The Role of AI in Cybersecurity Operations

Research, Education, and Outreach Challenges at Higher Education Institutions

Ricardo Morla
ricardo.morla@fe.up.pt

Faculty of Engineering and INESC TEC, University of Porto, Portugal

Abstract. Artificial Intelligence and Cybersercurity are extremely popular these days. Despite such popularity, it is reasonable to question the role, if any, that AI should have in securing a cyberphysical ecosystem from malicious behavior. The optimist will say that learning from data is the only solution to the problem of detecting malicious behavior that is subtly hidden in the ever larger amount of data that our systems generate. The pessimist will probably argue that the motivation that attackers usually have to outsmart defenders also applies to data and learning, and that any 'normal' behavior can be replicated with enough effort. The complexity of this discussion explodes when we bring in the diversity of target systems we need to secure – including the panoply of web systems and mobile applications, the increasing availability of IoT devices and robots, and the increasing proportion of communication mechanisms and hardware systems we thought were secure and that someone has managed to break. Given the highly technical nature of this discussion, in this paper we ask ourselves what can Higher Education Institutions do – in their Research, Education, and Outreach missions – to help clarify the role of AI in Cybersecurity operations and hopefully make the world somehow safer.

Keywords: Artificial Intelligence · Cybersecurity · Challenges · Higher Education.

1 AI in Cyber Ops

Cybersecurity operations can be narrowly seen as the management of an IT network from a security perspective. At a first level this tends to involve automatically collecting and analyzing data and also enacting countermeasures to prevent further compromises of the network. Chapter 8 of the Cybersecurity Body of Knowledge 2019 compilation [1] provides a detailed overview of this first level security operations. More resourceful security operation centers tend to also delve into second and third level aspects such as malware analysis, reverse engineering, forensics, and software, hardware, and network security; and they also tend to cover more technologies than just IT networks, with cyber-physical

systems in industry, power, transportation, medical, and robotics becoming extremely relevant. See parts II, IV, and V of [1] for more details on different aspects of Cybersecurity operations.

Although [1] refers the use of AI in cybersecurity operations, it does not deeply or in a very structured way delve into the many advanced challenges and implications of learning from data in an adversarial setup such as those in Cybersecurity. A frequent assumption for machine learning is that if some underlying process is generating some specific pattern of random data, a simpler or more advanced model can be used to learn that pattern and use it e.g. for some classification or clustering task. A less frequently thought-of assumption – although almost always valid outside of Cybersecurity – is that the underlying process does not start generating data in a different way because a given model has been learned or used on that data. This is not necessarily true in Cybersecurity, as any decent attacker would e.g. try to change the nature of the attack data in order to break the classifier once some information about the defender's classifier is known. Moreover, attackers can also use AI to profile user data or to learn how to avoid detection – which puts us in a sort of battlefield between two AIs – the defender's and the attacker's – whose clash may lead us to concepts such as level playing field, AI strength, and morphing ability, and to consider how much information about the structure and data of an AI can the adversary learn. These challenges are likely shared with other areas in Cybersecurity where AI is used – for example video surveillance and biometrics. Finally, other advanced challenges of using AI in cybersecurity operations are shared with using AI at large but likely have specific implications and solutions – and include privacy, explainability, adversarial learning, and cryptographically-secure distributed learning and inference. This program for research, education, and outreach attempts to develop these advanced challenges for AI in Cybersecurity operations; please refer to [2] for a detailed and structured discussion of these challenges.

2 A HEI Program for AI in Cyber Ops

2.1 Identify Cybersecurity problems where AI solutions make sense

AI is not a panacea for cybersecurity operations. In fact, with all the hype on both Cybersecurity and AI, one of the added value of HEI is to be able to pull their resources from Research, Education, and Outreach to help distill and separate the wheat from the chaff of AI in Cybersecurity. Input to this process of identifying Cybersecurity problems where AI solutions make sense would come from:

- Literature review of well established AI in Cybersecurity problems
- Specific challenges from government or corporate partners with regard to AI and Cybersecurity
- Challenges in Cybersecurity and AI from technical, non-cybersecurity fields within the University

– Challenges in AI from technical or non-technical Cybersecurity fields within the University

2.2 Develop AI solutions for specific Cybersecurity tasks

Developing AI solutions for Cybersecurity is compelling given that specialized know-how both in AI and in Cybersecurity is required and both are in high demand. While some companies provide AI-based Cybersecurity solutions, developing AI solutions for specific Cybersecurity problems is not readily available in the market. HEI can play a relevant role helping to achieve solutions for new problems as well as validating and comparing existing and improved models. The following are cornerstone to this role:

– Highly specialized, Cybersecurity domain-specific set of success metrics and tests, together with relevant live or testbed data set capture process
– Cost-effective, systematic software and data mining approaches at reusing, developing, and performance assessment of complex AI models for different tasks
– Specialized techniques for learning in challenging environments – e.g. in Big Data environment with high performance devices or in resource-constrained environment with FPGA or other custom inference and learning hardware

2.3 Check the robustness of Cybersecurity solutions against advanced AI challenges

Developing a model and assessing its performance is not enough if AI solutions for Cybersecurity problems are to be at all meaningful; advanced challenges to AI in Cybersecurity must be addressed, including privacy, explainability, adversarial attacks, battlefield, and intelligence [2]. This is perhaps the most challenging part of this program for HEI. While AI and Cybersecurity has gained popularity, their advanced challenges have not been widely discussed and have been either cast aside as irrelevant or used as a showstopper that shows the possible dangers of using AI in Cybersecurity – and in any case not an easy sell for practitioners and decision-makers. Two dimensions are important for overcoming this challenge:

