internațională; superputere cibernetică.
Keywords:
China; cyber security; cyber sovereignty; cyber espionage; international cooperation; cyber superpower.

Info articol
Primit: 10 mai 2024; Evaluat: 10 iunie 2024; Acceptat: 13 iunie 2024; Disponibil online: 5 iulie 2024
Citare: Pierșinaru, A.M. 2024. „Considerații preliminare asupra cooperării internaționale a Chinei în domeniul securității cibernetice: legistație, instituții competente și provocări". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(2): 75-96. https://doi.org/10.53477/2065-8281-24-15

Securitatea cibernetică a devenit o parte esențială a politicii externe și de securitate a statelor, datorită globalizării și digitalizării accelerate. Ca una dintre cele mai mari economii și puteri tehnologice din lume, China a creat o strategie complexă de cooperare internațională în domeniul securității cibernetice. În ultimii ani, China și-a intensificat eforturile de a participa la discuții și parteneriate la nivel global, cooperarea multilaterală fiind astfel esențială pentru a aborda provocările cibernetice internaționale.
În literatura de specialitate, care tratează analize ale textelor legislative și evoluții subsecvente ale acestora în domeniul securității cibernetice, în China se regăsesc cercetări care abordează textele legislative dintr-o perspectivă fie istorică, fie analitică din punctul de vedere al cooperării internaționale.
Așadar, între studiile relevante cu privire la evoluția legislativă în materie de securitate cibernetică în China se regăsește studiul lui Rogier Creemers, care oferă o prezentare amănunțită a etapelor evoluției legislației chineze în materie de securitate cibernetică.

De la sfârșitul anilor ’90, China a adoptat o politică de „informatizare” – 信息化 (xìn xī huà) –, care implică utilizarea tehnologiei digitale în activitățile economice, sociale și guvernamentale. Această politică a evoluat odată cu înființarea, în 2014, a Grupului central de conducere pentru securitate cibernetică și informatizare, prezidat de președintele Xi Jinping. Astfel, în timpul administrației Xi, a fost dezvoltată „Strategia privind puterea cibernetică” sau „网络强国战略” (Wǎngluò qiángguó zhànlüè), care are ca scop principal îmbunătățirea capacităților tehnologice ale Chinei și modernizarea guvernanței de stat, incluzând proiecte, precum informatizarea judiciară și sistemul de credite sociale (Creemers 2023).

Un alt studiu de referință în literatura de specialitate este și cel al lui Meirong Guo „Legile chineze de securitate cibernetică, relevanța acestora pentru infrastructurile critice și provocările cu care se confruntă”. Studiul său aduce o interpretare nouă a Legii Securității Cibernetice, adoptată în 2016, care, din perspectiva sa, nu a fost implementată eficient, deoarece securitatea cibernetică a fost integrată în mai multe legi sau regulamente administrative deja existente la nivel departamental și nu a existat o coerență centralizată. Guo subliniază, de asemenea, că Republica Populară Chineză nu avea reglementări legale specifice pentru securitatea cibernetică, înainte de adoptarea Legii Securității Cibernetice în 2016, subliniind, totodată, importanța participării Chinei la cooperarea internațională în domeniul securității cibernetice, pentru a formula standarde tehnice internaționale și pentru a face față amenințărilor cibernetice globale (Guo 2018).

În acest context, China s-a angajat să construiască parteneriate de cooperare extinse cu toate părțile comunității internaționale, să dezvolte platformele de dialog și să promoveze un cadru de securitate cibernetică echitabil pentru toți participanții, China adoptând această abordare în cadrul cooperării cu ASEAN și cu Organizația de Cooperare de la Shanghai cu privire la răspunsurile de urgență în domeniul securității rețelelor și informațiilor (MFA CN 2017).

În toate textele normative și discursurile liderilor chinezi, China se declară deschisă cooperării în domeniul securității cibernetice, demonstrând acest interes prin participarea activă la summiturile mondiale privind societatea informațională și alte conferințe internaționale sau regionale legate de securitate cibernetică. China a fost gazda primului Summit Mondial privind Securitatea Cibernetică, organizat de Institutul EastWest din Dallas. Acest eveniment este menționat de liderii chinezi în toate prezențele publice relaționate domeniului securității cibernetice pentru a poziționa China ca lider în domeniu și ca unul dintre inițiatorii dialogului internațional în materie de securitate cibernetică (Chinese Embassy in UK 2011). De asemenea, China declară că susține un sistem global de guvernanță a internetului multilateral, democratic și transparent și include sprijinirea Națiunilor Unite în rolul de lider în guvernanța digitală globală și crearea de reguli, subliniind necesitatea unei abordări deschise și echitabile pentru guvernanța cibernetică (MFA CN 2023).

Un alt pilon al strategiei Chinei este cooperarea în cercetare și dezvoltare pentru a crește nivelul securității cibernetice prin parteneriate industriale și academice. Aceasta include colaborarea cu instituții de cercetare și cu universități internaționale (Zhang și alții 2022).
În acest context, China a anunțat, încă din 2017, pilotarea unui proiect pentru dezvoltarea a patru până la șase institute de securitate cibernetică de renume mondial până în 2027. Aceste institute vor avea ca obiective principale formarea profesioniștilor în securitatea rețelelor, derularea de cercetări academice relevante și cooperarea cu companii și departamente guvernamentale. Unul dintre obiectivele majore ale acestor institute este cooperarea internațională, care include sprijinirea formării în străinătate a personalului academic cheie și dezvoltarea colaborării în cercetarea academică în cadrul unor consorții internaționale (Chinese Ministry of Education 2017).

Conform studiului publicat, în 2021, de Centrul pentru Securitate și Tehnologii Emergente, China a stabilit Centrul Național de Securitate Cibernetică (NCC) în Wuhan[1], care include șapte centre pentru cercetare, dezvoltarea talentelor și antreprenoriat. NCC găzduiește două laboratoare, axate pe cercetarea în domeniul securității cibernetice pentru uz guvernamental, și un incubator pentru susținerea inovației în sectorul privat (Figura1). Acest centru este susținut de la cele mai înalte niveluri ale Partidului Comunist Chinez (PCC) și are ca scop reducerea dependenței de tehnologiile străine și promovarea inovației naționale (Cary 2021).

Price Waterhouse Cooper (PWC) menționează, într-un raport publicat în anul 2023, că, în pofida asumării publice a deschiderii pentru cooperare în securitate cibernetică, cooperarea internațională afectează politica internă a Chinei în domeniu, forțând Beijingul să implementeze reglementări și legi

[1] Video despre NCC în limba chineză : https://www.bilibili.com/video/BV1Vz411z7gT/?t=0h0m54s.

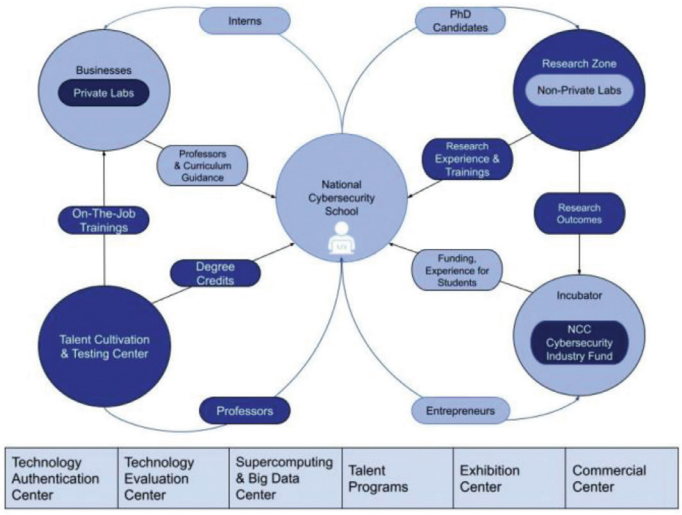

Figura 1 **Centrul pentru Securitate și Tehnologii Emergente** (Cary 2021)

stricte pentru a gestiona fluxurile de date și pentru a proteja infrastructurile critice (PwC Indonesia 2023).
În ciuda eforturilor sale de a deveni o superputere cibernetică, China se confruntă cu probleme semnificative, cum ar fi acuzațiile de spionaj cibernetic și preocupările cu privire la metodele sale interne de supraveghere și control al informațiilor (Julian 2021).

