https://asce-uok.edu.pk/journal
DOI: https://doi.org/10.56384/jes.v38i2.252

Policies of Artificial Intelligence in the EU: Learning Curve from the UK and China?

Tanzeela Jameel[*]
Adam Saud[**]

Abstract

Artificial Intelligence (AI) can be traced back to John McCarthy who is considered as one of the pioneers of the AI discipline.[1] AI has emerged as one of the most important realities in the first quarter of the 21st century. AI is being used in many industries including healthcare, production and manufacturing, military modernization, etc. Whereas there are many benefits of AI, it has its drawbacks as well. There is always a possibility that technology getting into the wrong hands. This malicious use of AI is commonly known as "adversarial AI", which cannot just cause financial loss to countries but also increase the ratio of cybercrimes. This work sheds light on the impact of adversarial AI from the point of view of governance. More specifically, it takes a detailed look at the AI policies of the European Union (EU) and identifies different cyber-security loopholes. Based on some recent events, this study also highlights the role of adversarial AI in promoting cybercrimes in the form of phishing and data breach attacks in the EU. Finally, we provide arguments on how the EU can learn from some countries, like China and the UK, in order to strengthen its AI policies.

Keywords: Artificial Intelligence, Adversarial AI, Cyber security, the EU policy, UK and China.

[*] Ms. Tanzeela Jameel is an IR Graduate at the Bahria University, Islamabad. Email: tanzilajameel26@gmail.com

[**] Dr. Adam Saud is Professor at the Bahria University, Islamabad. Email: asaud.buic@bahria.edu.pk. ORCID: https://orcid.org/0000-0001-8606-9874.

[1] 1956, Dartmouth Conference, Dartmouth College, Hanover, New Hampshire, http://jmc.stanford.edu.

Introduction

A detailed study of history will reveal that the world is all about revolutions, which arise from human needs. The digital revolution carries immense significance for the 21st century. The prime objective of technology is to make human life easier. Artificial Intelligence (AI) has been playing the most vital and effective role in this regard. Though AI was introduced in 1956 by John McCarthy, it has now become the necessity of this world.[2]

Now the question comes, what is AI? AI is a form of intelligent computing. Machines are formed to work and act like human beings using algorithms that give them direction to make decisions. They behave intelligently. They analyze the situation and conduct specific actions to achieve the targeted goals. AI is performing its magic in two forms: it may be purely software-based, for instance, language translator, facial recognition or it can be hardware implanted like driverless cars and drones.[3] It is facilitating the world with its immense advantages but at the same time it is an issue in the field of cyber security.

AI played a major role in shaping global competitiveness and improving economic and socio-strategic advantages. As the speed of AI advancement and improvement gets supported by advancement in big data and high-performance computing, the United States and China both are racing to get the all-out advantage of this technology and gain maximum benefits. Europe, in the meantime, appears to be lagging behind in this race. Just like other countries, the EU member states are also highly dependent on AI. Once you are dependent on the technology of AI, you have to face the consequences that come with the advantages of AI. All the organizations, banks and companies are using software to run their business or firms; if technology is used anywhere then there are chances of cyber-attacks as well. According to the EU, there are many threats due to adversarial AI, and new methods of systematic attacks and manipulation of data including many other threats will arise. These challenges to privacy and data protection have

[2] Manas Madhukar Patankar, "Artificial Intelligence and its Applications", Master Thesis, (The Pennsylvania State University, 2020).

[3] Woodrow Barfield and Ugo Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing, 2018).

the potential to disrupt the EU in many domains such as economic, technological, political, societal, and security areas.[4]

While there are countless benefits of AI, Adversarial AI first appeared as an anti-hero approach. Hardly a day passes since 2007 when there is no news regarding cybersecurity attacks in the EU. The first cybersecurity attack took place in Estonia by Russia.[5] Keeping these daily bases cyber-attacks in view, the governments understand and realize that this is the important factor to be highlighted and fixed.

