Vahid Behzadan

Assistant Professor of Computer Science

Department of Electrical and Computer Engineering
University of New Haven
+1 (203) 479 4723
vbehzadan@newhaven.edu
www.vbehzadan.com

Academic Appointments

Aug 2019 – **Assistant Professor (Tenure-Track) of Computer Science and Data Science**, *University of New Haven*.

Aug 2019 – **Founder and Director**, *Secure and Assured Intelligent Learning (SAIL) lab*, University of New Haven.

Education

Aug 2014 –June 2019 **Ph.D. in Computer Science**, *University of Nevada, Reno & Kansas State University*, United States, Dissertation topic: *Security and Safety of Deep Reinforcement Learning*.

2014–2016 GPA:4.0/4.0 **M.S. in Computer Science**, *University of Nevada, Reno*, United States, Dissertation topic: *Real-Time Inference of Topological Structure and Vulnerabilities for Adaptive Jamming Against Covert Ad Hoc Networks.*.

2012–2014 GPA:N/A **Ph.D. in Microwave Engineering**, *University of Birmingham*, United Kingdom, Research: *Design and Analysis of Nonlinear Metamaterial Radio Front-ends for Millimeter-wave and Terahertz Applications*.
Transferred to UNR

2009–2012 Grade: Upper Second Class with Honours **B.Eng. in Computer and Communication Systems Engineering**, *University of Birmingham*, Birmingham, United Kingdom, Final Project: *Reconfigurable Planar Antennas for Cognitive Radio Applications Using Substrate Integrated Waveguides*.

Research Interests

- Artificial intelligence safety and security (focus on deep reinforcement learning)
- Applications of machine learning in cybersecurity
- Resilience and security of complex adaptive systems
- Game theory for networks

Research Experience

2017–2019 **Research Assistant**, *Knowledge Discovery and Databases Lab*, Kansas State University.
- Project leader for automated cyber threat intelligence collection and analysis with focus on Open-Source Intelligence (OSINT)
- Research on the adversarial manipulation of reinforcement learning models for algorithmic stock trading

2016–2018 **Research Assistant**, *Intelligent Systems, Computer Architecture, Analytics, and Security Lab*, University of Nevada, Reno & Kansas State University.
- Co-founded the AI Safety Research Initiative at K-State
- Research on AI safety with focus on policy manipulation attacks in deep reinforcement learning
- Developed RL-Attack, an open-source platform for experimental investigation of training and test-time attacks on deep RL.
- Research on security aspects of deep RL in the context of autonomous navigation
- Developed models and frameworks for butterfly attacks on Complex Adaptive Systems with focus on security analysis of smart cities
- Proposed a self-organization mechanism for optimal resource management in distributed and heterogeneous IoT
- Developed a game-theoretic model for self-organizing behavior in heterogeneous IoT networks
- Developed a computational framework for optimal destabilization of covert terrorist organizations based on network formation games, inverse game theory, social network analysis, and reinforcement learning

2014–2016 **Research Assistant**, *Computer Networking Lab*, University of Nevada, Reno.
- Implemented frequency agile cognitive radio testbed using USRP and GNU Radio.
- Developed online spectrum defragmentation techniques for non-contiguous cognitive radio networks
- Developed an algorithm for beam-nulling as a mitigation technique against jamming in ad hoc networks
- Implemented a testbed to study vulnerabilities in ad hoc UAV networks
- Developed a novel technique for real-time topological inference of tactical ad hoc networks
- Proposed a vulnerability measurement framework for adaptive jamming attacks in ad hoc networks
- Developed a Flying Ad Hoc Network (FANET) testbed with modified Parrot AR2 Quadcopters for experiments on topology control and inference
- Investigated analytical techniques for topological inference and vulnerabilities of covert networks

2012–2014 **Research Assistant**, *Communications Research Group*, University of Birmingham.
- Research on active and Reconfigurable Metamaterial Antennas and Front-ends for mm-wave and THz Applications
- Designed a novel reconfigurable CRLH leaky-wave antenna with integrated switchable frequency doubler
- Implemented a novel method for co-simulation of electromagnetic and nonlinear circuit analysis of CRLH radiators
- Left the program due to lack of funding

Grants and Awards

Grants

2020-2021 **Source: Love Justice International**, *Project: Combating Human Trafficking via Automated Intelligence Collection, Validation, and Fusion*, Amount: $38,000, PI: Vahid Behzadan.

