Supliment al revistei „Strategic Impact”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 5 (213) / 2023
Indexat în
CEEOL și ROAD

DOI: 10.53477/1842-8096-23-05

REZILIENȚA INFRASTRUCTURILOR CRITICE ÎN CONTEXTUL INSECURITĂȚII CIBERNETICE PROVOCATE DE AMENINȚĂRILE DE TIP HIBRID*

Ionuț-Cosmin BUȚĂ

Critical infrastructure resilience in the context of cyber insecurity caused by hybrid threats

Abstract: *Nowadays, as state and non-state actors have developed new hybrid methods to promote their interests, the concept of critical infrastructure protection has gained new value from a resilience perspective, and today, most security incidents occur in cyberspace.*

This article examines the interconnection between the concepts of “hybrid warfare - critical infrastructures - cyber-attacks”. Therefore, we begin with the assumption that cyberspace is the most susceptible environment to vulnerabilities and potential attacks, subsequently impacting vital services for populations numbering in the millions. Accordingly, our research endeavors to address the following question: Within the realm of hybrid threats, can minor vulnerabilities in cyberspace generate strategic-level effects on critical infrastructures? To accomplish this, we have used the analytical tool Connected Papers to identify scientific papers that explore the correlation between “hybrid war - critical infrastructures - cyber-attacks”. Subsequently, we expanded our analysis to encompass articles focused on studying either two or even a single concept among those mentioned.

The results of our analysis demonstrate that vulnerabilities exploited within a Wi-Fi network or an industrial control panel of a critical infrastructure in cyberspace can have far-reaching consequences that may impact the vital services required by the population, resulting in a temporary disruption. Such an attack, originating from minimal efforts in terms of time, personnel, and financial resources, can lead to substantial property damage.

Keywords: *resilience, critical infrastructures, hybrid warfare, hybrid threats, cyberspace.*

Reziliența infrastructurilor critice în contextul insecurității cibernetice provocate de amenințările de tip hibrid

Rezumat: *Odată cu dezvoltarea metodelor hibride ale actorilor statali și non-statali pentru promovarea intereselor naționale, conceptul de protecție a infrastructurilor critice a căpătat noi valențe mai ales din perspectiva asigurării rezilienței acestora, iar astăzi cele mai numeroase incidente de securitate se desfășoară în spațiul cibernetic.*

Prezentul articol analizează relația dintre conceptele “război hibrid - infrastructuri critice - atacuri cibernetice”, în care am pornit de la premisa conform căreia spațiul cibernetic reprezintă acel mediu în care vulnerabilitățile sunt cele mai predispuse atacurilor, afectând astfel serviciile esențiale pentru populații de până la ordinul milioanelor de locuitori și vom încerca să oferim răspuns următoarei întrebări de cercetare: În contextul amenințărilor hibride, micile vulnerabilități din spațiul cibernetic pot produce efecte de nivel strategic asupra infrastructurilor critice? Pentru aceasta, am utilizat programul analitic Connected Papers cu scopul de a identifica în cadrul literaturii de specialitate lucrările științifice care analizează relația “război hibrid - infrastructuri critice - atacuri cibernetice”, iar ulterior am extins analiza și asupra unor articole științifice care au ca obiect de studiu doar două sau chiar și un singur concept din cele prezentate.

Rezultatele analizei noastre ne indică faptul că în spațiul cibernetic vulnerabilitățile exploatate într-o simplă rețea Wi-Fi sau în cadrul unui panou de control industrial al unei infrastructuri critice poate produce consecințe majore care să afecteze pentru o perioadă de timp serviciile esențiale necesare populației, transformând astfel un efort care implică resurse de timp, de personal și financiare foarte mici într-un atac care poate produce pagube materiale semnificative.

Cuvinte-cheie: *reziliență, infrastructuri critice, război hibrid, amenințări hibride, spațiu cibernetic.*

* Această lucrare a fost publicată în cadrul proiectului „Centrul de excelență pentru securitatea cibernetică și reziliența infrastructurilor critice (SafePIC)”, contract nr. 270/23.06.2020, ID 120436, finanțat în cadrul Programului Operațional Competitivitate 2014-2020, Axa prioritară 1 – Cercetare, dezvoltare tehnologică și inovare (CDI) în sprijinul competitivității economice și dezvoltării afacerilor, Acțiunea 1.2.1.

