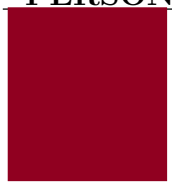
CURRICULUM VITAE

PERSONAL DETAILS



Name	YISROEL MIRSKY
Date and Place of Birth	18/04/88, CANADA
Date of Immigration	09/09/09
Work	Department of Software and Information Systems Engineering Ben-Gurion University of the Negev POB 653, Beer Sheva 84105, Israel yisroel@{post.bgu.ac.il, bgu.ac.il}
Home	3/23 Jacob Marsh, Beer Sheva, Israel, 8470915 +972 52 534 8770 (mobile) ymirsky1@gmail.com
Web	ymirsky.github.io offensive-ai-lab.github.io
Affiliations	Ben-Gurion University of the Negev
Statistics (Google Scholar)	**h-index:** 20 **Number of citations:** 3733

EDUCATION

B.Sc.	2009-2013	**Jerusalem College of Technology** -– Communication Systems Engineering Graduated with Excellence
M.Sc.*	2013-2015	**Ben-Gurion University** — Software and Information Systems Engineering Advisors: Prof. Bracha Shapira and Prof. Yuval Elovici Title of Thesis: Context Space Theory for Cyberspace Security.
Ph.D.	2015-2018	**Ben-Gurion University** — Software and Information Systems Engineering Advisors: Prof. Bracha Shapira and Prof. Yuval Elovici Title of Dissertation: Online Anomaly Detection Algorithms for Securing the Internet of Things
P.D.†	2019-2021	**Georgia Institute of Technology (Georgia Tech)** Institute for Information Security & Privacy (IISP) under Prof. Wenke Lee (h-index 100)

$*$ *Completed as part of the Direct Track Ph.D. program (M.Sc.+Ph.D. in 5 years).*

† *Georgia Tech is ranked #1 in Cyber Security (USA) and #1 in Computer Science Research (Global) [U.S. News & World Report '21, Times Higher Education '21]*

EMPLOYMENT HISTORY

2021-present **Title**: Tenure-track Lecturer, Zuckerman Faculty Scholar
Institution: Department of Software and Information Systems Engineering, Ben-Gurion University of the Negev.

2019-2021 **Title**: Post-doctoral Fellow, Researcher
Institution: Georgia Institute of Technology (Georgia Tech)

2014-2021 **Title**: Cyber Security Researcher & Research Project Manager
Institution: Cyber Security Research Center at BGU.

2016-2020 **Title**: Lecturer
Course: Intro to Cyber Security and Machine Learning
Institution: Department of Information Systems Engineering, BGU.

2013-2016 **Title**: Graduate Teaching Assistant
Lab: Intro to Software Engineering
Institution: Department of Information Systems Engineering, BGU.

2013-2014 **Title**: Graduate Teaching Assistant
Lab: Intro to Data Communication
Institution: Department of Information Systems Engineering, BGU.

2010-2013 **Title**: Research Assistant
Institution: Dep. of Computer Science, Jerusalem College of Technology.

2010-2013 **Title**: Undergraduate Teaching Assistant
Lab: Business Calculus
Institution: Dep. of Computer Science, Jerusalem College of Technology.

PROFESSIONAL ACTIVITIES

(a) **Positions in academic administration**

(b) **Professional Functions Outside Universities/Institutions**

2022 Reviewer - *research grant review*
NRF: National Research Foundation - *Singapore*
Description: Served as an NRF reviewer for an AI-related grant from researchers in Singapore, the US, and Europe.

2022 Reviewer - *research grant review*
ISF: Israeli Science Foundation
Description: Served as a reviewer for an ISF grant proposal in the domain of offensive AI.

2021 Panelist - *research grant review board*
NSF: US National Science Foundation
Description: Served as a reviewer for grants received by the NSF for their Secure and Trustworthy Cyberspace (SaTC) program [NSF 21-500], in the domain of offensive AI.

2018-Present Chair, Security for AI Workgroup, and INCS-CoE Community Fellow
INCS-CoE: InterNational Cyber Security Center of Excellence
Description: The world's first international Cyber security center of excellence. Members include Stanford, UC Berkeley, MIT, University of Maryland, and Northeastern University, Oxford, Cambridge, Imperial College London, University of Tokyo, Keio University, BGU, and the Technion.

Sept 2013 COST IC0905 "TERRA" Short Term Scientific Mission (STSM)
Sponsor: COST: European Cooperation in Science and Technology
Host: Kings College London (UK), Dr. Oliver Holland.
Subject: Power Efficient Modeling for Outdoor Femtocell Distributions

(c) **Significant Professional Consulting**

August 2019 Company: Integrated Health Information Systems (IHIS), Singapore
Description: Cyber Security in Healthcare (R&D)

(d) **Editor or member of editorial board of scientific or professional journal**

2024 Program committee member for the 3rd Workshop on Audiovisual Deepfake Generation and Detection at ACM Multimedia 2022
(Co-located with Rank A)

2023 Sensors, MDPI. Editor for a Special Issue: Adversarial Machine Learning: Attacks, Defences and Outlooks
Impact factor 3.3 (**Q1**, 147/670)

2023 Program committee member for the 2nd Workshop on Audiovisual Deepfake Generation and Detection at ACM CCS 2023
(Co-located with Rank A)

2021-2023 Sensors, MDPI. Topic Board, Editor
Impact factor 3.3 (**Q1**, 147/670)

2022 Program committee member for the 1st Workshop on Audiovisual Deepfake Generation and Detection at ACM Multimedia 2022
(Co-located with Rank A)

2021 Sensors, MDPI. Editor for a Special Issue: Advances in the detection of Audio and Video Deepfakes
Impact factor 3.3 (**Q1**, 147/670)

2020 Program committee member for 29h International Joint Conference on Artificial Intelligence, IJCAI (Main Track).
Rank A*

2019 Program committee member for 28th International Joint Conference on Artificial Intelligence, IJCAI (Main Track).
Rank A*

2017 Technical Chair for the Twelfth International Conference on Internet Monitoring and Protection (ICIMP'17).
Average acceptance rate 24%.

