INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA STIINȚIFICĂ STUDENȚEASCĂ
CONFERENCE PROCEEDINGS

VOLUMUL 4
2025

Editura Academiei Naționale de Informații
„Mihai Viteazul”

INTELLIGENCE
ȘI CULTURA DE SECURITATE

nr. 4 – 2025

– Conferința Științifică Studențească –

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

Bucureşti, 2025

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”
© ANIMV
Bucureşti, 2025
Telefon: 0377720.000/1216
Fax: 0377721.134; 0377721.125
ISSN 2972 – 1350 ISSN-L 2971 – 8139

CUPRINS

CRIMINALITATEA DE MEDIU
ŞI SECURITATEA GLOBALĂ 5
Livia MANDU, Cornel RACOVEANU

CÂND ATACATORII DEVIN VICTIME:
VULNERABILITĂŢILE GRUPĂRILOR DE CRIMINALITATE
CIBERNETICĂ 25
Claudia – Alecsandra GABRIAN

NOUA ORDINE MONDIALĂ ÎN CONTEXTUL DIFUZIEI PUTERII –
ÎNTRE IERARHIE ŞI DEZORDINE 41
Octavian-Alexandru-Ştefan BROŞTEANU

ASTROTURFING ŞI RĂZBOIUL PSIHOLOGIC PE FACEBOOK:
GRILE DE VERIFICARE A CONTURILOR FALSE 59
Cristian HAIDĂU

FRANCE AND EUROPEAN STRATEGIC AUTONOMY:
BETWEEN REGIONAL LEADERSHIP AND NATO COMMITMENTS 91
Daniel-Aurel BUCUR

MUTAREA CENTRULUI DE GREUTATE AMERICAN ÎN ASIA-PACIFIC:
COMPETIŢIA SINO-AMERICANĂ ÎNTRE REALISM
ŞI BLUF STRATEGIC 119
Paul-Alexandru SITEA

AUTONOMIA STRATEGICĂ – ELEMENT DISCURSIV
ŞI REALITATE EUROPEANĂ 135
Mălina-Maria RÎNDAŞU

THE GRAY ZONE PROBLEM, SECURITY ISSUES ARISING FROM THE
INTERSECTION OF MILITARY AND CIVILIAN AFFAIRS 159
George-Mihai NICULA

TRACE: A STRUCTURED AI-SUPPORTED MODEL FOR CULTIC RISK
AND NATIONAL SECURITY THREAT ASSESSMENT 177
Iancu-Marius BUFNEA

DRAGNETING THE DRAGON: THE PEOPLE'S REPUBLIC OF CHINA, EUROPEAN UNION AND FIVE EYES, CAUGHT IN THE WEB OF MUTUAL ESPIONAGE 211
Alida Monica Doriana BARBU

ADVANCING A C2I FRAMEWORK FOR ENHANCED INTELLIGENCE SECURITY IN THE SHIPPING INDUSTRY 227
Anastasios-Nikolaos KANELLOPOULOS

BUNE PRACTICI ÎN PREVENIREA RADICALIZĂRII ȘI A EXTREMISMULUI VIOLENT LA NIVEL EUROPEAN: REVIZUIREA SISTEMATICĂ A LITERATURII DE SPECIALITATE 245
Ioana CHIȚĂ

DRAGNETING THE DRAGON: THE PEOPLE'S REPUBLIC OF CHINA, EUROPEAN UNION AND FIVE EYES, CAUGHT IN THE WEB OF MUTUAL ESPIONAGE

Alida Monica Doriana BARBU[*]

Abstract:

The Intelligence world can be depicted as a global Panoptikon, with multiple layers of surveilling eyes, except that the distinction between guards and prisoners is erased. The transfer from one side to the other is more than likely to occur due to the unclear sepia colours of the espionage environment and deep tides that drag people from one "shore" to the other.

The EU's nuanced strategy towards China since 2019 Strategic Outlook Joint Communication is continued today by the De-risking or De-coupling Strategy. The People's Republic of China is considered a partner for negotiation and cooperation, an economic competitor and a systemic rival, whereas the US National Defense Strategy treats China as an enemy of the United States. These strategies are translated in the approach of Intelligence agencies. Even if espionage incidents and cyber attacks occur on a daily basis, the war between USA and China is openly declared, whereas EU has a more moderate public approach.

Keywords: *European Union Intelligence Agency, People's Republic of China, Russian Federation, Five Eyes, Club of Berne, CGT, Hafnium, Equifax, Echelon-Prism-XKeyscore Triad, VPNs.*

Introducere

Five Eyes reprezintă o organizaţie strategică în timpul Noului Război Rece (Abrams 2022). Regatul Unit, membru al *Five Eyes*, face parte și din *Clubul de la Berna*, al cărui partener nelipsit este SUA. Colaborarea între SUA şi Uniunea Europeană este strânsă din punct de vedere al comunicării informaţiilor de Intelligence, având în vedere Strategia de Securitate Naţională (NSS) a SUA din 2022 care a identificat Federaţia Rusă şi Republica Populară Chineză drept ameninţări la adresa

[*] Alida Monica Doriana Barbu, PhD and PhD candidate, Babes Bolyai University, History and Philosophy Faculty, Doctoral School of International Relations and Security Studies, Cluj-Napoca, email: alida.barbu7@gmail.com. alida.barbu@ubbcluj.ro.

intereselor SUA, în timp ce Uniunea Europeană recunoaşte China drept un rival sistemic. Scopul articolului este de a reliefa lupta Est-Vest care se poartă atât la nivel ideologic, cât şi în domeniul şi prin instrumentarul acţiunilor de Intelligence între aliatele *Five Eyes*+Uniunea Europeană şi rivala China, evidenţiind elementele de noutate din peisajul geopolitic. Obiectivele urmărite sunt familiarizarea publicului cu mijloacele folosite de Republica Populară Chineză în vederea obţinerii supremaţiei mondiale. Prezenta cercetare utilizează metoda calitativă a analizei de discurs. Rezultatele obţinute constau în găsirea punctelor slabe atât ale agenţiilor de Intelligence europene, cât şi ale alianţei *Five Eyes*, în timp ce contribuţia personală vine sub forma unor soluţii menite a creşte reziliența societăţii civile la ingerinţele autocraţiilor şi a unor recomandări de corijare a vulnerabilităţilor serviciilor de informaţii.