*Lt. col. instr. avs. **Ionuț-Cosmin BUȚĂ** este doctorand în domeniul Științe Militare în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: cosmin_buta@yahoo.com).*

Introducere

Modul în care a evoluat noul tip de război, pe care specialiștii îl denumesc „război hibrid", de cele mai multe ori poate fi mai ușor descris decât definit. Acest lucru se datorează, pe de o parte, faptului că lucrurile sunt într-o evoluție atât de accelerată încât realitatea din teren se desfășoară cu o viteză mult mai mare decât poate fi conceptualizată și definită de către specialiști, iar, pe de altă parte, pentru că metodele coercitive și subversive utilizate de către agresor cu scopul de a submina și destabiliza oponentul au loc într-o arie foarte diversificată de domenii (Steingartner, Galinec și Kozina, 2021, 4).

Dacă, în urmă cu câțiva ani, era suficient să analizăm acest tip de război din punct de vedere al domeniilor PMESII (politic, militar, economic, social, informații și infrastructură), ulterior acestora li s-au alăturat și cel tehnologic, legislativ și de mediu, creând un nou model de analiză denumit PESTLE (politic, economic, social, tehnologic, legal, de mediu). În prezent, combinarea celor două acronime încearcă să cuprindă complexitatea pachetelor de atacuri sincronizate din partea unor agresori care folosesc metode de război hibrid (Ibidem).

Complexitatea acestui nou tip de război nu este dată numai de faptul că utilizează metode coercitive și subversive, ci și că recrutarea și directa implicare a unor actori de tip *proxy* dezvoltă caracteristica de ambiguitate a acestuia (Ibidem). Un bun exemplu este reprezentat de grupările criminale care acționează în mediul cibernetic și exploatează vulnerabilitățile din acest domeniu, contribuind la ceea ce specialiștii denumesc astăzi „operațiuni cibernetice".

Revoluția informațională a contribuit la creșterea complexității mediului de securitate actual (Șușnea, 2018, 427), iar informația a fost considerată un aspect important al proiectării instrumentelor de putere DIME (diplomatic, informațional, militar și economic). Odată cu dezvoltarea noilor tehnologii de tip *cloud*, *AI*, *machine learning*, *deep learning*, *5G* etc., informația și-a modificat inclusiv mediul în care operează, trecând de la hârtie la computer, din plic în director și din autovehiculele de transport poștal în rețele de calculatoare securizate. În aceste condiții, progresul tehnologic înseamnă îmbunătățirea condițiilor de viață, dar și superioritate tehnologică ce poate fi utilizată ca un cal troian (Gimiga și Stanciu, 2022, 506) în vederea obținerii unor avantaje în domeniile PMESII.

Metodologia de cercetare

Domeniul protecției infrastructurilor critice este abordat în mod diferit în literatura de specialitate. Astfel, există abordări din perspectiva analizei componentelor arhitecturale, precum cele fizice și cibernetice (Aradau, 2010, 491), fizice și digitale (Merabti, Kennedy și Hurst, 2011, 1) sau a relațiilor dintre acestea (Bessani și alții, 2008, 44), din perspectiva managementului riscurilor (Giannopoulos, Filippini și Schimmer, 2012, 3) sau a influenței tehnologiilor emergente (Pătrașcu, 2021, 423-424) asupra infrastructurilor critice.

Pentru operaționalizarea întrebării de cercetare de la care am pornit prezentul demers științific, am utilizat programul analitic *Connected Papers* cu scopul de a identifica în cadrul literaturii de specialitate lucrările științifice care analizează relația „război hibrid - infrastructuri critice - atacuri cibernetice". Ulterior, am extins analiza și asupra unor articole științifice care au ca obiect de studiu doar două sau chiar și un singur concept din cele prezentate.

Connected Papers reprezintă un instrument de vizualizare a conexiunilor dintre articolele științifice, conectat la *Semantic Scholar Paper Corpus*, ce are rolul de a ajuta cercetătorii să găsească și să exploreze lucrări relevante pentru domeniul lor de interes. În urma interogării, programul emite un grafic în care articolele sunt aranjate în funcție de asemănarea subiectelor abordate și grupează vizual lucrările din domenii similare fără a face conexiunea citărilor dintre acestea (Connected Papers, 2023).

