SECURITATEA INFORMAȚIONALĂ LA NIVEL EUROPEAN

Autor: Tatiana Busuncian
Dr., conferențiar universitar

Conținuturi; Obiective de referință; Termeni-cheie.

Conținuturi:

1. caracteristicile terorismului informațional în spațiul European.

2. implementarea acțiunilor UE în sporirea schimbului de informații

3. criminalitatea informațională, eforturile întreprinse pentru asigurarea securității informaționale.

Obiective de referință:

- să definească caracteristicile terorismului informațional în spațiul european;
- să determine instrumentele și metodele de luptă cu amenințările cibernetice;
- să influențeze implementarea acțiunilor UE în sporirea schimbului de informații, intensificarea verificărilor la frontierele externe, îmbunătățirea controalelor armelor de foc, digitalizarea cooperării judiciare, prevenirea radicalizării online, blocarea finanțării terorismului și altele;
- să evalueze motivele criminalității informaționale și să descrie eforturile întreprinse pentru asigurarea securității informaționale.

Termeni-cheie: *nivel european, război informațional, război hibrid, propagandă, amenințări cibernetice, schimb de informații, frontiere.*

Terorismul informațional în spațiul european

Actualmente, cel mai mare pericol pentru lumea contemporană îl reprezintă terorismul. Terorismul ca fenomen social-politic are rădăcini istorice profunde. De la începuturi, fenomenul terorismului a avut un caracter intern, manifestându-se doar la nivel național, în calitate de factor de influență asupra sferei social-politice și altor domenii ale vieții, ajungând să fie statuat în legislația fiecărui stat.

Terorismul cauzează prejudicii considerabile sub aspect politic, economic, social și moral, acesta constituie o problemă serioasă, soluționarea căreia este în interesul întregii comunități mondiale, inclusiv pentru reprezentanții mediului științific. Încă la începutul secolului trecut au fost întreprinse tentative de creare a unor mecanisme internaționale eficiente de prevenire și combatere a terorismului

Prin acțiunile întreprinse de teroriști ne dăm seama despre tipul de război. Terorismul vizează distrugerea fizică, în numele unor idealuri sau al unor „vocații” mesianice, spectaculoase, crearea unor situații-limită care să ducă la înfricoșarea populației și a conducerii politice, în cele mai multe cazuri, la bază este obiectivul politic.

Războiul informațional și mediatic, chiar dacă vizează tot un obiectiv politic urmărește, potrivit principiilor enunțate de Sun Tzî cu două milenii și jumătate în urmă, să învingă pe cât posibil fără a distruge fizic, să obțină supremația strategică informațională, de regulă, fără distrugerea sistemelor și, mai ales, fără pierderi inutile de vieți omenești.

La etapa actuală dezvoltarea societăţii se caracterizează prin aceea că informaţia, tehnologiile informaţionale şi de comunicaţii, precum şi relaţiile ce se formează în procesul de colectare, prelucrare, stocare, transmitere şi diseminare a informaţiei, au un impact direct şi din ce în ce mai puternic asupra dezvoltării economice, sociale şi spirituale atât în cazul anumitor state, în mod paricular, cât şi în privinţa întregii comunităţi mondiale, în ansamblu. Aceasta ne atage atenţia asupra faptului că, în condiţiile actuale, informaţia şi modul în care este gestionată această resursă devine principalul instrument pentru realizarea scopurilor şi obiectivelor noii ordini mondiale. Oficial, despre aceasta s-a declarat la data de 22 iulie 2000, în Japonia, în cadrul procesului de semnare de către conducătorii celor mai influente opt state din lume a Cartei privind Societatea Informaţională Globală, în textul căreia se menţionează că „tehnologiile informaţiei şi comunicaţiilor au devenit unul dintre cei mai importanţi factori în modelarea societăţii secolului XXI”.