Adversarial artificial intelligence

The "Adversarial AI" is the malicious development and misuse of advanced digital technology which has rational/intellectual developments specifically related to human behavior. It includes the ability to learn from data that the machine already possesses. The attackers use adversarial inputs in machine learning models, forcing these machines to make mistakes. These inputs are like visual delusions for machines. ZeroFOX is a cyber-security firm that was asked in 2016 whether human beings were better hackers or machines; it answered in favour of the machines. ZeroFOX used Twitter as a podium to spear-phishing attacks.[6] The results were in favor of the machines as they were much better at making humans click on malicious links.

Recent Studies

The adversarial AI is dangerous because machines can be fooled by the systems. If we look at the below picture and ask the AI system to define it, the AI system will swiftly tell that this is a Hummingbird. However, if we make a minor perturbation in the image which changes the pixel values a little bit then the AI system may reply that this is a hammer. Both pictures

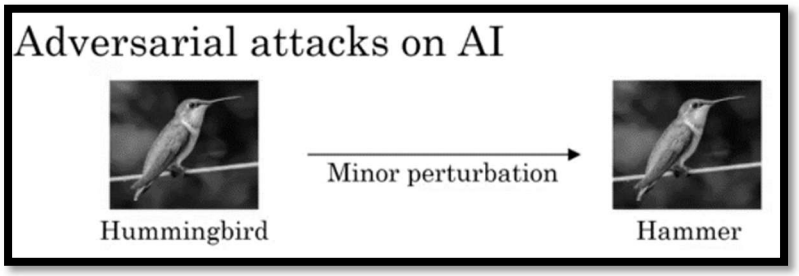
[4] B. Caroline, B. Christian, B. Stephan, B. Luis, D. Giuseppe, et al., "Artificial Intelligence Cybersecurity Challenges; Threat Landscape for Artificial Intelligence", (2020).

[5] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, strategic and organisational changes in cyber security", *International Journal of Cyber Warfare and Terrorism* 1, No.1 (July 2013): 24-34.

[6] Eric Lancaster, Tanmoy Chakraborty, and V. S. Subrahmanian, "MALTP: Parallel Prediction of Malicious Tweets", *IEEE Transactions on Computational Social Systems* 5, no. 4 (2018): 1096-1108. Visit at https://ieeexplore.ieee.org/document/8472279?denied=.

look the same by the human eye but the AI system will immediately tell what it sees in deep learning.[7]

Application of AI and result after minor perturbation



Source: (AI for Everyone 2020)

The researchers at Samsung and the Universities of Washington experimented that making small tweaks to the stop sign could make driverless cars invisible to computer vision algorithms. It could force the machine to speed up the car, which would be extremely dangerous for the public.[8] The most concerning thing about such hostile attacks is that a bad actor needs no information about the attacking model. Luckily, we are not highly dependent on technology at this point. The adversarial AI examples are not just applicable to images (a neural network that processes graphical data). There is research on adverse machine learning on text, audio, and video as well.

In 2018, researchers at UC Barkley controlled the conduct of a computerized discourse acknowledgment framework through an automated speech recognition system with adversarial samples. Just as Amazon uses “Alexa”, Apple “Siri”, and Microsoft has “Cortana” which act as automated speech recognition platforms.[9] For videos, we can take the example of a YouTube

---

[7] Muhammad Shoaib, “AI-Enabled Cyber Weapons and Implications for Cybersecurity", (2020). https://www.semanticscholar.org/paper/AI-Enabled-Cyber-Weapons-and-Implications-for-Shoaib/705c17ce88d1c4d88b14159abd617314afab461e.

[8] Mike Wolterman, “Infrastructure-based collision warning using artificial intelligence." U.S. Patent 7,317,406, issued on January 8, 2008. See https://patents.google.com/patent/US7317406B2/en.