După prima interogare a platformei *Connected Papers*, căutând articolele științifice care analizează conceptele „război hibrid - infrastructuri critice - atacuri cibernetice", am identificat lucrările prezentate în figura nr. 1. Modelul relațional rezultat a cuprins un singur articol științific care să corespundă zonei de interes a prezentei cercetări, în care autorul subliniază conceptele-cheie de „război hibrid" și „atac cibernetic" pentru a evidenția rolul jucat de către personalul de conducere și a celui medical pentru protejarea infrastructurii digitale critice (Wells, 2022). Toate celelalte articole științifice identificate abordează strict domeniul medical și mai puțin al infrastructurilor critice, atacurilor cibernetice sau al amenințărilor hibride.

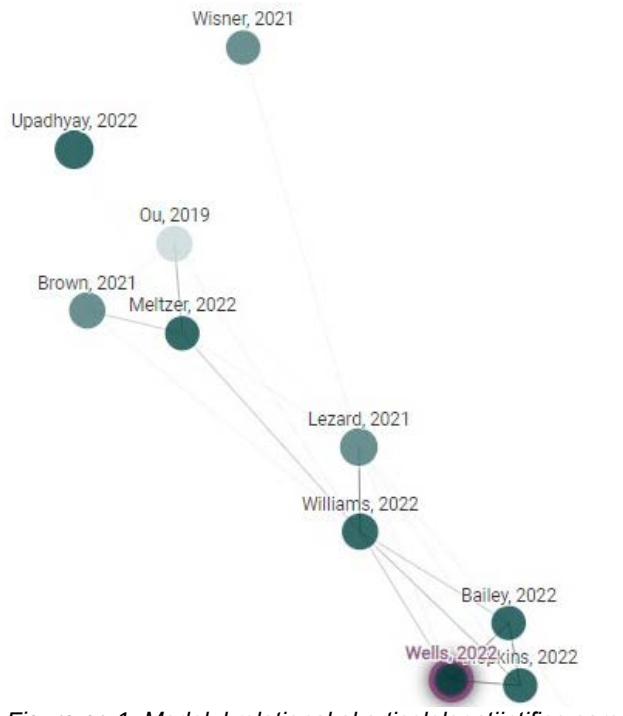

Figura nr. 1: Modelul relațional al articolelor științifice care analizează conceptele „război hibrid-infrastructuri critice-atacuri cibernetice" (Connected Papers 2023)

Ulterior, analiza noastră s-a restrâns doar la conceptele de „atac cibernetic” și „amenințare hibridă”, iar rezultatele sunt prezentate în figura nr. 2. Și în această situație, majoritatea articolelor abordează domenii, precum baze de date, analiză a datelor și modalități de interogare a acestora.

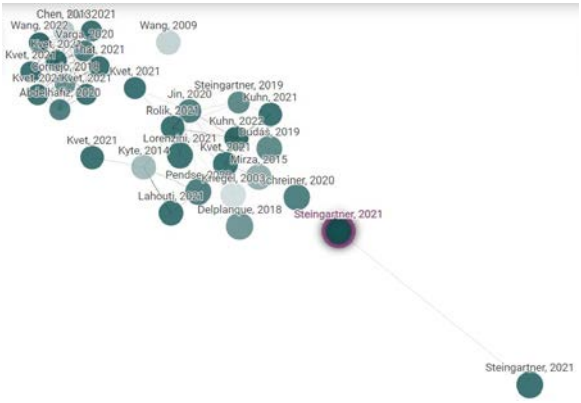

Figura nr. 2: Modelul relațional al articolelor științifice care analizează conceptele „atac cibernetic” și „amenințare hibridă” (Connected Papers 2023)

Rezultatele celor două interogări ale platformei *Connected Papers* au demonstrat faptul că există puține cercetări științifice care să analizeze relația dintre „război hibrid - infrastructuri critice - atacuri cibernetice”. De aceea, demersul nostru științific s-a concentrat în continuare pe analiza literaturii care abordează conceptele separat și care identifică anumite legături de cauzalitate între acestea.

Astfel, pentru a aborda problema securității cibernetice din perspectiva amenințărilor hibride, am utilizat modelul conceptual de interconectare a sistemelor deschise (OSI) al Organizației Internaționale pentru Standardizare (prezentat în figura nr. 3) și am analizat modul în care poate fi utilizată informația, care sunt vulnerabilitățile acesteia și care este rolul securității cibernetice în contracararea acestor amenințări. Acest model conceptual de interconectare a sistemelor deschise a fost creat tocmai cu scopul de a vizualiza și înțelege modul în care diferite sisteme cibernetice comunică utilizând protocoale standard (Cloudflare, 2023).