Five Eyes

Alianţa *Five Eyes* (FVEY) este alcătuită din SUA, Regatul Unit al Marii Britanii, Canada, Australia şi Noua Zeelandă, cele cinci părţi semnatare ale Acordului UKUSA. Iniţial, preexistent a fost Acordul BRUSA care a fost semnat la data de 17 mai 1943 de către Departamentul de Război al SUA şi GC&CS (United Kingdon), urmărindu-se schimbul de informaţii între cele două ţări în vederea sprijinirii forţelor americane din Europa în timpul celui de-al Doilea Război Mondial. BRUSA a stat la baza Acordului UKUSA, semnat la 5 martie 1946 de către colonelul Patrick Marr-Johnson în numele Consiliului de Informaţii al Semnalelor din Londra şi de către locotenent-generalul Hoyt Vandenberg, preşedinte al Consiliului de Informaţii pentru Comunicaţii dintre Statul, Armata şi Marina SUA (STANCIB). În 1949 s-a alăturat UKUSA şi Canada, iar din 1956, împreună cu Australia şi Noua Zeelandă, formează Alianţa FVEY în componenţa sa actuală. Acordul nu a fost recunoscut oficial până în 2010, deşi se cunoştea existenţa sa încă din anii 1980 la nivelul marelui public. Ca parte a tendinţelor de transparentizare din lumea Intelligence-ului, cea de-a 75-a aniversare a parteneriatului formal dintre GCHQ (General Communication Head Quarters) din Marea Britanie şi Agenţia Naţională de Securitate a SUA (NSA) a fost celebrată la 5 martie 2021 (GCHQ 2021).

Scopul acordului menţionat este partajarea între semnatarii săi a informaţiilor bazate pe *Signal Intelligence* (SIGINT) – interceptarea semnalelor electromagnetice de transmisie. SIGINT se împarte în trei ramuri : *Communication Intelligence* (COMINT) – interceptarea apelurilor telefonice ale persoanelor şi a comunicaţiilor prin text, precum e-mailurile şi mesajele text ; *Electronic Intelligence* (ELINT) – utilizarea senzorilor

electronici pentru interceptarea semnalelor de la sisteme de rachete sol-aer sau radare ; *Foreign Instrumentation Signature Intelligence* (FISINT) – interceptarea şi analizarea semnalelor utilizate pentru operarea aeronavelor sau sateliţilor. Agenţiile de informaţii ale ţărilor din cadrul *Five Eyes* : NSA (Agenţia Naţională de Securitate din SUA), GCHQ (Sediul Central al Comunicaţiilor Guvernamentale din Marea Britanie), Institutul de Securitate a Comunicaţiilor din Canada (CSE), Direcţia Australiană de Semnale (ASD) şi Biroul de Securitate a Comunicaţiilor al Guvernului din Noua Zeelandă (GCSB) împărtăşesc informaţii între ele în special despre inamicii geopolitici. Acordul UKUSA, născut în urma Cartei Atlanticului din 1941, avea scopul originar de a monitoriza Uniunea Sovietică şi aliaţii acesteia, însă obiectivele alianţei au cunoscut extinderi şi în sfera colectării comunicaţiilor private din timpul Războiului contra Terorismului de după 11 Septembrie 2001 (Karbauskas 2025).

Fiecare membru este responsabil pentru culegerea şi interpretarea datelor din zona de pe glob atribuită lui. Statele membre colaborează prin intermediul sistemelor de informaţii integrate, care, alături de accesul la baze de date, presupun şi sisteme de procesare şi decodarea în domeniile cibernetic şi maritim. SIGINT a jucat un rol decisiv între 1939 şi1945 şi ulterior în limitarea comunismului. Recent, SUA şi Marea Britanie au oferit publicului informaţii declasificate în ianuarie 2022, înainte de începerea conflictului Rusia-Ucraina, pentru contracarea propagandei ruseşti. Abordarea tridimensională a informaţiilor integrează informaţii umane, semnale şi operaţii militare, SUA şi aliaţii NATO oferind Ucrainei informaţii esenţiale despre locaţia generalilor ruşi, dar şi tehnologie avansată, drone Switchblade, alături de date despre atacul rusesc asupra aeroportului Hostomel din 2022. Ucraina a valorificat informaţiile şi tehnologia primită, scufundând nava de asalt rusească Moskva în Marea Neagră (Sherazi 2025).

În cele ce urmează vom vedea mai în profunzime detaliile confruntării dintre Occident şi Republica Populară Chineză, alături de cazurile cele mai importante şi de rolul jucat de infrastructura *Five Eyes*.