[9] Sean Kennedy, Haipeng Li, Chenggang Wang, Hao Liu, Boyang Wang, and Wenhai Sun, “I can hear your alexa: Voice command fingerprinting on smart home speakers." In *IEEE Conference on Communications and Network Security (CNS*, 2019): 232-240. Visit https://ieeexplore.ieee.org/document/8802686.

song. When the song is played, it would send a voice command to the nearest smart speaker.[10] A human listener would not be able to notice the change. In any case, the smart assistance machines learning algorithm would get that disguised command and proceed to execute it. In 2019, a scientist at IBM Research created an adversarial example with the contribution of Amazon and the University of Texas, which could fool text classifier machine learning algorithms like spam filters and sentiment sensors. Text-based adversarial examples, also known as "paraphrasing attacks", modify the sequences of words in a piece of text to cause a misclassification error in the machine learning algorithms while maintaining coherent meaning to a human reader.[11]

Significance of study

Due to the increase in adversarial AI threats, it has become necessary to delineate how dangerous it could be for people as well as for the sovereign states. The cyber-crimes include malicious use of autonomous weapons, generation, and propagation of fake news, identity theft, and ransomware. This research addresses the adversarial AI threats and how it has affected the EU's cybersecurity policies and what measures the EU can take to reform its policies keeping those threats in view. This study provides a detailed account of the major cybercrimes conducted using adversarial AI in the EU. This research sheds light on the existing AI policies of the EU and highlights its key pillars. Since some recent attacks have exposed shortcomings of the EU's AI policies, this research explores what the EU can learn from the AI policies of the UK and China. These policy templates would ensure great improvements in the EU's policies and help strengthen the security of data.

Threats of adversarial AI

The adversarial AI is playing a malicious role to promote cybercrime, whose amount is increasing rapidly. The threats of adversarial AI are creating problems for people as well as for the governments. The protection of a nation's data is as necessary as the sovereignty of the country. The mishandling of data could have disastrous consequences for all countries. It

[10] Egor Lakomkin, Sven Magg, Cornelius Weber, and Stefan Wermter, "KT-speech-crawler: Automatic dataset construction for speech recognition from YouTube videos", *arXiv preprint* (2019). https://arxiv.org/abs/1903.00216.

[11] Tianyu Du, Shouling Ji, Jinfeng Li, Qinchen Gu, Ting Wang, and Raheem Beyah, "Sirenattack: Generating Adversarial Audio for End-to-End Acoustic Systems", in Proceedings of the *15th ACM Asia Conference on Computer and Communications Security*, (October 2020), 357-369.

may not sound as dangerous as a war but it can shake the pillars of the country if not handled wisely.[12] Adversarial AI threats not only cause economic losses, but also result in immense reputation losses. Below mentioned threats briefly describe how dangerous adversarial AI threats are and how they are damaging countries:

- Autonomous Weapon System
- Fake Media
- Identity Stealing
- Ransomware

Autonomous Weapon System

Autonomous Weapon Systems are also known as self-directed weapons. These weapons are designed in a way that the humans give commands to the machines to hit the target, and from then on, these weapons work on their own.[13] They are like the Air Defence Guns (ADG) which find their target in the sky and kill the target without any prior permission. Human intervention is not required to direct these guns.

On 1 June 2009, an Air France flight was travelling from Rio de Janeiro to Paris having 228 people on board. The plane got crashed into Atlantic Ocean within 4 hours after takeoff. The air speed and frozen wings suggested an incident; the plane got out of control and the pilot was no more able to connect with air traffic controller so he gave the control to the auto-pilot system. After giving control to the auto-pilot system, many errors started occurring and the plane lost its direction. Furthermore, the auto-pilot system was unable to locate the place to land. The auto-pilot system of the plane didn't really work at that time.[14] Poor handling of the auto-plane system gave the French government a lesson that it cannot work in long-term. Also, the French government decided not to give complete autonomy to the weapons or machines. Human control will be involved simultaneously because this technology is still not perfect and can malfunction. Adversarial

[12] Kevin M. Peters, *21st Century Crime: How Malicious Artificial Intelligence will Impact Homeland Security* (California: Naval Postgraduate School Monterey, 2019).

[13] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Routledge, 2016).

[14] Paul Scharre, "Autonomous Weapons and Operational Risk", Ethical Autonomy Project (February 2016), available at https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf?mtime=20160906080515&focal=none.