2020-2021 **Source: Office of Naval Research**, *Project: Cyber Operative REsearch Scholars (CORES)*, Amount: $252,407, PI: Ibrahim Baggili, Co-PI: Vahid Behzadan.

2020-2021 **Source: National Security Agency**, *Project: GenCyber Agent Academy*, Amount: $84,101, PI: Ibrahim Baggili, Co-PIs: Vahid Behzadan, Liberty Page.

Awards

2020 Research Development Award, University of New Haven

2020 Travel Grant, University of New Haven

2019 Travel Grant, University of New Haven

2018 Travel Grant, K-State

2017 Summer Fellowship, K-State

2016-2017 Federal Scholarship, UNR

2015-2017 Outstanding International Student Scholarship, UNR

2015 Graduate Students Association Travel Grant, UNR

2012-2014 International Students Scholarship, University of Birmingham

2009-2012 Departmental Bursary, University of Birmingham

2007-2009 Outstanding International Student Scholarship - Eastern Mediterranean University, North Cyprus

2007-2009 Outstanding Student Awards - Eastern Mediterranean University, North Cyprus

Teaching and Advising Experience

Classroom Teaching

Fall 2020 **Instructor**, University of New Haven, *Topic:* Artificial Intelligence.

Fall 2020 **Instructor**, University of New Haven, *Topic:* Distributed and Scalable Data Engineering.

Spring 2020 **Instructor**, University of New Haven, *Topic:* Artificial Intelligence.

Spring 2020 **Instructor**, University of New Haven, *Topic:* Distributed and Scalable Data Engineering.

Spring 2020 **Instructor**, University of New Haven, *Topic:* AI and Cybersecurity.

Fall 2019 **Instructor**, University of New Haven, *Topic:* Artificial Intelligence.

Fall 2019 **Instructor**, University of New Haven, *Topic:* Data Exploration.

2019 **Guest Lecturer**, Kansas State University, *Topic:* Reinforcement Learning (5 lectures).

2018 **Guest Lecturer**, Kansas State University, *Topic:* Reinforcement Learning (4 lectures).

2018 **Guest Lecturer**, Kansas State University, *Topic:* Adversarial Machine Learning (2 lectures).

2018 **Guest Lecturer**, University of Nevada, Reno, *Topic:* History of Cyber Warfare (1 lecture).

2014-2017 **Teaching Assistant**, University of Nevada, Reno, *Courses Taught:* Introduction to Programming.

2012-2014 **Teaching Assistant**, University of Birmingham, *Courses Taught:* Object Oriented Programming with Java, Data Communication Networks, Introduction to Communication Systems, Embedded Programming.

2007-2008 **Instructor**, Ebn-e-Sina Center- Tehran, Iran, *Courses Taught:* Observational Astronomy.

2006-2007 **Instructor**, Salam High Schools - Tehran, Iran, *Courses Taught:* Introduction to Astrophysics and Cosmology.

Graduate Advisement

May 2020 – Present **M.S. Advisor**, University of New Haven, *Project:* Security of Reinforcement Learning in Automated Stock Trading.

January 2020 – Present **M.S. Advisor**, University of New Haven, *Project:* Deep Learning for Fake News Detection.

Aug 2019 – Present **M.S. Advisor**, University of New Haven, *Project:* Adversarial Machine Learning.

Aug 2019 – Present **M.S. Advisor**, University of New Haven, *Project:* Automatic Collection and Analysis of Cyber Threats from the Darknet.

Aug 2019 – Present **M.S. Advisor**, University of New Haven, *Project:* Automatic Collection and Analysis of Cyber Threats from the Web.

Aug 2019 – January 2020 **M.S. Advisor**, University of New Haven, *Project:* Automatic Podcast Generation.