– Identify, collect, and make available for systematic and public use the set of existing techniques for privacy, explainability, adversarial, battlefield, and intelligence
– Contribute with novel insights on existing and new techniques that address these advanced challenges

2.4 Run AI Cybersecurity solutions live

Running a live system with actual users and real data and intrusions is arguably the best way to validate the impact of AI in Cybersecurity. It is also a effective approach to demonstrate the value of HEI contributions to society in this area. The following are key to this:

- Conduct in-depth monitoring and performance assessment of AI solutions with live data and real situations
- Compare different AI and non-AI solutions and cross-reference with existing cyber intelligence
- Support adversarial stress testing of the AI solutions

3 Capabilities for a medium-sized University

The following are specific capabilities at the know-how, infrastructure, human resources, and coordination levels that a medium-sized University – with a relatively broad scope of scientific areas, adequate IT and security team, and good interaction with government and the corporate world – should develop for the viability of this program.

3.1 Technical know-how

- Computer Science and Engineering at large: Hardware (Microelectronics, Processors, Communications), System (OS, Networking, Distributed), and Applications (Web, Mobile).
- Data science at large: Data Mining, Machine Learning, Parallel and Big Data Infrastructure.
- Cybersecurity at large: Security Engineering, Hardware, System, and Application Security, Ethical Hacking, Information Security, Applied Cryptography.
- Advanced challenges of AI in Cybersecurity: privacy, explainability, adversarial, battlefield, intelligence.

3.2 Infrastructure

- IT and IoT platform testbeds for Hardware, System, and Applications where Cybersecurity problems can be characterized, datasets collected, and AI solutions developed and tested.
- Red team vs. Blue team playground testbed where automated solutions for attacking and defending based on AI can be tested
- Cluster of AI and big data processing and storage where relevant datasets can be processed.
- Security Operations Center with capacity for deployment of experimental AI solutions, including interaction with SOC software and resorting to honeypots and other data and intelligence gathering mechanisms

3.3 People Motivation

- Student interest groups in Cybersecurity targeting different systems and including data-driven approaches
- Capture the flag competitions on advanced AI challenges in Cybersecurity
- CTF team on advanced AI challenges with own training program and training room
- Penetration testing challenges targeting live AI solutions

3.4 Coordination

- Between different researchers, research groups, and institutions within the scope of the University that have an interest in Cybersecurity and AI
- With privacy, explainability, adversarial AI researchers in non-cybersecurity-related areas
- With University Cybersecurity and IT teams
- With government and corporate Cybersecurity departments and institutions

4 Implementation of the Program at the University of Porto

The implementation of this plan depends on available resources at the target HEI. Specifically for the University of Porto, the proposed implementation of the program leverages existing work in AI for network security – and more specifically calls to investigate advanced AI challenges and solutions in three research areas (network privacy, malware detection, and blue vs. red team automation). While remaining fundamentally different in application, the three areas share advanced AI challenges including battlefield and intelligence, but also privacy and explainability, with computational performance in Big Data or resource-constrained scenarios being also an important aspect to assess. Competitive research funding and human resources for this program should be pursued, with the three areas wide enough for a post-doc or assistant professor and including Education and Outreach. Specifically for Education and Outreach, the implementation plan relies on the availability of courses in fundamental topics in Computer Science and Engineering, Data Science, and Cybersecurity at the University, as well as openness and collaboration with government and corporate institutions.

The following should be read in the context of the program and infrastructure sections (2 and 3) and the AI in Cybersecurity structured discussion paper [2].

4.1 Research

- Explore the problem of network privacy under encrypted communications, where attackers eavesdrop likely encrypted network traffic to infer user behavior and users may rely on traffic morphing to avoid detection
- Explore the problem of malware traffic detection, where defenders attempt to distinguish malicious command and control traffic from normal user traffic and attackers attempt to avoid such detection
- Explore the problem of blue vs. red team automation where defenders try to detect e.g. denial of service followed by vulnerability scans and lateral movements that may lead to intrusion and loss of critical information, and the attackers attempt to avoid such detection

4.2 Education

- Promote the development of Cybersecurity-related projects in traditionally non-Cybersecurity CS and Engineering courses like Hardware, Wireless, Robotics, etc.
- Develop courses specific for AI in Cybersecurity – including on the use of AI in the SOC, on infrastructure for Big Data and AI, and on advanced challenges for AI in Cybersecurity
- Develop small experiments text with related code and lab examples, shared in public repositories, that can be exercised in small to medium testbeds.
- Promote an adversarial learning competition on specific network security topics like malware detection or network privacy

4.3 Outreach

- Respond to requests from government or corporate Cybersecurity departments for checking viability and developing AI solutions related to network security, as well as assessing their robustness against advanced AI challenges and their computational performance
- Host staff from government or corporate departments related to Cybersecurity and network security in particular for short-term stays at the SOC to explore AI solutions and issues

References

1. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, and Andrew Martin, editors. *The Cyber Security Body of Knowledge*. The National Cyber Security Centre, Crown Copyright, 2019.
2. Ricardo Morla. Ten AI Stepping Stones for Cybersecurity. *arXiv:1912.06817 [cs]*, December 2019. arXiv: 1912.06817.