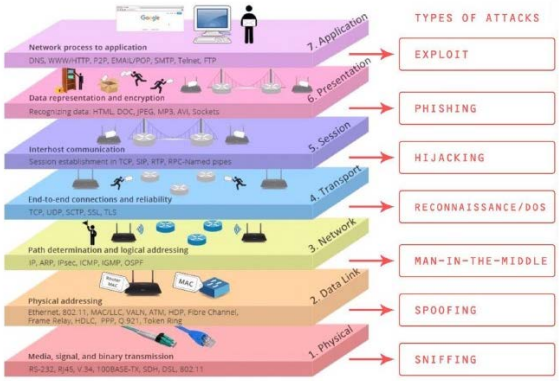

Figura nr. 3: Modelul conceptual de interconectare a sistemelor deschise și tipurile de atacuri utilizate asupra acestora (Steingartner, Galinec și Kozina, 2021, 5)

Odată cu modificarea mediului de operare și cu interacțiunea noilor tehnologii disruptive, au apărut vulnerabilități și amenințări noi ce trebuie gestionate de experții în securitate cibernetică astfel încât informația să circule mai repede și să fie mai sigură, practic să asigure cele trei mari caracteristici ale acesteia, precum: confidențialitate, integritate și disponibilitate (Cavelty, 2015, 401). Astfel, securitatea cibernetică a devenit o problemă de securitate atât națională, cât mai ales internațională, prin faptul că a crescut rolul și importanța informației în actualul mediu de securitate. Astăzi, informația oferă posibilitatea de a influența convingeri, de a produce sau insera idei și de a dezvolta cunoaștere (Ibidem). Mai mult, adoptarea rapidă de către organizații a sistemelor de tip *cloud* aduce foarte multe beneficii, dar creează și premise pentru extinderea orizontului vulnerabilităților în domeniul securității cibernetice.

Securitatea cibernetică reprezintă domeniul care conține atât spațiul fizic, cât și cel virtual, care abordează deopotrivă problema insecurității, dar și cele legate de tehnologie, de procese și proceduri, care contribuie la realizarea securității (Ibidem). În continuare, ne vom concentra pe conceptele de „atacuri informaționale” și „insecuritate cibernetică”.

Insecuritatea cibernetică și efectele asupra rezilienței infrastructurilor critice

În contextul amenințărilor hibride, „insecuritatea cibernetică” și „atacurile informaționale” reprezintă elemente esențiale ale mijloacelor neconvenționale (Hoffman, 2016, 30), utilizate de către actorii statali și non-statali, ce au un puternic impact psihologic asupra opiniei publice (Băhnăreanu, 2015, 57). Pe de altă parte, vulnerabilitățile, dar mai ales conexiunile dintre infrastructurile critice, au produs relații de interdependență prin care o infrastructură critică poate depinde de serviciile esențiale furnizate de către o altă infrastructură critică sau chiar de infrastructura în sine a acesteia (Alcaraz și Lopez, 2012).

Conform specialiștilor, se pot stabili patru tipuri de interdependențe între infrastructurile critice: fizică, geografică, cibernetică, logică (Rinaldi, Peerenboom și Kelly, 2001). Indiferent de tipurile de interdependență existente, un lucru este comun tuturor și anume informația și sistemele informatice. De aceea, alți autori fac referire la informații, procese și tehnologii informaționale care compun infrastructura critică informațională, a cărui perturbare poate conduce la afectarea performanței, fiabilității, securității și siguranței infrastructurilor critice dependente de acestea (Bendisch și alții, 2008) (Alcaraz și Zeadally, 2013).

Mai mult, indiferent de tipul serviciilor esențiale de care sunt dependente, fie că facem referire la energie electrică, gaze naturale sau apă, toate acestea sunt gestionate de către sisteme de control industrial (ICS) (Alcaraz și Zeadally, 2013) care sunt conectate la sisteme de control și achiziții de date (SCADA) (SCADA International, 2023). După cum se poate

observa în tabelul nr. 1, tocmai aceste tipuri de sisteme au făcut obiectul, în ultima perioadă, a celor mai importante atacuri cibernetice asupra infrastructurilor critice din întreaga lume.

