ELENA LAZĂR
NICOLAE DRAGOȘ COSTESCU

DREPTUL EUROPEAN AL INTERNETULUI

Editura Hamangiu
2021

Capitolul 6.
Operațiunile cibernetice și legislația privind securitatea cibernetică în UE

Secțiunea 1. Noțiuni introductive

Acest capitol analizează potențialele implicații ale acestor operațiuni/atacuri informatice asupra securității cibernetice, prezentând totodată cadrul legislativ al UE în materie de securitate cibernetică și principalii actori în combaterea criminalității informatice. Odată cu utilizarea tot mai intensă a tehnologiei în viața de zi cu zi, de la calculatoare personale la telefoane mobile, comerț electronic, etc., necesitatea de a proteja infrastructura electronică interconectată împotriva utilizării rău intenționate devine o problemă din ce în ce mai stringentă. Mai mult, societatea, în ansamblul ei, continuă să se bazeze pe sistemele computerizate în aproape toate domeniile vieții sociale, controlul traficului aerian, al trenurilor și metrourilor, coordonarea serviciului medical sau al securității naționale, sistemele de purificare a apei, de unde rezultă nevoia de a asigura o protecție sporită împotriva unor potențiale atacuri cibernetice. Securitatea cibernetică se ocupă de această nevoie.

„Securitatea cibernetică" abordează doar riscurile originare din „spațiul cibernetic"? „Securitatea cibernetică" are în vedere numai protecția activelor virtuale din interiorul „spațiului cibernetic"? „Securitatea cibernetică" se aplică și activelor fizice, cum ar fi sistemele de control industrial, linii de producție, centrale electrice etc.? Acestea sunt întrebările la care vom încerca să răspundem în prezentul capitol, în vederea asigurării unei înțelegeri adecvate a termenului „securitate cibernetică.

De asemenea un alt scop al acestui document este de a prezenta organizațiile care participă la standardizarea și asigurarea unui cadru normativ în domeniul securității cibernetice, oferind o prezentare generală a activităților acestora.

Securitatea cibernetică poate fi definită[1], la modul general, drept activitățile necesare pentru a proteja rețeaua și sistemele de informații,

[1] Definition of Cybersecurity Gaps and overlaps in standardization, ENISA guide, 2015.

utilizatorii acestora și persoanele afectate de amenințările cibernetice. „Amenințare cibernetică" reprezintă orice circumstanță sau eveniment potențial care poate afecta negativ rețeaua și sistemele de informații și utilizatorii acestora[1] sau altfel spus, un mijloc prin care o persoană/grup de persoane (cu rele intenții) **profită de vulnerabilitățile** existente pe un anumit sistem (server, calculator, echipament de rețea, aplicație etc.)

Aceste amenințări cibernetice au afectat până în prezent societatea civilă, computerele personale fiind de regulă ținta principală. Progresele realizate de literatura de specialitate în acest domeniu și diseminarea corectă a acesteia către public s-ar putea dovedi valoroase pentru o mai bună înțelegere a amenințărilor și a protecției oferite de dreptul european și internațional împotriva acestor amenințări.

Certitudinea asupra regulilor aplicabile, înțelegerea acestora și condițiile în care acestea se aplică operațiunilor cibernetice pot fi favorabile unui punct de plecare pentru o percepție uniformă a unui domeniu controversat. Așa cum vom arăta, terminologia din domeniul cibernetic este una foarte diversă[2]. Au existat mai multe cazuri în care jurnalele sau *site*-urile de știri au semnalat apariția a ceea ce au considerat a fi atacuri cibernetice. Cu toate acestea, mijloacele utilizate, contextul în care au fost realizate și efectele lor au diferit. Înainte de a încerca să abordăm aceste incidente dintr-o perspectivă strict juridică, capitolul se dedică și înțelegerii operațiunilor cibernetice în sensul lor tehnic, analizând unele dintre incidentele relevante care au avut loc în lumea reală, cu scopul de a ilustra efectele operațiunilor cibernetice, inclusiv cu exemple din viața reală.

Secțiunea a 2-a. Tipologia operațiunilor cibernetice

Malware-ul (*malicious software*) reprezintă un software rău intenționat, respectiv un program de computer destinat acțiunilor ostile împotriva

[1] US Navy, US Marine Corps, US Coast Guard, *The Commander's Handbook on the Law of Naval Operations*, July 2007, p. 8-17, UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, Oxford University Press, 2004, p. 118.