Având în vedere evoluțiile legislative ale Chinei în materie de securitate cibernetică, dar și obiectivul său strategic, de a deveni o superputere cyber în timpul administrației Xi, s-a considerat oportun un studiu introductiv al perspectivelor legislative actuale ale Chinei în materie de securitate cibernetică, care să cuprindă și o succintă prezentare a structurilor care asigură securitatea cibernetică la nivel național, având în vedere că acestea nu au fost identificate într-un mod unitar în literatura de specialitate parcursă, ci doar în textul Legii privind securitatea cibernetică. Nu în ultimul rând, se va analiza succint perspectiva strategiei de cooperare în domeniul securității cibernetice și vor fi prezentate câteva dintre provocările apărute în implementarea obiectivelor.

Metodologia și limitele cercetării

Prezentul studiu își propune să identifice considerentele preliminare cu privire la legislația și strategia Chinei în domeniul securității cibernetice, precum și efectele acestora asupra cooperării internaționale în materie de securitate cibernetică. Ipoteza prezentei cercetări este că dorința Chinei de a-și proteja suveranitatea cibernetică și de a-și consolida poziția de superputere cibernetică are un impact semnificativ asupra cooperării internaționale în domeniul securității cibernetice. Astfel, apare următoarea întrebare de cercetare: *Cum afectează legislația chineză în domeniul securității cibernetice cooperarea cu alte state?*

În testarea ipotezei, s-au folosit metode cantitative, pentru culegerea și analiza datelor: analiza datelor secundare (pentru literatura de specialitate) și analiza de conținut (pentru textele legislative). Analiza datelor secundare implică găsirea de răspunsuri la noi întrebări de cercetare prin utilizarea datelor care au fost deja colectate din alte studii (Fulton Library, fără an).

Articolul reprezintă o scurtă introducere în domeniul securității cibernetice a Chinei, care este limitat la prezentarea celor mai importante aspecte, din perspectiva autoarei, din Legea securității cibernetice a Chinei, dar și din Strategia de cooperare internațională a Chinei, precum și la identificarea câtorva provocări pe care guvernul chinez le are în îndeplinirea obiectivelor sale de cooperare internațională în domeniul securității cibernetice. De asemenea, în cadrul acestor considerente preliminare, se va face referire și la principalele atribuții ale structurilor care se ocupă cu implementarea planului de acțiuni al strategiei de securitate cibernetică, conform legii.
Toate acestea pot deschide noi oportunități de cercetare în domeniu prin aprofundarea studiului, folosind și alte metode de cercetare, care, din cauza constrângerii de timp, nu s-au putut dezvolta în prezentul articol. Elementele prezentate în cadrul studiului pot fi astfel folosite ca referință sau punct de plecare pentru viitoare analize sectoriale mai detaliate și structurate de către cercetătorii interesați de subiect, dar și de către experții în elaborarea unor politici și strategii în ceea ce privește cooperarea internațională a Chinei în domeniul securității cibernetice.

Articolul este structurat în două secțiuni principale, precedate de o scurtă introducere și de prezenta metodologie, însoțită de limitele cercetării, și se încheie cu o serie de concluzii. Prima secțiune este dedicată prezentării succinte a structurii aparatului de stat care se ocupă de securitatea cibernetică în Republica Populară Chineză și a cadrului legislativ în materie de securitate cibernetică în China. În ceea ce privește cadrul legislativ, s-a analizat doar Legea privind securitatea cibernetică a Chinei.

Cea de-a doua secțiune a articolului este dedicată prezentării unor aspecte introductive cu privire la Strategia Republicii Populare Chineze pentru Cooperare Internațională în domeniul securității cibernetice[2] și la provocările în atingerea obiectivelor enunțate în strategie. Cu privire la provocările Chinei în atingerea obiectivelor, enunțate în strategia de cooperare internațională, sunt analizate punctual trei cazuri de grupuri chineze relaționate spionajului cibernetic: APT10, APT 31 și APT41.

Concluziile studiului subliniază importanța tematicii și necesitatea aprofundării studiilor în domeniul securității cibernetice, mai ales cu privire la perspectivele care vin dinspre China, pentru o mai bună înțelegere a perspectivelor privind cooperarea internațională în securitatea cibernetică.

[2] Se analizează strategia per ansamblu. fmprc.gov.cn, 2017.

Prezentarea succintă a structurii aparatului de stat care se ocupă de securitatea cibernetică în Republica Populară Chineză și a cadrul legislativ în materie de securitate cibernetică în China (gov.cn)[3]

[3] Se analizează textul Legii privind Securitatea Cibernetică a Chinei, per ansamblu.

Pentru a înțelege structura aparatului de stat care se ocupă de securitatea cibernetică în China, este necesară amintirea faptului că, într-un stat autocratic precum China, nicio structură de tip guvernamental nu este independentă și nu funcționează de sine stătător fără impactul strategiilor și narativelor Partidului Comunist Chineze și al liderilor săi.

Așadar, având în vedere această structură piramidală, Comisia Centrală pentru Afaceri în Domeniul Spațiului Cibernetic (CCAC) a Comitetului Central al Partidului Comunist Chinez este organismul principal responsabil cu implementarea politicilor în materie de securitate cibernetică, fondată în 2018, ca o continuare a eforturilor inițiate de Grupul de Lucru pentru Securitate Cibernetică și Informatizare, înființat în 2014. CCAC este responsabilă de coordonarea activităților următoarelor agenții și entități subordonate, care comunică și colaborează între ele: Administrația Spațiului Cibernetic (CAC), Centrul de Informare al Opiniei Publice, Registrul DNS al Chinei, gestionat de China Internet Network Information Center (CNNIC), CNCERT (Centrul Național de Răspuns la Incidente de Securitate Cibernetică), TC260 – Comitetul Tehnic pentru Standardizarea Securității Informației Naționale din China – și Asociația de Securitate Cibernetică a Chinei. Coordonarea eficientă a acestor agenții și entități este esențială pentru implementarea politicilor de securitate cibernetică și pentru promovarea unei guvernanțe integrate a spațiului cibernetic din China. Reflectând importanța strategică pe care Partidul Comunist Chinez o acordă controlului și securității cibernetice, Xi Jinping, împreună cu Li Qiang și Cai Qi, prezidează CCAC.