Summer 2018 – Present **PhD Research Co-advisor**, Kansas State University, *Project:* Threat Intelligence Collection and Analysis from Twitter Data.

Fall 2017 **PhD Research Co-advisor**, Kansas State University, *Project:* Adversarial Deep Reinforcement Learning for Autonomous Navigation.

Undergraduate Advisement

Aug 2020 – Present **Senior Project Advisor**, University of New Haven, *Project:* Reinforcement Learning Agents for Automated Penetration Testing.

Aug 2019 – May 2020 **Senior Project Advisor**, University of New Haven, *Project:* Anomaly Detection and Prediction in Web Applications.

Aug 2019 – May 2020 **Senior Project Advisor**, University of New Haven, *Project:* Interactive and Conversational Mobile Robot.

Summer 2019 **Undergraduate Research Advisor**, Kansas State University, *Project:* Threat Intelligence Collection and Analysis from Twitter Data.

Spring 2018 **Capstone Project Advisor**, Kansas State University, *Project:* Inverse Reinforcement Learning for Ethical Decision-Making in Driverless Cars.

Fall 2014 **Senior Project Advisor**, University of Nevada, Reno, *Project:* Jamming Attacks in 802.11x WLANs.

2012-2014 **Final Project Co-Advisor**, University of Birmingham, *Projects:* Design, Fabrication and Measurement of Reconfigurable Planar Antennas.

Invited Talks and Presentations

Sept 2020 **Butterfly Effect in the Wind Tunnel - A Deep Reinforcement Learning Approach** , Industrial and Manufacturing Systems Engineering Research Seminar - Kansas State University.

Aug 2020 **Faults in our Pi Stars: Security Issues and Challenges in Deep Reinforcement Learning**, AI Village at DEF CON '20.

Aug 2020 **Security of Deep Reinforcement Learning in Finance**, Royal Bank of Canada.

Feb 2020 **Cybersecurity Panel**, University of New Haven Lockheed Martin Day.

Oct 2018 **Emperor's new clothes: The insecurity of AI-enabled security tools**, CANSec '18.

Sep 2018 **Adversarial Machine Learning**, K-State Research Seminar.

Aug 2018 **OWASP Joomscan**, Black Hat 2018 Arsenal.

June 2018 **OWASP Nettacker Tutorial**, OWASP Bay Area Chapter.

May 2018 **Machine Learning for Cybersecurity**, OWASP Nettacker/Google Summer of Code.

Apr 2018 **AI Safety Landscape**, K-State Research Seminar.

Nov 2017 **Cyber-physical Vulnerabilities in Unmanned Aerial Systems**, K-State Cyber Defense Club Seminar.

Oct 2017 **Security in Machine Learning Systems**, K-State Machine Learning Research Seminar.

Oct 2017 **Security in Machine Learning (In Farsi)**, Isfahan University of Technology (Iran).

June 2017 **Computational Framework for Strategic Induction of Instability on Dynamic Terrorist Organizations**, 2nd Symposium on the Structure and Mobility of Crime.

Media Coverage

2020 Fox61 News - Interview: Schools becoming common targets of Ransomware attacks

2020 NBC Connecticut - Interview: Classes Begin in Hartford After Ransomware Attack Postponed First Day of School

2020 AI and Machine Learning Podcast - Interview: Safety and Security of Machine Learning

2020 NBC News - Interview: Privacy in Contact Tracing Apps

2020 Lars Larson Show - Interview: Cyber-Attacks During Lockdown

2020 Unite.AI - Feature Interview

2020 Voice of America - Interview: Cyber Espionage and National Security

2020 Information Security Buzz - Expert Comment on U.S. Health Agency Cyber Attack

2020 CT Insider - Profile and Interview: On the front lines of Coronavirus

2020 Forbes - Interview: Coronavirus: Can AI Make A Difference?

2020 Humanoid Podcast - AI and Social Distancing

2018 AXIOS - Research Feature: AI Might Need a Therapist, Too

2018 CNET - Research Feature: Will AI Need Therapy in the Future?

2018 CNET - Research Feature: Will AI Need Therapy in the Future?

2018 Huffington Post France - Research Feature: Il faudra bientôt des psychologues pour intelligence artificielle, selon ces chercheurs

2018 ABC News (Radio) - Research Feature: Need for AI Psychologists

2018 Yahoo News France - Research Feature: Il faudra bientôt des psychologues pour intelligence artificielle, selon ces chercheurs

Service

2020 **Chair of 3 faculty search committees**, University of New Haven.