Confruntarea Five Eyes cu China

Five Eyes deţine un rol strategic în eforturile depuse de ţările occidentale şi de SUA de a controla China. Five Eyes, NATO şi Uniunea Europeană (UE) au condamnat public Republica Populară Chineză în 2021 pentru implicarea în atacul cibernetic asupra Microsoft Exchange (MSE). Centrul Microsoft de Informaţii privind Ameninţările (MSTIC) are ca atribuţii investigarea şi răspunsul la atacuri, descoperind astfel

hackerii din guvernul chinez denumiți *Hafnium* care intraseră în serverele Exchange. Microsoft a urmărit doar din iunie 2020 acest grup, care avea ca mod de operare țintirea sistemelor neactualizate ale companiilor medicale, agențiilor guvernamentale și universităților. Intrușii au reușit accesul în serverele Exchange și preluarea controlului din cauza unor erori de codare. Condițiile necesar a fi îndeplinite erau doar două: departamentul IT al companiei să controleze local sistemele, „on premises", iar sistemele să fie conectate la internet. Din fericire, *Office 365* de la Microsoft nu a fost afectat de breșa de securitate, datorită rulării sale în cloud, ceea ce conferă o protecție mai mare. Atacatorii au plasat cod, de îndată ce au pătruns în serverele Exchange, solicitând documente, e-mail-uri, PDF-uri, păcălind serverele de la celălalt capăt că solicitarea era legitimă. Atacul cibernetic a căpătat amploare, provocând răspunsuri guvernamentale din partea consilierului pentru securitate națională din timpul administrației Biden, Jake Sullivan. Agenția pentru Securitate Cibernetică și Infrastructură, Grupul de lucru convocat de Casa Albă și FBI s-au implicat, obținând o hotărâre judecătorească pentru scanarea legală a internetului în încercarea de a găsi serverele sparte de chinezi și apoi a elimina proactiv virușii (Temple-Raston 2021).

Atacul cibernetic de la *Office of Personnel Management* a permis hackerilor chinezi să acceseze și să-și însușească 21,5 milioane de înregistrări din baza de date a guvernului federal. Breșa de securitate *Equifax*, un veritabil succes al Serviciului de Contrainformații ale Partidului Comunist Chinez, a oferit pe tavă Republicii Populare Chineze datele financiare a 147,9 milioane de americani. Infractorii cibernetici au furat 78 de milioane de numere de securitate socială, nume și date de naștere de la asigurătorul de sănătate *Anthem Inc*. În 2018, hackerii chinezi au spart bazele de date ale hotelurilor *Marriott* și au preluat toate informațiile despre carduri de credit, rezervări, pașapoarte a 500 de milioane de persoane. Reprezentanții serviciilor de informații americane opinează că China deține în prezent informațiile personale de identificare a 80% dintre cetățeni și colectează informații despre restul de 20%. Prin datele obținute de la Anthem, OPM, Marriott, Equifax, despre cardurile de credit, împrumuturi, ipoteci, scor de credit, americanii sunt susceptibili la a fi abordați de către ofițeri de informații chinezi și de a răspunde afirmativ, fie în urma șantajului, fie a oferirii de avantaje materiale în cazul în care contul în bancă nu e substanțial sau deținătorul întâmpină probleme financiare (Temple-Raston 2021).

Chinezii au adunat cantități uriașe de date care fac parte dintr-un plan mai amplu de dezvoltare a inteligenței artificiale. În 2017, Partidul Comunist Chinez a anunțat că inteligența artificială de anvergură

mondială a devenit o prioritate naţională, concentrându-se pe formarea informaticienilor în scrierea algoritmilor şi hrănirea algoritmilor cu un număr imens de informaţii pentru a putea învăţa. Interesul Chinei în inteligenţa artificială este demonstrat de cele peste 1.000 de firme de inteligenţă artificială, iar faptul că are o populaţie de peste 1 miliard de oameni despre care colectează informaţii, la care se adaugă furturile imense de date, ajută la dezvoltarea inteligenţei artificiale la scară globală. Pericolul constă în rolul tot mai important pe care îl dobândeşte inteligenţa artificială în viaţa noastră, prin acordarea creditelor, aprobarea ipotecilor şi accesul la datele noastre medicale (Temple-Raston 2021).

Directorul GCHQ Anne Keast-Butler a declarat la Centrul Naţional de Securitate Cibernetică (NCSC), CYBERUK din Birmingham, că statul chinez reprezintă un risc cibernetic în creştere pentru Regatul Unit şi că acesta intenţionează să folosească capacităţile sale cibernetice pentru atingerea deziderateloor naţionale. Provocarea chineză devine prioritatea principală a GCHQ, cu cele mai multe resurse alocate în comparaţie cu oricare altă misiune, conlucrând alături de aliaţi şi colegii din mediul academic şi privat pentru a combate şi descuraja ameninţările cibernetice din partea statelor naţionale şi a actorilor ostili (GCHQ 2024).

Drept contrareacţie occidentală, Meng Wanzhou, directorul financiar al companiei chineze Huawei, a fost arestată în 2020 graţie *Five Eyes* de către autorităţile americane în Canada pentru acuzaţia de încălcare a securităţii naţionale. Mai mult decât atât, patru dintre naţiunile *Five Eyes* au interzis Huawei şi tehnologia sa 5G. Canada a interzis nu doar Huawei, ci şi firma ZTE şi tehnologia 5G. Liderii *Five Eyes* au criticat public China pentru furtul drepturilor de proprietate intelectuală şi spionaj după o întâlnire din 2023 cu companii din Silicon Valley, Beijing-ul respingând acuzaţiile. *Five Eyes*, SUA şi Australia au oferit informaţii guvernului canadian despre uciderea liderului separatist sikh Hardeep Singh pe teritoriul canadian de către Research and Analysis Wing (RAW), agenţia de informaţii externe indiană (Rajput 2023). În octombrie 2024, Canada a expulzat diplomaţi indieni, în timp ce SUA a îndemnat India să coopereze cu Canada. În timpul operaţiunilor NATO din Afganistan după 11 septembrie, operaţiuni conduse de SUA, membrii *Five Eyes* au cooperat cu Pakistanul împotriva acţiunilor insurgente şi a terorismului transfrontalier. Cu toate acestea, *Five Eyes*, îndeosebi SUA, favorizează în prezent India în parteneriatele lor strategice, ceea ce reprezintă o provocare pentru Pakistan (Sherazi 2025). Agenţia de informaţii a Noii Zeelande a denunţat ingerinţele străine din partea

Chinei și Federației Ruse, care ar putea aduce atingere securității naționale. Serviciul de Informații de Securitate al Noii Zeelande (NZSIS) a anunțat public acțiunile de spionaj și ingerință "în și împotriva" țării din partea serviciilor de informații chineze, dar și faptul că aliații vor fi alături de Noua Zeelandă (Financial Intelligence 2023).