2013 International Conference on Advances in Vehicular Systems, Technologies and Applications (VTC 2013). Publisher: IEEE.
Rank A

(e) **Ad-hoc Reviewer for Journals**

2023 Transactions on Information Forensics and Security (T-IFS), IEEE.
Impact factor 6.2 (**Q1**)

2023 Artificial Intelligence Review (AIR), Springer Nature.
Impact factor 5.7 (**Q1**)

March 2023 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

July 2022 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

Mar 2022 PeerJ Computer Science.
Impact factor 2 (**Q1**)

Dec 2022 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

Dec 2021 Artificial Intelligence Review (AIR), Springer Nature.
Impact factor 5.7 (**Q1**)

Dec 2021 Transactions on Image Processing (TIP), IEEE.
Impact factor 10.9 (**Q1**)

Feb 2021 Artificial Intelligence Review (AIR), Springer Nature.
Impact factor 5.7 (**Q1**)

Feb 2021 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

Jan 2021 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

Jan 2021 Transactions on Neural Networks and Learning Systems (TNNLS), IEEE.
Impact factor 7.9 (**Q1**)

Nov 2020 The New England Journal of Medicine (NEJM)
Impact factor 74.7 (**Q1**, 1/2180)

Aug 2020 Transactions on Biometrics, Behavior, and Identity Science (T-BIOM), IEEE.

Aug 2020 Transactions on Information Forensics and Security (T-IFS), IEEE.
Impact factor 6.2 (**Q1**)

July 2020 Signal Processing-Image Communication,Elsevier.
Impact factor 2.8 (**Q2**)

May 2020 Sensors, MDPI
Impact factor 3.0 (**Q1**)

Oct 2019 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

2019 Transactions on Information Forensics and Security (T-IFS), IEEE.
Impact factor 6.2 (**Q1**)

Aug 2019 Transactions on Dependable and Secure Computing (TDSC), IEEE.
Impact factor 6.4 (**Q1**)

2018 Transactions on Neural Networks and Learning Systems (TNNLS), IEEE.
Impact factor 7.9 (**Q1**)

2018 Transactions on Information Forensics and Security (T-IFS), IEEE.
Impact factor 6.2 (**Q1**)

2017 Transactions on Information Forensics and Security (T-IFS),IEEE.
Impact factor 6.2 (**Q1**)

2016 Journal in Neural Computing and Applications, Springer.
Impact factor 4.2 (**Q1**)

2016 Information Fusion: An International Journal on Multi-Sensor, Multi-Source Information Fusion, Elsevier.
Impact factor: 6.6 (**Q1**)

EDUCATIONAL ACTIVITIES

(a) **Courses Taught**

2023-present Elements of Computing Systems, B.Sc., BGU

2021-present Database Systems Implementation, B.Sc., BGU

2021-present Computer Architecture & Operating Systems, B.Sc., BGU

2021-present Offensive AI, M.Sc. Ph.D., BGU

2017 Applied and Machine Learning in Security, M.Sc., Hochschule für Telekommunikation Leipzig, University of Applied Sciences, Germany

2014-2016 Intro to Software Engineering (lab)*, B.Sc., Ben-Gurion University
*Structured and rewrote the course

2014 Intro to Data Communications (lab), B.Sc., Ben-Gurion University

2012-2014 Calculus for Business (lab), B.Sc., Jerusalem College of Technology

(b) **Research Students**

Ph.D. 1. Guy Amit

M.Sc.
2. Moshe Mizrachi (M.Sc), 2022
   Other supervisor: Prof. Yuval Elovici
3. Shmulik Froimovich (M.Sc), expected 2024
4. Bar Avraham (M.Sc), expected 2024
5. Guy Frankovits (M.Sc), expected 2024
6. Maor Biton (M.Sc), expected 2024
7. Roey Bokobza (M.Sc), expected 2024
8. Daniel Ayzenshteyn (M.Sc), expected 2025
9. Freddy Grabovsky (M.Sc), expected 2025
10. Lior Yasur (M.Sc), expected 2025
11. Yaniv Hacmon (M.Sc), expected 2025
12. Amit Kravchik (M.Sc), expected 2025
13. Roy Weiss (M.Sc), expected 2025

External
14. Shashank Preyan (M.Sc), Intern
15. Sanket Badhe (M.Sc) Instagram
16. Leyan Pan (M.Sc) Georgia Tech
17. Tapdig Maharamli (M.Sc) BHOS

Research Students - as their technical advisor

Ph.D.
1. Evan Downing (Ph.D.), expected 2023
   Other supervisor: Prof. Wenke Lee, Georgia Institute of Technology, USA
2. Guy Amit (M.Sc), expected 2023
   Other supervisor: Prof. Yuval Elovici