AI in future can also disrupt the auto pilot systems. Many countries around the world are working on input attack capabilities that manipulate the data fed to systems, signal jamming, and communication hacking technologies, which are AI powered.[15]

Recently, a Chinese graduate student created an autonomous weapon. It was more like a drone, which was capable of finding the target and killing it through inserted bullets. Through machine learning, the drone was able to recognize the specific face/person. After giving the command to the drone, the student took a flight to another country. The drone could complete the given task and destroy itself, leaving no proof left behind of the mastermind of such killing. Such autonomous weapons not only promote the assassination market but also are an issue for the police to find the criminals because facial recognition technology fails to locate the person.

Fake media

In the domain of adversarial AI, fake media is considered to be the most abusive form of AI. It involves AI converting fake audiovisual content into an authentic one. A combination of deep learning and fake media create deep fakes that deceive the audience and lead them to believe that the content is original. While it can be differentiated through machines, the normal public cannot differentiate fake from true media.[16] Because of social media, fake media can reach millions with unprecedented speed.

Fake media can distort reality for evil purposes. For instance, a video of a Malaysian political aide was released having physical relations with a cabinet minister. The video was released in 2019. The cabinet minister was asked to investigate the alleged corruption. It shook the government of Malaysia as well as their cybersecurity directorate.[17]

---

[15] Comiter, Marcus. 2021. "Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It". *Belfer Center for Science and International Affairs*. https://www.belfercenter.org/publication/AttackingAI.

[16] Hussain, Shehzeen, Paarth Neekhara, Malhar Jere, Farinaz Koushanfar, and Julian McAuley. "Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples." In *Proceedings of the IEEE/CVF winter conference on applications of computer vision*, pp. 3348-3357. 2021.

[17] Barari, Soubhik, Christopher Lucas, and Kevin Munger. "Political Deepfake Videos Misinform the Public, But No More than Other Fake Media." *OSF Preprints* 13 (2021).

Like other countries, the EU also has taken steps to tackle all kinds of misinformation, including fake media. In 2018, Brussels issued a strategy to tackle disinformation and deep fakes. The strategy basically scatters guidance among the public. The public must know what the source of information is, how it is produced, and whether it is trust worthy or not.[18] The EU strategy also calls for the creation of an independent European network of fact-checkers to help analyze the sources and processes of content creation.

Identity stealing

Identity stealing means when someone uses your identity and pretends to be you to commit a crime to get financial profits. Your identity includes your full name, date of birth, email address, residential address, login password, passport number, bank account number, security, and driving license number. Once the criminal gets this information, it is easy for him to steal your money or maybe to sell this information on the dark web. (The dark web is also known as the darknet. It is a part of the deep web, which refers to the websites that do not appear on search engines).[19]

All over the world, but specifically in Europe, cyber attackers are taking advantage of the COVID-19 pandemic by sharing the prevention from the virus routines by asking users the symptoms. The users unintentionally reveal their personal information, which is the ultimate target of cyber criminals. The users click on malware links/attachments on their computers that help the attackers to acquire the personal information of a user.

In 2020, Germans lost €10 million. The German government had failed to build a safe and secure website for the distribution of the Corona emergency fund. The cyber criminals created copies of the official website. Many users gave details on those websites, which the cyber criminals then used to collect funds from government on their behalf. In the official records, the

[18] Commission, European. 2021. "Communication - Tackling Online Disinformation: A European Approach". *Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach.

[19] Phua, Clifton, Vincent Lee, Kate Smith, and Ross Gayler. "A comprehensive survey of data mining-based fraud detection research." *arXiv preprint arXiv:1009.6119* (2010).

people of Germany were given the emergency funds. In reality, however, it was all transferred into the coffers of the phishing attackers.[20]

Online ransomware

The cybercrime of online ransomware is rising rapidly. The criminals try their best to collect the information online of not only one person but the whole family, to make it look more authentic. They break into the victim's phone by planting spyware to gather personal details. They wait until the loved ones of the victim share the post on social media. For instance, being on a trip to somewhere. The criminals call them to falsely claim that their loved ones are with them and that they will have to pay such and such an amount to save their lives. Mostly, it happens with those parents whose kid is at school and can't be reached for some reason. However, in reality, nothing happens to the kid. The traumatized parents under a different impression, nevertheless, are willing to pay the money to the criminal to save the life of their child/loved one. To make the call more genuine, the criminals provide the details of the children. Even sometimes the criminals add background crying or screaming noises to make the situation look more real. Their only motive is to get the victim's personal information and collect the money as fast as possible.[21]

In May 2017, numerous companies and organizations were hit by the "wannacry" ransomware that is also known as "wannacrypt", "Wcryp0r", and "WCRY".