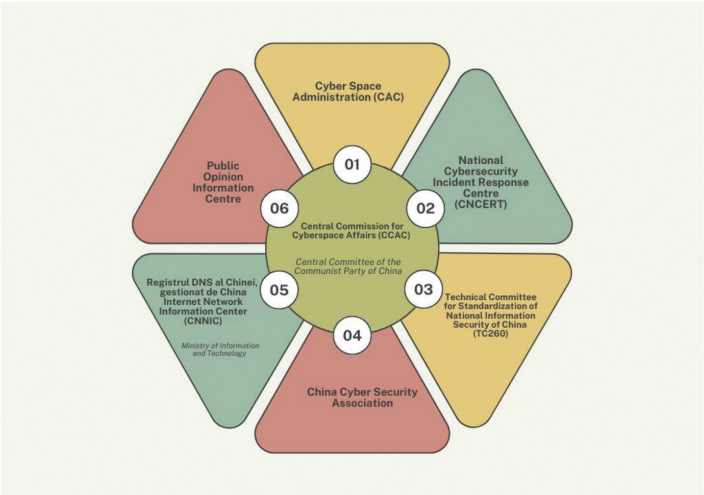

Figura 2 **Structura aparatului de stat în ceea ce privește spațiul cibernetic și securitatea cibernetică din China**[4]

[4] Interpretare personală, conform Legii Securității Cibernetice a Chinei.

În continuare, a fost elaborată de către autoare diagrama structurii aparatului de stat care se ocupă de spațiul cibernetic și, implicit, de securitatea cibernetică din China, pentru o înțelegere mai precisă a celor prezentate anterior. După prezentarea diagramei, se va urmări o scurtă prezentare a atribuțiilor fiecărei instituții.

Administrația Spațiului Cibernetic (CAC) este autoritatea națională de reglementare în domeniul cibernetic din China. Pe lângă reglementarea în domeniul cibernetic național, CAC se ocupă și de cenzura cibernetică și stabilește politici specifice în acest sens. Această entitate este vitală pentru sistemul de guvernanță cibernetică a Chinei, deoarece este responsabilă de supravegherea și controlul internetului pentru a se asigura că întregul conținut care apare în acest spațiu îndeplinește cerințele Partidului Comunist Chinez (PCC). De asemenea, CAC, prin responsabilitățile aferente managementului spațiului cibernetic, stabilește reguli pentru companiile de tehnologie și urmărește comunicarea online pentru a preveni răspândirea informațiilor considerate periculoase sau destabilizatoare pentru stat (CAC, fără an).

În 2019, CAC a demarat un proiect pentru a elimina pornografia, violența, jocurile de noroc, frauda, superstiția, parodia, amenințările și răspândirea „stilurilor de viață neadecvate" și „culturii populare proaste", care a impus un nivel de control al conținului online ridicat, favorizând imaginea PCC online (Xinhua 2019).
În același an, CAC a emis un regulament care prevedea că orice comportament considerat fraudulos online va fi adăugat în sistemul de credite sociale – care prevede pedepsirea răufăcătorilor prin imposibilitatea accesării unor credite bancare sau altor facilități cetățenești (Dandong 2019).

O altă instituție importantă a aparatului de stat în domeniul securității cibernetice este și *Centrul de Informare al Opiniei Publice,* care reunește eforturile guvernamentale de cenzură și supraveghere a informațiilor pe internet, monitorizează și analizează opiniile publice pe internet. Există mențiuni cu privire la acest centru doar în textul legii. În cadrul studiului, nu au fost identificate, până în prezent, alte surse care să prezinte sau să discute despre acțiunile centrului.

Structura responsabilă de gestionarea *Registrului DNS al Chinei* este *China Internet Network Information Center* (CNNIC). În ceea ce privește gestionarea și operarea domeniului de nivel superior (TLD), CNNIC este responsabil pentru domeniile „.cn". Acesta include supravegherea înregistrărilor de domenii și asigurarea că infrastructura DNS, asociată cu aceste domenii funcționează bine. Pe de altă parte, CNNIC-ului îi revine o responsabilitate importantă în protejarea datelor personale și în securitatea cibernetică: asigurarea securității infrastructurii DNS și protejarea datelor utilizatorilor. Acest obiectiv include stabilirea de reguli de securitate pentru a preveni abuzurile și atacurile cibernetice, precum și pentru gestionarea datelor WHOIS, care conțin informații despre deținătorii de domenii. Pentru a se conforma standardelor internaționale în gestionarea numelor de domeniu, CNNIC lucrează cu ICANN și cu alte organizații internaționale de gestionare a internetului. Acest lucru include implicarea activă în procesele globale de politică și în implementarea

deciziilor internaționale în sistemul de domenii al Chinei. Nu în ultimul rând, CNNIC susține crearea și utilizarea numelor de domeniu internaționalizate (IDN), care permit utilizarea caracterelor chinezești în numele de domeniu. Aceasta facilitează accesul la internet în limba maternă a vorbitorilor de chineză (CNNIC fără an).

CNCERT (Centrul Național de Răspuns la Incidente de Securitate Cibernetică) supraveghează eforturile de prevenire a amenințărilor cibernetice, anticipând și blocând potențialele atacuri, înainte ca acestea să afecteze rețelele sau infrastructurile critice naționale, și asigură o recuperare cât mai completă și cât mai rapidă posibil după gestionarea unui incident, restabilind serviciile și sistemele afectate. CNCERT lucrează cu echipe similare din alte țări și cu organizații internaționale pentru a gestiona incidentele de securitate cibernetică ce pot afecta diverse state. CNCERT este membru al Forumului de Echipe de Răspuns la Incidente de Securitate (FIRST) și unul dintre fondatorii Grupului de Răspuns la Incidente de Securitate Computerizate din Asia Pacific (APCERT). CNCERT informează publicul și organizațiile în legătură cu riscurile de securitate cibernetică și cu cele mai bune practici de protecție, colectează și distribuie date privind vulnerabilitățile de securitate prin China National Vulnerability Database (CNCERT/CC, fără an).

Obiectivul principal al *Comitetului Tehnic pentru Standardizarea Securității Informației Naționale din China (TC260)* este crearea standardelor naționale pentru securitatea cibernetică. Acest comitet este responsabil pentru stabilirea și menținerea continuă a unui cadru de standarde care reglementează diferitele aspecte ale securității cibernetice în China, cum ar fi securitatea produselor și serviciilor de rețea, protecția infrastructurii critice de informații și managementul incidentelor de securitate cibernetică. TC260 lucrează împreună cu alte entități guvernamentale și organizații din sectorul privat pentru a se asigura că standardele de securitate cibernetică sunt coerente și eficiente. Acest lucru presupune implicarea persoanelor juridice care nu sunt membre ale administrației publice, cum ar fi companiile naționale și internaționale. Conform datelor publice care apar pe pagina oficială a organizației, TC260 a publicat până în prezent aproximativ 300 de standarde tehnice de securitate informațională și continuă să le îmbunătățească pentru a răspunde nevoilor în continuă schimbare din domeniul securității cibernetice (TC260, fără an).

Asociația de Securitate Cibernetică a Chinei (CSAC) coordonează politicile dintre mediul privat, public și academic. CSAC influențează legislația chineză privind securitatea cibernetică prin activitățile sale. Acest aspect include promovarea bunelor practici în industrie și a standardelor de securitate. CSCAC susține că bunurile și serviciile tehnologice chinezești contribuie la securitatea țării, așa că recomandă folosirea acestora, în detrimentul concurenților străini. Asociația lucrează pentru a promova și a apăra interesele de securitate cibernetică ale Chinei la nivel internațional, participând la discuții și negocieri cu privire la standardele și legislația internațională în domeniul securității cibernetice (Cyber Security Association of China (CSAC), fără an).

