Artificial Intelligence

Crime, War, and Justice

Edited By

Nathalie Rébé

Artificial Intelligence: Crime, War, and Justice

Edited By Nathalie Rébé

This book first published 2023

Ethics International Press Ltd, UK

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Print Book ISBN: 978-1-80441-302-9

eBook ISBN: 978-1-80441-303-6

Table of Contents

Part III: Justice

Preface

In the increasingly strong AI context, technology plays a key role in crime and prevention, war, and in the justice system development. This edited volume will provide a cross disciplinary approach by legal and IT specialists on how the legal system can be abused or reinforced with the use of Artificial Intelligence.

Through a series of examples, experts will discuss the effect of AI on resolving crimes, and in the development of weapons and military strategies. This work will also explain how AI can benefit the enforcement and justice system and the creation of a fairer judicial system that respects human rights without bias.

Editorial note

I dedicate this important work to my esteemed colleagues and dear friends who contributed to this edited volume on Artificial Intelligence. I want to warmly thank these amazing experts, lawyers, judges, and academics who believed in me and in my project and joined the team to build this valuable collection of essays. Together, their works on AI Crime, War, and Justice, represent the landscape of such a complex hot topic which deserves more consideration at the international level.

A very special recognition should also go to Elena Lazar for her unwavering friendship, and great knowledge of the Law.

Last, I would like to heartfully thank Sarah and Ben from Ethics Press for their professionalism. It was truly a pleasure to work with them.

About the Editor

Dr Nathalie Rébé holds a Doctorate in Business Administration (DBA) from Paris School of Business, and a Doctorate in Juridical Science (JSD) on Financial Crimes from Thomas Jefferson School of Law (USA). She has participated in various international conferences as an academic author, and taught on both International Criminal Law, and Business Administration university level courses.

With a Post Graduate Diploma in Cyber Law from the University of Montpellier, Dr Rébé's research and publications have been focused on New Technologies, and Regulatory matters**.** She is the author of "*Artificial Intelligence: Robot Law, Policy and Ethics, Brill Nijhoff, 2021*" and of "*Regulating Cyber Technologies: Privacy vs Security, World Scientific, 2023".*

About the Contributors

Maria-Ruxandra Bodea is a PHD student at the University of Bucharest, Faculty of Law, studying AI as a topic. She also holds a Master's Degree in Romanian Private Law, and in Public International Law. She is currently a lawyer at one of the biggest law firms in Romania, Stoica and associates and her area of practice encompasses Romanian civil law, human rights, and intellectual property.

Hon Dr Fausto Martin De Sanctis is a Federal Appeals Judge at the Federal Court of Appeals for the 3rd Region, in Sao Paulo, Brazil. Previously, he was a São Paulo State Judge (1990-1991), Public Prosecutor of the Municipality of São Paulo, and Public Prosecutor of the State of São Paulo, in the area of the Public Defender's Office. He was a professor at São Judas Tadeu University for 12 years. PhD in Criminal Law from São Paulo University (USP) and Specialist in Civil Procedure from Brasília University (UnB), he has written over 40 legal works published in Brazil and abroad, in addition to articles.

Dr Hossam Nabil Elshenraky is an Associate Professor in Criminal Investigation at the Dubai Police Academy. He holds a Bachelor of Law, and Police Sciences he received in 1992 from the Police College, as well as a Master's Degree, and a PhD in Cybercrime Investigation.

He was an investigation officer from 1996 until 2018, but also worked with peacekeeping forces in Darfur, Sudan for two years and 3 months as a police sector commander. Now retired as a brigadier general, he is currently a Scientific Adviser in the police Department for Future Foresight, a teaching staff, as well as a certified trainer with the Dubai Police Academy. He supervised dozens of master's and doctoral dissertations at the Dubai Police Academy in the field of police sciences and security crisis management.

Dr Hossam Nabil Elshenraky taught many training courses in criminal investigation, and information crimes, as well as presented and chaired

in many international conferences. Dr. Elshenraky's areas of focus are: criminal investigation, information technology crimes, leadership and decision making, cyber crisis management, digital transformation, and cyber security.