Mai târziu s-a declarat despre faptul că omenirea a trecut la o nouă treaptă de dezvoltare – „etapa societăţii informaţionale”. Conform datelor UNESCO, volumul tranzacţiilor de pe piaţa serviciilor şi tehnologiilor informaţionale depăşeşte suma de două trilioane de dolari şi reprezintă circa 15% din economia mondială. Trecerea civilizaţiei noastre în „era informaţională” a coincis, practic, cu declanşarea „războiului împotriva terorismului” – o luptă ce se desfăşoară sub toate aspectele, inclusiv cel informaţional. Spre regret, în afară de beneficiile evidente la nivel mondial ale revoluţiei în domeniul tehnologiei informaţiei au fost generate, concomitent, noi potenţiale ameninţări în adresa comunităţilor, statelor şi cetăţenilor săi, dar şi cu referire la societatea mondială, în general. În mare parte, toate acestea se referă la terorism, evoluţia căruia, potrivit experţilor, în cea mai mare măsură se realizează în domeniul informaţional.

Dezvoltarea rapidă a noilor tehnologii a extins foarte mult posibilitățile organizațiilor teroriste de a manipula cu conştiinţa publică, mai ales în procesul de pregătire şi desfăşurare a acțiunilor teroriste. Aceste acțiuni au următoarele caracteristici ale terorismului contemporan:

- orientarea spre un impact emoţional puternic asupra societăţii ca rezultat al acţiunilor sale, exprimat prin atingerea stării de teamă şi nesiguranţă în rândul populaţiei atacate şi tendinţa de acceptare şi simpatie din partea adepţilor săi;
- concentrarea pe diseminarea către un public cât mai larg a informaţiilor cu privire la un act terorist comis;
- realizarea atacurilor asupra unor obiecte care au o semnificaţie deosebită pentru societate, simbolizând anumite valori;
- folosirea violenței de către teroriști este percepută în societate (în special în țările dezvoltate) ca una nenaturală, improprie, ce intră în conflict cu normele sociale şi generează ca urmare o stare de anxietate, nesiguranţă, neîncredere şi incertitudine.

Dezvoltarea tehnologiilor informaţionale în întreaga lume contribuie la apariţia şi răspândirea largă a comunităţilor criminale transnaţionale, de tip reţea organizaţională. Una din caracteristicile specifice a comunităţilor criminale transnaţionale este coordonarea activităţilor prin intermediul canalelor de informare şi comunicare. Activităţile informaţional-subversive ale teroriştilor pot fi de natură explicită şi pot fi efectuate în mod deschis sau secret, efectuate din numele anumitor forţe sau anonim.

Scopul principal al teroriştilor este de a face actul terorist cunoscut publicului şi autorităţilor, având o rezonanţă cât mai mare. O astfel de rezonanţă publică generează frică şi panică în rândul membrilor societăţii, are ca rezultat pierderea încrederii populaţiei în autorităţile statului şi, în cele din urmă, provoacă instabilitate politică. Un pericol real îl constituie tendinţa organizaţiilor teroriste internaţionale de a utiliza mijloacele de informare în masă în calitate de instrument pentru atingerea scopurilor lor criminale. Astfel, teroriştii contemporani au transformat în câmp de luptă inclusiv şi ecranul televizorului.

Dezvoltarea mijloacelor electronice de informare în masă cu efect transfrontalier contribuie în mod semnificativ la extinderea capacităţilor organizaţiilor teroriste internaţionale în ceea ce priveşte manipularea cu conştiinţa maselor. O astfel de manipulare, având ca „ţintă" întreaga societate, are ca scop schimbarea conştiinţei şi a comportamentului într-un mod avantajos pentru terorişti. În acest caz, lipsa culturii informaţionale a unei anumite părţi a populaţiei, slaba protecţie a acesteia contra influenţei ideologiei extremiste, conduce la faptul că cei manipulaţi de multe ori nu îşi dau seama că idealurile lor, valorile, necesităţile şi, în general, modul de gândire sunt, de fapt, determinate în mare măsură de interesele antisociale ale celor care manipulează cu ei şi tind să-şi instaureze dominaţia asupra lumii lor spirituale.