2020 **Proposal Review Panelist**, National Science Foundation.

2020 **Program Committee Member**, SafeAI 2021 (Co-Located with AAAI 2021).

2020 **Program Committee Member**, FOSINT-SI 2020 (Co-Located with ASONAM 2020).

2020 **Program Committee Member**, WAISE 2020 (Co-Located with SafeComp 2020).

2019 **Program Committee Member**, SafeAI 2020 (Co-Located with AAAI 2020).

2019 **Member of search committee**, University of New Haven.

2018 **Program Committee Member**, Artificial Intelligence Safety 2019 (Co-Located with IJCAI 2019).

2018 **Technical Committee Chair**, 2nd Offsec Conference on Cybersecurity (Iran).

2018 **Program Committee Member**, 8th EAI International Conference on Game Theory for Networks (Gamenets 2018).

2017–present **External Research Advisor**, OWASP Nettacker Project.

2014–2016 **Elected board member of the Graduate Students Club (GSC) for 4 consecutive terms**, UNR Computer Science.

2008–2009 **Elected Treasurer of IEEE Student Branch**, Eastern Mediterranean University, North Cyprus.

2014–present **Reviewer**, IEEE Transactions on Network Science and Engineering, IEEE Communications Magazine, IEEE Vehicular Technology Magazine, Elsevier's International Journal of Computer and Communications Networks, IEEE Consumer Electronics Magazine, Elsevier's International Journal of Electronics and Communications, IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Hindawi's International Journal of Distributed Sensor Networks, IEEE International Conference on Industrial Technology..

Selected Work Experience

Aug 2012-Oct 2012 **Lead RF and DSP Engineer**, Renata Aviation Technologies, *Responsibility:* Development of integrated radio avionics and ADS-B Mode S Module.

2010-2011 **Founder and CTO**, Genosign Technologies, *Responsibility:* Development of Biometric Solutions for UK-based and European clients.

Apr 2010-Aug 2011 **Radio Communications Consultant**, Iranian National Observatory Project, Institute for Research in Fundamental Sciences, *Responsibility:* Design and implementation of wireless links for the Virtual Observatory network.

Apr 2003-Aug 2006 **Founder and Administrator**, Hyper-Security Team, *Responsibility:* Penetration testing services, open-source training for security enthusiasts in Iran.

Technical Skills

Subjects Deep Learning, Deep Reinforcement Learning, Statistical Modeling, Complex Network Mining, Complex Adaptive Systems, Social Network Analysis, Game Theory, Wireless Security, Traffic Analysis, Topology Inference, Mobile Ad hoc Networks, Aerospace Communications, Cognitive and Software Defined Radios, Microwave and Antenna Engineering, Digital Signal Processing

Programming Python, C/C++, Java, PHP/MySQL, Perl, Matlab

Machine Learning TensorFlow, Scikit-Learn, Keras, PyTorch, OpenAI Gym/Universe/Retro/Baselines, Pandas

SDR GNURadio, Ettus USRP, OpenBTS, Osmocom TETRA

Software UML 1.x/2.x, Agile/Scrum, ED-12B/DO-178B

Hardware Active HDL, FPGA, ARM Architectures, NVIDIA GPU

Security Web/Network/Mobile/Cloud/RF Penetration Testing, ICS & SCADA Security Management, Anti-Drone Technologies, Anti-Jamming Solutions, Threat Intelligence (Specializing in OSINT), Security Data Science, Metasploit Framework, Kali Suite, OWASP Nettacker

Cloud & Distributed Computing OpenMP, MPI, CUDA, Kubernetes, Amazon AWS, IBM Watson, Microsoft Azure, Google Cloud, Paperspace

Publications

[1] Bibek Upadhayay and **Vahid Behzadan**. Sentimental LIAR: Extended Corpus and Deep Learning Models for Fake Claim Classification. *proceedings of IEEE ISI 2020 arXiv preprint arXiv:2009.01047*, 2020.