Dr Hossam Nabil Elshenraky is a peer reviewer for the Journal of Cybercrime, a member of the editorial board of the Naif Arab University's journal for Security Sciences, arbitrator at the Journal of Digital Forensic, and a security expert accredited by the Naif Arab University for Security Sciences listed in its database of security experts. He is a member of the Editorial Board of the Journal of the International Police Science Organization (IPSA) in the USA, as well as a Member of the Editorial Board of the Security and Law Magazine.

Dr Elshenraky has more than 12 scientific research papers published in scientific journals in Egypt and the UAE, and is the author of 5 academic books.

Mauricio Kimura is pursuing a Ph.D at the University of Waikato, Te Piringa Faculty of Law, New Zealand His research topic is *"Should we ascribe Legal Personality for Autonomous Artificial Intelligence Humanoid? And if so, what kind?"*. Kimura has completed his LL.B at the Sao Bernardo do Campo School of Law, Brazil, and LL.M at the George Washington University, USA. Prior to becoming an academic, he worked as a lawyer in various industries, from media to technology for over 20 years.

Dr Elena Lazar is a lecturer in Public International Law and EU Internet Law at the University of Bucharest Law Faculty in Romania, as well as a lawyer at the Bucharest Bar. Her area of practice as a lawyer comprises human rights, data protection and data privacy. She also holds a post-Doctorate degree in AI and international law from Paris II University-Pantheon Assas, France.

Dr Michal Matyasik holds a Ph.D. in Political Science from the Jagiellonian University in Cracow, Poland. He has specialized in various security-oriented topics such as warfare, intelligence and strategy. In 2012-2013 he was deployed in Afghanistan as a member of the civil-

military cooperation unit within ISAF. Recently, he was employed as an instructor at the Rabdan Academy in the United Arab Emirates and is providing vocational trainings to the police, militaries and other governmental agencies.

Dr Tal Pavel is the founder and director of CyBureau – The Institute for Cyber Policy Studies, Israel, and a lecturer for academic institutions worldwide. Dr. Pavel is an academic lecturer, researcher, and speaker specializing in the tangent lines between international relations, political science, and cyberspace, such as cyber conflicts, cyberwarfare, cyber threats, and nation-state cyber actors. He has served as a keynote speaker at international conferences and has been interviewed as an expert cyber by major media outlets. Dr. Pavel holds a PhD in Middle Eastern Studies from Bar-Ilan University, Israel on "Changes in Governmental Restrictions over the Use of the Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between 2002 – 2005".

Dr Nikola Protrka is a serving Police officer. As a national expert on Cybercrime he worked in most investigative areas related to Cybercrime, from computer fraud to ransomware, DDOS attacks, digital evidence, computer forensics and data protection. With both an operational and strategic police background and over 25 years of training and development experience his passions are Cyber Intelligence/ Surveillance/Defence, operational risk and business continuity related issues, and learning to improve performance, employee awareness and professionalism. He is an experienced training manager and facilitator with a reputation for producing a positive and productive learning environment, with national and international experience at both the strategic and operational levels. He became a professor at the Police Academy Zagreb in 2011 and represented the Croatian Ministry of the Interior internationally, designing and delivering training on various topics related to digital evidence, computer forensics, cybercrime, artificial intelligence etc. He has considerable operational experience in criminal investigations and he is a contact point of European Union Agency for Law Enforcement Training - CEPOL. Dr Protrka is recognised expert included in various EU projects.

Marta Stroppa is a PhD Candidate in Human Rights and Global Politics at the Sant'Anna School of Advanced Studies and Research Fellow of the Information Society Law Center of the University of Milan. Her research focuses on the legal implications of new technologies in the use of force and conduct of hostilities. She previously worked in the Legal Affairs Office of the Permanent Mission of Italy to the United Nations in New York and in the Global Maritime Crime Programme of United Nations Office on Drugs and Crime. Stroppa holds a Bachelor's and Master's Degree in International Relations from the University of Milan and a Master of Laws in International and Human Rights Law from Tilburg University.