M.Sc.
3. Eran Fienman (M.Sc.), 2017
   Other supervisors: Prof. Lior Rokach and Prof. Bracha Shapira
4. Liron ben Kimon (M.Sc.), 2018
   Other supervisors: Prof. Lior Rokach and Prof. Bracha Shapira
5. Tomer Doitshman (M.Sc.), 2018
   Other supervisors: Dr. Asaf Shabtai and Prof. Yuval Elovic
6. Naor Kalbo (M.Sc.), 2018
   Other supervisors: Dr. Asaf Shabtai and Prof. Yuval Elovici
7. Tomer Golomb (M.Sc) 2019
   Other supervisors: Prof. Yuval Elovici
8. Nimrod Harris (M.Sc) 2019
   Other supervisors: Dr. Niv Gilboa and Prof. Yuval Elovici
9. Dvir Cohen (M.Sc), 2020
   Other supervisor: Dr. Asaf Shabtai
10. Guy Amit (M.Sc), 2021
    Other supervisor: Prof. Yuval Elovici
11. Simon Dzanashvili (M.Sc.), expected 2021
    Other supervisor: Dr. Asaf Shabtai

12. Yotam Intrador (M.Sc), expected 2021
    Other supervisors: Dr. Asaf Shabtai, Dr. Gilad Katz
13. Hodaya Binyamini (M.Sc), expected 2021
    Other supervisor: Dr. Asaf Shabtai

B.Sc. Proj.

14. Daniel Deri, Dor Amsalem (B.Sc.), 2023

15. Marina Trostyanetsky, Reut Pravda, and Roi Vaknin (B.Sc.), 2016
    Other supervisor: Prof. Bracha Shapira

AWARDS, CITATIONS, HONORS, FELLOWSHIPS

(a) Honors, Citation Awards

2023 International Congress of Basic Science (ICBS)
Frontiers of Science Award
A prestigious award for scientific contributions in the last 5 years. The award is nominated by leaders in the respective fields including Turing Award and Nobel Prize winners. The award is funded by the Chinese Ministry of Science and the Government of Beijing and was presented to Dr. Mirsky in the Great Hall of the People.

2021 AutoSec NDSS'21 Workshop
Best Demo Award
Attacking Tesla Model X's Autopilot Using Compromised Advertisement

2020 CSAW'20 Applied Research Competition in Security
Best Paper Award Regional Finalist
Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks

2019 IEEE Computer Society
Best Paper Award from Pervasive Computing
N-baiot—network-based detection of iot botnet attacks using deep autoencoders
(IF 3.3, 53/262, **Q1**)

2018 Ben-Gurion University, Department of Information Systems Engineering
Excellence in Ph.D. Studies

2017 Ben-Gurion University
Dean's Award for Highest Excellence in Ph.D. Studies

2016 Ben-Gurion University, Department of Information Systems Engineering
Excellence in Ph.D. Studies

2015 Ben-Gurion University, Department of Information Systems Engineering
Excellence in Ph.D. Studies

2013 Jerusalem College of Technology
Excellence in Research, graduation award

2013 Jerusalem College of Technology
Excellence in B.Sc. Studies, graduation award

(b) **Fellowships** – Total Funding: $1.05 million

2021-2025 **Title**: Zuckerman Faculty Scholar
Granting Foundation: Zuckerman Institute, Zuckerman STEM Leadership Program
Amount: $700K **Description**: A prestigious fellowship for new faculty members to help them build a new research lab over four years. The nominees are a selected from all of Israel's universities by the Zuckerman Foundation and the Israeli Council for Higher Education.

2019-2021 **Granting Foundation**: The Israeli National Cyber Bureau
Amount: $250K
Purpose: A scholarship to perform post-doctoral studies abroad in the domain of cyber security. The purpose of the grant is to help advance national strength in the cyber field.

2013-2018 **Granting Foundation**: Milgat Darom, Amitai Lahish Foundation
Amount: $85K
Purpose: A prestigious scholarship awarded to exemplary Ph.D. students to support them during their direct track program.

2018 **Granting Foundation**: Strage-BGU Foundation
Amount: $2K
Purpose: Awarded to excellent cyber security researchers, to be used in funding their travel to conferences.

2016 **Granting Foundation**: Benny Gantz Award for Excellence in Cybersecurity Research
Amount: $10K
Purpose: To support excellent researchers in cyber security

2010-2013 **Granting Foundation**: Jerusalem College of Technology
Amount: $1.5K
Purpose: Annual award for students with an average over 90 that voluntarily tutor fellow students.