[2] Ibrahim Baggili and **Vahid Behzadan**. Founding the domain of AI Forensics *proceedings of SafeAI 2020 arXiv preprint arXiv:1912.06497*, 2020.

[3] **Vahid Behzadan** and William Hsu. Sequential Triggers for Watermarking of Deep Reinforcement Learning Policies *proceedings of AI Safety 2019 arXiv preprint arXiv:1906.01126*, 2019.

[4] **Vahid Behzadan** and William Hsu. Adversarial Exploitation of Policy Imitation *proceedings of AI Safety 2019 arXiv preprint arXiv:1906.01121*, 2019.

[5] **Vahid Behzadan**, James Minton and Arslan Munir. TrolleyMod v1.0: An Open-Source Simulation and Data-Collection Platform for Ethical Decision Making in Autonomous Vehicles *proceedings of AAAI/ACM Conference on Artificial Intelligence, Ethics and Society (AIES 2019) arXiv preprint arXiv:1811.05594*, 2019.

[6] **Vahid Behzadan**, Roman V. Yampolskiy and Arslan Munir. Emergence of Addictive Behaviors in Reinforcement Learning Agents *AAAI Workshop on Artificial Intelligence Safety (SafeAI) 2019 arXiv preprint arXiv:1811.05590*, 2019.

[7] **Vahid Behzadan** and Arslan Munir. What Does Not Kill Deep Reinforcement Learning, Makes It Stronger. *proceedings of the AAAI Workshop on Artificial Intelligence Safety (SafeAI) 2019*, *arXiv preprint arXiv:1712.09344*, 2019.

[8] **Vahid Behzadan**, Carlos Aguirre, Avishek Bose, and William Hsu Corpus and Deep Learning Classifier for Collection of Cyber Threat Indicators in Twitter Stream *proceedings of IEEE CyberHunt 2018*

[9] **Vahid Behzadan** and Arslan Munir. Faults in Our Pi Stars: Security Issues and Open Challenges in Deep Reinforcement Learning *under review at IEEE Transactions on Neural Networks and Learning Systems arXiv preprint arXiv:1806.01368*, 2018.

[10] **Vahid Behzadan** and Arslan Munir. Adversarial Reinforcement Learning Framework for Benchmarking Collision Avoidance Mechanisms in Autonomous Vehicles. *IEEE Intelligent Transportation Systems arXiv preprint arXiv:1806.01368*, 2019.

[11] Nicolas Papernot, Fartash Faghri, Nicholas Carlini, Ian Goodfellow, Reuben Feinman, Alexey Kurakin, Cihang Xie, Yash Sharma, Tom Brown, Aurko Roy, Alexander Matyasko, **Vahid Behzadan**, Karen Hambardzumyan, Zhishuai Zhang, Yi-Lin Juang, Zhi Li, Ryan Sheatsley, Abhibhav Garg, Jonathan Uesato, Willi Gierke, Yinpeng Dong, David Berthelot, Paul Hendricks, Jonas Rauber, Rujun Long, Patrick McDaniel cleverhans v2.1.0: an Adversarial Machine Learning Library. *arXiv preprint arXiv:1610.00768*, 2018.

[12] **Vahid Behzadan** and Arslan Munir. Adversarial Exploitation of Emergent Dynamics in Smart Cities. *Proc. of IEEE International Smart Cities Conference (ISC2), Kansas City, Missouri*, 2018.

[13] **Vahid Behzadan**, Arslan Munir, and Roman V. Yampolskiy. A Psychopathological Approach to Safety Engineering in AI and AGI. *Proc. of First International Workshop on Artificial Intelligence Safety Engineering (WAISE) @International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2018)*, *arXiv preprint arXiv:1805.08915*, 2018.