Ransomware is a malicious software that is used to hack AI machines until the required amount is paid to the hacker. Ransomware acts as a bacterium in the system. It automatically starts creating problems for a user to access his/her data.[22] The ransomware campaign affected around 150 countries (including the EU). It infected more than 230,000 systems. The attack took place on Friday 12th May 2017.

---

[20] Fontanilla, Marites V. "Cybercrime pandemic." *Eubios Journal of Asian and International Bioethics* 30, no. 4 (2020): 161-165.

[21] Márcio Ricardo Ferreira and Cynthia Kawakami, "Ransomware-Kidnapping Personal Data for Ransom and the Information as Hostage," (2018).

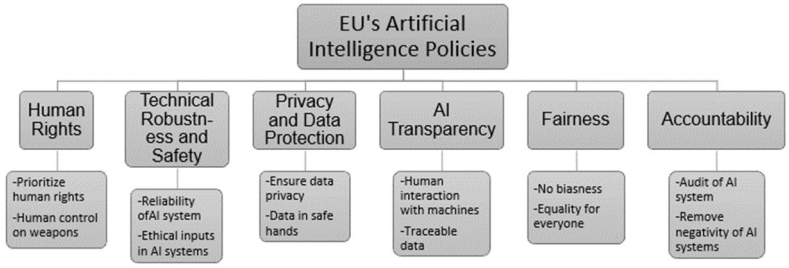
[22] Qian Chen and Robert A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of Wannacry Ransomware," in *16th IEEE International Conference on Machine Learning and Applications*, (2017), 454-460.

Current AI policies of the EU

To secure the development of ethical AI systems, the EU has formulated its AI policies with the aim:

- To improve the economic conditions as well as strengthen the military of member countries.
- To improve the education system, labor market, training systems, changeovers, and adoption of new technologies to improve social protection system.
- To ensure that there should be no biasness and that everyone should get equal benefits of AI development.
- To keep the privacy and security factor in view making an ethical and legal framework and boundaries for both government and private sectors in the process of developing AI in Europe.

An illustration of major pillars of AI policies of the EU



Source: Trustworthy AI in the Age of Pervasive Computing and Big Data (2020)

Human rights

The most prioritized policy of the EU towards AI is that no human right should be overlooked. The policies should be followed keeping human rights in view. Moreover, people should have the basic knowledge to interact with AI machines. They must know their fundamental rights while following the policies of AI. It also includes that the machines will not be able to make the decision solely. Human involvement should be a necessary component.[23] For instance, there should be a control button to abort the procedure or operation.

[23] Koulu, Riikka. "Human Control over Automation: EU Policy and AI Ethics." *European Journal of Legal Studies* 12 (2020): 9.

Technical robustness and safety

Having reliable AI systems and software is another essential policy of the EU. A reliable AI system requires algorithms to be secure, trustworthy, and robust enough to deal with errors or inconsistencies during all life-cycle phases of an AI system.[24] The chief objective of this policy is to ensure cybersecurity against crimes. All types of cyberattacks should be kept in view while developing any algorithm. It should be tested beforehand to avoid any danger or harm. For instance, if the system is causing any harm, its abortive mechanism should be under human control.

Privacy and data protection

In the EU, all the data controls and privacy concerns are linked with the General Data Protection Regulation (GDPR). The major concern of the GDPR is to provide maximum protection to the user's data. The users should also possess complete control over their data. The data should not be in the hand of anyone other than the government.[25] In short, an AI system should be designed in a way that ensures privacy and protection of the data.