Denumirea	Anul	Infrastructura afectată	Sistemul atacat	Efectul produs
Stuxnet	2010	Centrala nucleară	SCADA	Primul atac cibernetic din lume care a avut ca obiectiv atacarea sistemelor SCADA pentru afectarea rețelei
Night Dragon	2010	Companii din domeniul energetic	SCADA	Night Dragon a sustras informații referitoare la infrastructura critică, însă fără a prelua controlul asupra unui HMI, care ar fi putut apoi să le ofere atacatorilor controlul de la distanță al sistemelor energetice critice
Duqu, Flame și Gauss	2011		SCADA	Duqu – sustragerea de informații utilizând camere web, microfoane, fotografii; Flame – putea trimite informații utilizând Bluetooth și conexiunile USB; Gauss – sustragerea de informații, precum parole, conexiuni de rețea, BIOS etc.
Shamoon	2012	Companii energetice din Arabia Saudită și Qatar	SCADA	Sistemul devenea inoperabil prin suprascrierea datelor
Target Stores	2013	Target Stores	SCADA	Furtul de date de pe cardurile de credit
New York Dam				Exploatarea sistemelor SCADA conectate la Internet cu ajutorul modem-urilor telefoniei celulare
German Steel Mil	2014	Oțelărie germană	SCADA	Obținerea accesului la informațiile oțelăriei
Ukraine Power Grid	2015	Stații electrice	SCADA	Întreruperea curentului electric la 30 de substații și privarea de electricitate pentru șase ore a unui număr de 230.000 de oameni
"Kemuri" Water Company	2016	Companie de apă potabilă	SCADA	Accesarea debitului apei și a sistemelor de tratare chimică modificând modul de tratare al apei
SamSam	2018	Atalanta, Georgia, Departamentul de transport din Colorado	SCADA	Atacul a provocat o întrerupere de mai multe săptămâni a site-ului Atlanta, afectând plățile, acordarea licențelor de afaceri și procesarea amenzilor

Tabelul nr. 1: Principalele atacuri cibernetice asupra infrastructurii critice (Hemsley, Fisher, 2018)

În acest context, principalele instrumente utilizate de către atacatori sunt *malware*-ul (acel *malicious software*) și atacurile *Distributed Denial of Service* (DDoS) capabile de a întârzia, perturba, corupe, exploata, distruge, sustrage sau modifica informațiile folosite în spațiul cibernetic. O posibilă soluție ar fi utilizarea în cadrul protecției infrastructurilor critice a tehnologiilor de tip *cloud computing*, care să ofere redundanță sistemelor și să asigure accesul permanent asupra datelor (Alcaraz și alții, 2011). În această situație, sistemele SCADA care realizează controlul supravegherii și achiziția de date în cazul proceselor industriale (Dan-Șuteu și Gânsac, 2020, 356) pot fi afectate în urma unui atac, dacă nu există un alt sistem în *cloud* care să utilizeze protocolul ICCP și infrastructura cloud pentru interogarea și transmiterea informațiilor esențiale operării sistemului.

Un alt element important în realizarea protecției infrastructurilor critice din punct de vedere al securității cibernetice îl reprezintă conectivitatea *wireless*, care oferă o mobilitate mult mai mare infrastructurii (Alcaraz și Zeadally, 2015, 57). Prin urmare, tot mai utilizate sunt rețelele de tip *Wireless Personal Area Network* (WPANs), întrucât acestea dispun de o amprentă mică zonală, cu toate că pot apărea întârzieri de transmitere de date sau interferențe radio care pot afecta volumul și viteza de transmitere a datelor.

Cu toate acestea, factorul uman rămâne elementul esențial în cadrul procesului de reziliență a infrastructurilor critice, deși evoluția tehnologică căpătă valențe tot mai însemnate (Lehaci, 2015, 348). Astfel, ținând cont de această evoluție tehnologică și de complexitatea evenimentelor din mediul de securitate, crizele actuale pot fi evitate, diminuate ca impact sau soluționate printr-o atitudine proactivă (Petrescu, 2017, 45) a factorilor umani și prin dezvoltarea de politici și strategii solide ale actorilor statali.