[14] **Vahid Behzadan** and Arslan Munir. Mitigation of Policy Manipulation Attacks on Deep Reinforcement Learning with Parameter-Space Noise. *Proc. of First International Workshop on Artificial Intelligence Safety Engineering (WAISE) @International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2018)*, *arXiv preprint arXiv:1806.02190*, 2018.

[15] **Vahid Behzadan** and Arslan Munir. Models and Framework for Adversarial Attacks on Complex Adaptive Systems. *Under review by ACM Transactions on Autonomous and Adaptive Systems*, *arXiv preprint arXiv:1709.04137*, 2018.

[16] **Vahid Behzadan** and Arslan Munir. A Novel UAV-Enabled Fog Architecture for Sustainable Smart Farming. *Under review by Elsevier Journal of Computer and Electronics in Agriculture*, 2018.

[17] **Vahid Behzadan**, Amin Noormohammadi, Murat Yuksel, and Mehmet Gunes. Computational Framework for Strategic Destabilization of Dynamic Terrorist Networks. *Advances in Social Networks Analysis and Mining (ASONAM), IEEE/ACM International Conference on.*,

[18] **Vahid Behzadan**, Amin Noormohammadi, Murat Yuksel, and Mehmet Gunes. On Fighting Fire with Fire - A Computational Framework for Strategic Induction of Destabilization on Dynamic Terrorist Organizations. *2nd Symposium on the Structure and Mobility of Crime*, 2017.

[19] **Vahid Behzadan** and Arslan Munir. Vulnerability of Deep Reinforcement Learning to Policy Induction Attacks. In *Machine Learning and Data Mining in Pattern Recognition - 13th International Conference*, *arXiv preprint arXiv:1701.04143*, 2017.

[20] **Vahid Behzadan** and Banafsheh Rekabdar. A Game-Theoretic Model for Analysis and Design of Self-Organization Mechanisms in IoT. *7th EAI International Conference on Game Theory for Networks*, 2017. *arXiv preprint arXiv:1701.04562*, 2017.

[21] **Vahid Behzadan**. Real-Time Inference of Topological Structure and Vulnerabilities for Adaptive Jamming Against Tactical Ad Hoc Networks. *M.S. Dissertation, University of Nevada, Reno*, 2016.

[22] Suman Bhunia, **Vahid Behzadan**, Paulo Alexandre Regis, and Shamik Sengupta. Adaptive Beam Nulling in Multihop Ad Hoc Networks Against a Jammer in Motion. *Elsevier Computer Networks*, 109:50–66, 2016.

[23] Suman Bhunia, **Vahid Behzadan**, and Shamik Sengupta. Enhancement of Spectrum Utilization in Non-Contiguous DSA with Online Defragmentation. In *IEEE Military Communications Conference (MILCOM)*, 2015.

[24] Suman Bhunia, **Vahid Behzadan**, Paulo Alexandre Regis, and Shamik Sengupta. Performance of Adaptive Beam Nulling in Multihop Ad Hoc Networks Under Jamming. In *International Symposium on Cyberspace Safety and Security (IEEE CSS)*, 2015.

[25] Mohammad Sadegh Ebrahimi, Mohammad Hossein Daraei, **Vahid Behzadan**, Anahid Khajooeizadeh, Shervin Ardeshir Behrostaghi, Milad Tajvidi. A Novel Utilization of Cluster-Tree Wireless Sensor Networks for Situation Awareness in Smart Grids. In *Innovative Smart Grid Technologies Asia (IEEE ISGT)*, 2011.

References

William Hsu — **Professor**, Department of Computer Science, Kansas State University.
Email: bhsu@ksu.edu

Roman Yampolskiy — **Associate Professor**, Departments of Computer Science & Computer Engineering, University of Louisville.
Email: roman.yampolskiy@louisville.edu

Murat Yuksel — **Professor**, Department of Electrical and Computer Engineering, University of Central Florida.
Email: murat.yuksel@ucf.edu

David Feil-Seifer — **Assistant Professor**, Department of Computer Science and Engineering, University of Nevada, Reno.
Email: dave@cse.unr.edu