REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
04/01/2021

2. REPORT TYPE
Technical Report

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Odyssey: A Systems Approach to Machine Learning Security

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Winder, Ransom K.; Jubinski, Joseph P; Giannella, Chris; Jones, Malachi;

5d. PROJECT NUMBER
0720N05Z-0A

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
300 Sentinel Drive
Suite 500 & 600
Annapolis Junction, MD 20701

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-20-3341 / MTR200598

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Secretary of Defense

10. SPONSOR/MONITOR'S ACRONYM(S)
OSD

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This paper provides a systems approach to addressing attacks, consequences, and mitigations for systems using Machine Learning (ML). It explains each of these over the lifecycle of an ML technology, providing clear explanations of what to worry about, when to worry about it, and how to mitigate it while presuming little incoming knowledge of ML specifics. Our discussion of ML vulnerabilities, attacks, and mitigations utilizes the taxonomy developed in NISTIR 8269.

15. SUBJECT TERMS
Artificial Intelligence; Computer Security; Information Security Engineering; machine learning; ML; attack mitigation;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		42	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646