Triada Echelon-Prism- XKeyscore versus VPNs

După cum s-a precizat în primul capitol, FVEY s-a specializat în domeniul SIGINT. Misiunea capitolului prezent devine aceea de a-l imersa pe cititor în detaliile tehnice ale practicilor de Intelligence. *Five Eyes* utilizează programul global *ECHELON*, prin care interceptează comunicațiile private cu ajutorul sateliților de comunicații, comunicații stocate și apoi analizate. *ECHELON*, primul sistem de supraveghere *Five Eyes*, datează din 1971, cu scopul de a monitoriza comunicațiile diplomatice și militare ale Uniunii Sovietice și ale partenerilor săi din blocul estic în timpul Războiului Rece. *PRISM*, înființat în 2007, este un sistem de supraveghere al *Five Eyes*, ce adună date despre comunicații ale cetățenilor americani cu sprijinul giganților de tehnologie Microsoft, Yahoo!, Google, Facebook etc. *XKeyscore* este un alt sistem de urmărire recent al *Five Eyes*, care oferă NSA posibilitatea de a ști locația oricărui dispozitiv *smart* și de a citi orice comunicare online (Karbauskas 2025).

Țările din Alianța *Five Eyes* partajează datele private privind comunicațiile transfrontaliere. *Patriot Act* din SUA a dat undă verde din 2001 supravegherii în masă a cetățenilor americani. În 2016, Regatul Unit al Marii Britanii a adoptat *Carta Snoopers*, agențiile de informații putând colecta date despre comunicațiile cetățenilor, în timp ce companiile de telecomunicații și furnizorii de servicii de internet sunt obligați să stocheze date despre utilizatori. Australia a adoptat o lege asemănătoare, modificând legea privind telecomunicațiile, solicitând furnizorilor de servicii de internet să stocheze datele utilizatorilor timp de 2 ani. Țările semnatare ale Acordului UKUSA au pledat pentru eliminarea criptării și pentru alte încălcări ale confidențialității, invocând securitatea statelor și a cetățenilor. Cetățenii au apelat la servicii VPN, e-mail-uri securizate și aplicații de mesagerie criptată, însă dacă acestea au sediul într-o țară din Grupul *Five Eyes*, confidențialitatea totală nu e asigurată. *Five Eyes* au declarat în 2018 că vor depune toate diligențele pentru ca backdoor-uri de criptare să fie asigurate de către companiile de tehnologie. Australia a votat deja un proiect de lege care obligă companiile să predea agențiilor guvernamentale datele utilizatorilor și să creeze backdoor-uri pentru

datele criptate. William Barr, Procurorul general al SUA, a cerut la rândul său un proiect de lege similar, fiind secondat de către Canada, Regatul Unit şi Noua Zeelandă. Companiei Apple i s-a solicitat de către Marea Britanie în 2025 să ofere acces la datele utilizatorilor. Guvernele Regatului Unit şi al SUA obligă VPN-urile să partajeze datele utilizatorilor cu organele de aplicare a legii în câteva ocazii, fără a li se aduce la cunoştinţă cetăţenilor imvestigaţi (Karbauskas 2025).

Lavabit, un furnizor de e-mail din SUA, a fost închis după ce a refuzat să ofere agenţiilor chei de criptare în 2013, cînd era vizat Edward Snowden. Riseup, un furnizor de VPN/email din SUA, a asigurat accesul la datele utilizatorilor urmare a 2 mandate şi a păstrat tăcerea asupra acestui fapt. O reţea VPN importantă din SUA, IPVanish, a colectat şi a oferit datele utilizatorilor la cererea FBI-ului în 2016, deşi susţinea că respectă politica de neînregistrare. HideMyAss, un furnizor VPN din Marea Britanie, furnizează autorităţilor date despre utilizatori şi recunoaşte asta în mod public. Graţie Acordului UKUSA, datele internauţilor pot ajunge la agenţiile de informaţii din SUA, Australia, Canada sau ale partenerilor, dacă se impune. Private Internet Access a fost hotărâtă în a nu păstra datele utilizatorilor, reprezentând cea mai bună strategie de marketing. IPVanish a fost descoperit când se conecta la conturi, deşi avea atunci un alt proprietar, iar HideMyAss e obligat prin lege să colecteze date despre utilizatori. Hushmail, un serviciu canadian de email privat, a predat în 2007 la solicitarea FBI-ului 12 CD-uri cu e-mailuri. Tutanota (Germania) a fost obligată de instanţă să ofere backdoor-uri de criptare. CounterMail (Suedia) nu mai primeşte înregistrări noi (Karbauskas 2025).

Clubul de la Berna

Dacă până acum am luat cunoştinţă de cartografia cooperării naţiunilor de limbă engleză, acum ne vom îndrepta atenţia spre Europa continentală unde echivalentul FVEY este Clubul de la Berna. Acesta din urmă a coordonat activităţile de informaţii ale statelor europene şi ale altor state timp de decade. Organizaţia odată informală, care reuneşte şefii serviciilor de securitate ale UE, a ajuns să opereze la nivel transnaţional. Ziarul austriac „Oesterreich" a publicat în luna noiembrie a anului 2019 un document intern al Clubului de la Berna (CdB), reprezentând cea mai mare scurgere de informaţii din istoria lui. Cel puţin în 2011, CIA, FBI şi Mossad, alături de alte servicii, au făcut schimburi de informaţii în cadrul CdB, contrazicând schimbul intra-

european între serviciile de informaţii prezentat până atunci publicului. Istoricul elveţian Aviva Guttmann a descoperit în urma cercetărilor sale în cadrul Arhivelor Federale Elveţiene că Clubul a făcut schimb de informaţii în afara Europei imediat după înfiinţarea sa în 1969, când nouă servicii secrete din Europa de Vest au început să partajeze informaţii despre teroriştii palestinieni cu serviciile secrete israeliene Shin Beth şi Mossad, dar şi cu FBI prin sistemul de telegrame criptat *Kilowatt*. Din 1974, sistemul de telegrame *Megaton* se referea la terorismul non-palestinian. Munca de cercetare a lui Guttmann nu trece mai departe de anii 1980, deoarece nu pot fi desecretizate documentele mai recente de 50 ani (Jirat 2020).