[2] E. LAZĂR, D. COSTESCU, *Los ciberataques: una noción sin tipificación, pero con un futuro, Anuario de Derecho Internacional*, p. 157-175, vol. 22/2018, http://revistas.udc.es/index.php/afd/issue/view/afdudc.2018.22.0.

sistemului pe care se găsește (*software* malitios care vrea sa ne fure, distrugă sau corupă datele stocate pe dispozitivele noastre). Termenul are o semnificație generică destinată să acopere diferite tipuri de *software* ostile, cum ar fi viruși, viermi, troieni, bombe logice, *software* de administrare la distanță, *rootkit*-uri, *spyware* sau *ransomeware*[1]. Clasificarea acestor tipuri de malware se bazează pe criterii tehnice ale modului în care funcționează/operează fiecare.

Pe scurt, virușii sunt programe *software* care se reproduc în momentul execuției, ceea ce înseamnă că necesită activarea interacțiunii umane[2]. Virușii au impact negativ asupra datelor și integrității computerului.

Viermii (*worms*)[3]sunt coduri rău intenționate care se reproduc de la sine, o formă de *malware* care odată ce infectează un dispozitiv (PC, laptop, server etc.) va face tot posibilul să se extindă și să infecteze altele din rețea. Ele sunt, de asemenea, destinate distrugerii datelor sau pur și simplu consumă resursele rețelei. Astfel un *worm* reușește să **încetinească** *device*-urile conectate la rețea (prin consumul de resurse CPU și RAM), astfel chiar și rețeaua, calculatoarele infectate generând un consum anormal de trafic.

Un cal troian[4] reprezintă un tip de virus care acționează ca un cod legitim pentru a evita detectarea, practic constituie un program conceput să pară în folosul celui care îl utilizează, dar în spatele căruia se regăsește un cod maliții os care are cu totul alte intenții. Spre deosebire de viruși, troienii nu se înmulțesc, nu infectează alte fișiere și nu produc nici copii.

O bombă logică[5] este, de asemenea, un tip de cod rău intenționat care se activează la îndeplinirea anumitor condiții, de exemplu, detectarea anumitor tipuri de sisteme de operare.

---

[1] R. Moir, *Defining Malware: FAQ*, Microsoft, 2003, answer to question 1, disponibil la https://technet.microsoft.com/en-us/library/dd632948.aspx, accesat la 12 martie 2019.

[2] C.D. De Luca, *The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors*, Pace International Law Review Online Companion, Vol. 3, 2013, p. 282.

[3] *Ibidem.*

[4] J. Andress, S. Winterfield, *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners*, Syngress, 2011, p. 32-33.

[5] *Ibidem*.

Un software de administrare la distanță[1] (în versiunea sa rău intenționată cunoscut sub numele de troian de acces la distanță, RAT pe scurt) este un program în aparența legitim care permite unui operator să controleze un sistem fără a avea acces fizic la acesta.

Ransmoware[2] reprezintă un tip de *malware* care criptează datele utilizatorului și le va elibera doar în schimbul unei plăți.

Spyware-ul[3] caută de obicei informații specifice din sistem, reprezentând un program conceput cu scopul de a extrage anumite date de la utilizatori. Acesta nu are ca scop să îngreuneze (prin consumul de resurse) sau să afecteze în vreun fel victima, ci pur și simplu să extragă date și sa le trimită către „serverele mama" (cele care au inițiat „spionajul").

Deși atacurile cibernetice pot, în anumite situații, să fie efectuate fără utilizarea *malware*-ului, în majoritatea cazurilor au fost utilizate diferite forme de *software* ostil. Următoarele vor prezenta câteva dintre modalitățile prin care se desfășoară aceste atacuri, recurgând la *malware*.

Refuzul de serviciu (cunoscut în mod obișnuit ca DoS[4],[5]) constituie o formă de atac cibernetic ce implică utilizarea computerelor pentru a efectua apeluri în mod repetat (adică a trimite mesaje, solicitări, solicitări etc.) pe ținte (adică computere, rețele, *site*-uri *web* etc.) până când le copleșește. DoS-ul are astfel loc prin trimiterea a unui număr impresionant de trafic către un serviciu „*targhetat*" cu scopul de a-l întrerupe. Primind foarte multe cereri, un *server web*, spre exemplu, nu ar face față și s-ar „bloca" pe moment. Practic, aceste atacuri sunt concepute pentru a duce la o prăbușire a rețelei de date a unei companii sau a unui *site* de comerț electronic prin bombardarea acesteia cu un volum mare de trafic de date, ca și cum mii de oameni ar fi apelat în mod repetat același număr de telefon cu intenția de a-l ține ocupat.