AI transparency

According to policymakers of the EU, AI transparency should be explainable. Humans must know why a machine made a particular decision and whether it is beneficial or harmful. AI transparency also means that the data which is used to create an application should be reliable and traceable. Moreover, humans should be able to know that they are interacting with AI systems.[26]

Fairness

AI developers should ensure that the design of algorithms is not biased. Every individual should be treated the same through AI. There should be no biases of caste, color, gender, or culture. The AI system should treat every individual equally, keeping human abilities, skills, and requirements in view. Also, it should ensure the access of AI systems to people with disabilities.

---

[24] Seán Pender, "The creation of an ethical Artificial Intelligence [AI] policy? An exploration into the early days of the European Union's ethical rhetoric in the field of AI." *Public Integrity* 12, no. 4 (2019): 21-27.

[25] Grzegorz Mazurek and Karolina Małagocka, "Perception of Privacy and Data Protection in the Context of the Development of Artificial Intelligence," *Journal of Management Analytics* 6, No. 4 (2019): 344-64.

[26] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Transparent, Explainable, and Accountable AI for Robotics", *Science Robotics* 2, No. 6 (2017). Available at https://www.science.org/doi/10.1126/scirobotics.aan6080.

Accountability

The accountability of an AI system is one of the better policies of the EU with regard to AI. The EU council team conducts internal and external audits of AI systems. The objective of these audits is to assess the negative impact of AI systems so as to know how it is affecting firms and governments in general and human rights in particular. If there is any need for ethical requirements, the team is responsible to make a report to fix it for its betterment.

Adversarial AI and Cybercrimes in the EU

Adversarial AI threats have made cybercrimes quite easy. There are plenty of examples which show how adversarial AI is promoting cybercrime in the EU. The details of those crimes are mentioned below:

Malware

Malware is also known as malicious software. Its branches are viruses, worms, ransomware, etc. It is used to make cyberattacks that can harm the AI system through information/identity theft or service disruption. In 2017, cybercriminals used an extremely delicate technique to misguide users. "Ursnif Trojan" is an app that was used to steal login credentials and access internet banking through malware techniques. The method was to ask users to log in through this app to collect confidential information and make a financial profit.[27] All the while, the actual bank had no idea about these transactions. The developer of the app was arrested and imprisoned. The alarming issue is that the code of "Ursnif" has been leaked and it can also be used by other cybercriminal attackers.

Similarly, when we visit public places, we usually get connected to public Wi-Fi. Some of these connections are unencrypted. They give cyber criminals a chance to access your data, and, if your device is vulnerable handling such malware, it can even give the criminal access to your data.[28] It can result in a financial as well as reputational losses (in case criminals share things with others causing harm to your reputation). Moreover, the criminals use different types of techniques to install malware into another person's device. Malware has the ability to access the device information and store it. It includes viruses, spyware, trojans, and key loggers.

---

[27] Ali Gezer, Gary Warner, Clifford Wilson and Prakash Shrestha, "A Flow-based Approach for Trickbot Banking Trojan Detection", *Computers & Security* 84 (2019): 179-192.

[28] Daojing He, Sammy Chan and Mohsen Guizani, "Mobile Application Security: Malware Threats and Defenses", *IEEE Wireless Communications* 22, No. 1 (2015): 138-144.

Phishing

Cybercriminals send falsified emails or text messages that may look valid and authentic. When the user clicks on such links or text messages it takes them directly to a website not useful for them. Meanwhile, the malicious software takes the data from your personal computer and sends it to the remote computer. This is the most common way cyber criminals use to steal data.[29]

Distributed Denial of Service (DDoS)

Distributed denial of service (DDoS) attack is a spiteful attempt to interrupt the normal traffic of a targeted server. This attack uses multiple systems as the source of attack traffic. It will send numerous requests to the attacked web resource. The aim of sending requests is to increase the capacity of the website to handle the request and this stops the website from functioning properly. In June 2020, a DDoS attack was reported on a reputed European bank. The attack peaked at 809000000 packets per second, which was the largest ever packet volume. This attack was developed in such a way that it overwhelmed the network gear and applications in the target's data center by sending billions of small (29 bytes including IPv4 header) packets. Akamai researchers analyzed that it was the biggest DDoS attack as the attacker used a large number of IP addresses.[30] Almost 600 IP addresses were used per minute. It results in stealing the customer's information as well, as it could be sold on the darknet.