Documentul secret al CdB, făcut public de *Oesterreich* se referă la un control de securitate efectuat în februarie 2019 de *Soteria*, un grup intern al CdB incluzând serviciile secrete din Elveţia, Marea Britanie, Germania şi Lituania, la serviciul secret austriac BVT (Oficiul Federal pentru Protecţia Constituţiei şi Combaterea Terorismului). Raportul despre BVT a relevat deficienţe în domeniul securităţii clădirilor şi în verificările de securitate asupra personalului, iar securitatea cibernetică evaluată drept neglijentă. Până şi hackerii de talie mijlocie ar fi putut utiliza reţeaua internă BAT pentru a penetra reţeaua IT a CdB - *Poseidon*. Încă din anii 1970, CdB a devenit o reţea globală. Reţeaua de comunicare a Clubului numită *Capriccio* organizează schimbul de informaţii despre extremismul islamic, în timp ce *Toccata* organizează schimbul de informaţii despre terorismul non-islamic. Spre deosebire de Capriccio, *Toccata* nu include CIA, Mossad sau ISA (Agenţia Israeliană de Securitate), în timp ce extremismul de stânga şi de dreapta sunt tratate de *RILE*. În 2011, alături de cele 27 de servicii ale UE şi serviciile din Norvegia şi Elveţia, au apărut şi serviciile secrete non-europene cu următoarele coduri: 12 CSIS (Ottawa), 06 Mossad (Tel Aviv), 19 FBI (Washington), 25 NZSIS (Wellington), 22 ASIO (Canberra), 94 ISA (Tel Aviv), 28 CIA (Bruxelles) (Jirat 2020).

Grupul Antiterorist (CTG) a fost fondat în 2001 ca un subgrup CdB, interfaţă cu UE în domeniul combaterii terorismului, oferind analize ale ameninţărilor politicienilor de rang înalt din UE. Astfel, CTG influenţează discursul politic privind securitatea din statele membre UE, fără să aibă mecanisme de supraveghere şi prevederi statutare. Agenţia de Poliţie Europol a efectuat două exerciţii de simulare cu CTG în 2018, la care au participat şi Centrul pentru Introducerea Clandestină de Migranţi (EMSC), Centrul pentru Combaterea Terorismului (ECTC) şi Oficiul Europol pentru Divulgarea Conţinutului de pe Internet. Deşi UE

nu are mandat, va continua să coopereze cu CTG şi cu CdB. Istoricul şi expertul în informaţii austriac Thomas Riegler remarcă faptul că cele două nu sunt oficial integrate în arhitectura UE şi nu există niciun acord contractual. Clubul de la Berna şi Grupul Antiterorist sunt ţinute să respecte doar legile naţionale ale statelor respective şi nicio regulă imperativă, controlul fiind imposibil (Jirat 2020).

Andrej Hunko, membru al Bundestagului german, este de părere că serviciul secret intern german – *Oficiul Federal pentru Apărarea Constituţiei (BfV)* – a devenit un serviciu secret extern din 2016 odată cu folosirea platformei operaţionale CTG, acest lucru reclamând informarea publicului. Serviciul de informaţii elveţian a răspuns că FIS colaborează cu peste 100 de servicii partenere străine, listă aprobată de Consiliul Federal şi clasificată, iar FIS nu comentează despre cooperarea cu serviciile sale partenere. În noiembrie 2016, netzpolitik.org a relatat despre o platformă operaţională a CTG la sediul serviciului secret olandez AIVD, lângă Haga. AIVD a refuzat să comenteze despre Clubul de la Berna, la fel şi autoritatea independentă de supraveghere a activităţilor de informaţii din Elveţia - AB-ND, organismului parlamentar de supraveghere GPDel şi Comisarului federal elveţian pentru protecţia datelor. Baza de date *Phoenix* a CTG colectează date cu caracter personal despre jihadişti, conform Autorităţii de supraveghere olandeze CTIVD. Serviciile de informaţii americane deţin statut de observator în cadrul CTG. Istoricul elveţian Adrian Hänni menţionează că CdB este vârful aisbergului platformelor care operează în secret: grupul SIGINT Seniors cu sediul la Paris, Grupul de combatere a terorismului (CTG) al Clubului de la Berna, G 13+ şi Grupul de lucru al poliţiei privind terorismul (PWGOT). Legile naţionale, precum noua Lege privind Serviciul Elveţian de Informaţii, permit cooperarea cu serviciile străine, dar nu există nicio bază legală pentru cooperarea multilaterală în domeniul informaţiilor în cadrul CdB şi nicio prevedere pentru supraveghere (Jirat 2020).

Dată fiind această arhitectură organizaţională, modul cum aceasta răspunde provocărilor întrunite ale Moscovei şi Beijingului devine subiectul următorului capitol.

Încercarea de destabilizare a Occidentului din partea alianţei sino-ruse

Chiar dacă poate ideologia nu mai joacă un rol atât de important astăzi ca în timpul Primului Război Rece, acţiunile de spionaj şi contraspionaj, recrutările şi interceptările nu şi-au pierdut valabilitatea.