Nici o ţară din lume, nici chiar SUA, nu-şi mai poate asigura securitatea prin forţe proprii, şi aceasta din cel puţin două motive:

1. mondializarea informaţiei, dezvoltarea şi proliferarea fără precedent a sistemelor de arme şi mijloacelor de distrugere;
2. omniprezenţa şi omnipotenţa ameninţărilor asimetrice, îndeosebi a celor de natură endogenă, care îşi mută centrul de greutate în sfera informaţională, mai târziu posibil în cea a ecosistemelor şi chiar în cea genetică, afectând direct mecanismul intim al vieţii umane – informaţia ereditară – acizii nucleici.

De aici, viitorul va configura, probabil, un sistem de reacţie care se va baza pe mutarea accentului pe alte modalităţi de a duce războiul. Cercetătorii ar trebui să analizeze și să prezică ameninţările de mâine și care va fi configuraţia războiului viitor. Terorismul – îndeosebi cel ciberinformaţional – pare a fi doar un prim semnal care configurează, sumar dar semnificativ, dimensiunea confruntărilor de mâine.

Terorismul mediatic incumbă două aspecte:

- cel al folosirii de către teroriști a mass-media pentru atingerea scopurilor lor criminale, violente
- şi cel al terorizării populaţiei de către instituţii sau reprezentanţi ai media.

Terorismul mediatic pleacă de la posibilitatea manipulării prin media, a negocierii între teroriști şi organele de ordine chiar pe postul naţional de televiziune, a popularizării cauzei unor grupări teroriste prin mijloacele de comunicare, a atragerii, pe această cale, de simpatizanţi din rândul oamenilor paşnici.

Tot mai dependenți de informații am devenit în veacul XXI. O serie de sectoare critice precum energia, sănătatea, finanțele, transporturile și altele au devenit tot mai dependente de tehnologiile digitale pentru a-și desfășura activitățile de bază. Digitalizarea oferă oportunități enorme și asigură soluții pentru multe dintre provocările cu care se confruntă Europa, nu în ultimul rând în timpul crizei provocate de pandemia de COVID-19 și războiului din Ucraina, dar, în același timp, expune economia și societatea la amenințări cibernetice.

În întreaga Europă atacurile cibernetice și criminalitatea informatică devin tot mai numeroase și mai sofisticate. Se preconizează că această tendință va continua să crească în viitor, date fiind previziunile conform cărora 22,3 miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor până în 2024 global.

Liderii Uniunii Europene în octombrie 2020 au solicitat consolidarea capacității uniunii de a:

- se proteja împotriva amenințărilor cibernetice;
- asigura un mediu de comunicare securizat, în special prin criptarea cuantică;
- asigura accesul la date în scopuri judiciare și de asigurare a respectării legii.

Comisia Europeană și Serviciul European de Acțiune Externă (SEAE) au prezentat o nouă strategie de securitate cibernetică a UE în decembrie 2020. Scopul acestei strategii este de a consolida reziliența Europei la amenințările cibernetice și de a asigura faptul că toți cetățenii și toate întreprinderile pot beneficia pe deplin de servicii și instrumente digitale fiabile și de încredere. Noua strategie conține propuneri concrete de punere în aplicare a unor instrumente de reglementare, de investiții și de politică.

La 22 martie 2021, Consiliul a adoptat concluzii privind Strategia de securitate cibernetică, care subliniază că securitatea cibernetică este esențială pentru construirea unei Europe reziliente, verzi și digitale. Miniștrii din UE au stabilit ca obiectiv-cheie atingerea autonomiei strategice, menținând în același timp o economie deschisă. Aceasta include consolidarea capacității de a face alegeri autonome în domeniul securității cibernetice, cu scopul de a consolida poziția de lider a UE în domeniul digital și capacitățile sale strategice.

Noua Agenție a UE pentru Securitate Cibernetică se bazează pe structurile predecesoarei sale, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor, având acum un rol consolidat și un mandat permanent. În plus, agenția a adoptat același acronim, ENISA.