---

[1] How to protect yourself against Remote Access Trojans and other malware | Europol (europa.eu), accesat la data de 20 noiembrie 2020.

[2] S. Mehmood, *Enterprise Survival Guide for Ransomware Attacks*, SANS Institute InfoSec Reading Room, 2016, disponibil la at https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962.

[3] *What is spyware? And how to remove it (norton.com)*, accesat la data de 20 noiembrie 2020.

[4] O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, *The Law of Cyber-Attack*, California Law Review, 2012, p. 22, disponibil la http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf.

[5] C.D. DeLuca, *op. cit*., p. 282-283.

Deoarece ținta poate procesa doar o anumită cantitate de apeluri simultan, atunci când un atacator trimite o cantitate exorbitantă de cereri de date, *server*-ul nu va putea răspunde, interzicând astfel accesul la acel *server*, computer, rețea sau *site*-ul *web*. Așa cum este ilustrat de un autor *„[tot] ce trebuie să facă „soldatul" cibernetic (este – n.n.) să seteze pagina să se actualizeze automat la fiecare trei până la cinci secunde și de atunci browser-ul va continua să trimită mii de interogări pe site-urile web […], ajutând să le suprasolicite și să le doboare*[1]".

O formă mai severă de DoS[2] este *Refuzul de serviciu Distribuit* (sau DDoS), care folosește un număr mare de computere pentru a cauza închiderea mai multor ținte. DDoS-ul **are loc** așadar prin intermediul mai multor **calculatoare infectate** cu *malware* care trimit un număr impresionant de Gbps în trafic. Aceste calculatoare se regăsesc în **întreaga lume** și nu au o locație specifică, acesta fiind unul dintre motive pentru care DDoS este foarte greu de identificat și combătut. O astfel de rețea de calculatoare infectate cu *malware* mai poartă și denumirea de *Botnet*. Angajarea DoS sau DDoS se face deci prin utilizarea coordonată a ceea ce este cunoscut sub numele de computere *zombie*, adică computere care au fost deturnate de la proprietarul lor folosind troieni cu acces la distanță. Aceste RAT sunt plantate în bombe logice trimise spre exemplu ca atașamente la conturi de *e-mail* aleatorii și sunt activate atunci când utilizatorii le deschid.

Efectele indirecte ale unor astfel de operațiuni pot varia de la simple neplăceri, atunci când vizează, de exemplu, *browsere web* sau servere de mail, la distrugerea proprietății sau pierderea de vieți omenești, atunci când vizează, de exemplu, sisteme de control al traficului aerian[3], astfel că răspunsul nostru la întrebarea adresată la începutul prezentului capitol este da, securitatea cibernetică se aplică și activelor fizice. Un atac cibernetic care oprește efectiv transmiterea informațiilor prin Internet ar putea doar să incomodeze populația, dar ar putea avea și mai multe consecințe. De exemplu, ar putea determina spitalele să nu poată comunica informații

[1] L. SWANSON, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, Loyola of Los Angeles International and Comparative Law Review Vol. 32, 2010, p. 319.

[2] O.A. HATHAWAY ș.a., *op. cit.*

[3] R. OTTIS, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, International Journal of Cyber Warfare and Terrorism, 2011, p. 2.

vitale, ceea ce duce la pierderea de vieți omenești sau ar putea conduce chiar la prăbușirea unui avion.

Oare toate atacurile cibernetice au aceeași amploare, aceleași efecte? Cum le putem deosebi de alte acțiuni cibernetice precum *cybercrime*? În acest sens vom aborda pe rând noțiunile de *cyber crime* (infracțiuni informatice), *cyber attack* (atac cibernetic) *cyber terrorism* (terorism cibernetic), și *cyber warfare* (război cibernetic).

În ceea ce privește noțiunea de *cybercrime,* nu există o definiție universal acceptată a criminalității informatice (*cyber crimes*). *Convenția de la Budapesta privind Criminalitatea Informatică*[1] nu oferă nici ea o definiție a acestei noțiuni, mulțumindu-se doar cu a enumera categoriile de infracțiuni informatice ce îi fac obiectul.

Europol (2018)[2] a făcut următoarea distincție în cadrul conceptului de *cyber crimes*, respectiv infracțiuni obiect: care pot fi comise doar asupra unor computere, rețele de calculator sau altor forme de tehnologie informațională, obiectivul fiind chiar atingerea funcționalității/integrității unui sistem/calculator/bază de date; și infracțiuni instrument (adică, crime tradiționale facilitate de internet și tehnologii digitale).