Legea Securității Cibernetice a Chinei (gov.cn 2016), aprobată într-un prim format la data de 7 noiembrie 2016 și intrată în vigoare la 1 iunie 2017, constituie baza legislativă în materie de securitate cibernetică în China. Legea are ca obiectiv general asigurarea securității rețelelor, siguranței în spațiul cibernetic, securității naționale și intereselor publice, protejarea drepturilor și intereselor legitime ale cetățenilor, precum și promovarea unei digitalizări economice și sociale sănătoase. Statul prevede măsuri de monitorizare, apărare și gestionare a riscurilor și amenințărilor de securitate a rețelelor care provin din interiorul granițelor Chinei și din afara acestora, protejează infrastructurile critice de potențiale atacuri și amenințări, prevede sancțiuni pentru infracțiuni informatice și menține ordinea și securitatea în spațiul cibernetic. Un alt aspect important menționat în lege este cel referitor la localizarea datelor. În China, legea prevede ca datele personale esențiale și alte date personale, colectate din spațiul cibernetic, să fie stocate în țară. Operatorii infrastructurilor critice sunt obligați să asigure acest lucru conform legii. În art.2, Cap.1, se menționează următoarele:

„Prezenta lege se aplică activităților de prelucrare a datelor și supravegherii securității și reglementării acestor activități pe teritoriul Republicii Populare Chineze. În cazul în care prelucrarea datelor în afara teritoriului Republicii Populare Chineze dăunează securității naționale, intereselor publice sau drepturilor și intereselor legale ale persoanelor sau organizațiilor din Republica Populară Chineză, răspunderea juridică va fi investigată în conformitate cu legea." (NPC.GOV.CN 2021)

De asemenea, complementară Legii privind Securitatea Cibernetică este Legea privind securitatea datelor (2021) care impune noi reguli pentru întreprinderile care interacționează cu cetățenii chinezi atât în țară, cât și în străinătate, observându-se influența legislației interne care migrează către spațiul extern, cu implicații în ceea ce privește cooperarea internațională a Chinei în domeniul securității cibernetice.

Legea privind securitatea cibernetică a Chinei prevede și perspectiva cooperării internaționale, guvernanța spațiului cibernetic, cercetarea în tehnologia rețelelor și crearea standardelor pentru combaterea criminalității cibernetice. De asemenea, se subliniază angajamentul Chinei de a construi un spațiu cibernetic cât mai sigur și deschis, care să reflecte valorile unei guvernanțe transparente, democratice și multilaterale, după cum prevede textul legii (gov.cn 2016). În plus, guvernul chinez încurajează adoptarea diferitelor politici de formare profesională a talentelor în domeniul securității cibernetice, schimburile internaționale de talente și implicarea institutelor de cercetare și a companiilor private activ în dezvoltarea standardelor naționale de securitate a rețelelor. În ceea ce privește acest proces, Administrația Spațiului Cibernetic al Chinei (CAC) este responsabilă de autorizarea și testarea tuturor produselor de rețea înainte de a fi comercializate, asigurându-se că acestea îndeplinesc standardele stricte de securitate, impuse la nivel național (Cyberspace Administration of China 2017).

La 12 septembrie 2022, au fost introduse amendamente importante la Legea Securității Cibernetice a Chinei. Aceste amendamente au introdus noi amenzi și

sancțiuni pentru încălcarea regulilor generale de securitate a rețelelor. În plus, au fost revizuite sancțiunile administrative pentru infracțiunile informatice săvârșite de operatorii infrastructurilor critice și au fost adăugate o serie de sancțiuni administrative și interdicții pentru alte acte ilegale care nu erau menționate în legislația administrativă anterioară. Amendamentele aduse Legii Securității Cibernetice subliniază angajamentul Chinei de a întări securitatea cibernetică și de a răspunde dinamic la provocările care apar în domeniu (gov.cn 2016).

Astfel, atât cadrul legislativ în materie de securitate cibernetică, cât și obiectivele CACC, prin toate agențiile și entitățile subordonate, consolidează capacitatea Chinei de a controla și de a reglementa spațiul cibernetic național. Aceste structuri nu numai că aplică politici, dar și influențează peisajul informațional, publicul țintă fiind atât cel național, cât și cel internațional. Astfel este important de reflectat asupra rolului pe care aceste structuri îl joacă în promovarea securității cibernetice, precum și în cenzurarea conținutului online, având un impact semnificativ asupra libertății de exprimare și asupra drepturilor omului în era digitală, mai ales atunci când se fac referiri la cooperarea internațională a Chinei în domeniul securității cibernetice.
În secțiunea următoare, se vor analiza câteva aspecte introductive și tematici relevante, din perspectiva autoarei, cu privire la strategia de cooperare internațională în materie de securitate cibernetică a Chinei.

Strategia Republicii Populare Chineze pentru Cooperare Internațională în domeniul securității cibernetice[5] și provocările în atingerea obiectivelor enunțate în strategie – Scurtă prezentare a celor mai importante puncte

[5] Se analizează strategia per ansamblu. fmprc.gov.cn, 2017.

Strategia Chinei pentru cooperare internațională în spațiul cibernetic (lansată încă din anul 2015, dar actualizată periodic – ultima actualizare: 2022) (Xinhua News Agency 2017) se aliniază gândirii Președintelui Xi Jinping, conform căreia țările sunt interconectate, au interese comune și trebuie să coopereze pentru a-și atinge obiectivele comune de menținere a păcii și securității. Astfel, promovarea deschiderii și cooperării în spațiul cibernetic sunt interesele comune, dar și responsabilitățile întregii comunități internaționale.
Modelul chinezesc al cooperării internaționale (așa cum apare, oficial, în toate actele normative și mai ales în discursurile liderilor chinezi) este promovarea unui nou tip de cooperare în relațiile internaționale: win-win. Acest model este prezent și în strategia Chinei de cooperare internațională în spațiul cibernetic.

În textul strategiei, se regăsește frecvent formularea 网络强国 (*wǎngluò qiángguó*), care se poate interpreta ca expresie a obiectivului principal al strategiei: transformarea Chinei într-o „superputere cyber" sau „transformarea Chinei într-o putere națională în spațiul cibernetic", iar printre obiectivele secundare

ale strategiei, se identifică necesitatea unui stat de a controla și de a guverna propriul spațiu cibernetic (Xinhua News Agency 2017).

Așa după cum reiese din textul strategiei, cele șase obiective ale Chinei sunt:

1. apărarea suveranității și securității naționale în spațiul cibernetic;
2. dezvoltarea unui sistem de noi reguli și norme internaționale pentru spațiul cibernetic;
3. promovarea guvernării echitabile a internetului: pledează pentru o guvernare corectă și echitabilă a internetului la nivel internațional;
4. protejarea drepturilor și intereselor legitime ale cetățenilor: se concentrează pe protejarea drepturilor și intereselor persoanelor în spațiul cibernetic;
5. promovarea cooperării în domeniul economiei digitale: își propune să consolideze cooperarea în economia digitală la nivel internațional;
6. construirea de platforme relevante pentru schimbul cultural cibernetic: subliniază importanța schimbului cultural în spațiul cibernetic (Xinhua News Agency 2017).

În strategie, se menționează că statul chinez promovează cooperarea internațională bazată pe principiile stipulate în cadrul formatului UN World Summit on Information Society (WSIS): construirea unei societăți a informației inclusive, centrată pe oameni și orientată spre dezvoltare (Sustainable Development 2016).

