MINISTERUL ADMINISTRAȚIEI ȘI INTERNELOR
ACADEMIA DE POLIȚIE ”ALEXANDRU IOAN CUZA”

TEZĂ DE DOCTORAT

ÎN DOMENIUL
”ORDINE PUBLICĂ ȘI SIGURANȚĂ NAȚIONALĂ”

CRIMINALITATEA INFORMATICĂ – FACTOR DE RISC MAJOR PENTRU ORDINEA PUBLICĂ ȘI SIGURANȚA NAȚIONALĂ

CONDUCĂTOR DE DOCTORAT
PROF.UNIV.DR.
ȚUȚU PIȘLEAG

DOCTORAND
COROIU VIOREL

BUCUREȘTI
2011

Cuprins

ABREVIERI

AR – Analiza de risc

CERT – Computer Emergency Response Team

DCCO – Direcția de Combatere a Crimei Organizate

DIICOT - Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism

DOS – Denial of Service

DNS – Domain Name System

EGC – European Government CERT

HDD – Hard Disk Drive

IGPR – Inspectoratul General al Poliției Române

IGPR-IC – Institutul de Criminalistică din cadrul IGPR

ISO – International Standard Organization

IR – Infrared

IT – Tehnologia Informației

MAI – Ministerul Administraţiei şi Internelor

NIST – National Institute of Standards and Technology

RFS – Remote Forensic Software

SIE – Serviciul de Informații Externe

SIM – Subscriber Identity Module

SMS – Short Message Service

SRI – Serviciul Român de Informații

SSL – Secure Socket Layer

TIC – tehnologia informației și comunicațiilor

UE - Uniunea Europeană

URL – Uniform Resource Locator

VPN – virtual private network

WEB –World Wide Web, rețeaua mondială

Introducere

Lumea de astăzi,presupune o modalitate de trai şi de a lucra într-o lume de conectivitate la nivel mondial. Putem face schimb de conversaţie sau putem realiza tranzacţii de milioane de dolari tranzacţii monetare cu oamenii de pe partea cealalta a planetei rapid şi ieftin. Proliferarea de calculatoare personale, acces facil la Internet, precum şi o piaţă în plină expansiune pentru noile dispozitive de comunicare ne-au schimbat modul în care ne petrecem timpul liber şi modul în care facem afaceri.

Totodată această evoluţie, rapidă şi radicală, ridică o serie de probleme de ordin socioeconomic sau juridic, şi chiar în sectorul activităţii criminale - calculatorul deschizând posibilitatea unor acţiuni ilegale cu un caracter înalt sofisticat sau la săvârşirea unor infracţiuni clasice cum este furtul sau frauda.

Toate aceste acţiuni ilegale au făcut să apară necesitatea ocrotirii valorilor sociale tradiţionale împotriva atacurilor ilicite prin intermediul calculatoarelor, susceptibile să producă pagube economice semnificative. Deoarece dreptul tradiţional a devenit insuficient, neputând acoperi noile probleme, devine obligatorie modificarea normativului existent sau crearea unor noi categorii de infracţiuni, dacă alte măsuri se dovedesc nesatisfăcătoare.

Modalităţile în care criminalii comit infracţiuni sunt, de asemenea în continuă schimbare. Accesibilitatea digitală universală deschide noi oportunităţi pentru cei lipsiţi de scrupule. Milioane de dolari sunt pierdute de către ambele părți, întreprinderi şi consumatori datorită activității criminale. Mai rău, computere şi reţele pot fi folosit pentru a hartui victime sau pentru atacuri violente, Acestea pot să coordoneze şi să desfăşoare activităţi teroriste care ne ameninţă pe noi toţi.

Din păcate, în multe cazuri, agenţiile de aplicare a legii au rămas în spatele acestor criminali, lipsite de tehnologie şi personal calificat pentru a

aborda această ameninţare nouă şi în creştere, care a fost numită criminalitate informatică.

Chiar dacă interesul şi gradul de conştientizare a fenomenului criminalităţii informatice au crescut în ultimii ani, tehnologia informaţiei (IT) şi ofiţerii de poliţie au dus lipsă de instrumentele şi expertiza necesare pentru a rezolva problema. Pentru a îmbunătăți lucrurile, legile vechi, care nu se potrivesc destul de bine crimelor de acest gen au fost abrogate sau modificate, fiind angajate, noi legi destul de prinse în realitate.

În plus, dezbaterile asupra unor probleme de confidenţialitate îngreunează capacitatea agenţilor de executare pentru a aduna probele necesare pentru a urmări aceste cazuri noi. Nu în cele din urmă, a existat și o anumită cantitate de antipatie, sau cel puţin, neîncrede între cei doi dintre cei mai importanți jucători în orice luptă eficientă împotriva criminalităţii informatice: agenţii de aplicare a legii şi profesioniştii în calculator.

Cu toate acestea, o cooperare strânsă între cele două este crucială dacă dorim să se controleze problema criminalităţii informatice şi să se facă din internet un sistem în condiţii de siguranţă, plăcut, pentru utilizatorii săi. Personalul de aplicare a legii înţelege mentalitatea penală şi cunoaște elementele de bază de colectare a dovezilor şi aducerea infractorilor în faţa justiţiei.

Personalul IT înţelege calculatoarele şi reţelele, cum lucrează, şi cum se pot urmări în jos informaţii cu privire la acestea. Fiecare are jumătate din cheia de la înfrângerea cybercriminalității.