SCIENTIFIC PUBLICATIONS

h-index: 20 **Total citations:** 3733 **Publications:** 44

(a) **Authored books**

(b) **Editorship of collective volumes**

(c) **Refereed chapters in collective volumes and Conference proceedings**

1. Yoram Haddad, and Yisroel Mirsky. *Power efficient femtocell distribution strategies*. 19th International Conference on Software, Telecommunications and Computer Networks, 2011.
   [link] Cites: 10
2. Yisroel Mirsky, and Yoram Haddad. *A linear downlink power control algorithm for wireless networks*. IEEE Wireless Telecommunications Symposium (WTS), 2013.
   [link] Cites: 2
3. Mordechai Guri, Matan Monitz, Yisroel Mirsky, and Yuval Elovici. *Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations*. IEEE 28th Computer Security Foundations Symposium (CSF), 2015.
   [link] (**Rank A**) Cites: 201
4. Yisroel Mirsky, Noam Gross, and Asaf Shabtai. *Up-High to Down-Low: Applying Machine Learning to an Exploit Database*. International Conference for Information Technology and Communications, 2015.
   [link] (Acceptance rate 33%)
5. Yisroel Mirsky, Bracha Shapira, Lior Rokach, and Yuval Elovici. *pcstream: A stream clustering algorithm for dynamically detecting and managing temporal contexts*. Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2015.
   [link] (**Rank A**) Cites: 22
6. Yisroel Mirsky, Aviad Cohen, Roni Stern, Ariel Felner, Lior Rokach, Yuval Elovici, and Bracha Shapira. *Search problems in the domain of multiplication: Case study on anomaly detection using markov chains*. Eighth Annual Symposium on Combinatorial Search (SoCS), 2015.
   (Acceptance rate: 43%) Cites: 3
7. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. *GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies*. USENIX Security Symposium, 2015.
   [link] (**Rank A***) Cites: 193
8. Yisroel Mirsky, Asaf Shabtai, Lior Rokach, Bracha Shapira, and Yuval Elovici. *Sherlock vs moriarty: A smartphone dataset for cybersecurity research*. Proceedings of the 2016 ACM workshop on Artificial intelligence and security (AISec), 2016.
   [link] (Acceptance rate: 31%, co-located with ACM CCS (Rank A*)) Cites: 71
9. Liron Ben Kimon, Yisroel Mirsky, Lior Rokach, and Bracha Shapira. *User verification on mobile devices using sequences of touch gestures*. The 25th Conference on User Modeling, Adaptation and Personalization, 2017.
   [link] (**Rank A**, Acceptance rate: 10%) Cites: 2
10. Yisroel Mirsky, Tal Halpern, Rishabh Upadhyay, Sivan Toledo, and Yuval Elovici. *Enhanced situation space mining for data streams*. Proceedings of the Symposium on Applied Computing (ACM SAC), 2017.
    [link] (Rank B, Acceptance rate: 23%) Cites: 8
11. Mordechai Guri, Yisroel Mirsky, and Yuval Elovici. *9-1-1 DDoS: attacks, analysis and mitigation*. IEEE European Symposium on Security and Privacy (EuroS&P),

2017.
[link] (**Rank A**) Cites: 35

12. Yisroel Mirsky, Mordechai Guri, and Yuval Elovici. *HVACKer: Bridging the Air-Gap by Manipulating the Environment Temperature*. Depth Security Vol. II (Book Chapter), Magdeburg Institute for Security Research, 2017.
[link] Cites: 24
13. Tomer Golomb, Yisroel Mirsky, and Yuval Elovici. *CIoTA: Collaborative IoT anomaly detection via blockchain*. Workshop on Decentralized IoT Systems and Security (DISS), 2018.
[link] (Co-located with NDSS, Rank A*) Cites: 106
14. Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai. *Kitsune: an ensemble of autoencoders for online network intrusion detection*. The Network and Distributed System Security Symposium (NDSS), 2018.
[link] (**Rank A***, Acceptance rate: 15%) Cites: 889
15. Yisroel Mirsky, Yoram Haddad, Orit Rozenblit, and Rina Azoulay. *Predicting Wireless Coverage Maps Using Radial Basis Networks*. IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018.
[link] (Rank B) Cites: 9
16. Liron Ben Kimon, Yisroel Mirsky, Lior Rokach, and Bracha Shapira. *Utilizing sequences of touch gestures for user verification on mobile devices*. Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2018.
[link] (**Rank A**) Cites: 4
17. Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici. *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. USENIX Security Symposium, 2019.
[link] (**Rank A***) Cites: 209
18. Ben Nassi, Yisroel Mirsky, Dudi Nassi, Raz Ben-Netanel, Oleg Drokin, and Yuval Elovici. *Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks*. Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS), 2020.
[link] (**Rank A***) Cites: 61
19. Lior Sidi, Yisroel Mirsky, Asaf Nadler, Yuval Elovici, and Asaf Shabtai. *Helix: DGA Domain Embeddings for Tracking and Exploring Botnets*. Proceedings of the 29th ACM International Conference on Information and Knowledge Management (CIKM), 2020.
[link] (**Rank A**) Cites: 6
20. Dvir Cohen, Yisroel Mirsky, Yuval Elovici, Rami Puzis, Manuel Kamp, Tobias Martin, and Asaf Shabtai. *DANTE: A Framework for Mining and Monitoring Darknet Traffic*. The 25th European Symposium on Research in Computer Security (ESORICS), 2020.
[link] (**Rank A**) Cites: 17
21. Yisroel Mirsky, Benjamin Fedidat, and Yoram Haddad. *An Encryption System for Securing Physical Signals*. 16th EAI International Conference on Security and Pri-

vacy in Communication Networks (SecureComm), 2020.
[link] (Rank B)

22. Evan Downing, Yisroel Mirsky, Kyuhong Park, and Wenke Lee. *DeepReflect: Discovering Malicious Functionality through Binary Reconstruction*. USENIX Security Symposium, 2021.
[link] (**Rank A***) Cites: 10
23. Ben Nassi, Yisroel Mirsky, Dudi Nassi, Raz Ben-Netanel, Oleg Drokin, and Yuval Elovici. *Attacking Tesla Model Xs Autopilot Using Compromised Advertisement*. Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2021.
(Co-located with NDSS, Rank A*)
24. Yisroel Mirsky. *Discussion Paper: The Integrity of Medical AI*. Proceedings of the 1st Workshop on Security Implications of Deepfakes and Cheapfakes, 2022.
[link]
25. Yisroel Mirsky, George Macon, Michael Brown, Carter Yagemann, Matthew Pruett, Evan Downing, Sukarno Mertoguno, and Wenke Lee. *VulChecker: Graph-based Vulnerability Localization in Source Code*. USENIX Security Symposium, 2023.
[link] (**Rank A***) Cites: 2
26. Guy Frankovits, and Yisroel Mirsky. *Discussion Paper: The Threat of Real Time Deepfakes*. Proceedings of the 2nd Workshop on Security Implications of Deepfakes and Cheapfakes, 2023.
27. Lior Yasur, Guy Frankovits, Fred M Grabovski, and Yisroel Mirsky. *Discussion Paper: The Threat of Real Time Deepfakes*. The 18th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023), 2023.
(**Rank A**)
28. Guy Amit, and Yisroel Mirsky. *Transpose Attack: Stealing Datasets with Bidirectional Training*. Network and Distributed System Security (NDSS) Symposium 2024, 2024.
(**Rank A***)