Printre inițiativele concrete ale Chinei în cooperarea internațională în spațiul cibernetic, conform planului de acțiuni al strategiei, se enumeră (Xinhua News Agency 2017):

- promovarea guvernării echitabile a internetului: China a pledat pentru o guvernare corectă și echitabilă a internetului la nivel internațional;
- aprofundarea cooperării cibernetice cu alte țări: China a lucrat pentru aprofundarea cooperării cibernetice cu ONU, SUA, Rusia și UE (activități comune, întâlniri la nivel de experți și dezvoltarea de proiecte de cooperare prin inițiative ale economiei digitale);
- formularea regulilor comerciale în spațiul cibernetic și coordonarea politicilor: China și-a exprimat sprijinul pentru formularea de reguli comerciale în spațiul cibernetic și coordonarea eficientă a politicilor dintre state;
- aplicarea dreptului internațional în spațiul cibernetic: China își propune să aplice dreptul internațional în spațiul cibernetic pentru a-și consolida poziția în ordinea digitală globală;
- China va continua să organizeze Summitul anual de la Wuzhen (Conferința Mondială a Internetului) și alte conferințe și forumuri internaționale: the Conference on Interaction and Confidence Building Measures in Asia (CICA), Forum on China-Africa Cooperation (FOCAC), China-Arab States Cooperation Forum, Forum of China and the Community of Latin American and Caribbean States și Asian-African Legal Consultative Organization;
- va continua discuțiile și consultările în format China-Japonia-Korea, ASEAN Regional Forum și Boao Forum în ceea ce privește politicile cibernetice;
- China promovează cooperarea în domeniul securității cibernetice în cadrul Shanghai Cooperation Organization (SCO) și BRICS.

De asemenea, în ceea ce privește tehnologiile avansate, China își propune să devină lider mondial în domeniu. Acest obiectiv are un impact semnificativ asupra spațiului cibernetic global. Se vor puncta în continuare obiectivele strategice ale Chinei în dezvoltarea de procesoare și de alte tehnologii înalte, precum și efectele acestora asupra spațiului cibernetic global. Reducerea dependenței de produsele tehnologice de origine străină, în special de cele care provin din Statele Unite și din alte țări occidentale, este obiectivul principal al Chinei. Acest lucru se referă la crearea de software și de procesoare autohtone pentru a înlocui produsele importate. Așadar, un pas important în acest demers a fost interzicerea utilizării procesoarelor Intel și AMD pe computerele și serverele guvernamentale (Zulhusni, fără an).

Guvernul chinez investește substanțial în tehnologii emergente, precum inteligența artificială (AI), *quantum computing* și altele. De exemplu, China a construit procesoare de tip open-source RISC-V și a lansat sateliți de comunicații cuantice. Aceste procesoare sunt utilizate în diferite industrii, cum ar fi vehiculele autonome și inteligența artificială (Goswami 2023; Cheung 2023).
Prin exportul de tehnologie, prin standarde proprii și prin promovarea suveranității cibernetice, China încearcă să-și sporească influența globală. Acest lucru include și promovarea standardelor care susțin modelul de guvernare a internetului din China și implicarea activă în organizații internaționale de standardizare (Cary 2023). Astfel integrarea tehnologiei chineze în infrastructurile vitale ale altor state poate genera vulnerabilități, care pot determina ulterior activitățile de spionaj cibernetic (Pleil 2023).

Strategia de cooperare internațională a Chinei în materie de securitate cibernetică promovează instituirea unei ordini mondiale în spațiul cibernetic, bazată pe reguli, stabilite de comun acord la nivelul comunității internaționale, prevede extinderea continuă a parteneriatelor în spațiul cibernetic, are în vedere aprofundarea cooperării internaționale în combaterea terorismului cibernetic și a criminalității cibernetice și promovează reforma sistemului global de guvernanță a internetului (Xinhua News Agency 2017).

Este atribuită o atenție importată în strategie opiniei publice și prezenței acesteia în spațiul online. Se are în vedere că prezența online a opiniei publice a devenit cea mai importantă sarcină a propagandei chineze și, ca atare, se subliniază necesitatea menținerii unei "energii pozitive" online și offline pentru a "ține lucrurile sub control" după cum este menționat în textul strategiei (Xinhua News Agency 2017). Publicitatea pozitivă în mediul online trebuie să devină din ce în ce mai puternică, astfel încât ideile partidului să devină întotdeauna cea mai puternică voce în spațiul cibernetic. O caracteristică importantă a securității cibernetice a Chinei este controlul și supravegherea stricte ale guvernului chinez asupra internetului, așa după cum reiese și din Art.12, Cap.1 al Legii Securității Cibernetice a RPC:

„Orice persoană și organizație care utilizează internetul trebuie să respecte Constituția și legile țării, să respecte ordinea publică și să respecte moralitatea socială; nu trebuie să pună în pericol securitatea cibernetică și nu poate folosi internetul

pentru a se angaja în activități care pun în pericol securitatea națională, onoarea națională și interesele naționale; nu trebuie să submineze suveranitatea națională, să răstoarne sistemul socialist, să incite separatismul, să rupă unitatea națională, să susțină terorismul sau extremismul, să susțină ura etnică și discriminarea etnică, să disemineze informații violente, obscene sau sexuale, să creeze sau să difuzeze informații false pentru a perturba ordine economică sau socială ori informații care încalcă reputația, confidențialitatea, proprietatea intelectuală sau alte drepturi și interese legale ale altora și alte asemenea acte."

Pentru a se asigura de implentarea cu succes a Art.12, Cap.1, citat anterior, China a dezvoltat sistemul de control și monitorizare, cunoscut sub numele de „Marele Firewall". Acesta presupune monitorizarea activității online a utilizatorilor și blochează accesul la numeroase site-uri internaționale. Prin prevenirea răspândirii informațiilor considerate subversive sau dăunătoare, această metodă centralizată și cuprinzătoare urmărește să mențină stabilitatea politică și socială. China supraveghează și cenzurează conținutul care apare: blochează sau cenzurează informații sensibile despre guvern sau despre drepturile omului, utilizatorii sunt monitorizați în detaliu pentru toate activitățile lor online, inclusiv istoricul de navigare, mesajele și postările pe rețelele sociale; informațiile personale, cum ar fi numerele de telefon sau cărțile de identitate sunt colectate de furnizorii de servicii internet; site-urile chineze au obligația de a cenzura conținutul considerat inadecvat, precum și de a colabora cu autoritățile pentru a urmări și a raporta activitățile suspecte (Stanford, fără an).

În ceea ce privește cooperarea internațională cu alte regiuni, China folosește platforma BRICS (Brazilia, Rusia, India, China și Africa de Sud, Iran, Egipt, Etiopia și Emiratele Arabe Unite), pentru a promova cooperarea în domeniul securității cibernetice. China a încercat în cadrul acestui grup să colaboreze în proiecte comune pentru a combate criminalitatea cibernetică și pentru a îmbunătăți securitatea informațională. Într-o abordare mai largă, aceste eforturi fac parte dintr-un obiectiv legat de construirea unei rețele de alianțe cu țările în curs de dezvoltare și de contracarare a influenței occidentale asupra guvernanței globale a internetului (Li 2018).
China a făcut pași importanți, de asemenea, în cooperarea în domeniul securității cibernetice cu Thailanda, pentru a crea un spațiu cibernetic mai sigur și pentru a proteja cetățenii de activitățile malițioase. Această colaborare include schimbul de informații, bune practici și inovații tehnologice pentru a combate amenințările cibernetice (Saffa 2024).

În Asia de Est însă, țări, precum India, Vietnam, Japonia și Coreea de Sud, consideră China o putere cibernetică agresivă, în ciuda eforturilor Chinei de a se poziționa ca lider în cooperarea cibernetică prin BRICS. Aceste națiuni sunt preocupate de abilitatea Chinei de a exploata puterea cibernetică în scopuri de supraveghere și spionaj, situație care a generat tensiuni regionale și a stimulat inițiative de întărire a securității cibernetice (Wagner 2019).