Aşadar, Republica Populară Chineză recrutează politicieni ai Uniunii Europene care au manifestat simpatie faţă de Moscova, operaţiunile de spionaj, recrutare şi influenţă ale Moscovei şi Beijingului ajungând să se suprapună tot mai mult în UE. Şeful agenţiei de informaţii interne a Republicii Cehe, Michal Koudelka, a subliniat că cele două puteri au aceleaşi intenţii de subminare a sprijinului pentru Ucraina, de destabilizare a Occidentului şi de antagonizare a societăţii civile din democraţiile liberale. Politicienii anti-occidentali marginali din Europa sunt ţintele predilecte de recrutare de către China şi Federaţia Rusă, însă colaborarea agenţiilor chineze şi ruseşti de informaţii este doar tangenţială, demonstrând precauţie. Nu se urmăreşte coordonarea serviciilor lor de informaţii, ci doar lupta împotriva unui inamic comun, Occidentul colectiv. POLITICO a oferit dreptul la replică ambasadelor Republicii Populare Chineze sau Federaţiei Ruse din Belgia, însă acestea nu au răspuns invitaţiei. Koudelka este primul oficial european de informaţii de rang înalt care a vorbit public despre operaţiunile de spionaj chineze şi ruseşti din Europa de când agenţia de informaţii a Republicii Cehe a descoperit o campanie majoră de influenţare rusească în martie 2024. Membri ai Parlamentului European au fost invitaţi la emisiunea TV *Vocea Europei*, despre care s-a aflat ulterior că era finanţată de agenţi pro-Kremlin, în timp ce mai mulţi participanţi la programele *Vocea Europei* erau plătiţi de China (Vinocur 2024).

Liderii europeni nu au acuzat făţiş Beijing-ul, spre deosebire de omologii americani. Un exemplu este Josep Borrell care a negat cunoaşterea vreunei dovezi de furnizare de arme Rusiei de către China în războiul din Ucraina, lucru care a dat apă la moară şefilor spionajului chinez, care au căutat profiluri de politicieni simpatizanţi ai Rusiei. Un exemplu al unei astfel de recrutări încrucişate este Frank Creyelman, un politician naţionalist flamand, exclus din partidul său Vlaams Belaang în 2023 pentru acceptarea de plăţi de la un spion chinez în schimbul traficului de influenţă în favoarea Beijingului. Creyelman demonstrase anterior o poziţie pro-rusă, prin opunerea publică la ideea ajutorului Vestului pentru Ucraina şi prin călătoriile în capitala rusă. Alte cazuri reprezentative sunt asistentul parlamentarului european de extremă dreapta german Maximilian Krah, acuzat şi arestat pentru spionaj în favoarea Chinei sau Filip Dewinter, un membru al aceluiaşi partid, ce a efectuat misiuni de observare a alegerilor din Rusia înainte de a fi căutat de un şef al spionajului chinez. Raportul belgian susţinea că Dewinter a acceptat plăţi de la companii-fantomă şi de la *Asociaţia Chineză pentru*

Contact Prietenos Internațional (CAIFC), o faţadă pentru serviciile secrete chineze, conform anchetei belgiene. Dewinter a negat contactul cu CAIFC în Belgia sau faptul de a fi lucrat cu bună ştiinţă pentru serviciul secret chinez, singurele sale contacte fiind cu *Fundaţia Europeană pentru Cultură şi Educaţie*. POLITICO nu a putut verifica existenţa acestei fundaţii, în schimb a descoperit că Dewinter a fost asociat cu *China Europe Foundation of Culture and Education*, cu sediul în Olanda, a cărei misiune era de a consolida legăturile educaţionale şi culturale dintre China şi Europa. Dewinter nu a fost demis din partidul Vlaams Belang, spre deosebire de Creyelman (Vinocur 2024).

Wiegand, cercetător invitat la German Marshall Fund, coautor al unui raport despre alinierea China-Rusia, cât şi Filip Jirous, un analist independent specializat în China, afirmă că în vederea antagonizării ţărilor UE şi a răcirii relaţiei acestora cu Washingtonul, agenţii ruşi şi mai nou chinezi recrutează oficiali europeni, vulnerabili fie la promisiuni, fie ideologic. Politicieni de extremă dreapta şi de extremă stânga (membri ai Alternativei pentru Germania, Adunării Naţionale din Franţa şi Vlaams Belaang, etc.) din mai multe ţări ale Uniunii Europene participă la misiuni care servesc intereselor Moscovei, precum cele de observare a alegerilor într-un teritoriu contestat (ex. zonele ocupate de Rusia din Ucraina), creând o bază solidă de posibili recruţi. Conform relatărilor din Spiegel, Le Monde şi Financial Times, Creyelman a acceptat plăţi ani de zile de la spionul Daniel Woo, al cărui interes era slăbirea parteneriatului dintre Europa şi Statele Unite prin propaganda chineză şi influenţarea Bundestag-ului german. Deşi reţeaua europeană a lui Woo a fost destructurată, nu e singurul chinez care urmăreşte ademenirea parlamentarilor sau angajaţilor parlamentari (Vinocur 2024).

Fostul preşedinte finlandez Sauli Niinistö a declarat că UE are nevoie de propria agenţie de informaţii în lupta cu sabotorii şi agenţi străini care operează în ţările de pe întreg continentul, ca răspuns la solicitarea din partea preşedintei Comisiei Europene, Ursula von der Leyen, de a redacta un raport referitor la pregătirea UE pentru război şi apărarea civilă. Un serviciu de cooperare în domeniul informaţiilor la nivelul UE ar acoperi atât nevoile strategice, cât şi cele operaţionale, în opinia sa. Mulţi diplomaţi au fost expulzaţi din capitalele europene fiind acuzaţi de spionaj, iar Bruxelles-ul a devenit centrul de activitate al agenţilor, prin prisma multitudinii de instituţii şi ambasade din oraş. Din moment ce totuşi adunarea informaţiilor cade în sarcina statelor membre, îmbunătăţirea fluxului de informaţii constituie primul pas. Apoi

pregătirea unui număr cât mai mare de experți în securitate cibernetică și includerea civililor în apărarea națională (Posaner 2024).