Criminalitatea cibernetică, se referă la infracţiunile comise prin intermediul internetului sau un alt reţea de calculatoare ca o componentă a crimei.

Deasemenea evoluţia fenomenului terorist în întreaga lume a demonstrat faptul că, de cele mai multe ori activitatea infracţională a fost pregătită şi realizată cu ajutorul calculatorului. Cu ajutorul acestei tehnici

moderne şi pe bună dreptate, se produc sume mari de bani care alimentează actele teroriste, se transferă sume mari de bani fără a fi contabilizate sau urmărite de autorităţi, bani care asigură costurile activităţilor teroriste de orice natură.

Activitatea ilicită desfăşurată pe calculator aduce atingere nu numai indivizilor, ca şi componenţi ai societăţii ci şi societăţii în ansamblu. Atinge grav sub diferite forme patrimoniul naţional şi chiar securitatea naţională.

Pornind de la aceste aspecte, precum si de la alte considerente sociale manifestate zilnic în viaţa social, prin demersul de cercetare ştiinţifică încercăm să semnalăm importanţa fenomenului nou creat si totodată să lămurim o serie de aspecte ce trebuiesc orientate spre o direcţie benefică societăţii şi dezvoltării acesteia, prezentând totodată o serie de metode şi modalităţi în acest sens.

Domeniul investigat este foarte vast şi într-o continuă mişcare. El prezintă acea specificitate care impune o cercetare din mai multe unghiuri sau laturi. Vom sesiza o latură pur tehnică şi este normal, considerăm noi, deoarece fără progresul tehnic nu am mai fi vorbit astăzi de asemenea riscuri.

Latura legislativă, componentă importantă a activităţii de prevenire şi combatere a fenomenului, se face observată ca o necesitate stringentă, în toate acţiunile organismelor statului cu atribuţii în domeniu. Ca o continuare firească apare latura investigativă ce ţine de prezenţa şi capacitatea organismelor specializate ale statului de drept.

Nu în ultimul rând apare latura umană, ca o prezenţă special necesară. Aici se pune problema participanţilor la activitatea infracţională, a infractorilor, pe de o parte şi participanţii la acţiunile ample de prevenire şi combatere a fenomenului.

Legat de latura umană apare latura instituţională alcătuită bineînţeles din totalitatea instituţiilor şi organismelor, interne, şi internaţionale, care

concură, având la bază o serie întreagă de convenţii şi tratate, la stăpânirea acestei situaţii nou create.

Astfel, teza abordează problematica destul de diversă şi complexă a criminalităţii informatice din prisma pericolului pe care-l crează pentru ordinea socială. Evident, fenomenul este perpetuu şi impune necesitatea cunoaşterii sale în amănunt pentru a putea fi stăpânit, prevenit şi sancţionat corect.

CAPITOLUL I
CRIMINALITATEA INFORMATICĂ – O AMENINȚARE GLOBALĂ ACTUALĂ

În ultimii ani, activitatea infracțională de pe palierul criminalității informatice s-a amplificat. Spre deosebire totuși de anii precedenți, se constată o creștere a atacurilor provenite din statele în curs de dezvoltare. Ultimul raport al Symantec (aprilie 2010) aduce pentru prima dată în atenție un stat care, ca nivel de agresivitate pe linia cybercrime, se situează în top trei, și nu este vorba despre SUA, Germania ori China, ci, paradoxal, despre Brazilia. Nivelul de creștere al amenințărilor informatice din acest stat este atât de alarmant, încât a determinat factorii politici să prioritizeze adoptarea unei noi legislații în acest domeniu[1].

Deși China ocupă detașat primul loc în topul statelor cu cel mai înalt nivel de amenințare în domeniu, studiile efectuate de firma Zscaler au indicat faptul că America de Sud[2], prin Brazilia dar și alte state, constituie un puct fierbinte pe harta lumii în materia surselor de risc de nivel informatic. Dealtfel, continentul american este gazda a nu mai puțin de șapte dintre cele mai periculoase state care găzduiesc servere furnizoare de malware[3].

În ultimii ani, amenințările informatice s-au transformat din fenomene individuale, dobândind caracter organizat. Infractorii cibernetici pot lucra singuri, dar mai ales ca membri ai unui grup extins. Unii acționează ca și mercenari, alții în numele unor interese proprii (altele decât cele financiare, ca de exemplu angajații unor instituții care au acces la informații de nivel înalt).

[1] http://www.fbi.gov/about-us/investigate/cyber/cyber.
[2] http://www.zscaler.com/.
[3]Lubic, Jr., Paul E. "Global Cyber Crime: The Playing Field, The Players – The Perfect Storm." Bill Mullins Tech Thoughts. June 2, 2010

Un aspect de evoluție al fenomenului infracțional în constituie faptul că, raportat la situația din urmă cu câțiva ani, sindicate și carteluri de crimă organizată se implică din ce în ce mai mult în explozia fenomenului criminal-informatic.

Amenințările informatice pot îmbrăca diverse forme. Din ce în ce mai mult se constată faptul că infractorii informatici nu se mai limitează la țintele tradiționale, ci țintesc dincolo de acestea. În acest context, se poate remarca proliferarea unor noi ținte, dar și de noi moduri de operare.