Data breach

Once your data is breached, your personal information/ identity can be at risk. It can either be used to make a financial benefit or it can be sold on the dark web. Data breaching is not difficult in the presence of AI. The data can be stolen or used without the knowledge of the user. The Equifax data breach (a major credit reporting agency) exposed the data of 147 million people in 2017. The company was punished later on with the settlement of up to US$425 million to help people affected by the data breach.[31] This is not

---

[29] Ram Basnet, Srinivas Mukkamala and Andrew H. Sung, "Detection of Phishing Attacks: A Machine Learning Approach", in *Soft Computing Applications in Industry*, (Berlin: Springer, 2008), 373-83.

[30] Kiran Salunke and U. Ragavendran, "Shielding Techniques for Application Layer DDoS Attack in Wireless Networks: A Methodological Review", *Wireless Communications: An International Journal* 120, No.4 (October 2021).

[31] Alvaro Puig, "Equifax Data Breach Settlement: What You Should Know", (2019). Available at https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know.

the whole story. There are many other adversarial AI techniques to steal the user's data to get financial benefits. The EU is seriously concentrated to fix these issues. The EU's Cyber Security Act describes complete guideline to enhance the EU's cybersecurity policies.[32]

Rethinking AI policies of the EU

Cyber-attacks have been consistently happening since 2007. They have compelled the EU to rethink its cybersecurity policies to improve the privacy and security concerns. The attacks mentioned in this paper are adversarial AI attacks that cause economic and reputational damage. Although three major data protection laws are already working for the enhancement of the EU's policies, still, these policies need improvement. The EU needs to rethink its AI policies while learning from China and the UK. China introduced a development plan of new generation artificial intelligence in 2017. The plan aims that AI must be trustworthy and reliable. Keeping adversarial AI threats in view, China took the initiative and created a committee for data protection namely the Ministry of Science and Technology (MOST).[33] China has developed many AI hubs for the follow-up of its policies keeping itself updated with new developments in the field of AI.

The names of these institutes are:

- Beijing Municipal Science Technology Commission
- China National Center for Biotechnology Development
- Chinese Academy of Science and Technology for Development
- Institute of Scientific and Technical Information of China
- National Center for Science and Technology Evaluation
- Shaanxi Science and Technology Department

The collective aim of these organizations is to give maximum protection to the data and to catch malicious AI before any attack. China's policies are one step ahead of the EU. For instance, data information and security are the basic requirement of AI ethical principles. Major Powers like the US, EU, and China have made policies to protect data security and privacy. China enacted the cybersecurity law for the country to protect data and to avoid adversarial

[32] Visit at https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[33] Chunbo Zhang, "The Institutional Framework of the United Nations Development Programme – Ministry of Science and Technology (UNDP - most) Tele-Center Project in Rural China," *Information Technologies & International Development* 4, No. 3 (2008): 39.

AI attacks in 2017. Likewise, the EU developed GDPR in 2018 for the same purpose.

EU Laws to Secure Cyber Systems

Data protection laws	Objective
Network and information system directive (NIS)	The purpose of this directive is to strengthen the security of network and information. It is also known as the NIS directive. The EU Commission issued an act of implementation. It is precisely concerned with digital service providers, security requirements, and reporting of incidents to take action as soon as possible.
European Union Agency for Network and Information (ENISA)	Antedate and support the EU to face upcoming network and information security challenges. Making network and information security the EU's priority policy
General Data Protection Regulation (GDPR)	Support the EU to maintain NIS abilities. Promote and develop the European NIS Community. ENISA assists the capable authorities by lending its representative in the cooperation group

Source: "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." Computer Law & Security Review 2019.

Moreover, the United Kingdom (UK) has incredible AI policies which make it different from other countries. The UK's strategy for AI policies focuses on the development of the economy as well as educational institutes. At the beginning of April 2018, the UK issued its National AI strategy namely, AI Sector Deal (AISD). The strategy was updated in May 2019 for the betterment of the policies. A web portal was developed by the ministerial department for business, which aims to implement the ethical AI policies in sectors such as energy, industrial strategy, sports, media, culture, and human rights. For smooth working, an office was developed by the name of "Office for AI", and AISD is in-charge of that office.