În ceea ce privește noțiunea de *cyber attack*[3] o definiție regăsim în lexiconul publicat în 2011, în cadru Comandamentului cibernetic al Statelor Unite, pentru utilizare militară în operațiunile cibernetice, care includea prima definire militară oficială a atacului cibernetic. respectiv: *Un act ostil folosind calculatoarele sau rețelele sau sistemele conexe, destinat să perturbe și/sau să distrugă sistemele, activele sau funcțiile cibernetice critice ale unui adversar*. Apreciem că această definiție, deși în aparență una complexă, se dovedește a fi neclară, netrasând o graniță clară între ceea ce ar putea constitui *cybercrime* și ceea ce ar putea constitui un *cyberattack*.

În acest sens, în cadrul prezentei lucrări înțelegem să adoptăm o definiție restrânsă a atacului cibernetic, una menită să concentreze atenția asupra amenințării unice pe care o reprezintă tehnologiile cibernetice: astfel, un atac cibernetic constă în orice acțiune întreprinsă pentru a submina funcțiile

[1] Convenția Consiliului Europei privind criminalitatea informatică – Budapesta, 23 noiembrie 2001– ETS nr. 185.

[2] Cybercrime | Crime areas | Europol (europa.eu), accesat la 13 ianuarie 2020.

[3] GEN. J.E. CARTWRIGHT, *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations* 5, Noiembrie 2011.

unei rețele de calculatoare/sistem informațional în scop politic sau scopuri legate de securitatea și siguranța națională.

Un scop politic sau de securitate națională distinge atacul cibernetic de criminalitatea cibernetică simplă. Astfel, pentru a trasa o linie între cele două noțiuni, o infracțiune cibernetică care nu este realizată în scopurile prezentate mai sus, cum este, de altfel, cazul celor mai multe fraude pe Internet, precum furtul de identitate și piraterie de proprietate intelectuală, nu se încadrează acestui element final al scopului unui „atac cibernetic" și reprezintă, prin urmare, o simplă *cybercrime*.

Mergând mai departe, ne oprim asupra noțiunii de „*cyber terrorism*". În acest sens apreciem că internetul și computerele pot fi utilizate în scopuri legate de terorism, cum ar fi răspândirea „*propagandei (inclusiv recrutarea, radicalizarea și instigarea la terorism); finanțarea [terorismului]; formarea [teroristului]; planificarea [atacurilor teroriste] (inclusiv prin comunicare secretă și informații cu sursă deschisă); executarea [atacurilor teroriste] și atacurile cibernetice*"[1].

La fel cum nu există un consens cu privire la o definiție a criminalității informatice, nu putem vorbi nici în cazul *cyber* terorismului de o definiție universal și unanim acceptată. Mai mult, nu există în prezent nici măcar un consens asupra definiției noțiunii de terorism în dreptul internațional clasic, ci doar trimiteri în mai multe convenții asupra a ceea ce ar putea constitui fapte de terorism.

Totuși, în încercarea de a defini această noțiune, ne vom raporta la definiția acceptată și utilizată de FBI[2] – „*atacul premeditat, motivat politic, împotriva informațiilor, sistemelor de calculatoare, programelor și operărilor de date, ce conduce la violențe împotriva obiectivelor civile și necombatanților, atac exercitat de grupări subnaționale sau agenți clandestini*". Putem observa din definiție că, în acest caz, terorismul cibernetic poate fi atribuit doar unor entități private, particulari, iar nu unor entități statale.

Cyberwarfare este utilizat pentru a descrie acele atacuri cibernetice care compromit și perturbă sistemele de infrastructură critice, atacuri ce constituie un atac armat. Doar guvernele, organele statului sau grupurile conduse/direcționate sau sponsorizate de stat se pot angaja în *cyberwarfare*,

[1] UNODC, The use of internet for terrorist purposes, 2012, p. 3, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, accesată 28 ianuarie 2020.

[2] http://www.crime-research.org/articles/cyber_terrorism_new_kind_terrorism/, accesat 18 ianuarie 2020.

acesta reprezentând un act al statului, spre deosebire de *cyber terrorism*. Conceptul de *cyberwarfare* și regulile aplicabile în această situație au fost abordate de Manualul Tallinn 1.0 privind Dreptul Internațional aplicabil în războiul cibernetic (2013)[1].