În luna noiembrie a anului 2025 s-a accentuat ideea înființării unei agenții de informații europene, de data aceasta sub conducerea președintei Comisiei Europene, Ursula von der Leyen, ceea ce a ridicat probleme sub aspectul distribuirii suveranității între statele europene și Bruxelles în deciziile legate de securitatea națională. Scopul declarat al agenției de informații europene este coordonarea informațiilor colectate de serviciile statelor europene și de Uniunea Europeană. Un purtător de cuvânt al UE a declarat către DPA, agenția de presă germană, că agenția se află într-un stadiu incipient de formare, cu posibilitatea de a recruta personal din serviciile secrete naționale (Höller 2025).

Financial Times menționează că cele 27 de țări membre ale UE ar putea ridica obiecții legate de suveranitate. Conducerea actualului serviciu secret al Uniunii Europene – Serviciul European de Acțiune Externă (SEAE) – nu e de acord cu o agenție coordonată de von der Leyen. Un prim motiv invocat este duplicarea activității SEAE, dar punctul cel mai sensibil este încălcarea suveranității naționale. Securitatea națională cade în sarcina exclusivă a statelor naționale, conform tratatelor UE. În ciuda faptului că războiul din Ucraina a condus la integrarea europeană în domeniul apărării, suveranitatea statelor nu este negociabilă, cu atât mai mult cu cât țările membre au loialități diferite, unele înclinând puternic în favoarea Federației Ruse (Höller 2025).

Conform ziarului FT, diplomații UE văd în această agenție sub conducerea Ursulei von der Leyen, o creștere substanțială a influenței președintelui Comisiei Europene, dar și posibila periclitare a propriilor cariere și reducerea puterii Kajei Kallas, Înaltul Reprezentant al Uniunii Europene pentru Afaceri Externe și Politica de Securitate. Paula Pinho, purtătoarea de cuvânt a Comisiei Europene, a menționat că noua agenție va veni în sprijinul Serviciului European de Acțiune Externă și va anticipa Colegiul de Securitate, alcătuit din von der Leyen și cei 26 de comisari. Colegiul de Securitate a avut prima întrunire în luna martie a anului 2025, când Comisia și-a extins prerogativele în materie de securitate (Euronews 2025).

Cele 27 de state membre nu au fost consultate încă în privința agenției europene și se așteaptă să opună o rezistență delegării competenței de informații către Bruxelles, deși această agenție se dorește a fi funcțională și pentru a contracara amenințarea hibridă reprezentată de

Federaţia Rusă pe fondul reducerii schimbului de informaţii şi a garanţiilor de securitate din partea S.U.A. (Euronews 2025).

Uniunea Europeană are o politică restrictivă şi în privinţa Republicii Populare Chineze, faţă de care îşi ia precauţii în domeniile de cercetare vizând securitatea civilă şi digitală, bioeconomie, climă, cultură şi sănătate. Începând din 2026, China nu va mai putea fi parte în proiectele de cercetare finanţate de Horizon Europe pentru dezvoltarea noilor tehnologii (Naujokaitytė 2026).

Ameninţările chineze sub forma spionajului sunt întâmpinate cu iniţiativa formării agenţiei de informaţii UE şi reducerea riscului reprezentat de dependenţa de furnizorii de tehnologii chineze (reţele 5G, infrastructură critică), care au ajuns să fie ori restricţionaţi, ori interzişi (Reuters 2026).

Kaja Kallas, Înaltul Reprezentant al UE pentru afaceri externe şi politica de securitate a UE, consideră interesul Chinei pentru zona arctică un risc major de securitate. Zona arctica se află in prim-planul competiţiei mondiale pentru energie, resurse, rute comerciale, lanţuri de aprovizionare, materii prime critice ca importanţă strategică. (Pala 2026).

Comisia Europeană urmăreşte nu doar protejarea proprietăţii intelectuale europene de transferuri către China, ci şi creşterea securităţii cibernetice împotriva manipulării informaţiilor străine (FIMI) din China. Drept răspuns, *European Democracy Shield* (Scutul Democraţiei Europene), format de Comisia Europeană şi Serviciul European de Acţiune Externă (SEAE), are ca ţel menţinerea integrităţii spaţiului informaţional legat de alegeri şi procese democratice, combaterea infiltrărilor din mediul privat (FIMI) şi a dezinformării (EUvsDisinfo 2026). O democraţie solidă se întemeiază pe jurnalismul liber, pe educaţia civică şi informarea corectă.

Concluzii

Din moment ce operaţiunile de contrainformaţii intră în sfera competenţelor naţionale, măsuri împotriva acestui lucru pot fi luate la nivel naţional, însă e de dorit şi conştientizarea la nivel european din partea serviciilor naţionale de informaţii care colaborează pentru contracararea operaţiunilor de manipulare a agenţiilor străine non-europene.