The objective of AISD is to bring about ethical AI development in the fields of economy and society. It provides technology advancement to various sectors for developing AI technologies. The public authority has reserved a

financial plan of £0.95 billion for the execution of the AISD, which is enhanced with £1.7 billion originating from the Industrial Strategy Challenge Fund.[34]

More investment in AI policies is making the UK stronger than other states because AI developments are controlling adversarial AI attacks in the UK. However, the EU's situation is not remarkable in this regard as mentioned above. The rapidly increasing adversarial attacks in the EU are not just damaging the EU's financial condition but also affecting the reputation of the EU globally. China and the UK's policies are worth stating as their AI policies are controlling the adversarial AI attacks efficiently.

General lessons for EU from UK and China's AI policies

AIDP* of China is an interesting learning lesson for the EU with regards to the planning and execution of strategies. China wants to achieve predominance through this strategy by 2030. China's quickly expanding improvements in the field of AI will affect human culture just as they will enhance China's status on the planet. To accelerate the improvement of a creative nation and world's innovation and science power center, this strategy is given due importance for successful implementation. China prominently defined in this plan its place in the next 10 years.

Power ascendency is a desire of every other state. This is heavily motivated by the desire of controlling others that is why the popular phrase of international politics is "politics is a game of power, to gain power and to maintain power".

China's rapid development in the field of AI is making it a regional hegemon. Chinese AI innovation is good enough to be exported overseas. It knows that providing advanced technologies to eager states will make them dependent on China. The more states will rely over Chinese AI, the more pressure they will feel to align with Beijing's strategic interests. China's AI policy includes

---

[34] Vincent Van Roy, *AI Watch - National Strategies on Artificial Intelligence: A European Perspective in 2019*, No. 119974, JRC Report 2020. Available at http://publications.jrc.ec.europa.eu/repository/handle/JRC119974.

* AIDP is China's new generation Artificial Intelligence Development Plan (AIDP). State Council of China issued a plan in 2017 to launch a high level design identifying China's approach to develop new AI applications to cater the needs of the country upto 2030. https://digichina.stanford.edu.

diversity which means that others can also get benefit from the Chinese AI developments especially those country which are economically weak like Zimbabwe.

Moreover, China and the UK do not compromise on their security and sovereignty. London witnessed a horrible attack when on 7 July 2005 56 people were killed. From that day onwards more than 6 million facial recognition cameras were installed in London alone. Likewise, China installed the same facial recognition cameras in the whole of Beijing in 2012, which shows hundred percent coverage 24/7. Beijing is one of the cities with maximum surveillance installed cameras in the region.[35]

The UK as of now has an innovative, rising network protection industry and incredibly skilled researchers. It has a self-supporting channel that has the capabilities to meet public necessities across the board, in general as well as private areas. These capacities make the UK better than different nations and beat dangers to public safety.

Artificial intelligence policies have consistently been an unsettling issue for every state. Initiators of the programme can make boundaries to secure the land, yet, it is difficult to control adverse AI attacks. The EU has many lessons to learn from the UK and China's AI policies to bring about betterment in the field of AI and cyber security.

Conclusion

AI policies have always been a concerning issue for every state. Leaders can make borders to protect the land, but adversarial AI attacks are not easily controllable. This article has highlighted some of the threats posed by adversarial AI. We have also provided a detailed account of the AI policies of the EU and their major aspects. There is little doubt that these policies have not been quite effective in preventing the attacks. Like every other state, the EU has its own AI policies towards adversarial AI, but those policies need rethinking and betterment. It is now clear that the EU needs to rethink its AI policies. Doing so could help it to prevent future data breaches as well as making it capable to swiftly control adversarial AI attacks.

[35] Tanzeela Jameel, Rukhsana Ali, and Shumaila Ali. "Security in Modern Smart Cities: An Information Technology Perspective," in *2nd International Conference on Communication, Computing and Digital Systems* (IEEE, 2019), 293-298.

- B L A N K -