Jimena Viveros is a Mexican lawyer with experience in public international law, International Criminal Law, International Humanitarian Law, and International Human Rights Law. She has an LL.M. in public international law from Leiden University in The Netherlands and is pursuing her PhD at the University of Cologne in Germany, conducting her doctoral thesis on the impact of Artificial Intelligence and Autonomous Weapons Systems on the International Peace and Security Law and Policy Framework, perspectives from International Criminal Law, International Humanitarian Law and public international law, and concrete propositions on how to move forward, under the supervision of Dr Claus Kreß. On the international field, she has worked at the International Criminal Court, the International Criminal Tribunal for the former Yugoslavia, the International Criminal Tribunal for Rwanda, the Organization for the Prohibition of Chemical Weapons, the United Nations Verification Mission in Colombia for the disarmament of the FARC; additionally, she has worked at the Lebanon Supreme Court, in addition to several NGOs in Kenya, Cambodia, and Palestine. In Mexico, she has held leadership positions such as Head of International Affairs in both the Ministry of Security and Civilian Protection, and at the Federal Tax and Finance Prosecutor's Office, as Chief of Staff of former Federal Judicial Council Member and currently Supreme Court Justice, Dr Loretta Ortiz Ahlf.

List of abbreviations

ABMS	Advanced Battle Management System
ACLU	American Civil Liberties Union
ACM FAT	Assoctiation for Computing Machinery Conference on Fairness, Accountability, and Transparency
ADM	Automatic Decision-Making
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine Learning
AP	Additional Protocol
API URL	Application Programming Interface Uniform Resource Locator
APT	Advanced Persistent Threats
AR	Augmented Reality
ART	Augmented Reality Tool
AWS	Autonomous Weapons System
BCW	Body-Worn Camera
BI	Bureau of Investigation
BLM	Black Lives Matter
BPA	Blood Stain Pattern Analysis
BPUFF	Basic Principles on the Use of Force and Firearms
BWC	Body-Worn Cameras
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Human Apart
CAT	Computer-Aided Technology
CBP	US Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear weapons

CBT	Computer-Based Test
CCTV	Closed-Circuit Television
CCW	Convention on Certain Conventional Weapons
CEO	Chief Executive Officer
CEPEJ	European Commisssion for the Efficiency of Justice
CEPOL	European Union Agency for Law Enforcement Training
CHAT	Chat Generative Pre-trained Transformer
CIA	Central Intelligence Agency
CNJ	National Council of Justice
CoE	Council of Europe
CoM	Committee of Ministers
COVID-19	Coronavirus Disease 2019
CRT	Civil Resolution Tribunal
CV	Curriculum Vitae
CWC	Chemical Weapons and on their Destruction
Cyber HQ	Cyber High Quality
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DHS	US Department of Homeland Security
DLA	Defense Logistics Agency
DNA	Distributed Network Attack
DoD	US Department of Defense
DOJ	Department of Justice
DRC	Democratic Republic of the Congo
DSPE	Electronic Judicial Process Systems Division
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights

ECPE	European Code of Police Ethics
ECtHR	European Court of Human Rights
ENCCLA	National Strategy to Combat Corruption and Money Laundering
EOD	Explosive Ordnance Disposal
EU	European Union
EUR	Euro
EUROPOL	European Union Agency for Law Enforcement Cooperation
FAA	Federal Aviation Administration
FAT	Fairness, Accountability and Transparency
FGV	Foundation Getulio Vargas
FRT	Facial Recognition Technology
FRY	Federal Republic of Yugoslavia
G20	Group of Twenty
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
GEOINT	Geospatial Intelligence
GGE	Group of Governmental Experts
GHQ	General Headquarters
GIFCT	Global Internet Forum to Counter Terrorism
GIT	Global Information Tracker
GPS	Global Positioning System
HDM	Hidden Dynamic Model
HDR	Human Rights Defense
HRC	Human Right Council
HRD	Human Rights Defender in France