(d) **Refereed articles and refereed letters in scientific journals**

1. Yisroel Mirsky, Asaf Shabtai, Bracha Shapira, Yuval Elovici, and Lior Rokach. *Anomaly detection for smartphone data streams*. IEEE, Pervasive and Mobile Computing, 2017.
[link] (IF 3.0, 11/77, **Q1**) Cites: 35
2. Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. *N-baiot: network-based detection of iot botnet attacks using deep autoencoders*. IEEE, Pervasive Computing, 2018.
[link] (IF 3.3, 53/262, **Q1**) Cites: 1032
3. Orit Rozenblit, Yoram Haddad, Yisroel Mirsky, and Rina Azoulay. *Machine Learning Methods for SIR Prediction in Cellular Networks*. Elsevier, Physical Communication, 2018.
[link] (IF 1.58, 181/266, Q3) Cites: 15

4. Benoit Desjardins, Yisroel Mirsky, Markel Picado Ortiz, Zeev Glozmand, Lawrence Tarbox, Robert Hornf, and Steven C. Horii. *DICOM images have been hacked! Now what?*. American Roentgen Ray Society (ARRS), American Journal of Roentgenology (AJR), 2019.
[link] (IF 3, 68/2180, **Q1**) Cites: 35
5. Yisroel Mirsky, Naor Kalbo, Asaf Shabtai, and Yuval Elovici. *Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs*. IEEE, Transaction on Forensics and Security, 2019.
[link] (IF 6.2, 5/103, **Q1**) Cites: 38
6. Yisroel Mirsky, Naor Kalbo, Asaf Shabtai, and Yuval Elovici. *The Security of IP-based Video Surveillance Systems*. MDPI, Sensors, 2020.
[link] (IF 3.28, 33/539, **Q1**) Cites: 50
7. Yisroel Mirsky, Tomer Golomb, and Yuval Elovici. *Lightweight Collaborative Anomaly Detection for the IoT using Blockchain*. Elsevier, Journal of Parallel and Distributed Computing (JPDC), 2020.
[link] (IF 1.8, 103/413, **Q1**) Cites: 35
8. Yisroel Mirsky, and Mordechai Guri. *DDoS Attacks on 9-1-1 Emergency Services*. IEEE, Transactions on Dependable and Secure Computing (TDSC), 2020.
[link] (IF 6.4, 4/52, **Q1**) Cites: 8
9. Yisroel Mirsky, and Wenke Lee. *The Creation and Detection of Deepfakes: A Survey*. ACM, ACM Computing Surveys (CSUR), 2021.
[link] (IF 7.99, 4/108, **Q1**) Cites: 387
10. Yisroel Mirsky, Ambra Demontis, Jaidip Kotak, Ram Shankar, Deng Gelei, Liu Yang, Xiangyu Zhang, Maura Pintor, Wenke Lee, Yuval Elovici, and Battista Biggio. *The Threat of Offensive AI to Organizations*. Elsevier, Computers & Security (COSE), 2022.
(IF 5.1, 34/246, **Q1**) Cites: 29
11. Luis Marti Bonmati, Ana Miguel Blanco, Amelia Suarez, Mario Aznar, Jean Paul Beregi, Laure Fournier, Emanuele Neri, Andrea Laghi, Manuela Franca, Francesco Sardanelli, Tobias Penzkofer, Philippe Lambin, Ignacio Blanquer, Marion Irene Menzel, Karine Seymour, Sergio Figueiras, Katharina Krischak, Ricard Martinez, Yisroel Mirsky, Guang Yang, and Angel Alberich. *CHAIMELEON project: Creation of a pan-European repository of health imaging data for the development of AI-powered cancer management tools*. Frontiers, Frontiers in Oncology, 2022.
(IF 6.2, **Q1**) Cites: 9
12. Yisroel Mirsky. *IPatch: A Remote Adversarial Patch*. Springer Nature, Cybersecurity (CYSE), 2023.
(IF 4.2, **Q1**) Cites: 6
13. Ben Nassi, Yisroel Mirsky, Jacob Shemesh, Raz Netanel, Dudi Nassi, and Yuval Elovici. *Protecting Semi/Fully Autonomous Cars from Phantom Attacks*. ACM, Communications of the ACM (CACM), 2023.
(IF 14, 1/110, **Q1**)

(e) **Published scientific reports and technical papers**

1. Yisroel Mirsky^{PI}, Yuval Elovici (*Ben-Gurion University*), Wenke Lee (*Georgia Institute of Technology*), Battista Biggio (*University of Cagliari*), Yang Liu (*Nanyang Technological University*), Xiangyu Zhang (*Purdue*), Benjamin I. P. Rubinstein (*University of Melbourne*)
   White Paper: Understanding how AI Impacts the Cyber Kill Chain.
   Published at The Keio University International Cybersecurity Symposium, 2021.