Uniunea Europeană lucrează în mod activ la îmbunătățirea mediului digital în beneficiul tuturor europenilor. Viața digitală a europenilor trebuie să fie sigură, ușoară și să respecte libertățile fundamentale. Tehnologiile digitale schimbă viețile oamenilor – de la modul în care comunicăm până la modul în care trăim și lucrăm. Digitalizarea are potențialul de a oferi soluții pentru multe dintre provocările cu care se confruntă Europa și europenii și oferă oportunități cum ar fi:

- crearea de locuri de muncă;
- promovarea educației;
- stimularea competitivității și a inovării;
- combaterea schimbărilor climatice și facilitarea unei tranziții verzi.

UE este un domeniu care cuprinde totul, de la rețelele de informații și telecomunicații, infrastructură și datele pe care le sprijină până la sistemele informatice, operatori și persoanele împuternicite de operatori.

UE cooperează în domeniul apărării în spațiul cibernetic prin activitățile Agenției Europene de Apărare (AEA), în colaborare cu Agenția UE pentru Securitate Cibernetică și cu Europolul. AEA sprijină statele membre în construirea unei forțe de muncă militare competente în domeniul apărării cibernetice și asigură disponibilitatea unei tehnologii proactive și reactive în domeniul apărării cibernetice.

Strategia de securitate cibernetică a UE, adoptată în decembrie 2020 de Comisie și SEAE, consolidează:

- coordonarea apărării cibernetice
- cooperarea și consolidarea capabilităților de apărare cibernetică.

Componente naţionale şi internaţionale de cooperare

• Sistemele de supraveghere şi de monitorizare a terorismului presupun structuri şi infrastructuri cu foc continuu, distribuite în aşa fel încât să acopere întreaga planetă sau, într-o primă etapă a războiului antiterorist, zonele care ating pragul de importanţă ce se ia în consideraţie de factorii de decizie. Aceste sisteme trebuie să fie integrate, dar şi suficient de flexibile pentru a face faţă flexibilităţii tactice şi aleatorii a terorismului, şi să asigure bazele de date şi informaţii necesare organizării corespunzătoare a acţiunii şi reacţiei. Tot ele trebuie să aibă componente naţionale şi internaţionale, care să acţioneze, prin cooperare în toate mediile şi în toate spaţiile.

Fiecare din aceste structuri trebuie să includă:

• componente de supraveghere electronică de mare sensibilitate;

• componente de cercetare directă, prin agenţi şi agenţi de influenţă;

• componente de comunicaţii rapide şi securizate;

• componente de analiză a datelor şi informaţiilor;

• componente de decizie rapidă;

