MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susținere
Şef departament:
Ion Fiodorov, conferențiar universitar, doctor în informatică
_____
„____” _____ 202_

Măsuri de securitate cibernetică pentru contracararea amenințărilor hibride

Teză de master

Student: **Jovmir Cristina,**

st.gr. SI-201M

Coordonator: **Alexandru Putere,**

lector univ.

Chișinău, 2022

ADNOTATION

For the master thesis "Cyber security measures in counteracting cyber threats"

The purpose of the thesis: This paper aims to analyze the main cyber security risks and challenges of the Republic of Moldova in counteracting hybrid threats, the study of current achievements such as the legislative and interinstitutional framework and the premises of this government with regard to further development of cybersecurity. prosperous digital societies and for citizens.

Keywords: cyber security, hybrid threats, hybrid warfare, national resilience, security culture, cyber vulnerability, cyber security risks.

Thesis structure: Introduction, 5 chapters, conclusions, 7 figures, 2 tables, no appendices, 17 bibliographic sources, 41 pages of basic text.

Chapter I: The first chapter is dedicated to the analysis of the cybersecurity aspects on hybrid threats regarding national security. In this chapter, we studied the basic concepts of hybrid threats and conflicts arising from threats to national security. The chapter describes the evolution of conflicts and the concept of hybrid warfare, reaching data from current statistics.

Chapter II: In this chapter, the current situation of the Republic of Moldova regarding the national cyber security was analysed, in terms of legislative and inter-institutional framework. Most of Moldova's security vulnerabilities have an internal origin that is constantly fuelled by external factors. The challenges posed by hybrid threats are becoming increasingly complex as the concept continues to expand, along with the specific features of information technology. This well-known phenomenon has become popular in Eastern Europe, counteracting these special security threats by becoming a serious struggle for the less resilient countries, as in the case of the Republic of Moldova.

Chapter III: Chapter 3 describes the international models for counteracting hybrid threats targeting cyber security and national security itself. The chapter describes the EU model and the NATO Plan to address current hybrid threats.

Chapter IV: Chapter 4 includes a study on R.M.'s international cooperation projects in terms of cyber resilience and cyber security in terms of cyber governance as a complex mechanism in national defense.

Chapter V: Chapter 5 examines R. M's vulnerabilities related to hybrid threats, identifies vectors of national development, and analyses and describes strategic models for counteracting conflicts by (escalating) them. The study also outlines the cross-sectoral threat escalation strategy and a number of security measures to ensure an acceptable level of cyber security in the face of current hybrid threats.

Adnotare

La teza de master cu tema „Măsuri de securitate cibernetică pentru contracararea amenințărilor hibride" a **st.gr. SI-201M, Cristina Jovmir**

Scopul tezei: Prezenta lucrare are drept scop analiza principalelor riscuri și provocări de securitate cibernetică ale Republicii Moldova în contracararea amenințărilor hibride, studiul realizărilor curente precum cadrul legislativ și interinstituțional și premisele prezentei guvernări cu referire la acțiunile de dezvoltare ulterioară a securității cibernetice în scopul dezvoltării unei societăți digitale prospere și pentru cetățeni.

Cuvinte-cheie: securitate cibernetică, amenințări hibride, război hibrid, reziliență națională, cultură de securitate, vulnerabilitate cibernetică, riscuri de securitate cibernetică.

Memoriu explicativ: Introducere, 5 capitole, concluzii, 7 imagini, 2 tabele, fără anexe, 17 surse bibliografice, 41 pagini text de bază.

Capitolul I: Primul capitol este dedicat analiza domeniul propus pentru studiu. În cadrul acestui capitol au fost studiate conceptele fundamentele despre amenințările de tip hibrid și conflictele derivate din amenințări ce vizează securitatea națională. Au fost asemenea atins subiectul despre evoluția conflictelor și conceptului de război hibrid și impactul criminalității cibernetice, atingând date din statistici curente.

Capitolul II: În cadrul acestui capitol a fost analizată situația actuală a R.M aferent securității cibernetice naționale, sub aspect de cadru legislativ și interinstituțional. Majoritatea vulnerabilităților de securitate ale Moldovei au o origine internă care este alimentată constant de factori externi. Provocările reprezentate de amenințările de tip hibride devin din ce în ce mai complexe pe măsură ce conceptul se extinde continuu, împreună cu caracteristicile specifice ale tehnologiilor informaționale. Acest fenomen bine-cunoscut a devenit popular în Europa de Est, contracararea acestor amenințări speciale de securitate devenind o luptă serioasă pentru țările mai puțin rezistente, ca în cazul Republicii Moldova.

Capitolul III: Capitolul 3 descrie modelele internaționale de contracarare a amenințărilor de tip hibrid ce vizează securitatea cibernetică și respectiv securitatea națională în sine. Capitolul descrie modelul UE și Planul NATO aferent contracarării amenințărilor hibride actuale.

