

# ALESIA CHERNIKOVA

Ph.D. Candidate, Northeastern University, Boston, USA

chernikova.a@northeastern.edu — 1-781-350-0139 — [www.linkedin.com/in/alesia-chernikova](http://www.linkedin.com/in/alesia-chernikova) — [achernikova.github.io](http://achernikova.github.io)

## RESEARCH INTERESTS

---

Adversarial machine learning, fair and ethical AI, deep learning, network science, mathematical modeling, epidemiology, network robustness, cybersecurity, and threat intelligence.

## EDUCATION

---

**Northeastern University**, Boston, USA

Doctor of Philosophy in Computer Science

Advisor: Prof. Alina Oprea

09/2017 — Present

GPA: 3.9/4.00

**Belarusian State University**, Minsk, Belarus

Bachelor of Science: Applied Mathematics

Advisor: Prof. Vladimir Malugin

Thesis: "Development of risk management algorithms based on derivatives contracts."

09/2009 — 06/2014

GPA: 3.8/4.00

## ACADEMIC EXPERIENCE

---

**Northeastern University**

*Research Assistant*

Boston, USA

09/2017 — Present

- Proposed a new compartmental model of epidemiology to represent self-propagating malware (SPM) propagation in the networks using real-world WannaCry traces. Rigorously studied the characteristics of the SPM propagation process under homogeneous mixing assumption and on arbitrary networks.
- Proposed new defense algorithms leveraging spectral graph theory and extensively tested the behavior of existing defense techniques to improve network robustness of the large enterprise network in the face of SPM.
- Proposed a new framework for evasion attack algorithms that preserve possible feature dependencies to evaluate the robustness of deep learning models in constrained environments such as cybersecurity or healthcare. Evaluated the success of existing defense algorithms against proposed attack methodology.
- Demonstrated first evasion attacks against both classification and regression deep learning models used in the domain of self-driving cars.

**Amazon Web Services (AWS)**

*Research Scientist Intern*

Boston, USA

05/2020 — 08/2020, 05/2021 — 09/2021

- Collaborated with project manager and senior research scientists to identify AWS customer needs, proposed directions of possible research questions to address them, and described the relevant methodologies to solve the research questions.
- Created a scalable algorithm for tracing the activity in the AWS cloud represented as a heterogeneous graph to allow further research based on AWS cloud activity data.
- Proposed and implemented the methodology for lateral movement detection in the AWS cloud environment using Bayesian statistics and network science perspectives.
- Designed experiments and analyzed data to evaluate the effectiveness of developed methodologies utilizing Scala, Spark, GraphX, and MLlib.

**Belarusian State University**

*Undergraduate Research Assistant*

Minsk, Belarus

01/2012 — 12/2013

- Collaborated with a team of 9 people, including professors, post-doctoral, graduate, and undergraduate students, and a scientist from the National Bank of the Republic of Belarus in the research project on the estimation and evaluation of credit rankings of national enterprises using their real-world financial data.
- Participated in creating the methodology for credit rankings estimation using mathematical, statistical, and econometric methods and models.
- Independently achieved and managed the results for the building enterprise section.
- Collaborated in the development of the package for automated calculation of credit scores based on the proposed credit rankings evaluation methodology.

## TEACHING EXPERIENCE

---

**Northeastern University**

*Teaching Assistant for CS4100: Artificial Intelligence*

Boston, USA

09/2022 — 12/2022, 09/2023 — Present

- Held weekly office hours to answer questions, provide support, and review course material. Led discussions and answered questions to ensure students thoroughly understood the material.
- Graded assignments, exams, and research projects for a class of 90+ students.
- Assisted professor with homework and exam preparation.
- Advised students regarding research projects.

## PROFESSIONAL EXPERIENCE

---

### IBA Group

Senior Software Engineer

Minsk, Belarus

11/2013 — 07/2017

- Participated in the development of a large-scale IBM GSAR web portal.
- Tested software for bugs, fixed them, and maintained the portal's performance.
- Assisted the software architect with the efficiency and usability improvement of the portal.

## PUBLICATIONS

---

**Modeling Self-Propagating Malware with Epidemiological Models.** Applied Network Science 2023

A. Chernikova, N. Gozzi, S. Boboila, N. Perra, T. Eliassi-Rad, and A. Oprea.

**Cyber Network Resilience against Self-Propagating Malware Attacks.** ESORICS 2022

A. Chernikova, N. Gozzi, S. Boboila, N. Perra, P. Angadi, J. Loughner, M. Wilden, T. Eliassi-Rad, and A. Oprea.

**Fence: Feasible Evasion Attacks on Neural Networks in Constrained Environments.** ACM TOPS 2022

A. Chernikova and A. Oprea.

**Are Self-Driving Cars Secure?** SafeThings IEEE S&P Workshop 2019

**Evasion Attacks against Deep Neural Networks for Steering Angle Prediction.**

A. Chernikova, A. Oprea, C. Nita-Rotaru and BG. Kim

## TALKS

---

**"Towards Resilient Cybernetworks against Adversarial Attacks."** Amazon Web Services, 2023

**"Cybernetwork Resilience against Self-Propagating Malware Attacks."** ESORICS, 2022

**"Feasible Evasion Attacks in Constrained Environments."** CRA Seminar, 2022

**"Graph-based Statistical Detection of Anomalous Role Assumption Events."** Amazon Web Services, 2020

**"Feasible Evasion Attacks on Neural Networks in Constrained Environments."** ARL Meeting, 2020

**"Evasion Attacks against Deep Neural Networks for Steering Angle Prediction."** SafeThings Workshop, 2019

## SERVICE

---

Reviewer

ACM TOPS

Technical Program Committee

IEEE MILCOM AI for Cyber 2023

## AWARDS

---

**IEEE S&P and GREPSEC Travel Grant** 2019

**Khoury College of Computer Science Fellowship** 2017 — 2018

**National Bank of the Republic of Belarus Merit Scholarship** 2013 — 2014

**Belarusian State University Excellence Merit Scholarship** 2012 — 2014

## SKILLS

---

- **Programming:** Python, Java, Scala, Javascript, C/C++
- **Frameworks and Libraries:** PyTorch, Tensorflow, Keras, Spark

## SELECTED COURSES

---

Advanced Machine Learning (Bayesian methods for probabilistic modeling and inference), Data Visualization, Machine Learning, Advanced Algorithms, Data Mining (Unsupervised Learning), Distributed Systems, Theory of Probabilities and Mathematical Statistics, Methods of Optimization, Multivariate Statistical Analysis, Mathematical Theory of Forecasting, Discrete Mathematics and Graph Theory, Differential Equations, Matrix Analysis, Real and Complex Analysis, Algorithms and Data Structures, Game Theory, Macroeconomics, Microeconomics, Social Theory, Philosophy.