HRW	Human Rights Watch
IACA	International Association for Court Administration
IBM	International Business Machines Corporation
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICTY	International Criminal Tribunal for the former Yugoslavia
IDF	Israel Defense Forces
IDS/IPS	Intrusion Detection System/Intrusion Protection System
IED	Improvised Explosive Devices
IEEE	Institute of Electrical and Electronics Engineers
IHL	International Humanitarian Law
IHRL	International Human Rights Law
IIA	Israel Innovation Authority
ILA	International Law Association
ILC	Internaiontal Law Commission
IoT	Internet of Things
IP	Internet Protocol
IPEJA	Institute for Research and Advanced Legal Studies
IRIS	Institute for Research on Internet and Society
IRS	Internal Revenue Service
ISIS	Islamic State in Iraq and Syria
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITI	International Transparency Index

ITLOS	International Tribunal for the Law of the Sea
IVA	Intelligent Virtual Assistant
JADS	Jheronimus Academy of Data Science
LAWS	Lethal Autonomous Weapons Systems
LEA	Law Enforcement Agencies
LED	Law Enforcement Directive
LIAA-3R	Laboratory of Applied Intelligence of the 3 Region
LIDAR	Light Detection and Ranging Sensors
LLB	Bachelor of Laws
LLM	Large Language Models
LLM	Master of Law or Latinum Legum Magister
LSTM	Long Short-Term Memory
MIT	Massachusetts Institute of Technology
MTA	Mail Transfer Agent
NAIH	National Authority for Data Protection and Freedom of Information
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information
NGO	Non-Governmental Organization
NIS	Network and Information Systems
NISA	National Information Security Authority
NISIS	National Initiative for Secured Intelligent Systems
NLP	Natural Linguistic Processing
NYPD	New York Police Department
NYSBA	New York State Bar Association
OAS	Organization of American States

OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the High Commissioner for Human Rights
OP	Operational Environments
ORCID	Open Researcher and Contributor IDentifier
OSINT	Open-Source Intelligence
PDA	Personal Digital Assistant
PDPJ	Digital Platform of the Judiciary Power
PhD	Doctor in Philosophy
PLF	Passenger Locator Form
Q-UGVs	Quadrupedal Unmanned Ground Vehicles
RTS	Radio Televizije Serbije
SARS-Cov-2	Severe Acute Respiratory Syndrome Coronavirus 2
SCARA	Selective Compliance Assembly Robot Arm or Selective Compliance Articulated
SDGs	Sustainable Development Goals
SETI	Secretariat of Information Technology
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SKALA	State Office of Criminal Investigations in North Rhine-Westphalia
SNAP-R	Simplified Network Application Process - Redesign
STF	Brazilian Supreme Court
STJ	Brazilian Superior Court of Justice
SUPACE	Supreme Court Postal for Assistance in Court Efficiency
T-CY	Cybercrime Convention Committee
TJRO	Court of Justice of Rondônia
TRF3	Federal Appeals Court for the 3rd Region

TSA	Transportation Security Administration
TST	Superior Labor Court
TV	Television
UAS	Unmanned Aerial Solution
UAV	Unmanned Aerial Vehicle
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNCCT	United Nations Counter Terrorism Centre
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Education, Science and Culture Organization
UNHCHR	United Nations High Commissioner for Human Rights
UNODA	United Nations Office for Disarmament Affairs
UNSC	United Nations Security Council
URL	Uniform Resource Locator
US	United States
USB	Universal Serial Bus
USD	U.S. Dollar
USP	University of Sao Paulo
UVs	Unmanned Vehicles
WHO	World Health Organization

Introduction
Artificial Intelligence: Crime, War, and Justice

Dr Nathalie Rébé

The structuring of the book

The aim of this book is to provide the reader with a comprehensive understanding of the usage of Artificial Intelligence (AI) by criminals, the police, militaries, and the justice system, and explain the opportunities and threats related to AI. This book is divided into three parts, *Crime, War, and Justice*. This work brings together some of the most important essays in this area written by leading scholars, lawyers and judges, and offers significant contributions to help us comprehend the evolution and future of AI. This introduction will present the essays included and provide some general background.