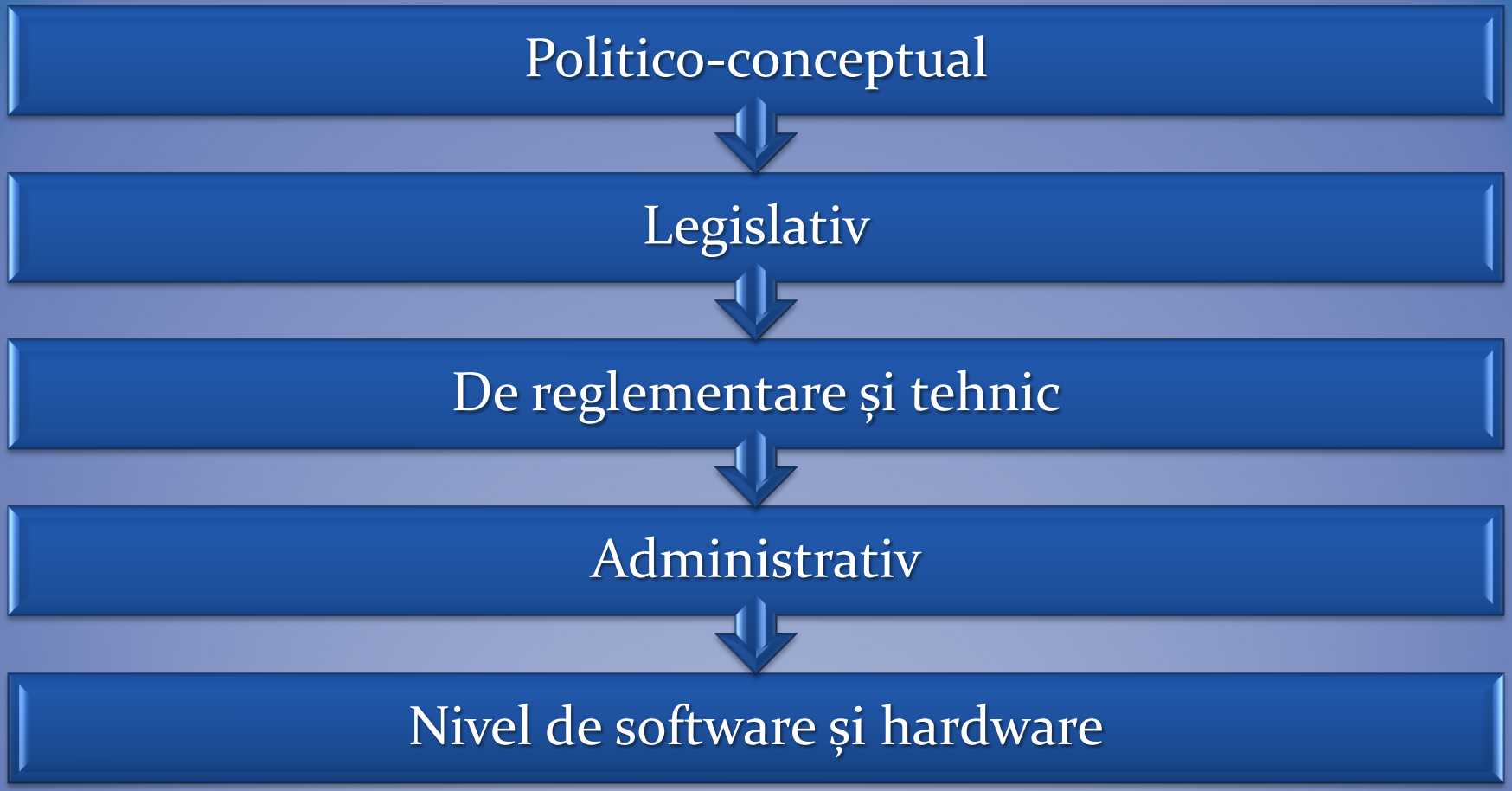
• componente de validare şi corectare oportună a acestor decizii.

Factorul cel mai important în supravegherea structurilor, infrastructurilor şi acţiunilor teroriste îl reprezintă omul, agentul de informaţii, dotat cu toate mijloacele necesare şi ajutat de un sistem tehnic-informaţional permanent şi eficace.

Componente naţionale şi internaţionale de cooperare

- Republica Moldova colaborarează cu Organizația Tratatului Atlanticului de Nord. Colaborarea cu NATO nu poate afecta neutralitatea Republicii Moldova. Organizația Tratatului Atlanticului de Nord este o alianță politico-militară, înființată prin Tratatul Atlanticului de Nord semnat la Washington la 4 aprilie 1949. Alianța este o asociere de state libere unite prin hotărârea lor de a-și proteja securitatea, prin garanții reciproce și relații stabile cu alte țări.
- Scopul esențial al NATO este de a asigura libertatea și securitatea tuturor membrilor săi prin mijloace politice și militare, în conformitate cu Tratatul Nord-Atlantic și cu principiile Cartei Națiunilor Unite. Cele trei sarcini fundamentale ale Alianței sunt: apărarea colectivă, gestionarea crizelor și securitatea prin cooperare.
- Totodată, NATO cooperează cu state terțe, pentru dezvoltarea capabilităților de apărare și creșterea rezilienței acestora, dar și cu organizații internaționale, în special cu Uniunea Europeană, Organizația Națiunilor Unite și Uniunea Africană în domenii de interes comun. Toate deciziile adoptate la nivelul NATO sunt luate prin consensul celor 30 de state aliate.
- Statele partenere NATO: Pe lângă statele membre, NATO are și un Parteneriat pentru Pace (PfP), care a fost introdus în ianuarie 1994. La momentul actual, din acest parteneriat fac parte 20 de țări, inclusiv Moldova.
- Scopul principal al Parteneriatului este de a întări stabilitatea și securitatea din întreaga Europă. Acest lucru este posibil datorită unui Document Cadru semnat între statele partenere și NATO.
- Documentul include sarcini specifice pe care fiecare participant trebuie să și le asume în cooperarea cu NATO.