CAPITOLUL II
RAMIFICAȚIILE CRIMINALITĂȚII INFORMATICE ÎN DOMENIUL PROTECȚIEI INFRASTRUCTURII CRITICE

Creșterea, fără precedent, în ultimele decenii, a riscurilor, pericolelor şi amenințărilor la adresa obiectivelor vitale ale statelor şi ale organismelor internaţionale, concomitent cu creşterea numărului şi vulnerabilităţii acestora, a condus la sedimentarea şi statuarea unui nou concept, denumit generic: *infrastructură critică*.

Pe linia tehnologiei informației și comunicațiilor, următoarele elemente pot fi integrate în categoriile așa-zise ”critice”:

-sisteme informatice (desktop, laptop, PDA etc.) care sunt implicate în procesele de acces și/sau control ale unor elemente vitale pentru funcționarea unui proces, sistem, operațiune etc.;

-sisteme informatice (desktop, laptop, PDA etc.) care conțin date esențiale pentru funcționarea unor procese ori operațiuni private ori guvernamentale, dar cu signifianță pentru statul ori regiunea respectivă;

-medii de stocare care înmagazinează date din categoria celor enunțate mai sus;

-sisteme informatice de acces la sistemele de mai sus;

-elemente de interconectare între sistemele de acces enunțate, indiferent de categoria acestora (cabluri, WLAN, Bluetooth, IR etc.);

-elemente de sustenabilitate fizică a funcționării sistemelor informatice, a mediilor de stocare și a elementelor de interconectare (surse de curent, surse de protecție la supratensiune etc.);

-elementele de securizare fizică a accesului la sistemele informatice ori mediile de stocare, precum și la elementele de interconectare;

-elementul uman organizat necesar pentru buna funcționare a mediilor de stocare, a sistemelor informatice și a celorlalte elemente, inclusiv pentru intervenția în caz de necesitate;

-programele informatice necesare pentru buna funcționare a oricărui element prezentat anterior;

-elementele de securitate virtuală în legătură cu cele de mai sus ș.a.

CAPITOLUL III
LEGISLAȚIA DIN DOMENIUL CRIMINALITĂȚII INFORMATICE

Până la a se ajunge la actualul stadiu legislativ, legislaţia existentă la nivelul structurilor statale şi instituţionale, precum şi a diferitelor organisme a trecut prin momente iniţiale, de adaptare la noile realităţi. Criminalitatea informatică a reprezentat un aspect de noutate pentru toată lumea, obligând la diverse iniţiative, până la a se ajunge la stadiul actual – culmea, care nu pare a fi aproape deloc adaptat realităţii.

Convenţia Consiliului Europei privind criminalitatea informatică a fost adoptată la Budapesta în anul 2001 şi reprezintă instrumentul - cadru de la nivel european pentru lupta împotriva criminalităţii informatice.

Protocolul de la Strasbourg a fost adoptat de către statele semnatare ale Convenţiei de la Budapesta în anul 2003 şi are în vedere completarea

prevederilor actului semnat în 2001 prin incriminarea actelor de natură rasistă ori xenofobă comise prin intermediul sistemelor informatice.

Totodată, în prezentul capitol am abordat elemente de drept comparat, respectiv prevederile privitoare la criminalitatea informatică în diverse state europene, precum Olanda, Franța, Belgia, Marea Britanie ș.a.

Capitolul este completat cu analiza principalelor prevederi din legislația internă referitoare la criminalitatea informatică, atât prin prisma Codului penal în vigoare, dar şi prin cea proiectului de Cod penal prevăzut a intra în vigoare în viitorul apropiat.

CAPITOLUL IV
CONCEPTE PRIVITOARE LA SECURITATEA INFORMATICĂ

Securitatea informaţiilor constituie o forţă motrice pentru dezvoltarea economică regională şi trebuie să se desfăşoare simultan cu infrastructura din domeniul TIC[4]. Beneficiile de la tehnologiile de implementare a serviciilor de informare sunt dependente de o dezvoltare şi însoţire a infrastructurii TIC, măsuri suficiente de securitate şi un cadru legal de reglementări.

Securitatea informatică, într-un sens larg, incluzând cadrul legal, este esenţială pentru atragerea actorilor economici pentru dezvoltarea unui mediu de afaceri favorabil. Societatea informaţională globală şi economia bazată pe cunoaştere sunt limitate de dezvoltarea şi acceptanţa generală a unui cadru internaţional cibernetic. Valabilitatea unui astfel de cadru sau model necesită o abordare multidimensională pentru provocare cibernetică - de la indivizi la organizaţii şi state.

Dezvoltarea de modele şi soluţii de securitate nu este suficientă pentru a proteja resursele informaţionale. Dacă măsurile tehnice de securitate trebuie să fie dezvoltate şi puse în aplicare, concomitent trebuie să existe şi măsuri

[4] N.A. – tehnologiei informațiilor și comunicației.

juridice, pentru a preveni şi descuraja un comportament infracţional care foloseşte omniprezenţă reţelelor ca o ţintă a infracţiunii(noi tehnologii - noi infracţiuni) sau utilizează reţeaua omniprezentă ca un mijloc pentru a realiza o infracţiune (infracţiuni adaptate la noua tehnologie). Dimensiunea juridică a securităţii în domeniul TIC ar trebui să fie considerată ca un factor de afaceri ce operează la nivel mondial, care va contribui la minimizarea oportunităţilor infracţionale.