(f) **Unrefereed professional articles and publications**

1. Mordechai Guri, Yisroel Mirsky, and Yuval Elovici. *Attackers can make it impossible to dial 911.* The Conversation, 2017.
   [link]
2. Eran Fainman, Bracha Shapira, Lior Rokach, and Yisroel Mirsky. *Online Budgeted Learning for Classifier Induction.* arXiv preprint arXiv:1903.05382, 2019.
   [link] Cites: 1
3. Ben Nassi, Yisroel Mirsky, Dudi Nassi, Raz Ben-Netanel, Oleg Drokin, and Yuval Elovici. *Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems.* Cryptology ePrint Archive, 2020.
   [link] Cites: 52

(g) **Classified articles and reports**

1. Yisroel Mirsky, Yuval Elovici, Asaf Shabtai. 2017-2018. Vulnerabilty Assessment and Mitigation Tactics. NEC Cooperation Japan.
2. Yisroel Mirsky, Wenke Lee, Sukarno Mertoguno, Carter Yageman, Michael Brown. 2019-2020. Research Development Reports. DARPA.

LECTURES, PRESENTATIONS, AND INVITED SEMINARS

(a) **Invited plenary lectures at conferences/meetings**

1. **Helsinki University Hospital** 4th AI Conference (Helsinki 2020)
   (**Keynote Lecture**) *–delayed by COVID*
   Medical Data Trolling – How Medical Data can be Easily Fabricated
2. **ACM CCS'20** - The ACM Conference on Computer and Communications Security
   Co-author of keynote lecture given by Prof. Wenke Lee (Online 2020)

(b) **Presentation of papers at conferences/meetings (oral or poster)**

1. IEEE International Software Conference on Software - Science, Technology & Engineering, PhD Symposium (Israel, **SWSTE** 2016)
   Unsupervised Situation Space Mining for Smartphone Security
2. **CODE BLUE** (BlackHat Japan) Security Conference (Tokyo, 2016)
   Air-Gap Security: State-of-the-art Attacks, Analysis, and Mitigation

3. In-depth Security Conference (Austria, **DeepSec** 2016)
   Bridging the Air-Gap – Data Exfiltration from Air-Gap Networks
4. BigData with Coudera and Hadoop, workshop (Israel, 2017)
   SherLock vs Moriarty: A Massive Sensor Dataset for Cyber Security research.
5. Data Mining and Business Intelligence (Israel, **DMBI** 2017)
   Securing IoT Video Surveillance Systems with Online Machine Learning
6. **Keio University** 7th International Cybersecurity Symposium (Tokyo 2018)
   Panelist: The Future for the Security of AI
7. **Keio University** 9th International Cybersecurity Symposium (Tokyo 2019)
   The Security of AI
8. **Black Hat,** Asia (Singapore 2019)
   Briefing: See Like a Bat: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs
9. **DEF CON 27** AI Village (USA 2019)
   Automated Injection & Removal of Medical Evidence in CT and MRI Scans
10. **RSA Security Conference** (USA 2021)
    Securing Tesla & Mobileye From Split-Second Phantom Attacks

(c) **Presentations at informal international seminars and workshops**

1. Israel Networking Day at Google Tel-Aviv (Israel, 2014)
   A linear downlink power control algorithm for wireless networks.
2. The CyberWire, community cyber security news podcasts from industry and academia:
   A regular guest speaker talking about a wide range of cyber security topics. 2016-2019. https://thecyberwire.com/

(d) **Seminar presentations at universities and institutions**

1. **Bell Labs** Research Center, Nokia (2018)
   Online Anomaly Detection Algorithms for Securing the Internet of Things
2. **MIT - Massachusetts Institute of Technology** Research Seminar (2019)
   An invited talk on my research at the ALPHA group of CSAIL.
3. **Royal Holloway University of London** Invited Talk – Research Seminar (2019)
   Medical Deepfakes: How malware can automatically tamper CT and MRI Scans
4. **Australia's National Science Agency - CSIRO Data61** Invited Talk – Research Seminar (2022)
   The Threat Horizon of Deepfakes

PATENTS

1. (**2013**) A harmonic based encryption and decryption system for waveform signals
   Inventors: Yisroel Mirsky, Benjamin Fedidat, and Yoram Haddad
   International Application No.: PCT/EP2015/050060, WO2015097312A1

2. (**2017**) Detection of Malicious Network Activity
   Inventors: Yisroel Mirsky, Yuval Elovici, Asaf Shabtai, Oleg Brodt, and Nakae Masayuki
   US Patent No.: 11,201,882

3. (**2017**) Machine Learning Methods for SIR Prediction in Cellular Networks
   Inventors: Yisroel Mirsky, Yoram Haddad, Rina Azoulat, Orit Rozenblit
   Patent No.: WO2019211792A1

4. (**2018**) Echo Detection of Man-in-the-Middle LAN Attacks
   Inventors: Yisroel Mirsky, Naor Kalbo, Yuval Elovici, Asaf Shabtai
   Patent No.: WO2019116370A1, US Patent App. 16/772,985

5. (**2018**) Method and for Clustering Darknet Traffic Streams with Word Embeddings
   Inventors: Dvir Cohen, Yisroel Mirsky, Asaf Shabatai, Yuval Elovici, Rami Puzis, Tobias Martin, Manuel Kamp
   US Patent No.: 16/838,136 EU: EP3719685A1

