medium.com

# Prof. Arash Habibi Lashkari — Weaponizing the World with Intelligent Security Gadgets

*Patrick John*

8–10 minutes

Technology is great until it's used against you — protect yourself from hacker attacks!

All companies and organizations take ample precautions to protect their data from online breaches. For instance, cybersecurity specialists align with government officials to protect confidential data. They communicate with the military to keep hackers and online thieves away from private information. Cybersecurity is essential in the healthcare sector to secure patients' personal data or in the business world to protect information related to financial transactions. In a nutshell, all sectors are highly dependent on cybersecurity.

Today, cybersecurity has become a global threat. Everyone, from personal users to huge multinational companies, is vulnerable and exposed to cybercrimes. According to the Global Cybercrime Report, between 2023 and 2025, the estimated cost of cybercrime will increase by 5.7 trillion U.S. dollars. This is indeed a scary situation.

Throughout the years, various methods have been implemented to lift the threat. Among numerous other precautionary techniques, Machine Learning (ML) and Deep Learning (DL) techniques were critical in detecting severe cyber threats. These techniques protect networks from internal and external attacks. Researchers have made extensive efforts to create these breakthrough antivirus systems. **Prof. Arash Habibi Lashkari** is a diligent researcher who has worked incessantly to develop a secure data communication network.

*Lashkari is an associate professor, educator, and author. He is professionally known for serving as a Canada Research Chair (CRC) in cybersecurity and founder and director of the Behavior-Centric Cybersecurity Center (BCCC). His research mobilization strategy, namely Understanding Cybersecurity Series (UCS), produces various resources, including datasets, open-source* *analyzers, academic and technical materials, and general public non-technical materials for researchers and readers of all backgrounds. Lashkari is among the highly cited researchers in cybersecurity. He is well-recognized for his research in Malware Analysis, Intrusion Detection Systems (IDS), Network Traffic, Dark web analysis, and threat detection.*

Lashkari has consistently demonstrated a profound interest in developing resilient Machine Learning (ML) and Deep Learning (DL) systems. He also encouraged fellow scholars to create, test, and evaluate infallible network security systems. The first branch of UCS resource materials will consist of datasets, which cybersecurity researchers and industry product developers seek to test and evaluate products and solutions before their publication or release. Lashkari and his team are pioneers in developing over 18 cybersecurity datasets, different detection and characterization solutions using ML and DL in cybersecurity areas, and several cybersecurity open-source analyzers.

Lashkari has his hands on the Encrypted traffic analysis and characterization. He created three datasets: VPN-NonVPN-2015, Tor-NonTor-2016, and Darknet-2020. Later, Lashkari proposed DIDarknet — a contemporary approach to detect and characterize darknet traffic using Deep Image Learning. In 2021, he proposed and developed a robust staking ensemble model for darknet traffic classification and characterization with his team.

Arash Habibi Lashkari, Assistant
fessor at UNB and Research
nator at CIC, New Brunswick
e, Cybersecurity Academic

In 2016, Lashkari and his team created a lightweight method for identifying and categorizing malicious URLs based on their attack types, such as spam, phishing, malware, and defacement. This led to the creation of the ISCX-URL-2016 dataset. Later, in 2020, he developed the first DoH tunnel analyzer with his team using Time-series classification and received funding from the Canadian Internet Registration Authority to produce the CIRA-CIC-DoHBrow-2020 dataset. In 2021, he collaborated with Bell Canada to propose a lightweight hybrid data exfiltration and malicious DNS traffic analysis at the Canadian Institute for Cybersecurity (CIC). Furthermore, from 2017 to 2020, he designed and implemented three different Android malware analysis systems with his team using ML and DL algorithms and proposed a systematic approach to generate Android Malware datasets. As a result, they produced four datasets on the Android Malware analysis domain, including AAGM-2017, CIC-AndMal-2017, CIC-InvesAndMal-2019, and CCCS-CIC-AndMal-2020. Lashkari and his team also collaborated with the Canadian Centre for Cybersecurity (CCCS) to propose two new Deep Learning-based Android malware characterization solutions: DIDroid and Entroplyzer.

In 2017, he and his team proposed a fast and robust ML-based intrusion detection and characterization system with his team and created the CIC-IDS-2017 dataset. They extended the project with support from AWS and produced the first and only IDS datasets for Amazon, namely CSE-CIC-IDS-2018. Lashkari and his team are the creators of the only available Distributed Denial of Service (DDoS) dataset known as CIC-DDoS-2019, which includes 12 common DDoS attacks such as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and

TFTP. Furthermore, in the last two years, he produced two datasets with his team: Source Code Authorship Attribution (YU-SCAA-2022) for profiling the malicious software programmers and SQL Injection Attack (BCCC-SFU-SQLInj-2023) to enhance the evasiveness and sophistication of the original malicious queries for cybersecurity analyst and researchers.

In parallel with creating and producing Cybersecurity datasets, he designed and developed cybersecurity open-source analyzers, as the second branch of the UCS materials, to support researchers and industry developers in exploring simplified versions of applicable information technology solutions. Dr. Lashkari and his team have developed five cybersecurity analyzers over the last five years: (1) the CICFlowMeter for network traffic analysis (Formerly ISCXFlowMeter); (2) the DoHLyzer for DNS message analysis; (3) the AndroidAppLyzer for Android malware analysis; (4) the VolMemLyzer for malware detection through memory analysis; and (5) the PDFMalLyzer to analyze and detect malicious PDFs. These will aid in enabling industry professionals to work on a customized version based on their specific situations, enabling production to be completed at a lower cost — with abundant support — and aided by a wealth of resources and informational tools. All open-source packages will be available on GitHub.

Apart from being a meticulous researcher, Lashkari and his team have authored over ten books and several articles on cybersecurity-related topics for the third branch of the UCS materials. A few of his books are *Understanding Cybersecurity Management in Decentralized Finance: Challenges, Strategies, and Trends, Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective*, *Understanding Cybersecurity Law* and *Digital Privacy*, *Understanding Cybersecurity Management in FinTech*, *Mobile Operating systems and Programming* and *Graphical User Authentication (GUA).* He also has contributed several cybersecurity articles, including notable ones such as "*Robust Stacking Ensemble Model for Darknet Traffic Classification Under Adversarial Settings*" in *Computers & Security Journal*, "*IoT Malware Analysis using Federated Learning: A Comprehensive Survey*" in IEEE Access, and "*IoT Malware: An attribute-based taxonomy, detection mechanisms, and challenges*" in *Peer-to-Peer Networking and Applications* journal.

Conclusively, Prof. Arash Habibi Lashkari, founder of UCS, is a highly esteemed academic with 26 years of experience in academia and industry. He is a senior member of IEEE and has served in multiple universities worldwide. His research is centered on the modeling and detection of cyber threats, the study of malware, the security of big data, the analysis of internet traffic, and the production of cybersecurity open-source analyzers and datasets. Lashkari has earned 15 awards at International Computer Security competitions, including three gold medals, and was named one of Canada's Top 150 Researchers for 2017. Moreover, Lashkari was awarded the University of New Brunswick's prestigious Teaching Innovation Award in 2020 for his personally created teaching methodology, the Think-Que-Cushion method.