Este responsabilitatea fiecăruia să promoveze în condiţii de siguranţă şi de încredere un mediu ciberspaţial, în contextul unei societăţi informaţionale în curs de dezvoltare. Un nivel minim de securitate pentru tehnologii de informare şi comunicare trebuie să fie furnizate la un cost accesibil. Securitatea nu trebuie să devină un factor de excludere pentru oricine care ar dori să desfăşoare activităţi private sau de afaceri pe Internet.

CAPITOLUL V
EVALUAREA ȘI ANALIZA RISCURILOR DIN DOMENIUL CRIMINALITĂȚII INFORMATICE

Elementele legate de problematica riscurilor, prezenței acestora, identificării și analizei lor, alături de măsurile luate efectiv pentru contracararea sau măcar minimizarea lor sunt luate din ce în ce mai mult în calcul de către structurile cu atribuții în aplicarea legii, dar și de către organismele civile victime ale expunerii la diverse categorii de riscuri. Cu atât mai mult, în contextul în care criminalitatea informatică se constituie într-un veritabil factor de risc pentru persoane fizice, instituții, organisme naționale și internaționale și, evident, pentru ordinea publică și siguranța națională, înțelegerea fenomenului – din perspectivă analitică – devine o necesitate.

În domeniul securității informațiilor riscul este considerat a fi "potențialul pe care îl are o amenințare dată de a exploata vulnerabilităţile unei structuri astfel încât să dăuneze organizaţiei"[5]. Spre exemplu, un computer legat la reţeaua metropolitană a Poliţiei Române (structură) poate fi infectat cu un malware (ameninţare) care intră în mediul informatic ca şi un attachment la un email obişnuit (vulnerabilitate).

În general, riscurile asociate unui sistem informaţional, pe care orice analist/auditor trebuie să le analizeze şi evalueze (tehnica frecvent utilizată în acest caz este chestionarul), în vederea aprecierii sistemului în sine, vizează categoriile prezentate în continuare.

CAPITOLUL VI
ORGANISME CU ROL ÎN LUPTA CONTRA CRIMINALITĂȚII INFORMATICE

Acest capitol abordează principalele instituții cu caracter internațional și care au rol în prevenirea/ combaterea infracțiunilor informatice. Sunt analizate atât organisme ce țin de mediul privat, dar și organisme cu ramificații guvernementale ori chiar aflate în subordinea unor macro-instituții (în subordinea Uniunii Europene, NATO ori Națiunilor Unite).

În partea a doua a capitolului sunt abordate probleme legate de structurile funcționale pe plan național, precum cele din subordinea Poliției Române, respectiv Direcția de Combatere a Crimei Organizate și institutul de Criminalistică, dar și alte instituții precum Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism. În plus, sunt aduse în discuție și instituții precum Serviciul Român de Informații și Serviciul de Informații Externe.

[5] ISO/IEC 27005:2008.

CAPITOLUL VII
INVESTIGAREA CRIMINALISTICĂ ÎN CAZUL PRODUCERII UNOR INFRACȚIUNI INFORMATICE

În exercitarea atribuţiilor lor, structurile cu rol în aplicarea legii ori apărarea unor interese legitime ale statului român şi instituţiilor acestuia desfăşoară diverse activităţi, cel mai adesea după modele preluate de la instituţii similare externe. Având în vedere faptul că, la momentul de faţă, procedurile de lucru utilizate de SRI, SIE, DIICOT, precum şi structurile menţionate de la nivelul IGPR sunt clasificate, trebuie acceptată sistematizarea elementelor conceptuale comune rezultate din studiul acestor materiale.

Natura infracţiunilor cere ca ancheta penală să se realizeze în cadrul unei echipe de investigatori. Necesitatea investigaţiei în echipă reiese din nevoia garantării unei obiectivităţi sporite şi eficiente, derivată din conjugarea competenţelor şi specializărilor membrilor echipei[6]. Atât datorită caracteristicilor speciale ale echipamentelor ce fac obiectul investigaţiei, cât şi a metodelor întrebuinţate în investigarea sistemelor informatice, membrii echipei de investigatori trebuie să posede cunoştinţe şi aptitudini adecvate specificului investigaţiei.

CONCLUZII ȘI RECOMANDĂRI

Criminalitatea informatică, deşi a apărut mai târziu, face parte integrantă din criminalitatea internaţională. Fără dubii, criminalitatea internaţională a avut o ascensiune deosebită în ultima perioadă neţinând cont de nici un criteriu de spaţiu, timp, orânduire socială, naţiune sau politică.

[6] Leroux, O. (2004). Legal admissibility of electronic evidence. International Review of Law, Computers and Technology, 18(2), 193-220.

Această stare de lucruri, a stat printre altele la baza fondării sistemelor de asistenţă judiciară în cadrul Uniunii Europene. Cu toate că la nivel de detaliu, se pot constata progrese importante, Uniunea Europeană nu a ajuns în general la o abordare comună în acest domeniu, cadrul actual neputând asigura nici rezultate optime, nici o protecţie perfectă a individului în faţa acţiunilor informatice ilicite.

În plan normativ, au apărut o serie de convenţii, complicate ca şi conţinut, dar numărul ratificărilor la nivel global este redus.

Guvernele europene colaborează oficial, prin acţiuni comune şi asistenţă instituţională, încă de la înfiinţarea Interpol-ului, în anul 1923, drumul fiind deja „bătut" la apariţia criminalităţii informatice.

Cu toate acestea, nu s-a reuşit destructurarea acelor reţele internaţionale care au atins prin activitatea lor ilicită până şi cele mai pregătite state sau cele mai importante Organisme (ex. O.N.U.).

De cele mai multe ori, deşi s-au desfăşurat acţiuni de răsunet, procurorii s-au mulţumit cu condamnări individuale, fără a afecta semnificativ ameninţarea pe care aceste reţele o reprezintă pentru economie, linişte şi siguranţă naţională.

Pe plan intern, România, nu a avut o serie de rezultate marcante, deşi au fost multe cazuri, fie cu autori „singuratici" sau cu autori organizaţi în reţele bine structurate.

Datorită fazei incipiente de pregătire a resursei umane, precum şi a dotării tehnice precare, ţara noastră, a fost obligată să accepte ajutorul informaţional şi de investigare al altor state. Acest lucru nu este condamnabil, dar de regulă „ajutorul" a venit în cazurile când activitatea infracţională a atins interesele acestor state. Cazurile rămase în interior, fie că nu au putut fi depistate, de multe ori chiar nefiind sesizate.

Este de notorietate exemplul activităţii infracţionale desfăşurate de o serie de angajaţi ai unor instituţii bancare, care transferă sume foarte mici de valută (ex. 1-2 cenţi) din conturile clienţilor într-un cont privat.

Pornind de la acest „banal" exemplu şi analizând radiografia ţării noastre cu privire la criminalitatea informatică se ajunge inevitabil la concluzia că majoritatea infracţiunilor incriminate de legile speciale în materie se produc, într-un ritm ascendent.

Urmând exemplul statelor Uniunii Europene şi a altor state, România a luat o serie de măsuri legislative pentru eradicarea fenomenului în discuţie. Astfel, asemenea prevederi şi incriminări se regăsesc, mai ferm, în noul Cod penal[7]. Referitor la infracţiunea în cauză s-au făcut precizări în cuprinsul tezei.

Legea nr. 161/2003, cuprinde de asemenea o serie de incriminări ale unor fapte considerate de legiuitor ca fiind infracţiuni. Şi despre acestea s-au făcut precizările necesare în cuprinsul tezei. Dar eforturile legislative concertate până în prezent de statul noastru nu au avut rezultatele scontate şi anume acelea de a eradica total fenomenul criminogen.

Considerăm că acţiunea voalată a autorităţilor române se datorează şi faptului că teritoriul ţării noastre nu a fost scena unor acţiuni teroriste grave şi nici structurile informatice ale principalelor instituţii ale statului nu au fost afectate de atacuri ilicite informatice.

În faza incipientă se află statul român şi ceea ce priveşte managementul riscurilor din domeniul criminalităţii informatice. Dacă în ceea ce priveşte activitatea de evaluare a riscurilor, au fost efectuate o serie de acţiuni la nivel naţional, atât separat pe domeniu sau în cadrul riscurilor de securitate naţională, în ceea ce priveşte procedurile de înlăturare a acestor riscuri, acţiunile sunt aproape insesizabile. Este adevărat că pe plan teoretic sunt încercări şi pe acest palier.

[7] Noul Cod penal, art. 360 (1).

S-au elaborat de asemenea, la nivelul instituţiilor care folosesc domeniul I.T., care produc asemenea componente, precum şi la nivelul instituţiilor abilitate cu combaterea fenomenului infracţional în acest domeniu, o serie de standarde de evaluare. Evident aceste standarde sunt aliniate la standardele internaţionale în vigoare.[8]

Un lucru de mare importanţă a fost stabilirea acestor standarde, privind în mod unitar sursa ameninţării, motivaţia şi acţiunile. Astfel şi România a luat în considerare ameninţări majore ca terorismul, spionajul industrial, spionajul economic, convingerile religioase etc.

O concluzie pertinentă nu poate exista fără a sesiza un aspect de mare fineţe şi anume; Analizele experţilor în domeniu conduc la ideea că ameninţările informatice devin din ce în ce mai sofisticate, atât datorită posibilităţilor tehnice oferite de către producători, cât şi situaţiei sociale care imprimă o necesitate de înavuţire ilicită şi în paralel o serie de conflicte sociale.

În acelaşi timp, aceleaşi analize duc la concluzia că nivelul de competenţă şi cunoştinţe necesare pentru a exercita o ameninţare informatică scade masiv. La o privire simplistă concluzia ar putea fi considerată anormală, dar nu este aşa. Un fenomen foarte complex cum este criminalitatea informatică, poate genera asemenea realităţi. Existenţa grupărilor organizate, formate din diferite structuri, specializate pe vânzarea de instrumente hardware sau software, ori pe schimbul de instrucţiuni sau programe, transformă chiar şi un novice în domeniul IT, dar dornic de ilicit, într-un potenţial făptuitor, într-o ameninţare.

Nu este un secret, faptul că se oferă spre vânzare, la vedere ’’fără perdea’’ baze de date complete. Acestea pot conţine id-uri de utilizatori, parole, date personale, date din documente personalizate şi chiar date de securizare a unor instrumente cum sunt cărţile de credit.

[8] N.I.S.T. – Standard 800-300.

Existenţa viruşilor informatici, duce, tehnic la concluzia existenţei unor anomalii în sistem care nu afectează însă lucrul cu sistemul. De cele mai multe ori se procedează la "deparazitare " şi folosirea unor programe antivirus.

Cercetările însă au stabilie o altă realitate. Remarca specialiştilor constă în creşterea riscului de infectare cu viruşi a sistemelor informatice prin reţele de tip file-shoring. Deci cu ajutorul viruşilor se încearcă şi de obicei se reuşeşte nu numai blocarea sistemelor informatice ci şi obţinerea de date de la alţi utilizatori.

Fenomenul cercetat atacă, aşa cum am mai precizat, înseşi economiile naţionale, bineînţeles prin atacurile asupra sistemelor informatice folosite de firmele de stat sau particulare sau de instiruţiile statului, producând prejudicii.

BIBLIOGRAFIE

a).Legislație

1.Constituția României

2.Codul Penal al României

3.Codul de Procedură Penală al României

4.Proiectele de Coduri Penal şi de Procedură Penală ale României

5. Legea nr.161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei

6. Legea nr.196/2003 privind prevenirea și combaterea pornografiei

7.Textul Convenției Consiliului Europei privind criminalitatea informatică, ratificat de România prin legea nr. 105 din

8.Directiva 2000/31/EC din 8 iunie 2000 referitoare la anumite aspecte juridice privind serviciile societății informaționale

9. Decizia-Cadru a Consiliului Uniunii Europene nr. 2001/413/JAI din 28 mai 2001 privitoare la combaterea fraudei și falsificării mijloacelor de plată, altele decât numerarul

10.Legea nr.365/2002 privind comerțul electronic

11.Ordonanţa de Urgenţă a Guvernului nr.22/2009 privind înfiinţarea Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii

12. Legea nr.239/2005 privind modificarea şi completarea unor acte normative din domeniul comunicaţiilor

13. Ordonanţa de Urgenţă a Guvernului nr.79/2002 privind cadrul general de reglementare a comunicaţiilor, aprobată cu modificări şi completări

14. Legea nr.304/2003 pentru serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice

15.Legea 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, cu modificările ulterioare

16. Legea nr. 1/1998 de organizare şi funcţionare a SIE actualizată şi modificată prin OUG nr. 154/2001 şi 98/2004.

b).Tratate, cursuri, monografii

b.1.Tratate, cursuri, monografii româneşti

1. Iosif Lucaci, Robert Marin, „Criminalitatea informatică", Editura Fed Prinţ S.A., 2003, Bucureşti.

2. Maxim Dobrinoiu, „Infracţiuni în domeniul informatic", Editura C.H. Beck, 2006, Bucureşti.

3. Victor-Valeriu Patriciu, „Criptografia şi securitatea reţelelor de calculatoare", Editura „Tehnică", 1994, Bucureşti.

4. Petru Blânda, „Prevenirea şi combaterea fraudării cărţilor de credit", Editura Pildner&Pildner, 2007, Târgovişte.

5. Tudor Amza, Cosmin-Petronel Amza, „Criminalitatea Informatică", Editura Lumina Lex, 2003, Bucureşti.

6. Alexandru Boroi, Gheorghe Nistoreanu, „Drept penal. Partea Generală", Editura AII Beck, 2004, Bucureşti.

7. Costică Bulai, „Drept penal român -partea generală", Editura Şansa SRL, 1992, Bucureşti.

8. Costică Bulai, Avram Filipaş, Constantin Mitrache, „Instituţii de drept penal", Ediţia a IlI-a, Editura Trei, 2006, Bucureşti.

9. Lazăr Cărjan, „Tratat de Criminalistică", Editura Pinguin Book, 2005, Bucureşti.

10. Lazăr Cărjan, Mihai Chiper, „Criminalistică. Tradiţie şi Modernism", Editura Curtea Veche, 2009, Bucureşti.

11. Marcel Cernovschi, „Particularităţile cercetării la faţa locului", Editura Sitech, 2008, Craiova.

12. Valerian Cioclei, „Drept penal. Partea specială. Infracţiuni contra persoanei", Editura Universul Juridic, 2007, Bucureşti.

13. Valerian Cioclei, „Codul Penal", Editura C.H. Beck, 2009, Bucureşti.

14. Aurel Ciopraga, „Criminalistica-Tratat de tactică", Editura Sania, 1996, Iaşi.

15. Aurel Ciopraga, Ioan Iacobuţă, „Criminalistica", Editura Chemarea, 1997, Iaşi.

16. Radu Constantin, Pompil Drăghici, Mircea Ioniţă, „Expertizele mijloc de probă în procesul penal", Editura Tehnică, 2000, Bucureşti.

17.Doru Ioan Cristescu, „Investigarea criminalistică a infracţiunilor contra securităţii naţionale şi de terorism", Editura Solness, 2004, Timişoara.

18. Daniel Curiac, Florin Drăgan, „Sisteme informatice pentru comerţ electronic", Editura Orizonturi Universitare, 2005, Timişoara.

19. Ioan Dascălu, Ion Tomescu, Diţă Bondarici, „Frauda în domeniul cârdurilor", Editura Sfinx 2000, 2003, Târgovişte.

20. Ioan Dascălu, Marin-Claudiu Ţupulan, Laurenţiu Giurea, Cristian-Eduard Ştefan, „Metodologia investigării infracţiunilor", Editura Sitech, 2008, Craiova.