În ultimii ani, organizații și chiar instituții ale statelor, se confruntă din ce în ce mai des cu amenințări informatice, securitatea cibernetică devenind o preocupare la nivel mondial. Astfel, *WannaCry*[2] (*ransomware* reprezentând, așa cum arătam mai sus, un *malware* al cărui scop este acela de a împiedica accesul victimelor la fișiere, sau chiar la întregul sistem informatic infectat, până la plata unei sume de bani cu titlu de răscumpărare) a generat, în luna mai 2017, disfuncții în funcționarea spitalelor aparținând *National Health Service* din Marea Britanie, cauzând probleme multor pacienți britanici. O lună mai târziu, un *malware* de tip *ransomware*, cunoscut sub numele *NotPetya*[3], creat cu o tehnologie mai avansată decât *WannaCry*, a afectat rețele informaționale din mai multă state, inclusiv companiile Merck, din SUA, Maersk din Danemarca, sau Rosnoft, din Federația Rusă, dar mai ales serviciile energetice, de transport și bancare din Ucraina.

Mergând un pas și mai în spate în timp, virusul *Stuxnet* a infectat în 2010 un program Siemens de control al automatelor industriale folosite în sectorul apelor, al platformelor petroliere și centralelor electrice, funcția sa fiind să modifice administrarea anumitor activități și funcții astfel încât să determine distrugerea fizică a instalațiilor. *Stuxnet* a afectat, în special, statul Iran, respectiv centrifugele iraniene ce produc uraniu îmbogățit. Actori importanți din presa internațională, ca The Guardian, BBC și The New York Times[4] au emis speculații cum că numai o țară ar fi putut produce un virus de complexitate, țară precum Israel, care, după cum se știe, nu se afla în relații deloc bune cu Iranul.

Întorcându-ne la definițiile prezentate anterior și calificarea operațiunilor cibernetice în *cyber crimes, cyber attacks, cyber terrorism și cyber warfare*, ne întrebăm în care din aceste noțiuni am putea încadra atacul *Stuxnet, Wannacry* sau *NotPetya*?

---

[1] 356296245.pdf (peacepalacelibrary.nl), accesat la 18 ianuarie 2020.

[2] *Ransomware WannaCry: All you need to know | Kaspersky*, accesat la data de 12 aprilie 2020.

[3] *NotPetya malware attack: Chaos but not cyber warfare | ZDNet*, accesat la data de 12 aprilie 2020.

[4] *What Is Stuxnet? | McAfee*, accesat la data de 14 mai 2020.

Impactul *NotPetya* sau *Stuxnet*, deși resimțite în întreaga lume, cu pagube considerabile, suspectate a fi opera unor state (despre *NotPetya* au existat presupuneri că ar fi reprezentat opera Rusiei, iar *Stuxnet* a Israelului), apreciem că nu depășesc un anumit prag cerut pentru a putea fi clasificate drept acte de război cibernetic (*cyberwarfare*). Având în vedere că principalul scop urmărit și efectul a fost subminarea economiei, iar scopul acestor *malware* nu a fost de constrângere sau cucerire, suntem de părere că acestea pot fi încadrate noțiunii de atac cibernetic (*cyberattack*). De asemenea, am putea spune că scopul politic urmărit de aceste *malaware* le disting de simple infracțiuni informatice.

Totuși nu putem nega faptul că *Stuxnet* nu a reprezentat un simplu atac cibernetic, ținând cont că a fost atacată infrastructura critică a unei țări (sistemul energetic al Iranului), existând inclusiv avarii fizice și, deși nu și-a atins ținta – distrugerea completă a instalațiilor nucleare, acesta a întârziat semnificativ programul nuclear al Teheranului.

Secțiunea a 3-a. Interesul UE față de securitatea cibernetică – legislația și principalii actori în domeniu

§ 1. Noțiune

În discursul său anual privind starea Uniunii din 2017, președintele Comisiei Europene, Jean-Claude Juncker, a declarat: „*În ultimii trei ani, am făcut progrese în ce privește menținerea siguranței europenilor în mediul online. Dar Europa nu este încă bine echipată când vine vorba de atacuri cibernetice. De aceea, astăzi, Comisia propune noi instrumente, inclusiv o Agenție Europeană pentru Securitatea Cibernetică, care să ne ajute să ne apărăm împotriva unor astfel de atacuri*”[1]. Justificarea din spatele inițiativelor legislative ale Uniunii Europene (UE) este, în practică, imprimată în Strategia de Securitate Cibernetică a Uniunii Europene, unde se afirmă că: „*Libertatea și prosperitatea noastră depind din ce în ce mai mult de un Internet robust și inovator, care va continua să înflorească dacă inovația sectorului privat și societatea civilă îi susțin creșterea. Dar libertatea online*

[1] *State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks (europa.eu)*, accesat la data de 18 ianuarie 2020.