Nivelurile securității informaționale



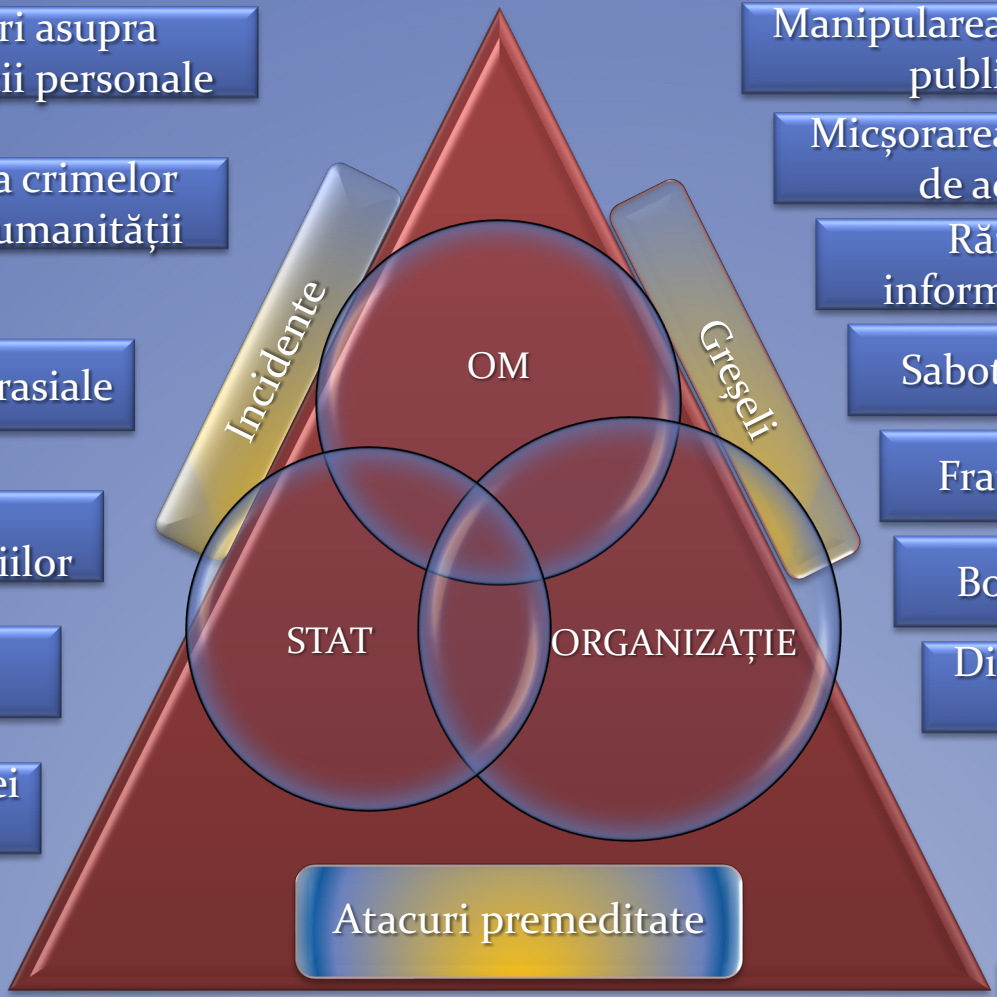
Spațiul cibernetic - teren de confruntare

Spațiul cibernetic a devenit un nou mediu de ducere a războiului (al cincilea după uscat, mare, aer, spațiu). Este evident faptul că toate conflictele în viitor vor avea o componentă virtuală, fie în faza inițială a conflictului, fie sub formă de agresiune în sensul direct al cuvîntului, fără desfășurarea altor forme de luptă.