21. Tudor Amza, „Criminologie", Editura Lumina Lex, 1998, Bucureşti.

22. Vasile Dobrinoiu, „Drept penal. Partea specială", Volumul I, Editura Lumina Lex, 2004, Bucureşti.

23. Vasile Dobrinoiu, Nicolae Conea, Ciprian-Romiţan, Maxim Dobrinoiu, Nor el Neagu, Camil Tănăsescu, „Drept penal. Partea specială", Volumul II, Editura Lumina Lex, 2004, Bucureşti.

24. Vintilă Dongoroz, Gheorghe Daringa, Siegfried Kahane, şi colectiv, „Noul Cod de procedură penală şi Codul de procedură penală anterior. Prezentare comparativă", Editura Politică, 1969, Bucureşti.

25. Vintilă Dongoroz, Siegfried Kahane, Ion Oancea, Iosif Fodor, Nicoleta Iliescu, Constantin Bulai, Rodica Stănoiu, Victor Roşea, „Explicaţii teoretice ale codului penal român. Partea specială", Volumul IV, Editura Academiei Române, 1972, Bucureşti.

26. Vintilă Dongoroz, Siegfried Kahane, George Antoniu, Constantin Bulai, Nicoleta Iliescu, Rodica Stănoiu, „Explicaţii teoretice ale Codului de procedură penală român. Partea Generală", Volumul I, Editura Academiei, 1975, Bucureşti.

27. Viorel Coroiu, Nicolae Grofu, Panfil Georgică, ”Elemente de criminalistică tactică”, Editura Estfalia, Bucureşti, 2010.

28. Constantin Drăghici, Adrian Iacob, „Tratat de tehnică criminalistică", Ediţia a Il-a, Editura Sitech, 2009, Craiova.

29. Bujor Florescu, „Investigaţia judiciară", Editura Bren, 2009, Bucureşti.

30. Augustin Fuerea, „Manualul Uniunii Europene", Editura Actami, 2001, Bucureşti.

31. Daniela Gărăiman, „Dreptul şi informatica", Editura AU Beck, 2003, Bucureşti.

32. Gilbert Gorning, Ioana Eleonora Rusu, „Dreptul Uniunii Europene, Editura C.H. Beck,

2006, Bucureşti.

33. Mihai Adrian Hotca, Maxim Dobrinoiu, „Infracţiuni prevăzute în legi speciale", Editura C.H. Beck, 2008, Bucureşti.

34. Mihai Adrian Hotca, „Noul Cod Penal şi Codul Penal anterior. Aspecte diferenţiale şi situaţii tranzitorii", Editura Hamangiu, 2009, Bucureşti.

35. Nicolae Ionescu-Cruţan, „Dicţionar de calculatoare englez-român", Editura Niculescu, 2007, Bucureşti.

36.Siegfried Kahane, „Dreptul procesual penal în România", Editura Didactică şi Pedagogică, 1963, Bucureşti.

37.Lars Klander, „Anti Hacker- Ghidul securităţii reţelelor de calculatoare", Editura AII Educaţional, 1999, Bucureşti.

38. Serge Le Doran, Philippe Rosé, „Cyber-Mafia", Editura Antet, 1998, Bucureşti.

39. Iosif Lucaci, Robert Marin, „Investigarea fraudelor informatice", Editura Ministerului de Interne, 2002, Bucureşti.

40. Gheorghe Alecu, Alexei Barbăneagră, „Reglementarea penală şi investigarea criminalistică a infracţiunilor din domeniul informatic", Editura Pinguin Book, 2006, Bucureşti.

41. Ion Marghescu, Gheorghe Bădescu, „Transmiterea discretă a semnalelor", Editura Tehnică, 1978, Bucureşti.

42. Gheorghiţă Mateuţ, „Procedură penală. Partea generală", Editura Fundaţiei „Chemarea", volumul II, 1997, Iaşi.

43. Ioan-Cosmin Mihai, Ion-Florin Popa, Bogdan-Gabriel Tătaru, „Securitatea în Internet", Editura Sitech, 2008, Craiova.

44. Ministerul Administraţiei şi Internelor. Secretariatul General. Serviciul Informare-Documentare, „Criminalitatea Informatică", Sinteză Documentară, Tipografia Ministerului Administraţiei şi Internelor, Anul VII, nr.2 (25), 2006, Bucureşti.

45. Constantin Mitrache, Cristian Mitrache, „Drept penal roman. Partea Generală", Ediţia a IlI-a, Editura Universul Juridic, 2004, Bucureşti.

46. Ion Neagu, „Tratat de procedură penală", Editura PRO, 1997, Bucureşti.

47. Ion Neagu, „Drept procesual penal. Partea generală", Editura Artprint, 2000, Bucureşti.

48. Ion Neagu, „Drept procesual penal. Partea specială. Tratat", Editura Global Lex, 2004, Bucureşti.

49. Gabriel Ion Olteanu şi colectiv, „Cercetarea activităţilor structurilor infracţionale", Editura Sitech, 2008, Craiova.