Concluzii

Amenințările hibride au fost utilizate încă din cele mai vechi timpuri, însă diferența majoră dintre acestea și cele utilizate în zilele noastre constă în faptul că actorii de azi apelează la acestea din urmă doar pentru că sunt mai eficiente și nu pentru că ar fi nevoiți. Analiza atacurilor hibride asupra infrastructurilor critice a reliefat faptul cele mai multe dintre acestea se petrec în spațiul cibernetic, întrucât sunt mai puțin costisitoare decât alte tipuri de atacuri, implică un număr diminuat de personal, costuri mai mici și o expunere redusă a atacatorilor. Astfel, un simplu atac asupra elementelor componente prezentate în cadrul modelului conceptual de interconectare a sistemelor deschise al Organizației Internaționale pentru Standardizare poate produce efecte de nivel strategic asupra infrastructurii critice atacate. Altfel spus, atacul asupra unei simple rețele *wireless*, a unui calculator sau unui panou de control industrial al unei infrastructuri critice poate produce consecințe majore asupra acestora și poate duce la indisponibilitatea asigurării serviciilor esențiale pentru populație, precum apă potabilă, electricitate, gaze naturale etc.

Mai mult, analizând conceptul de război hibrid și de amenințare hibridă, am constatat faptul că atacurile cibernetice reprezintă un mijloc la care apelează actorii statali și non-statali, în contextul utilizării tehnicilor și tacticilor de război hibrid asupra unui poten-

țial adversar. În aceste condiții, o modalitate eficientă de a dezvolta reziliența infrastructurilor critice pentru contracararea atacurilor cibernetice poate fi realizată cu ajutorul centrelor de securitate (SOC) în domeniul cibernetic (Murphy, Hoffman și Schaub, 2016, 28), construite în parteneriat public-privat, întrucât micile vulnerabilitățile din spațiul cibernetic pot produce efecte de nivel strategic asupra tuturor infrastructurilor critice.

În ziua de astăzi, aproape că nu există lucrător în cadrul unei infrastructuri critice care să nu opereze cu tehnică de calcul sau cu diferite dispozitive electronice. În acest context, odată cu implementarea digitalizării în cadrul societății, fiecare om a devenit un senzor și, în același timp, o potențială verigă sensibilă în cadrul procesului de protecție a infrastructurilor critice. Astfel, pentru diminuarea vulnerabilităților din spațiul cibernetic este necesară crearea unei culturi de securitate la nivelul fiecărui cetățean, cultură care să contribuie la creșterea rezilienței infrastructurilor critice. Acest deziderat poate fi realizat prin dezvoltarea de programe educaționale, începând cu programele de studii de nivel liceal și continuând cu cele de licență și master, care să creeze competențe profesionale și să explice legăturile de cauzalitate dintre vulnerabilitățile din spațiul cibernetic, mijloacele de tip hibrid utilizate și efectele dorite de către actorii statali și non-statali care apelează la astfel de metode, precum și prin atragerea de investiții în zona securității cibernetice.

Este de așteptat ca în viitorul apropiat, odată cu dezvoltarea inteligenței artificiale și a noilor tehnologii disruptive, atacurile din spațiul cibernetic să sporească atât din punct de vedere al intensității, cât și al numărului acestora. În această nouă normalitate, domeniul securității cibernetice va avea un rol deosebit de important în cadrul protecției infrastructurilor critice pentru asigurarea serviciilor esențiale populației.

Bibliografie:

Alcaraz, Cristina, Sherali Zeadally. January 2015. “Critical Infrastructure Protection: Requirements and Challenges for the 21st Century.” *International Journal of Critical Infrastructure Protection*, 8: 53-66.

Alcaraz, Cristina, Sherali Zeadally. October 2013. “Critical Control System Protection in the 21st Century.” *Computer*, 46(10): 74-83.

Alcaraz, Cristina, Javier Lopez. December 2012. “Analysis of Requirements for Critical Control Systems.” *International Journal of Critical Infrastructure Protection*, 5(3-4): 137-45.

Alcaraz, Cristina, Isaac Agudo, David Nunez, Javier Lopez. 2011. “Managing Incidents in Smart Grids à la Cloud.” *IEEE Third International Conference on Cloud Computing Technology and Science*, November-December 2011, Athens, Greece, 527-31.

Aradau, Claudia. October 2010. “Security That Matters: Critical Infrastructure and Objects of Protection.” *Security Dialogue*, 41(5): 491-514.

Bănănăreanu, Cristian. 2015. “The Evolution of Warfare from Classic to Hybrid Actions.” *Strategic Impact*, 2: 57-66.