În acest context, Vietnamul și Japonia au semnat un acord de securitate cibernetică pentru a combate atacurile cibernetice agresive ale Chinei. Acest acord este o consecință a preocupărilor ambelor țări în domeniul activităților cibernetice ale Chinei în zona indo-pacifică (Yamaguchi 2021). De asemenea, în ianuarie 2024, Vietnam a descoperit că grupurile de amenințări persistente avansate (APT), susținute de China, precum APT31, APT41, Grayling, Mustang Panda și SharpPanda, au fost implicate în acțiuni de spionaj cibernetic asupra agențiilor guvernamentale vietnameze. De asemenea, Japonia a intensificat cooperarea în domeniul apărării cibernetice cu Statele Unite, Australia și cu alte state, participând la exerciții cibernetice ale NATO și semnând acorduri de securitate cibernetică, pe lângă cel cu Vietnam și cu Singapore și Indonezia. Japonia a protestat în mod regulat împotriva prezenței gărzii de coastă chineze în apropierea insulelor Senkaku, controlate de Japonia, dar revendicate de China, indicând o preocupare constantă față de activitățile cibernetice și militare ale Chinei în regiune (Truong 2024).
Contrar statelor din Asia de Est, care sunt reticente față de cooperarea în materie de securitate cibernetică cu RPC, Federația Rusă și Insulele Solomon, ca și Thailanda sunt deschise cooperării cu China și au demarat deja acțiuni în acest sens.

În ceea ce privește relația cu Federația Rusă, începând cu 2017, Administrația Spațiului Cibernetic al Chinei (CAC) lucrează cu Roskomnadzor, autoritatea de reglementare și cenzură a internetului din Rusia. Această cooperare demonstrează că cele două state împărtășesc puncte de vedere similare cu privire la controlul și supravegherea internetului. Este, de asemenea, parte a unui efort mai larg de a promova suveranitatea cibernetică și de a contracara influența occidentală în ceea ce privește guvernanța spațiului cibernetic internațional (Kremlin 2017).
În 2023, China și Insulele Solomon au semnat un acord de cooperare în domeniul securității cibernetice și al poliției. Această înțelegere este o parte a eforturilor Chinei de a-și extinde influența în Pacificul de Sud, oferind asistență tehnică și formare în domeniul securității cibernetice (Smith 2023).

În ceea ce privește cooperarea în domeniul securității cibernetice dintre China și UE, deși a existat o serie discuții cu privire la cooperarea în spațiul cibernetic dintre cele două, până în prezent, nu există, încă, o cooperare reală între China și UE. În cadrul procesului de negociere a cooperării, s-au depus eforturi pentru a găsi un teren comun de cooperare în sfera digitală, inclusiv pentru dezvoltarea unui cadru comun de guvernanță a datelor electronice (EIAS 2023). Aceste eforturi sunt rezultatul recunoașterii reciproce a beneficiilor potențiale ale colaborării în combaterea criminalității cibernetice, în promovarea comerțului digital și protejarea infrastructurilor critice (Comisia Europeană 2019).

Dificultatea cooperării China – UE este cauzată inclusiv de activitățile cibernetice rău intenționate ale Chinei, desfășurate ca actor statal împotriva UE, care se vor detalia în continuare în această secțiune. Ca urmare a acestor incidente, UE a solicitat Chinei în 2021 să ia măsuri pentru încetarea acestor activități (Consiliul European 2021).

Deși în 2015, în timpul administrației Obama, SUA și China au ajuns la un acord important, prin care s-au angajat să se abțină de la cyberspionajul economic întreprinderilor din ambele state (The White House 2015), China este încă implicată în numeroase cazuri de spionaj cibernetic, vizând agenții guvernamentale și companii private. Grupurile APT10, APT31 și APT41 sunt recunoscute pentru atacurile lor complexe asupra infrastructurilor critice și furtul de proprietate intelectuală în SUA și Europa. În continuare, se vor analiza câteva cazuri de spionaj cibernetic chinez cu impact major asupra cooperării internaționale a Chinei în domeniul securității cibernetice care reprezintă o altă fațetă a provocărilor Chinei în cooperarea internațională în domeniul securității cibernetice .

Grupul de spionaj cibernetic sponsorizat de statul chinez APT10, cunoscut și sub numele de Cicada sau Stone Panda, activează de peste zece ani, cu obiectivul principal de a spiona companii din industria tehnologică și de apărare din SUA și Europa. Campania "Operation Cloud Hopper" (2014-2018) este un exemplu în acest sens, care a vizat furnizorii de servicii gestionate (MSP – Managed Service Provider) din mai multe țări, cum ar fi Statele Unite, Japonia, Canada și Australia. APT10 a pătruns în rețelele clienților MSP și a furat tehnologii și secrete comerciale (CYWARE 2022; Vijayan 2017).

Mai multe rapoarte de securitate cibernetică și surse oficiale au confirmat legătura dintre Ministerul de Stat al Securității din China și grupul de atacatori cibernetici APT10. Primul raport a fost realizat, în 2018, de un grup anonim de cercetători, numit Intrusion Truth, care a publicat un raport cu privire la Zhu Hua și Zhang Shilong, ca fiind membri ai grupului APT10 și având legături cu Ministerul de Stat al Securității din China. Și compania de securitate cibernetică CrowdStrike a confirmat acest fapt. (O'Donnell 2018). Guvernul SUA i-a acuzat, ulterior, de infiltrare în rețelele a peste 45 de companii tehnologice și agenții guvernamentale din Statele Unite și de furt de date private, inclusiv al unor informații despre personalul Marinei Statelor Unite (Office of Public Affairs 2018). În decembrie 2018, Regatul Unit al Marii Britanii și aliații săi au dezvăluit public că grupul APT10 a acționat în numele Ministerului de Stat al Securității (MSS) din China, pentru a lansa campanii cibernetice la scară largă, care vizau proprietatea intelectuală și date comerciale sensibile în Europa, Asia și Statele Unite (National Cyber Security Centre 2018).
Pe lângă APT10, mai sunt și alte grupuri de hacking care sunt considerate a avea legături cu Ministerul de Stat al Securității din China, cum ar fi APT31 și APT41.
APT31 (Zirconium, Judgment Panda, Bronze Vinewood, Red Keres) este un grup de hacking renumit pentru furtul de date sensibile și proprietate intelectuală. Acest grup a fost implicat în atacuri cibernetice care au vizat jurnaliști, politicieni, academicieni și instituții guvernamentale, precum și companii de securitate și instituții publice. SUA și Marea Britanie au susținut că APT31 este o armă a Ministerului Securității de Stat al Chinei – folosit de Departamentul de Securitate din Provincia Hubei, localitatea Wuhan – și a fost dezvoltat pentru a opri criticii regimului chinez și a compromite instituțiile guvernamentale (gov.uk 2024; US Department of the Treasury 2024).

În 2021, APT31 a atacat sistemele Comisiei Electorale din Regatul Unit, obținând datele personale a aproximativ 40 de milioane de alegători (Yerushalmy 2024) și a fost implicat în atacuri asupra unor infrastructuri critice ale Statelor Unite (apărare și energie). APT31 a fost acuzat, de asemenea, de piratarea software-ului serverului de e-mail Microsoft Exchange în 2021 și a e-mailurilor personale ale personalului de campanie care a lucrat pentru Joe Biden în 2020 (Office of Public Affairs 2024).
Ca urmare a acestor atacuri, guvernele american și britanic au sancționat persoane și organizații relaționate grupului APT31, inclusiv compania Wuhan Xiaoruizhi Science and Technology Company Limited, care a facilitat operațiunile cibernetice ale MSS (UK GOV 2024; US Department of the Treasury 2024).
Un alt grup de spionaj cibernetic chinez APT41, cunoscut și sub numele de Double Dragon, combină spionajul sponsorizat de stat cu infracțiuni cibernetice pentru a câștiga bani. Acest grup a lucrat în multe industrii, cum ar fi telecomunicații, tehnologie înaltă și sănătate (Fraser și alții 2019).
Un caz mediatizat al acțiunilor APT41 este atacul care a vizat compania de software NetSarang în 2017. Atunci, grupul a injectat un cod malițios într-un pachet de actualizare software care a fost semnat cu un certificat legitim al NetSarang. Sute de întreprinderi din întreaga lume au fost afectate de acest atac (Mandiant 2022).

Departamentul de Justiție al Statelor Unite a depus acuzații împotriva a șapte membri ai APT41 în 2020 pentru atacuri cibernetice care au vizat companii din tehnologie, telecomunicații și domeniul sănătății, precum și pentru furtul de proprietate intelectuală și date sensibile (Office of Public Affairs 2020). De asemenea, în martie 2021, în cazul atacului cibernetic care a vizat software-ul de e-mail al Microsoft, atacatorii au folosit o vulnerabilitate nedetectată anterior pentru a obține acces de la distanță la căsuțele de e-mail. NATO, Uniunea Europeană, Australia, Noua Zeelandă și Japonia au atribuit oficial acest atac actorilor chinezi sponsorizați de stat, în special grupului cunoscut sub numele de Hafnium (GMF 2021).

Având în vedere cele menționate anterior, se poate observa complexitatea asumării îndeplinirii tuturor obiectivelor stipulate în strategia de cooperare internațională a Chinei în domeniul securității cibernetice. China susține că fiecare națiune are dreptul de a avea control și ordine asupra spațiului cibernetic național și folosește acest discurs la nivel internațional, cu intenția de a proteja interesele naționale și statul împotriva influenței externe, în special din cauza conflictelor geopolitice cu Statele Unite și cu alte țări occidentale (Shen 2016). La polul opus, pentru a asigura un spațiu cibernetic deschis și liber, Uniunea Europeană susține un model de guvernanță cibernetică ce implică mai multe părți interesate, cum ar fi cooperările de tip public-privat, cu organizațiile neguvernamentale și instituțiile academice internaționale.

Concluzii

Studiul a răspuns întrebării de cercetare lansate în urma ipotezei și arată că dorința Chinei de a-și proteja suveranitatea cibernetică și de a-și consolida poziția de

superputere cibernetică, precum și legislația internă, bazată pe o monitorizare atât internă, cât și externă a bazelor de date care aparțin cetățenilor chinezi, are un impact major asupra strategiei de cooperare internațională în domeniul securității cibernetice. Astfel, apar provocări în îndeplinirea obiectivelor propuse în strategia de cooperare internațională în domeniul securității cibernetice, precum spionajul cibernetic, realizat de actori ai statului chinez.

Obiectivul Chinei de a proteja infrastructurile critice și datele personale ale cetățenilor chinezi este evidențiat de Legea Securității Cibernetice a Chinei, de Legea Protecției Datelor Personale și de amendamentele recente ale celor două legi. Deși aceste acte legislative au fost esențiale pentru crearea unei atmosfere de colaborare internațională, alături de Strategia de Cooperare Internațională în materie de Securitate Cibernetică, unele state din Asia de Est, SUA și Europa și-au exprimat îngrijorarea cu privire la obiectivele Chinei, acuzând China de spionaj cibernetic și de supraveghere excesivă.

Dorința Chinei de a-și proteja suveranitatea cibernetică este o componentă esențială a strategiei sale de cooperare internațională în domeniul securității cibernetice. China încearcă să-și consolideze poziția de superputere cibernetică și să își protejeze interesele prin implementarea unui sistem de guvernanță a internetului transparent și multilateral. Contrar dorinței Chinei, multe state și organizații internaționale nu sunt de acord cu eforturile Chinei de a construi un sistem global de guvernanță a internetului. Acuzațiile privind utilizarea tehnologiei pentru supravegherea internă, efectuarea în mod regulat a unor atacuri cibernetice, în calitate de actor statal, ori preocupările legate de practicile interne de supraveghere și control al informațiilor au afectat obiectivele Chinei în cooperarea internațională în domeniul securității cibernetice, potențialii parteneri fiind reticenți la adresa intenției guvernului chinez cu privire la o colaborare deschisă și sinceră.

În cadrul acestui scurt studiu introductiv, pe lângă referințele cu privire la cadrul legislativ în materie de securitate cibernetică în China, s-a făcut referire și la structurile care se ocupă de siguranța spațiului cibernetic în China și la faptul că toate sunt interdependente, coordonate ierarhic de Comisia Centrală pentru Afaceri în Domeniul Spațiului Cibernetic (CCAC) a Partidului Comunist Chinez. Având în vedere acest lucru, se poate concluziona că această comisie a PCC guvernează activitățile agențiilor și entităților din domeniul cibernetic (CAC, CNNIC, CNCERT, TC260 și CSAC) și trasează liniile prioritare de implementare a strategiilor în domeniu.

Această structură ierarhică, influențată de PCC, a determinat și reticența țărilor din afară care au identificat amenințări din ce în ce mai intensificate ale grupărilor controlate de statul chinez, precum APT10, APT31 sau APT41, care au ca scop principal spionajul cibernetic al infrastructurilor critice și de interes național din domeniul militar, telecomunicații, sănătate sau energie, conform rapoartelor de securitate cibernetică, menționate pe parcursul articolului.

În concluzie, China se află într-un amplu proces de a-și demonstra capacitatea de superputere cibernetică, pentru a contribui la crearea unui spațiu cibernetic mai sigur, dar cu obiectivul clar trasat de a menține în același timp și un spațiu cibernetic sigur la nivel național, care să reflecte pozitiv toate acțiunile PCC.

Referințe

ABC News. 2015. "US and China Reach Agreement to Stop Commercial Cyber Espionage." https://abcnews.go.com/US/us-china-reach-agreement-stop-commercial-cyberespionage/story?id=34041002.

Atlantic Council. 2023. *The 5×5—China's cyber operations*. https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

Carolan, Ciara. 2024. "Europe and Belgium are 'unresponsive' in the face of Chinese cyber-attacks, says hacked MP". https://www.brusselstimes.com/983253/europe-and-belgium-are-passive-in-the-face-of-chinese-cyber-attacks-says-hacked-mp.

Cary, Dakota. 2021. "China's National Cybersecurity Center. A Base for Military-Civil Fusion in the Cyber Domain". https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

—. 2023. "Community watch: China's vision for the future of the internet." https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/.

CCTV News. 2023. "Strategy for International Cooperation in Cyberspace." https://news.cctv.com/2023/11/07/ARTILliq1FlQi0B7msdoKsBn231107.shtml.

Cheung, Sunny. 2023. "Examining China's Grand Strategy For RISC-V". https://jamestown.org/program/examining-chinas-grand-strategy-for-risc-v/.

Chinese Embassy in UK. 2011. "China's Perspective on Cybersecurity". http://gb.china-embassy.gov.cn/eng/ambassador/dsjhjcf/2011lr/201106/t20110602_3386103.htm.

Chinese Ministry of Education. 2017. "Management Measures for the Demonstration Project of Building a First-Class Cibersecurity College." http://www.moe.edu.cn/srcsite/A16/s3342/201708/t20170815_311176.html.

China Internet Network Information Center, (CNNIC). fără an. "中国互联网络信息中心." https://www.cnnic.com.cn/.

Comisia Europeană. 2019. "EU-CHINA – A Strategic Outlook." https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf.

Consiliul European 2021. "China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory." https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/#:~:text=We%20continue%20to%20urge%2.