50. Dumitru Oprea, „Protecţia şi securitatea informaţiilor", Editura Polirom, 2003, Iaşi. SX.Edmond Nicolau, Alexandru Popovici, „Introducere în cibernetica sistemelor hibride", Editura Tehnică, 1975, Bucureşti.

b.2.Tratate, cursuri, monografii străine

1.Lubic, Jr., Paul E. "Global Cyber Crime: The Playing Field, The Players – The Perfect Storm." Bill Mullins Tech Thoughts. June 2, 2010

2.Research and Markets. "A Focus on Cybercrime from North Africa." April 22, 2010

3.C.Hadnagy, Social Engeneering, the art of human Hacking, Wiley, 2010

4.D. Barbará, Applications of Data Mining in Computer Security,volume6of Advances in Information Security. Springer, 2002

5.D. Barroso. Botnets - The Silent Threat. In European Network and Information Security Agency (ENISA), November 2007

6.R.T.Uda, Cybercrime, cyberterrorism, cyberwarfare, Xlibris Crorporation, 2009

7.R.Rhodes, Cyber Meltdown: Bible Prophecy and the Imminent Threat of Cyberterrorism, Harvest House Publishers, 2010

8.J.F.Dunnigan, The next war zone, Citadel Ed., 2003

9.Joffe, Rodney. "The Irretrievable Losses of Malware-Enabled ACH and Wire Fraud." Neustar, Inc. November 2, 2009

10.A.Colarik, Political terrorism, political and economical implications, Hershey publication, 2006

11.C.L.Jonsson, Police Use of Intelligence Networks for Reducing crime, LFB Scholarly Publishing, 2010

12.R.Radvanovski, A.McDougall, Critical Infrastructure: Homeland Security and Emergency Preparedness, Second Edition, CRC Press, 2009

13.T.Macaulay, Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies, CRC Press, 2008

14.T.G.Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley Interscience, 2006

15.Kerr, O. S. (2009). Computer crime law (2nd ed.). St. Paul. MN: Thomson/West

16.M.F.Grady, F.Parisi, The law and Echonomics of cybersecurity, Cambridge University Press, 2005

17.Marcella, Jr., A. J., & Greenfield, R. S. (2002). Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes. Boca Raton, FL: Auerbach

18.Ertoz, Eilertson, Lazarevic, Tan, Kumar, Srivastava, and Dokas. MINDS – Minnesota Intrusion Detection System. In Next Generation Data Mining, MIT Press

E.Cole, R.Krutz, J.W.Coley, Network security bible, second edition, Wiley Publishing Inc.,Indianapolis, 2009

19.L.V.Choi, Cybersecurity and homeland security, Nova science publishers, 2006

Know Your Enemy : Learning about Security Threats (2nd Edition), The Honeynet Project, Addison-Wesley Professional, 2004

20.E.Casey, Digital Evidence and Computer Crime, Second Edition, Academic Press, 2004

21.R.C.Newman, Computer forensics: Evidence collection and management, Auerbach publication, 2007

22.Ulrich Beck, World Risk Society, Cambridge Polity Press, 1998

23.Paul Hopkin – Fundamentals of risk management, IRM Kogan Page, 2010

24.Knight, F. H. (1921) Risk, Uncertainty and Profit, Chicago: Houghton Mifflin Company şi Rescher, Nicholas (1983). A Philosophical Introduction to the Theory of Risk Evaluation and Measurement. University Press of America

25.Bankoff, Greg, George Frerks and Dorothea Hilhorst. 2004. Mapping Vulnerability

26.M.Krouhy, D.Galai, R.Mark – The essentials of risk management, McGraw Hill 2006

27.R.B.Duffey, J.W.Saull – Managing risk.The human element, Wiley, 2005

28.B.J.Kuipers, D.Berleant, Using incomplete quantitative knowledge in quantitative reasoning, San Mateo C.A., 1988

29.H.Raiffa, Decision analysis, introduction lectures on choises under uncertainty, Addison-Wesley, 1970

30.C.O.Alexander – The handbook of risk management and analysis, John Wiley, 1998

31.Brown, C. L. T. (2010). Computer evidence: Collection and preservation (2nd ed.). Boston, MA: Course Technology

32.Cohen, F. (2008). Challenges to digital forensics evidence. Livermore, CA: ASP Press

33.F.D.Kramer, S.H.Starr, L.Wentz, Cyberpower and national security, National Defense University, 2009

c).Articole, studii

1.Colecția revistei ”Forum Criminalistic”

2.Colecția revistei ”Criminalistica”

3.Colecția revistei ”International journal of cyber criminology”

4.Colecția revistei ” International Journal of Cyber Crimes and Criminal Justice”

5.Colecția revistei ”Virginia Journal of Law and Technology”

6.Colecția revistei ”IT Security magazine”

7.Colecția revistei ”Forensic Investigators”

8.Colecția revistei ”Hakin9 magazine”

9.Colecția revistei ”Crime and Justice international magazine”

10.Colecția revistei ”Security and Privacy Magazine”

11.Colecția revistei ”Revista română de dreptul proprietăţii intelectuale”

12.Colecția revistei ”Revista de drept penal”

13.Colecția revistei ”Dreptul”

14.Colecția revistei ”Journal of Digital Forensics, Security and Law”

13.Colecția revistei ”Digital Investigation”

14.Colecția revistei ”International Review of Law, Computers and Technology”

d).Resurse web

1.www.fbi.gov
2.www.zscaler.com
3.www.infoworld.com
4.www.washingtonpost.com
5.www.law.jrank.org
6.www.usatoday.com
7.www.ndtv.com
8.www.internetnews.com
9.www.finextra.com
10.www.wikipedia.org
11.www.mcafee.com
12.www.bitdefender.com
13.www.cise.ufl.edu
14.www.thawte.com
15.www.ic3.gov
16.www.pulse2.com
17.www.igpr.ro
18.www.sie.ro
19.www.sri.ro