Part I: Crime

Artificial Intelligence can both assist criminals in their endeavors, and help the police catch them. After introducing AI crimes, Part I of this book will discuss the opportunities and threats related to the use of AI by law enforcement, as well as the inherent trade-off between safety and the fundamental right of privacy while tracking criminals.

In Chapter 1, Dr Nikola Protrka will discuss *The use of Artificial Intelligence (AI) by criminals* and the several scenarios in which AI may be utilized with wrong intentions. Protrka will explore AI as a crime, such as voice phishing, fake news, deep fake, password attack, military robots, and

drone attacks, and reflect on the ethical issues and threats which may arise from the use of AI technologies.

Artificial Intelligence has also made it easier for police officers to obtain information and forensic evidence regarding ambiguous criminal and terrorist crimes. In Chapter 2, *Implementing Artificial Intelligence in combating crime*, Dr Hossam Nabil Elshenraky discussed the advantages of AI, and methods for managing investigations, crime scenes, examining evidence, police surveillance, and other fields in which police agencies perform their work in the light of technological development.

AI has been an important tool to prevent crimes, and a quick alternative to identify the perpetrators of a delict. In Chapter 3, *Police and AI, the trade-off between privacy and safety*, Mauricio Kimura will focus on the use and implementation of Artificial Intelligence within the Police. Kimura will argue about the role of the Police to protect their citizens, and the dilemma of finding the right balance between safety and the fundamental right of privacy. According to the author, one right might have to be prioritized over the other under some specific circumstances.

Part II: War

The second part of this book will offer an overview on the advancement of Artificial Intelligence in the military field, and will discuss the use of force, as well as the law of war autonomous weapons may breach. We will also explore the future of Autonomous Weapons Systems (AWS), and the urgent need for regulation by countries.

In Chapter 4**,** Dr Michal Matyasik provides a case study, as an example of *the first AI war - operation Guardian of the Walls*. Matyasik will introduce and describe 'supposedly', the first existing case of AI application to an armed conflict which took place in May 2021 between Israel and Hamas. This Chapter will address the lessons learned, and a way forward for further expansion of AI into the military domain.

In Chapter 5, Marta Stroppa will explore the main legal implications of the use of AI weapons in armed conflicts in *Autonomous Weapon Systems (AWS) and the jus in bello.* Stroppa will explain how Autonomous Weapons Systems shall comply to international humanitarian law, with reference to the principles of distinction, proportionality and precautions in attack, as well as to the principles of humanity. The author will be argued that Autonomous Weapons Systems may be lawfully used only in uncluttered scenario, where civilians are not at stakes.

AWS are able to carry out surveillance, intelligence and reconnaissance activities, as well as engage in combat, and use lethal force. For this reason, In Chapter 6, *AWS and the use of force*, Jimena Viveros will argue that the unpredictable nature of Autonomous Weapons Systems may also bring dangers if used incorrectly, or for the wrong purposes. In this chapter, Viveros will present the controversies of the international law on the use of force, which States often exploit and interpret in a manner that justifies self-defense.

Part III: Justice

The third part of this book will discuss how Artificial Intelligence can play a key role in the construction of a fair justice system. Even if the use of AI by criminals, at warfare, and in courts, is still at an early stage, it already generates diverse jurisdictional and regulatory issues, and might trigger increased discriminations.

In Chapter 7, *Regulating AI based Cyber Attacks: Exploring multi-dimensional approaches and challenges,* Dr Tal Pavel analyses the typology of AI attacks, and reviews their impact on the international society. Pavel will then focus on the lack of regulations and their specificities, but also tackle the jurisdictional issues triggered by AI-based cyber-attacks.

Despite of the lack of policies related to its usage, AI might become an incredible ally for the Justice system, as its capacity to sort out and analyze an unlimited number of precedents to draw legal conclusions could reshape the future of trials. By their experience in court and relying

upon recent examples, the next authors will attempt to help us understand the pros and cons of the use of AI in courts, judicial decisions and research, as well as depict a picture of what they see for the future of AI. This is discussed in some detail in Chapter 8: *Automated justice*, by Maria-Ruxandra Bodea.