Capitolul IV: Capitolul 4 include un studiu aferent proiectelor de cooperare internațională a R.M în aspectul rezilienței cibernetice și securității cibernetice în aspect de securitate cibernetică drept mecanism complex în apărarea națională.

Capitolul V: Capitolul 5 se examinează vulnerabilitățile R.M aferente amenințărilor hibride, sunt identificați vectorii de dezvoltare națională, precum și se analizează și descrie modelele strategice de contracarare a conflictelor prin de(escaladare) al acestora. În baza studiului elaborat este prezentată de asemenea strategia trans-sectorială de escaladare a amenințărilor și un șir de măsuri de securitate pentru asigurarea unui nivel acceptabil de securitate cibernetică în fața curentelor amenințări hibride.

CUPRINS

INTRODUCERE **10**
1 Războiul hibrid – o nouă natură a conflictelor mondiale a secolului XXI **12**
1.1 Aspecte generale și definiții 12
1.2. Caracteristicile și premisele de dezvoltare a amenințărilor hibride 13
1.3 Actualitatea temei de cercetare 15
2 Analiza securității cibernetice naționale în Republica Moldova **19**
2.1 Securitatea informației la limita democrației 20
2.2 Conceptul național privind asigurarea securității cibernetice 21
2.3 Cadrul legislativ aferent securității cibernetice a Republicii Moldova 23
3 Modele internaționale de contracarare a amenințărilor hibride **28**
3.1 Cadrului comun al Uniunii Europene privind contracararea amenințărilor hibride 28
3.2 Planul NATO de contracarare a amenințărilor hibride 30
4 Cooperarea internațională a R.M în asigurarea rezilienței cibernetice **32**
5 Vulnerabilitățile Republicii Moldova din perspectiva amenințărilor hibride **37**
5.1 Vectori de dezvoltare națională în contracararea amenințărilor hibride 38
5.2 Modele strategice de contracarare a amenințării de tip hibrid 40
5.3. Abordarea strategiei trans-sectoriale de escaladare a amenințărilor hibride 43
CONCLUZII **50**
BIBLIOGRAFIE **53**

INTRODUCERE

Spațiul cibernetic reprezintă un mediu care oferă atacatorului posibilitatea de a acționa în anonimitate – disimulând atacul, locul de origine și identitatea atacatorului – și folosind resurse financiare, materiale și umane reduse în comparație cu o acțiune militară clasică.

Intensitatea și complexitatea tehnologică a acestor atacuri (de regulă atacuri de tip Advanced Persistent Threat – APT), țintele strategice vizate, rezultatele obținute (în termeni de exfiltrarea de informații strategice, de dezinformare și chiar de întrerupere a serviciilor) și, nu în ultimul rând, motivația atacatorilor (care este politică prin natura sa, și nu infracțională) atenționează asupra apartenenței lor la arsenalul amenințărilor de tip hibrid. Delimitarea față de atacurile aparținând criminalității cibernetice este clară. Atacurile cibernetice reprezintă așadar una dintre cele mai noi amenințări hibride, care câștigă din ce în ce mai multă publicitate în ultimii ani.

În ultimii ani mediul de securitate a suferit schimbări profunde. În aceste condiții și pe fondul provocărilor la adresa securității și stabilității în vecinătatea sudică și estică a Uniunii Europene, apare necesitatea adaptării și consolidării capacității de a asigura securitatea, de a contracara amenințările hibride și a asigura reziliența. Pregătirea unui răspuns eficient în fața amenințărilor cibernetice, ca parte a amenințărilor hibride, necesită dialog și cooperare atât la nivel politic și operațional, atât la nivelul statelor afectate, între instituțiile cu responsabilități în asigurarea securității cibernetice, cât și în format regional și internațional. Măsurile și acțiunile întreprinse trebuie să aibă în vedere consolidarea gradului de conștientizare a amenințării și creșterea rezilienței societății, infrastructurilor și instituțiilor prin identificarea celor mai bune forme de protecție.

Pentru a crește reziliența în fața amenințării cibernetice este important să fie înțeleasă natura amenințării, să fie cunoscute și asumate vulnerabilitățile pe care un adversar le-ar putea exploata. Fiecare stat trebuie să conștientizeze că nu poate asigura securitatea cibernetică fără consolidarea capacităților de cooperare și coordonare în culegerea și schimbul de informații, precum și identificarea și evaluarea riscurilor și vulnerabilităților.

De asemenea, în asigurarea rezilienței în fața amenințării cibernetice un rol important îl are existența capacității de a face față amenințării, de a se adapta și transforma, prin dezvoltarea unor capabilități de avertizare timpurie și răspuns și prin promovarea și dezvoltarea unei culturi de securitate cibernetică. Crearea și dezvoltarea unei culturi de securitate cibernetică, atât la nivelul societății civile, cât și la nivelul decidenților politici și instituțiilor publice, prin derularea de parteneriate public-private, programe educaționale, exerciții comune, conferințe, seminarii, dezbateri și prezentări publice pe tema amenințării cibernetice, ca parte a amenințărilor de tip hibrid.