Consiliul de Stat al Chinei. 1994. "Regulations of the People's Republic of China on Computer Information System Security Protection." https://www.gov.cn/gongbao/content/2011/content_1860849.htm.

Creemers, Rogier. 2023. "Cybersecurity Law and Regulation in China: Securing the Smart State." https://brill.com/view/journals/clsr/6/2/article-p111_001.xml.

Cyberspace Administration of China, (CAC). fără an. "中央网络安全和信息化委员会办室." https://wap.cac.gov.cn/.

Cyber Security Association of China (CSAC). fără an. "中国网络空间安全协会." https://www.cybersac.cn/.

Cyberspace Administration of China. 2017. "关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告 [Announcement on the release of the «Catalogue of Critical Network Equipment and Network Security Special Products (First Batch)»]. " https://www.cac.gov.cn/2017-06/09/c_1121113591.htm.

CYWARE. 2022. "APT10: A Chinese Threat on a Global Espionage Mission". https://cyware.com/resources/research-and-analysis/apt10-a-chinese-threat-on-a-global-espionage-mission-56fe.

Dandong, Han. 2019. *Legal Daily.* http://epaper.legaldaily.com.cn/fzrb/content/20190729/Articel04004GN.htm.

EIAS. 2023. "EU Digital Dialogue and Cooperation with China: The Way Forward?" https://eias.org/publications/op-ed/eu-digital-cooperation-with-china-the-way-forward/.

Fraser, Nalani, Fred Plan, Jacqueline O'Leary, Raymond Leong Vincent Cannon, Dan Perez, și Chi-en Shen. 2019. "APT41: A Dual Espionage and Cyber Crime Operation." https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation.

Fulton Library. fără an. "Quantitative Research Methodologies." https://uvu.libguides.com/methods/quantitative.

GMF. 2021. "NATO, EU, and allies attribute email intrusion to Chinese state-backed hackers." https://securingdemocracy.gmfus.org/incident/allies-attribute-email-hack-to-china-backed-hackers/.

Goswami, Namrata. 2023. "China Prioritizes 3 Strategic Technologies in Its Great Power Competition". https://thediplomat.com/2023/04/china-prioritizes-3-strategic-technologies-in-its-great-power-competition/.

gov.cn. 2016. "中华人民共和国网络安全法_滚动新闻_中国网 [Cybersecurity Law of the People's Republic of China]". https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

gov.uk. 2024. "UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity". https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

Guo, Meirong. 2018. "China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces." *International Journal of Critical Infrastructure Protection* vol. 22: 139-149. doi:10.1016/j.ijcip.2018.06.006.

Handler, Simon. 2023. *Atlantic Council* . 01 30. https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

Hmaidi, Antoni. 2023. *"Here to stay" – Chinese state-affiliated hacking for strategic goals.* https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals.

Julian, Nicholas. 2021. "United States' and China's Cybersecurity Policies: Collaboration or Confrontation?" https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation.

Kremlin. 2017. "Russia and China Enhance Cybersecurity Cooperation." https://www.kremlin.ru/events/president/news/55842.

Li, H. 2018. "BRICS and the Internet: Building a New Global Consensus." *International Affairs* 94 (5): 1125-1145.

Mandiant. 2022. "APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation." https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation.

Ministry of Foreign Affairs of the People's Republic of China. MFA CN. 2017. "Ministry of Foreign Affairs Holds Briefing for Chinese and Foreign Media on President Xi Jinping's State Visits to Russia and Germany and Attendance at 12th G20 Summit." https://www.fmprc.gov.cn/mfa_eng/topics_665678/2017zt/XJPDEDFWBCXGEODSECFH/201707/t20170704_703649.html.

—. 2023. "Proposal of the People's Republic of China on the Reform and Development of Global Governance". https://www.fmprc.gov.cn/eng/wjbxw/202309/t20230913_11142010.html.

National Computer Network Emergency Response technical Team/Coordination Center of China, CNCERT/CC. fără an. "国家互联网应急中心. " https://www.cert.org.cn/publish/main/34/index.html.

National Cyber Security Centre. 2018. "APT10 continuing to target UK organisations". https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations.

National Cybersecurity Standardization Technical Committee, (TC260). fără an. "全国网络安全标准化技术委员会." https://www.tc260.org.cn/.

NPC.GOV.CN. 2021. "Data Security Law of the People's Republic of China." http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

O'Donnell, Lindsay. 2018. "APT10 Under Close Scrutiny as Potentially Linked to Chinese Ministry of State Security". https://threatpost.com/apt10-under-close-scrutiny-as-potential-chinese-ministry-of-state-security-contractor/137139/.

Office of Public Affairs. 2024. "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians." https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.

—. 2020. "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally". https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

—. 2018. "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information". https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Pleil, Helen. 2023. "Being a Cyberpower – China's Ambitions in Cyberspace". https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/.

PwC Indonesia. 2023. "A comparison of cybersecurity regulations: China". https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html.

Saffa, Azizah. 2024. "Thailand and China Strengthen Cybersecurity Cooperation". https://opengovasia.com/2024/05/29/thailand-and-china-unite-for-cyber-resilience/.

Shen, Yi. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* vol. 1: 81-93. https://doi.org/10.1007/s41111-016-0002-6.

Smith, J. 2023. "China and Solomon Islands Sign Security Pact." https://www.theguardian.com/world/2023/apr/12/china-and-solomon-islands-sign-security-pact.

Stanford. fără an. "Free speech vs Maintaining Social Cohesion". https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

Sustainable Development. 2016. "World Summit on the Information Society (WSIS)." https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170.

The White House. 2015. "U.S.-China Cyber Agreement". https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/us-china-cyber-agreement.

Thomas, Nicholas. 2009. "Cyber Security in East Asia: Governing Anarchy." *Asian Security* 5 (1): 3-23.

Truong, Sylvie. 2024. "Chinese espionage campaigns and cyberattacks on critical infrastructure in Southeast Asia". https://thereadable.co/chinese-espionage-campaigns-and-cyberattacks-on-critical-infrastructure-in-southeast-asia/.

UK GOV. 2024. "UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity". https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

US Department of the Treasury. 2024. "Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure". https://home.treasury.gov/news/press-releases/jy2205.

Vijayan, Jay. 2017. "China-Based Threat Actor APT10 Ramps Up Cyber Espionage Activity". https://www.darkreading.com/cyberattacks-data-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity.

Wagner, B. 2019. "Cybersecurity in East Asia: Government Policies and Sectoiral Responses." *Journal of Cyber Policy* 4 (1): 55-72.

Xinhua. 2019. http://www.xinhuanet.com/yuqing/2019-01/04/c_1210030391.htm.

Xinhua News Agency. 2017. ”网络空间国际合作战略 [Cyberspace International Cooperation Strategy].” http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm.

Yamaguchi, Mari. 2021. ”Japan, Vietnam Look to Cyber Defense Against China.” https://thediplomat.com/2021/11/japan-vietnam-look-to-cyber-defense-against-china/.

Yerushalmy, Jonathan. 2024. ”China cyber-attacks explained: who is behind the hacking operation against the US and UK?” https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31.

Zhang, Duanhong, Wenjia Ding, Yang Wang, and Siwen Liu. 2022. ”Exploring the Role of International Research Collaboration in Building China’s World-Class Universities”. https://doi.org/10.3390/su14063487.

Zulhusni, Muhammad. fără an. ”China’s new tech policies challenge Intel and AMD in a shifting landscape”. https://techwireasia.com/03/2024/chinas-tech-shift-what-it-means-for-the-future-of-intel-and-amd/.