In Chapter 9, *AI Discrimination in the light of the ECHR system*, Dr Elena Lazar will argue that digital technologies tend to reinforce racial inequalities, discrimination and intolerance, since they are typically based on algorithms that make predictions to support or even fully automate decision-making. Dr Lazar will analyze how to find the proper balance between supporting the development of new technologies, and preventing discriminatory behavior that might affect human rights.

The final chapter of Part III on AI and Justice offers an important contribution from Brazilian Judge Fausto Martin De Sanctis on *Artificial Intelligence as a way to improve complex and sluggish appeals systems.* In Chapter 10, De Sanctis will debate on the use of virtual (online) sessions, and Artificial Intelligence (AI) in courts, while providing an insightful example of the Brazilian experience.

Conclusion

A final comment should be made about how these essays were selected for publication. We received submissions from all over the world, however, authors were chosen for their expertise on Artificial Intelligence, military, police, criminal, human rights, privacy, and legal matters regarding their selected topic.

Rather than offer a single narrative, the essays instead may be read in any order and present a number of important perspectives and insights on the topic that should help provide further clarifying illumination on central debates and ideas in this field. However, essays were organized in a specific order to discuss Artificial Intelligence and legal criminal matters in way that is coherent to the reader.

Readers interested in Artificial Intelligence will learn more on a variety of topics involving Crime, War, and Justice, thus discovering current and future technical and legal practices.

I hope that you will enjoy reading the essays in this book as much as I have. Finally, my most sincere thanks must be reserved for the authors for their contributions, and for sharing their knowledge and expertise in a world where Artificial Intelligence will never stop improving and forever represent a risk the world must anticipate and fight accordingly.

Dr Nathalie Rébé, Editor
Luxembourg, November 2023

Part I: Crime

Chapter 1
The use of Artificial Intelligence (AI) by criminals

Dr Nikola Protrka

Abstract

In today's world everything is automated and computerised, from education, sales, industry, self-driving, talent acquisition and human resources. Humans have benefited from such devices and technology in terms of efficiency and effectiveness. The adoption of the Internet of Things has resulted in a significant transformation in the way people live, work, and interact with one another. Captchas[1] and image recognition, virus creation, phishing and whaling, and other tactics utilised by the communities are also exploited by hackers. They're learning when to hide and when to attack. Instead of hiding behind masks to rob a bank, criminals are using artificial intelligence to conceal themselves. Human-like intelligence has been produced using self-aware systems. Machines are capable of surpassing the brightest humans in any discipline thanks to artificial intelligence and algorithms.

Introduction

The growth of technology and machine intelligence has reformed society in the past decades. This newly interconnected and symbiotic world has given rise to new societal and global challenges, and experts must face these head-on by using bold and creative solutions. We live in a world

[1] A CAPTCHA is a type of challenge–response test used in computing to determine whether or not the user is human. The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. The most common type of CAPTCHA was first invented in 1997 by two groups working in parallel.

awash in data. And as many organisations deploy technology solutions like augmented reality, body cameras, license plate readers, and smart sensors, they will likely generate more data each day than in their entire analogue histories. The success of future law enforcement strategies rests on being able to quickly and efficiently harness these immense volumes of data to support investigations and enforcement actions. But these mountains of data are too vast for any human to comb through, even if they dedicated an entire lifetime to searching them. Criminals are increasingly using Artificial Intelligence (hereinafter: AI) to link tools together so that they may be executed in parallel during an attack as former US president Barrack Obama expressed his concerns about AI-enabled bots attacking nuclear weapon silos and causing a launch. This intimates that the threat of AI enhanced attacks are a major concern even at the highest level of government (Greenberg, 2016). Before we start to go deeply to the subject, let's briefly explain a definition of this two terms. In 1950's Alan Turing give definition of AI as "Systems that act like humans", after he asked himself "Can machines think?" Then he proposes a test, now known as the "Turing Test," in which a human interrogator tries to tell the difference between a computer and a human written answer. While this test has been subjected to a great deal of criticism since its publication, it remains an essential element of AI history as well as a continuing philosophical topic since it makes use of language concepts (Turing, 1950).