Așadar, asigurarea securității cibernetice în fața unei amenințări care nu cunoaște frontiere și care poate viza atât entități publice, cât și private, trebuie să reprezinte o preocupare constantă nu doar pentru

guverne, dar și pentru entitățile private și pentru cetățeni. Aceste entități trebuie să coopereze în prevenirea și combaterea atacurilor cibernetice care devin din ce în ce mai numeroase și mai sofisticate, provocând prejudicii importante în lumea reală.

Republica Moldova abordează domeniul securității cibernetice ca o dimensiune importantă a securității naționale, asumându-și angajamentul de a asigura cadrul normativ în domeniu pentru a face față cerințelor internaționale și care să faciliteze, cooperarea bilaterală și schimbul prompt și eficient de informații între autoritățile competente cu responsabilități în combaterea utilizării Tehnologiei Informației și Comunicațiilor/ICT în scopuri teroriste sau criminale.

Amenințările hibride utilizează mijloace convenționale și neconvenționale pentru a-și atinge obiectivele. Această lucrare explorează amenințarea cibernetică ca un posibil aspect al amenințărilor hibride. De asemenea, discută contextul termenului război hibrid, modul în care a apărut și a călătorit pe măsură ce situațiile empirice au evoluat și au nevoie de noi definiții.

BIBLIOGRAFIE

[1] Frank G. HOFFMAN, *Hybrid Warfare and Challanges*, [citat octombrie 2021]. Disponibil : https://smallwarsjournal.com/documents/jfqhoffman.pdf

[2] *Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar* [citat octombrie 2021]. Disponibil : https://www.nato.int/cps/en/natohq/opinions_118435.htm

[3] Comunicare comună către Parlamentul European şi consiliu *Cadrul comun privind contracararea ameninţărilor hibride Un răspuns al Uniunii Europene JOIN/2016/018 final*. [citat octombrie 2021] Disponibil: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52016JC0018,

[4] Mikael WEISSMANN, *Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework*, © 2019 published by Sciendo, work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License. [citat octombrie 2021]. Disponibil: https://sciendo.com/article/10.2478/jobs-2019-0002

[5] *Fake news and disinformation online*, Eurobarometer, [citat octombrie 2021]. Disponibil: https://europa.eu/eurobarometer/surveys/detail/2183

[6] *Barometru de opinie publică,* Republica Moldova, 2019 [citat octombrie 2021]. Disponibil: https://ipp.md/wp-content/uploads/2019/02/BOP_02.2019-new.pdf

[7] Pagină oficială a Ministerului Afacerilor Interne, [citat octombrie 2021]. Disponibil: https://www.mai.gov.md/ro/atributiile-ministerului-afacerilor-interne

[8] *The future of work in the EU*, Pagină web oficială European Parliament, [citat octombrie 2021]. Disponibil: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599315.

[9] Cadrul comun privind contracararea ameninţărilor hibride, Un răspuns al Uniunii Europene JOIN/2016/018 final, [citat octombrie 2021]. Disponibil: https://eur-lex.europa.eu/legal content/RO/TXT/?uri=CELEX%3A52016JC0018

[10] David CATTLER, *Assistant Secretary General for Intelligence and Security, What is NATO doing to address hybrid threats?,* [citat octombrie 2021]. Disponibil: https://www.nato.int/cps/en/natohq/news_183004.htm

[11] Michael RÜHLE, Clare ROBERTS, *Enlarging NATO's toolbox to counter hybrid threats,2021* [citat noiembrie 2021]. Disponibil: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid threats/index.html?

[12] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_12/20171207_1207-BackgrounderNATO-Moldova_r.pdf

[13] Planul IPAP 2017-2019 al Republicii Moldova, [citat noiembrie 2021]. Disponibil: https://mfa.gov.md/en/content/individual-partnership-action-plan-ipap-republica-moldova-nato-2017-2019

[14] Pagina web Ministerului Economiei și Infrastructurii, [citat noiembrie 2021]. Disponibil: https://www.mai.gov.md/ro/institutii-subordonate/serviciul-tehnologii-informationale#Baza

[15] Sascha-Dominik, BACHMANN, *„Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management"*, Amicus Curiae, Vol. 88, 2011, [citat noiembrie 2021]. Disponibil: https://papers.ssrn.com/sol3/papers.cfmabstract_id=1989808

[16] King MALLORY, *New Challenges in Cross-Domain Deterrence,* [citat noiembrie 2021]. Disponibil: https://www.rand.org/pubs/perspectives/PE259.html

[17] DIMEL model framework of national power, [citat noiembrie 2021]. Disponibil: https://www.thelightningpress.com/the-instruments-of-national-power/