Bendisch, Uwe, Sandro Bologna, Gwendal Le Grand, Eric Luiijf. 2008. “Towards a European Research Agenda for CIIP: Results from the CI2RCO Project.” *Critical Information Infrastructures Security*, Second International Workshop, Javier Lopez, Bernhard Hämmerli (eds.), October 2007, Málaga, Spain,1-12.

Bessani, Alysson Neves, Paulo Sousa, Miguel Correia, Nuno Ferreira Neves și Paulo Veríssimo. November-December 2008. “The Crutial Way of Critical Infrastructure Protection.” *IEEE Security & Privacy*, 6(6): 44-51.

Cavelty, Myriam Dunn. 2016. “Cyber-Security.” *Contemporary Security Studies*, Alan Collins (ed.), Fourth Edition, Oxford University Press, 400-16.

Dan-Șuteu, Stefan-Antonio, Victor Gânsac. 2020. “Platform for Simulating Cyber Resilience of Critical Industrial Infrastructures – ICS-SCADA.” *International Scientific Conference “Strategies XXI”* (Technologies - Military Applications, Simulation and Resources), “Carol I” National Defence University, May 2020, Bucharest, Romania, 16: 356-60.

Giannopoulos, Georgios, Roberto Filippini, Muriel Schimmer. 2012. *Risk Assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. Scientific and Technical Research series. Joint Research Centre, Institute for the Protection and Security of the Citizen. Luxembourg: Publications Office of the European Union.

Gimiga, Silviu-Iulian, Cristian-Octavian Stanciu. 2022. “Transformations determined by the emergence of new technologies in the military field.” *International Scientific Conference “Strategies XXI”* (Technologies, Military Applications, Simulations and Cyberspace), “Carol I” National Defence University, June 2022, Bucharest, Romania, 18(1): 506-16.

Hemsley, Kevin E., Dr. Ronald E. Fisher. December 2018. *History of Industrial Control System Cyber Incidents*. Idaho National Laboratory, U.S. Department of Energy National Laboratory.

Hoffman, Frank G. 2016. “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War.” *2016 Index of U.S. Military Strength*, Dakota L. Wood (ed.), The Heritage Foundation, Washington, DC, 25-37.

Lehaci, Niculai-Tudorel. 2015. “Remarks regarding the evolution of the doctrinal command and control systems post-cold war.” *International*

Scientific Conference "Strategies XXI" (Technologies - Military Applications, Simulation and Resources), "Carol I" National Defence University, November 2015, Bucharest, Romania, 11(2): 348-53.

Merabti, Madjid, Michael Kennedy, William Hurst. 2011. "Critical Infrastructure Protection: A 21st Century Challenge." *International Conference on Communications and Information Technology*, March 2011, Aqaba, Jordan, 1-6.

Murphy, Martin, Frank G. Hoffman, Gary Schaub, Jr. November 2016. *Hybrid Maritime Warfare and the Baltic Sea Region*. The Centre for Military Studies, Department of Political Science, University of Copenhagen.

Pătrașcu, Petrișor. 2021. "Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructures Protection and Defence Sector." The Land Forces Academy Review, 26(4): 423-29.

Petrescu, Dan-Lucian. 2017. "Advanced Model for Configuring Hybrid Aggression." *Strategic Impact*, 2: 45-51.

Steingartner, William, Darko Galinec, Andrija Kozina. April 2021. "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model." *Symmetry*, 13(4): 597.

Steven M. Rinaldi, James P. Peerenboom, Kelly, Terrence K. December 2001. "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies." *IEEE Control System Magazine*, 21(6): 11-25.

Șușnea, Elena. 2018. "A Real-Time Social Media Monitoring System as an Open Source Intelligence (OSINT) Platform for Early Warning in Crisis Situations." *International Conference Knowledge-Based Organization*, June 2018, Sibiu, Romania, 24(2): 427-31.

Wells, John S. G. September 2022. "Preparing for Hybrid Warfare and Cyberattacks on Health Services' Digital Infrastructure: What Nurse Managers Need to Know." *Journal of Nursing Management*, 30(6): 2000-4.

Cloudflare. 2023. https://www.cloudflare.com.

Connected Papers. 2023. https://www.connectedpapers.com.

SCADA International. 2023. https://scada-international.com.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 439/28.06.2023

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro