Adversarial Artificial Intelligence (AI) Impacts on Cyber Security Policies of EU: What Should EU Learn from UK and China's AI Policies?

MS -IR Thesis

Tanzeela Jameel

Roll no: 01-257192-008

Supervisor: Dr Adam Saud

Department of Humanities and Social Science

Bahria University, Islamabad

BAHRIA UNIVERSITY, ISLAMABAD

APPROVAL SHEET

SUBMISSION OF HIGHER RESEARCH DEGREE THESIS

Candidate's Name: **Tanzeela Jameel**

Discipline: **MS International Relations**

Faculty: **Humanities and Social Science**

I hereby certify that the above candidate's work including thesis has been completed to my satisfaction and that the thesis is in a format and of an editorial standard recognized by the faculty/ department as appropriate for examination.

Principal Supervisor: _____

Date: _____

DECLERATION OF AUTHORIZATION

I, Tanzeela Jameel, Master of Science in International Relations Student in the Department of Humanities and Social Science, Bahria University, Islamabad certify that the research work presented in this thesis is to the best of my knowledge my own. All sources used and any help received in the preparation of this dissertation have been acknowledged. I hereby declare that I have not submitted this material, either in whole or in a part, for any other degree at this or other institute.

Signature: _____ Date: _____

PLAGIARISM UNDERTAKING

I, solemnly declare that work presented in the thesis titled "Adversarial Artificial Intelligence (AI) Impacts on Cyber Security Policies of EU: Why Should EU Learn from UK and China's AI Policies?" is solely my research work with no significant contribution from any other person. Small contributions/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

Signature: _____

Date: _____

ACKNOWLEDGMENT

First and foremost, I would acknowledge my limitless thank to Allah, the Ever-Magnificent; the Lord of the worlds. This research thesis has been successfully completed with the assistance of various authorities. I would like to thank all those who helped in carrying out this research and offering comments and suggestions. First, I would like to thank Bahria University for giving this opportunity to conduct this research as partial fulfillment of the requirement of Master's Degree in International Relations and providing complete research database in Library.

Secondly, I would like to express my gratitude to my research supervisor Dr. Adam Saud for his continuous and patient assistance, enthusiastic encouragement and beneficial critique. During the period of completing this research, Dr. Adam Saud provided guidance, advice, valuable suggestion, constructive comment and commitment to reply queries promptly throughout this research work. His willingness to give his precious time so generously is highly appreciated.

I also would like to express my wholehearted thanks to all my beloved friends and family, who have been supportive all long. Due to their unconditional support, I had the chance to complete this research.

ABBREVIATIONS

Artificial Intelligence	AI
Machine Learning	ML
European Union	EU
Autonomous Weapon System	AWS
Information Technology	IT
Human In The Loop	HITL
Human on the Loop	HOTL
Human In Command	HIC
General Data Protection Regulation	GDPR
Non-Governmental Organizations	NGOs
Network and Information System Directive	NIS
Operators of Essential Services	OES
European Union Agency for Network and Information	ENISA
National Cyber Security Center	NCSC
Artificial Intelligence Development Plan	AIDP

TABLE OF CONTENTS

Introduction

Chapter 1:

Abstract

In recent years, the use of Artificial Intelligence (AI) has grown exponentially. However, there is a concern regarding the misuse of this technology. This malicious use of AI is commonly known as adversarial AI which cannot just affect the countries with the financial loss but also increasing the cyber-crimes ratio. This research focuses on the impacts of adversarial AI on EU's cyber security policies and also provide arguments on Why the EU can learn from UK and China. EU has been taken as a case study. The major focus of the research is to find gaps that is causing rapidly increasing attacks in EU since 2007. Additionally, The research reveals potential threats of adversarial AI for EU and focuses cyber security policies of EU and to understand the adversarial AI framework. The research has emphasized that threats caused by adversarial AI, role of adversarial AI and its impact on EU's AI policies towards cyber security. The findings in research and attacks reflects that the EU AI policies need rethinking. Mentioned China and UK's AI policies are quite beneficial in terms of enhancement of AI policies of EU towards cyber security. This research analyze how EU can utilize UK and China's AI and cyber security polices as potential model. The research is qualitative in nature and deductive approach has been applied.

1. Introduction

The time period from 1940 to 1960 is known as the invention of technological development and its after effects. At that time Europe was in political chaos during World War II. Although it was a difficult time for Europe, technological developments were going on for dominating rivals. The desire of bringing together human mind, animals and machine was rising for security purposes. The rapid advancement of technology was coming up with advantages as well as disadvantages. The facilitation of technology, for instance, shifting the data from papers to softwares was facilitating the world likewise it was increasing cyber-crimes as well. At that time the pioneer of cybernetics Norbert Wiener aimed to unify electronics, mathematical theory and automation.[1] Cybernetics is defined as the control and communication in the animal and machine.[2] In the business, machines are dependent on artificial intelligence. Advanced mechanics and science have been very well known. Such a machine is ordinarily known as a cyborg. Cyborg is an entity that has both artificial and natural frameworks. This sort of life form can be viewed as an automatic human-machine that utilize sensor, computerized reasoning and feedback control frameworks.

John Von Neumann and Alan Turing are known as fathers of the Artificial Intelligence technology in 1950 and they made the progress from Pentium Computers to nineteenth century decimal rationale (which accordingly managed values from 0 to 9) and machines to paired rationale (which depend on Boolean variable-based math, managing pretty much significant chains of 0 or 1).[3] They realized that the machine is capable of doing tasks as per given command (programming). Turing test (human are unable to know whether they are dealing with machines or human being) on the other hand raised many questions as it highlights that the humans should be able to know whether they are talking to a fellow human or machine. Not knowing with whom communication is going was concern of many scholars and scientists and this concern was highlighted in many of the articles. The term "AI" can be credited to John McCarthy of Massachusetts Institute of Technology (MIT).[4] He programmed machines in a way that those can perform better and efficient than human beings for instance, perceptual learning, memory

[1] Ertel, Wolfgang. *Introduction to artificial intelligence*. Springer, 2018. 96
[2] Lepskiy and Vladimir, *"Evolution of Cybernetics: Philosophical and Methodological Analysis*, Kybernetes, 2018.
[3] John Smith, "'History of Artificial Intelligence,'" *Council Of Europe, 2021*, https://www.coe.int/en/web/artificial-intelligence/history-of-ai.
[4] Seto, Mae L., ed. *Marine robot autonomy*. Springer Science & Business Media, 2012.