Baker and Robinson stated that a bulldozer can clear acres of precious rainforest in an hour whereas a team of humans with axes might not clear even half an acre in a day. Similarly, AI-operated databases can keep accurate records of vast quantities of information and recall and analyse basic information in an instant. It can process volumes of data at speeds beyond the capacity of a single human mind. AI, in its most basic form, is a subject that combines computer science with large datasets to solve problems. It also includes the sub-fields of machine learning and deep learning, both of which are usually referenced when discussing AI. Artificial Intelligence algorithms are used in these areas to develop expert systems that make predictions or classifications based on input data (Baker, 2020). Criminals utilise AI and machine learning to take the

findings of one tool and teach other tools about it so they may use it against other systems. For example, if one tool discovers a password, that tool can pass the knowledge on to another tool or bot, which can then use the password to exploit one or more systems. A criminal can create a toolkit or bot to act like a "real" attacker using AI. For example, the tool or bot may execute a phishing assault on an organisation and then use the results to undertake various sorts of attacks, just like a human would. Criminals are developing toolsets and bots that employ AI techniques to avoid detection and prevent the procedures that are currently in place in most businesses. Many of these tools (which are usually open source) are readily available on the Internet. This allows anybody to use the tools against specific organisations (IBM Cloud Education, 2020b).

Because AI is so closely linked to physical space (e.g., autonomous vehicles, intelligent virtual assistants), AI-related criminality might cause actual harm to persons outside of cyberspace (Doowon, 2020).

A brief history of AI

The concept of a "thinking machine" stretches back to ancient Greece. In the year 1955, John McCarthy coined the phrase "Artificial Intelligence" at the first-ever AI conference at Dartmouth College. McCarthy is regarded as one of AI's founding fathers, with Alan Turing, Allen Newell, Herbert A. Simon, and Marvin Minsky. Turing proposed that if people use accessible knowledge, as well as reason, to solve issues and make decisions, why can't robots do the same, and introduces the Turing Test to determine if a computer can demonstrate the same intelligence (or the results of the same intelligence) as a human. The value of the Turing test has been debated ever since (Turing, 1950). Another important name is Frank Rosenblatt, who creates the Mark 1 Perceptron in the year 1967, the world's first computer based on a neural network that learns via trial and error. A year later, Marvin Minsky and Seymour Papert publish Perceptrons, which becomes a seminal work on neural networks as well as, at least for a time, an argument against future neural network research. With the passage of time, a wave of computers began to emerge in 1980's. They got quicker, more inexpensive, and capable of

storing more data as time passed. The finest thing was that they were able to think abstractly, recognise themselves, and do Natural Language Processing (DeSot, 2017).

The growth of finances and algorithmic tools has re-ignited AI research. The machine learnt from the user's experience using deep learning techniques. Backpropagation neural networks, which utilise a backpropagation algorithm to train itself, have proven popular in AI applications. In the 1997. the IBM's Deep Blue[2] beats a world chess champion in that time Garry Kasparov, in a chess match. The technology was successfully created after all of the failed attempts, but the major goals were not reached until the 2000s. Despite a dearth of government funding and public attention at the time, AI thrived. In a recent history we can mention that in a five-game battle, DeepMind's AlphaGo[3] software, which is powered by a deep neural network, defeats Lee Sodol, the world champion Go player in the 2016. Given the enormous number of possible movements as the game proceeds (nearly 14.5 trillion after only four plays!), the win is important. DeepMind was later bought by Google for a USD 400 million (Russel & Norvig, 2021).