În absența unor acorduri internaționale și a nedorinței de a conveni asupra normelor generale de interpretare a problemei, actorii cu intenții agresive posedă agilitate și flexibilitate în dezvoltarea și punerea în aplicare a potențialilor atacuri cibernetice.

Subiecții securității informaționale

Ținte și surse ale riscurilor cibernetice



Atacuri asupra demnității personale

Justificarea crimelor împotriva umanității

Contradicții rasiale

Crime împotriva copiilor

Calomnie

Furtul informației de identificare

Atacuri de saturație

Încălcarea confidențialității

Manipularea cu opinia publică

Micșorarea gradului de acces

Război informațional

Sabotaj

Fraude

Înrăutățirea încrederii

Boicot

Fraude

Distribuirea ilegală

Atacuri sistematice

Fraude financiare

Afectarea integrității

Terorism cibernetic

Șantaj

Furt

Autorii atacurilor cibernetice

- Hackerii amatori (hobbyiști);
- Grupe mici de hackeri;
- Organizații nonguvernamentale;
- Structuri de stat.

Surse de amenințări cibernetice asupra securității naționale

Propaganda

- Mai puțin de jumătate dintre cetățenii Republicii Moldova, mai exact, 44%, spun că ar cunoaște ce înseamnă termenul propagandă, arată datele unui sondaj național privind percepția populației despre mass-media și aptitudinile mediatice, publicat în toamna anului trecut. Mai mult, circa jumătate dintre respondenți au fost de acord cu afirmații precum că propagandă ar fi știrile care sperie populația sau care critică guvernarea, ceea ce nu este tocmai așa.
- Toată lumea vorbește despre propagandă, dar foarte puțini încearcă să răspundă la întrebarea ce este propaganda, pentru că dacă ar răspunde, atunci propaganda dispare. Foarte stranie îmbinarea – mass-media și propaganda, când mass-media ar trebui să facă altceva decât propagandă, propagandă are cine face.
- Propaganda este o informație sau niște mesaje ale cuiva care, transmițându-le, încearcă să te afilieze, să te facă să gândești ca și dânsul. Atunci când omul se apucă de capul propagandei, atunci propaganda devine un fenomen nociv, pentru că, în general, de la începuturi și până acum, propaganda vine pe filiera religioasă. Apropo, în Roma există strada Propagandei, adică este dedicată celor care transmiteau mesajele credinței catolice și încercau să aibă tot mai mulți susținători. Ei bine, în timp, propaganda a fost luată drept armă ideologică de multă lume.
- Foarte straniu că, și în secolul 21, când avem acces la o sumedenie de canale de informare, propaganda își face treaba și, mai ales acolo unde populația săracă predomină, este un mecanism foarte subtil.

Concluzii

- Securitatea informațională este un domeniu mult prea vast și cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este în continuă mișcare, cerințele de securitate și confidențialitate cresc pe zi ce trece, amenințările țin pasul.
- Dependența de informație este tot mai mare, chiar periculoasă. Există state care depind totalmente de informațiile oferite de componentele spațiului cibernetic național. Blocarea acestuia timp de câteva ore poate să conducă la instaurarea haosului în țara respectivă, afectând, în bună măsură, și securitatea sistemului informațional global.
- Tehnologiile avansate oferă un șir de soluții pentru multe dintre preocupările omenirii, inclusiv pentru domeniul militar. Războiul informațional, tehnologia care a ajuns la o treaptă de dezvoltare înaltă, oferă soluții la toate provocările existente, inclusiv militare, dar nu poate înlocui aspectele referitoare la resursa umană.