6. (**2019**) Collaborative IoT Anomaly Detection via Blockchain
   Inventors: Yisroel Mirsky, Tomer Golomb, and Yuval Elovici
   EU: EP3528457A2

7. (**2020**) Embedded DGA Representations for Botnet Analysis
   Inventors: Lior Sidi, Yisroel Mirsky, Asaf Shabtai, Yuval Elovici, Oleg Brodt, David Mimran
   European Patent: EP3614645A1

8. (**Pending**) Methods for detecting phantom projection attacks against computer vision algorithms
   Inventors: Yisroel Mirsky, Ben Nassi, Yuval Elovici

9. (**Pending**) Predicting Wireless Coverage Maps using Radial Basis Networks
   Inventors: Yisroel Mirsky, Yoram Haddad, Rina Azoulay, and Orit Rozenblit

10. (**Pending**) A Method for Detecting and Preventing Synthetic Voice and Video Calls
    Inventor: Yisroel Mirsky
    Provisional Patent Application 63/302,086

RESEARCH GRANTS

Number of Grants: 11 **Total Funding:** $35.6 million

(a) **Prestigious Grants**

2023 **Granting Institution:** (**TII**) The Technology Innovation Institute, Secure Systems Research Center (SSRC), United Arab Emirates (UAE)

Opportunity: DESA: Double Edged Sword of AI (DESA): Defending Autonomous Systems against Offensive AI

Subject: Threat research and the development of deception-based defences against the threat of AI-Powered malware.

Grantees: Yisroel Mirsky^{LeadPI}, Kobi Gal^{PI}

Duration: 2023-2026 (3 years)

Grant Size: $1.6 million

2022 **Granting Institution:** (**INCD**) Israel National Cyber Directorate

Opportunity: Mabadata (AutoDefenceML)

Subject: The research and development of a platform for automatic penetration testing and vulnerability analysis of machine learning models against adversarial attacks, and the automatic recommendation of defences for hardening given models against adaptive adversaries.

Grantees: Yisroel Mirsky^{LeadPI}, Yuval Elocivi^{PI}

Duration: 2022-2024 (2 years)

Grant Size: $0.6 million

2021 **Granting Institution:** (**BIRD**) Israel-U.S. Binational Industrial Research and Development Foundation

Opportunity: Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience:
U.S.-Israel Energy Center Cyber Topic CFP.

Subject: The research and development of tools for securing the energy sector against current and advanced cyber threats. My component deals with the detection of deepfake-based social engineering attacks.

Grantees: Ben-Gurion University (Yisroel Mirsky 1 of 6), Georgia Institute of Technology (4 PIs), Arizona State University (3), Nexant (5), RAD (3), OTORIO (2)

Duration: 2021-2024 (3 years)

Grant Size: $6 million

2021 **Granting Institution:** (**DARPA**) The Defense Advanced Research Projects Agency, Department of Defense, Unites States

Opportunity: Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS): *HR001120S0058.*

Subject: A platform for transforming legacy software, in the form of source code and/or non-obfuscated-binary, into a more efficient, robust, and formally verifiable version of it for enhanced security.

Grantees: Brendan Saltaformaggio^{PI}, Taesoo Kim^{PI}, Wenke Lee^{PI}, Alessandro Orso^{PI}, Qirun Zhang^{PI}, Yisroel Mirsky^{PI}, Martin Osterloh^{PI}, Jason Li^{I}, Michael Brown^{PI}, Sukarno Mertoguno^{PI}, UT Dallas Kevin Hamlen^{PI}, Nicholas Evancich^{I}

Duration: 2021-2025 (5 years)

Grant Size: \$10.6 million

2020 **Granting Institution:** (**DARPA**) The Defense Advanced Research Projects Agency, Department of Defense, Unites States

Opportunity: Artificial Intelligence Exploration (AIE) Opportunity, ReMath AI (Artificial Intelligence) Exploration program: *DARPA-PA-20-02*.

Subject: Automatic recovery of human interpretable mathematical models from legacy code in cyber physical systems using deep learning.

Grantees: Dr. J. Clayton Kerce^{PI}, Dr. Wenke Lee^{PI}, Dr. Yisroel Mirsky^{I}, Dr. Sukarno Mertoguno^{PI}, Mr. Michael Brown^{I}, Dr. James Fairbanks^{I}.

Duration: 2020-2022 (1.5 years)

Grant Size: \$1 million

2019 **Granting Institution:** (**DARPA**) The Defense Advanced Research Projects Agency, Department of Defense, Unites States

Opportunity: Artificial Intelligence Exploration (AIE) Opportunity, Artificial Intelligence Mitigations of Emergent Execution (AIMEE): *DARPA-PA-19-03-02*.

Subject: Research and development of a tool (HECTOR) which can detect emerging vulnerabilities in high-level code during design time, base on deep learning and formal verification (canonical execution)

Grantees: Prof. Wenke Lee^{PI}, Dr. Yisroel Mirsky^{I}, Dr. Sukarno Mertoguno^{PI}, Dr. Clayton Kerce^{PI}.

Duration: 2019-2021 (1.5 years)

Grant Size: \$1 million

2020 **Granting Institution:** (**Horizon 2020**) The EU Framework Programme for Research and Innovation (a prestigious research grant by the European Union)

Opportunity: A Public Health Imaging repository for AI Research. DT-TDS-05-2020

Subject: A project in cooperation with 18 companies and universities in the EU and UK. The project aims to set-up and populate a health imaging data repository, giving the AI research community access to large datasets of high quality anonymised data. My part of the project relates to researching methods towards detecting and preventing attacks on the AI which will be using this repository.

Grantees: Yisroel Mirsky^{PI} (Leading PI), Yuval Elovici^{PI}

Duration: 2020-2023 (4 years)

Grant Size: \$9.7 million, with \$580K awarded to our contribution ($\frac{1}{16}$th of the total in a project with 18 members).

2020 **Granting Institution:** (**TII**) The Technology Innovation Institute, Secure Systems Research Center (SSRC), United Arab Emirates (UAE)

Opportunity: End-2-End Security and Resilience in Cyber Physical and Autonomous Systems

Subject: Securing autonomous drones with real-time constraints by removing superfluous logic (debloating), simplifying communication protocols (dialecting), and detecting attacks through contextual analysis (diversification).

Grantees: Prof. Taesoo Kim^{PI}, Prof. Wenke Lee^{PI}, Yisroel Mirsky^{I}, Hyungjoon Koo^{I}, Dr. Kevin Stevens^{I}, Dr. Daehee Jang^{I}

Duration: 2020-2023 (3 years)

Grant Size: $1.5 million

2019 **Granting Institution:** (**NRF**) National Research Foundation, Singapore

Title: Enhancing Cyber Resilience of Deep Learning Models against Adversarial Cyber Attacks

Subject: In this project, we creating an automated framework for measuring the robustness of, and protecting deep neural networks in adversarial environments. We are also investigating cyber physical attacks on the hardware used to accelerate the deep learning.

Grantees: Liu Yang^{PI}, Thambipillai Srikanthan^{PI}, Yuval Elovici^{PI}, Asaf Shabtai^{PI}, Yisroel Mirsky^{I}, Lei Ma^{I}, Fuyuan Zhang^{I}, Xiaolu Hou^{I}.

Duration: 2019-2022 (3 years)

Grant Size: $2.3 million

(b) **Other Research Grants**

2019 **Granting Institution:** (**Samsung SDS**) South Korea

Title: Kumiho: Lightweight Network Intrusion Detection

Subject: A research project funded by Samsung on extending the Kitsune NIDS for Internet taffic and continuous learning in an adversarial setting.

Grantees: Dr. Yisroel Mirsky^{PI}, Prof. Yuval Elovici^{PI}, and Dr. Asaf Shabtai^{PI}.

Duration: 4 months

Grant Size: $55K

2017 **Granting Institution:** (**NCB**) The Israeli National Cyber Bureau

Title: An AI-based Anomaly Detection Ensemble for Cyber Security

Subject: Lightweight anomaly detection of both cyber and physical attacks on smartphones using plan recognition and heuristic search.

Grantees: Prof. Ariel Felner^{PI}, Prof. Shimony^{PI}, Dr. Kobi Gal^{PI}, Yisroel Mirsky^{I}, Reut Mirsky^{I}.

Duration: 2017 (1 year)

Grant Size: $200K

ADDITIONAL INFORMATION

(a) Recent Volunteer Work and Fundraising for BGU

Nov. '20 CABGU - New Technologies and Their Cyber Threats Webinar, Virtual – Panelist

Oct. '20 CABGU - Board meeting talk on BGU's advances in AI security

Mar. '20 AABGU - Cyber at BGU Fundraiser, Los Angeles USA – Panelist

Feb. '20 AABGU - Protecting Our Future Fundraiser, Houston USA – **Keynote**

(b) Notable Interviews

2022. Protocol

2020. World Health Organization (WHO), News Bulletin, The Mighty, Oncology Live

2019. Washington Post, CBS 58 News, The Mighty, Medscape, The Lancet

2016. Wall Street Journal, Washinton Post

(c) In the Media

September 2023. **Defences Against Deepfake Voices** Fortune

August 2022. **Threat of Real-time Deepfake Voices** Protocol

Febuary 2020. **Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems** deeplearning.ai (Andrew Ng's AI education startup), Ars Technica, ZDNet, Threat Post, TechXplore, Motor Trend, ...

January 2020. **DICOM images have been hacked! Now what?** American Journal of Roentgenology: Cover of April issue AJR Online and featured in Radiology Business and Radiology Smart Brief.

April 2019. **CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning**
The Washington Post –front page in Business, Forbes, BBC, Engadget, Computing.co.uk, PCMag.com, TechCrunch, Gizmodo, MedScape, The Inquirer, Extremetech, MedTech Dive, TheMighty, Healthimaging.com, Times of Israel, Jerusalem post, Global Security magazine, World Israel News, China.org.cn, PinkVilla, Radiology Business, Xinhua, Becker Hospital review, The Indian Wire, Slash Gear, Tech Xplore, Techspot, Hot Hardware, Slashdot, Radlink, Algolia, Mass Device, Health IT analytics, Antiscam.com, Cdrinfo.com, Qwerty.red, Smartwatchtechnology.com, ...

2016-2017. **9-1-1 DDoS: Attack, Analysis and Mitigation**
The Wall Street Journal, Washington Post, Washinton Times, The Hill, The Daily Beast, CNET, HackRead, IBTimes, DailyMail, SC Magazine, NewsWeek, GCN, ComputerWorld

March 2015. **BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulations**
Spectator, InfoWorld, Hacked, DailyMain, Geek, ThreatPost, NetworkWorld, ExtremeTech

July 2015. **Data Exfiltration from Air-Gapped Computers over GSM Frequencies**
Wired, SecurityWeek, theRegister.co.uk, ComputerWorld, SCMagazine, Infosecurity Magazine