How criminals can use AI

We may all be aware of the current scenario and the importance of AI in our life. AI gathers and organises vast volumes of data in order to generate inferences and estimates that are beyond the human ability to handle manually. The risk of a mistake and discovered unusual patterns is lowered as organisational efficiency increase. So, whether we're talking about spam or fraud, or the real-time warnings it sends to businesses

[2] Deep Blue was a chess-playing expert system run on a unique purpose-built IBM supercomputer. It was the first computer to win a game, and the first to win a match, against a reigning world champion under regular time controls. Development began in 1985 at Carnegie Mellon University under the name ChipTest.

[3] DeepMind Technologies is a British artificial intelligence subsidiary of Alphabet Inc. and research laboratory founded in September 2010. DeepMind was acquired by Google in 2014. The company is based in London, with research centres in Canada, France, and the United States.

about questionable activity, a lot has already been protected. Cost cutting has aided the company in increasing its profit share. For instance, "teaching" robots to take customer support calls and so eliminating several employees (DataFlair, 2019). Many security systems were built with the assumption that this would not change until computers have the ability to handle heuristic issues. It was simply not envisaged that a machine might guess a password, interpret a graphical Captcha, or learn how actual traffic behaves. We are now surrounded with security that has been rendered obsolete by AI. Many times, a system will need to verify that a user is, in fact, a human. This is because a computer programme can use or replicate every function that a computer can provide to a person. If you try to log in to Facebook more than three times, Facebook will ask you to verify that you are a human, not a computer programme trying to enter millions of passwords per second. A captcha approach is used by Facebook and many other services to do that. Until AI came along, this successfully separated programmes from people for years. Basic convolutional neural networks may now be used to recognise captcha pictures from a large dataset. Each captcha has a specific goal, and after a convent has been trained, it can work out future captchas. This is a simpler example in which only the fundamentals of neural networks are required. Brute force assaults are significantly more possible now that captchas can be circumvented. You may have also come across a captcha that asks you to "choose all photographs including a bus," which is just as easy for AI to get around. We all know how good object identification is - Google even included it as a basic feature in their search engine.

Phishing is a very common form of hacking. It entails sending an email that is graphically meant to resemble, say, Facebook and uses formal language similar to that of Facebook. It will claim that you need to update, view, or edit anything and will ask for your login information. Any information you enter will be forwarded to the criminal's server. By scanning any site, learning how it looks and communicates, and then mass-producing bogus emails based on particular findings to be sent out automatically on a huge scale, AI may enhance phishing (DataFlair, History of Artificial Intelligence, 2019). This isn't the only option, though.

Hackers may guess email addresses using the same principles that they used to guess passwords. It is possible to generate millions of email addresses, increasing the chances of locating technically unaware people. Many email providers, like Gmail, have sophisticated mechanisms in place to detect phishing emails; nevertheless, machine learning may be used to design emails that bypass these systems. The training set would consist of a collection of emails, some of which were unsuccessful in reaching a user owing to phishing detection and others which were successful. By learning which phishing attempts were recognised and which were not, a neural network may learn how to identify phishing.

Crimes including drug trafficking, selling, buying, and having illegal narcotics are on the rise, and they rely on AI planning and autonomous navigation technology like tools to increase smuggling success rates. Unmanned vehicles are being used by criminals to increase narcotics trafficking between businesses (DataFlair, Beware!, 2019). More than half of people prefer to text rather than converse on the phone, therefore a chatbot is becoming popular. Crime has also found a home in that neighbourhood. Chatbots are designed to initiate a discussion with users in order to persuade them to give sensitive financial or account information. With the assistance of AI, hackers may now create undetectable malware. These aid them in controlling cameras, stealing, and uploading, modifying, and manipulating files. Computer virus code is written by criminals, who then employ password scrapers and other tools to execute their infection. Criminals utilise neural networks in AI to discover and recognise passwords. Machines may be able to readily guess passwords that look like this – "password." With the aid of neural networks, criminals are able to crack a fraction of the passwords. It is now quite simple for a machine to crunch numbers and predict unknown passwords.

Criminals are using AI to boost the potency of their cyber assaults on businesses, but despite the increased sophistication of criminal techniques, there is a lot that businesses can do to defend themselves. While AI is not yet widely used as a key offensive weapon in cyber assaults, its use and capabilities are expanding and getting more