Concluzii

- Terorismul este un fenomen mult mai complex chiar decât războiul, care trebuie studiat și aprofundat nu doar pentru a-i limita efectele și a-i pedepsi pe cei vinovați, ci îndeosebi pentru a-i înțelege și a-i eradica mecanismele și cauzele.
- Terorismul lovește prin surprindere, de regulă, în punctele vulnerabile, astfel încât să ucidă, să distrugă și să înspăimânte, să creeze efecte spectaculoase și o atmosferă de infern și mizerie umană, dusă până la abject și insuportabil.
- Terorismul devine din ce în ce mai mult un instrument al politicii, și anume instrumentul ei cel mai rapid, cel mai ascuns, an cel mai veninos, cel mai greu de oprit, dar și de controlat și de stăpânit.
- Terorismul nu este un fenomen unitar, deși acțiunile lui, extrem de diversificate, au aceeași filozofie a distrugerii, a terorii. El dispune de structuri și forțe numeroase, infiltrate în toate palierele și ramificațiile societății omenești – unele dintre aceste structuri fiind active, altele, în conservare – și este în măsură să acționeze rapid, oricând și oriunde. Terorismul folosește o strategie a acțiunilor de tip rapid care, însumate, dau imaginea unui război-mozaic.
- Arma terorismului principală este omul – omul inteligent, omul fanatic, omul misionar -, care, în numele unor convingeri ce nu pot fi zdruncinate ușor, este în stare de orice sacrificiu și, mai ales, este în stare să inventeze mijloace de acțiune inteligente și deosebit de eficace, întrucât el pune în ceea ce face toată religia și toată ființa lui. Asemenea oameni nu pot fi ușor opriți.

Pentru contracararea cu succes a amenințărilor cibernetice este necesar a se concentra asupra următoarelor:

- Stabilirea unui cadru conceptual, instituțional (crearea sistemului național de securitate cibernetică, elaborarea legislației, dezvoltarea parteneriatului);
- Elaborarea programului național de dezvoltare a potențialului cibernetic (capacităților de prevenire, detectare și contracarare a atacurilor cibernetice, crearea unor structuri specializate, ridicarea nivelului de protecție, dezvoltarea producției produselor de profil);
- Consolidarea culturii de securitate informațională (informarea populației, instruirea adecvată a managerilor și a personalului tehnic);
- Perfecționarea cooperării internaționale (la nivel de acte normative, schimburi de experiență, de protecție colectivă împotriva atacurilor de amploare).

Bibliografie

- Aspectul informațional al luptei contemporane contra terorismului la nivel mondial. https://ibn.idsi.md/sites/default/files/imag_file/107-120.pdf
- Manualul UE privind asistență acordată victimilor terorismului. Ianuarie 2021.
- Concepția securității informaționale a Republicii Moldova
- Securitatea informațională 2013: conf. intern., 19 apr. 2013 (ed. a 10-a Jubiliară), coord. ed.: Serghei Ohrimenco. Chișinău: ASEM. 2013, 126 p.
- Chifu Iu., Nantoi O. Război informațional. Tipizarea modelului agresiunii.
- Drăgulean A. Arădăvoaice, Gheorghe; Iliescu, Dumitru; Niță, Dan Laurențiu, Terorism, antiterorism, contraterorism, Ed. Antet, București, 1997, 383 pag.
- Bădescu, Ilie; Dungaciu, Dan; Baltasiu, Radu, Istoria sociologiei. Teorii contemporane, Ed. Eminescu, București, 1996, 704 pag.
- Ce presupune parteneriat și cooperare cu NATO și de ce neutralitatea Republici Moldovei nu ar trebui să reprezinte un impediment. https://infocenter.md/ce-presupune-parteneriat-si-cooperare-cu-nato-si-de-ce-neutralitatea-republici-moldovei-nu-ar-trebui-sa-reprezinte-un-impediment-2/
- Katzman, Kenneth, Terrorism: Near Eastern Groups and State Sponsors, Congresional Research Center Report for Congress, 2001
- Popa, N.; Mihăilescu, I.; Eremia, M., Sociologie juridică, Ed. Universității din București, București, 1997, 124 pag.
- Rădulescu, Sorin M., Homo Sociologicus. Raționalitate și irațională în acțiunea umană, Casa de editură și presă "Șansa" – SRL, București, 1994, 302 pag.
- Snowden, Ben; Hayes, Laura, State-Sponsored Terrorism, 2001 XXX, Terorismul, Ed. Omega, București, 2001, 224 pag.
- Terorismul. București, 2002. https://cssas.unap.ro/ro/pdf_studii/terorismul.pdf
- Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.