Five Eyes şi Clubul de la Berna ar fi bune exemple pentru o reţea europeană de agenţii de Intelligence, care să partajeze informaţii

sensibile și să conlucreze. Un serviciu de informații european unificat ar putea proteja democrația de imixtiuni străine. Agențiile naționale de informații europene pot solicita și oferi informații una alteia. Necesitatea unei metode unificate de analiză a informațiilor din Uniunea Europeană prin dezvoltarea propriilor capacități de colectare a informațiilor este justificată pentru crearea unui front european rapid și mai asertiv în evaluarea amenințărilor, inclusiv a celor la adresa securității cibernetice. Amenințările interferențelor străine pretind un răspuns coordonat și unificat, care ar crește exponențial rezultatul eforturilor de la nivel național. Infiltrarea propagandei rusești sau chinezești în Uniunea Europeană reclamă un demers ferm din partea statelor europene pentru apărarea democrației și securității colective, cu accent pe unitatea și colaborarea în domeniul informațiilor. Un argument pentru înființarea unei agenții europene comune de informații îl poate constitui asigurarea securității și apărării colective, dar și a imaginii de solidaritate și coeziune pe care o oferă în exterior. Acest aspect este esențial într-o epocă a incertitudinii geopolitice și a schimbării alianțelor. Criticii vin cu contraargumentul atingerii aduse suveranității naționale și a dublării structurilor naționale de intelligence. Din acest motiv societatea civilă are o contribuție importantă în vederea combaterii dezinformării și a influențelor străine prin campaniile de informare, cooperarea cu organizațiile de verificare a faptelor, în coroborare cu Legea europeană privind serviciile digitale.

Reziliența democrației liberale depinde în mare măsură de capacitatea cetățenilor de a lua decizii informați și de alegerea parlamentarilor ce respectă valorile europene. În timp ce se prefigurează pericolul unei alianțe globale a autocrațiilor ce urmărește destabilizarea Occidentului, iar partidele extremiste câștigă teren, propaganda populistă și ingerințele străine trebuie combătute prin păstrarea echilibrului politic, reziliență, strategii eficiente, transparență și menținerea democrației și a statului de drept.

Bibliografie

1. Abrams, Elliott, ”The New Cold War”, Council on Foreign Relations, 04 march 2022, https://www.cfr.org/articles/new-cold-war-0

2. Euronews, ”Is the EU spy unit about to become reality? Von der Leyen wants her own secret service”, 11/11/2025 - 18:50 GMT+1, https://www.euronews.com/2025/11/11/is-the-eu-spy-unit-about-to-become-reality-von-der-leyen-wants-her-own-secret-service

3. EUvsDisinfo, ”FIMI and disinformation as global threats”, Disinformation Review, January 30, 2026, https://euvsdisinfo.eu/fimi-and-disinformation-as-global-threats/

4. Financial Intelligence, ”Noua Zeelandă denunţă riscuri pentru securitatea sa provocate de ingerinţe străine (raport)”, 11 august 2023, 12:23, https://financialintelligence.ro/noua-zeelanda-denunta-riscuri-pentru-securitatea-sa-provocate-de-ingerinte-straine-raport/

5. GCHQ, “A Brief History of the UKUSA agreement”, 5 March 2021. https://www.gchq.gov.uk/information/brief-history-of-ukusa

6. GCHQ, ”GCHQ and NCSC heads warn of increasing cyber risk from China”, 14 May 2024, https://www.gchq.gov.uk/news/cyberuk-2024

7. Höller, Linus, ”The European Union wants its own intelligence branch”, Defence News, Nov 12 2025, https://www.defensenews.com/global/europe/2025/11/12/the-european-union-wants-its-own-intelligence-branch/

8. Jirat, Jan, ”The Club de Berne: a black box of growing intelligence cooperation”, About Intel, 1. April 2020, https://aboutintel.eu/the-club-de-berne/

9. Karbauskas, Šarūnas, ”Five, Nine, and Fourteen Eyes alliances explained”, Cyber News, 22 April 2025, https://cybernews.com/resources/5-eyes-9-eyes-14-eyes-countries/

10. Naujokaitytė, Goda, ”Explained: China has been kicked out of most of Horizon Europe”, Science Business, 27 Jan 2026 | https://sciencebusiness.net/news/r-d-funding/horizon-europe/explained-china-has-been-kicked-out-most-horizon-europe

11. Pala, Melike, ”EU foreign policy chief warns about security risks from China's growing interest in Arctic”, AA, 03.02.2026, https://www.aa.com.tr/en/world/eu-foreign-policy-chief-warns-about-security-risks-from-chinas-growing-interest-in-arctic/3819220

12. Posaner, Joshua, ”Create a CIA-style European spy service, von der Leyen is told”, Politico, October 30, 2024 1:39 pm CET, https://www.politico.eu/article/europe-spy-service-cia-ursula-von-der-leyen/

13. Rajput, Neeraj, ”RAW ‘Hunts’ Mossad Style! Ex-Raw Officer Makes Sensational Claims On Hardeep Singh Nijjar’s Assassination”, The Eurasiantimes, 19 September 2023. https://www.eurasiantimes.com/raw-hunts-mossad-style-trudeau-accuses-india-of-assassinating-khalistani-leader-on-canadian-soil/

14. Reuters, ”EU moves to force the phase-out of Chinese suppliers from key infrastructure, FT reports”, January 17, 2026, 9:52 AM GMT+2, https://www.reuters.com/world/china/eu-bar-chinese-suppliers-critical-infrastructure-ft-reports-2026-01-17/

15. Sherazi, Anees Fatima, ”Critical Analysis of Five Eyes Alliance”, ISSRA, January 13, 2025, https://www.issra.pk/insight/2025/critical-analysis-of-five-eyes-alliance/insight.html

16. Temple-Raston, Dina, ”China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying”, NPR, August 26, 2021, 5:00 AM ET, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

17. Vinocur, Nicholas, ”‘Dragon-Bear’: How China and Russia’s spy operations overlap in Europe”, Politico, September 13, 2024 4:20 am CET, https://www.politico.eu/article/dragon-bear-how-china-and-russias-spy-operations-overlap-in-europe/

Aceasta este al patrulea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2025 - ICS 2025, publicat de Academia Națională de Informații „Mihai Viteazul" (ANIMV). ICS continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Intelligence și Securitate a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139