The Effect of GPT Chat on Indonesian and Italian National Security

Seniwati[1], Patrice Lumumba[2], Adi Suryadi Culla[3]
[1]International Relations Department, Hasanuddin University, Indonesia
[2]International Relations Department, Hasanuddin University, Indonesia
[3]International Relations Department, Hasanuddin University, Indonesia

ABSTRACT: The features contained in ChatGPT are centered on providing conversations. One of ChatGPT's capabilities is that it can imitate real-life conversations because its learning is further supervised and uses a perfect language model, so its coverage differs from other smart technologies. ChatGPT has a way of expanding its functions and features, namely with plugins that can provide services to users so that this system can maximize applications. With other plugins, ChatGPT can access and control these third-party services. ChatGPT's biggest weakness is that it sometimes produces text that when read sounds correct but is incorrect information. ChatGPT also does not provide clear references, resulting in copyright problems. Therefore, ChatGPT has been banned by several countries due to copyright issues. The Italian government immediately blocked ChatGPT because there were no special regulations regarding this application. Meanwhile, the Indonesian government has not yet responded to the ChatGPT problem. The two countries have different views regarding ChatGPT, especially regarding national security.

KEYWORDS: ChatGPT, incorrect information, national security, smart technologies, weakness.

I. INTRODUCTION

ChatGPT is a chatbot service developed by a company from the United States, namely OpenAI (Nerdynav, 2023). ChatGPT is designed to help people by providing information and answering questions. This service was recorded as having been used by more than 100 million people in January 2023, making it the fastest application (Romana, 2023). This paragraph explains that ChatGPT is a service created by a company called OpenAI and this service was created to help provide information to people. This service program can reach 100 million users because it has a fast system in the program.

Even though ChatGPT is designed to help and make work easier, this service has many shortcomings that are considered to threaten the security of personal data. The OpenAI company does not show how this service was developed so there is no transparency. Transparency in AI research is important so that people can know the purpose of developing these services (Romana, 2023). This service still has many shortcomings and can threaten the security, especially of someone's data. This service is not transparent in the manufacturing process.

ChatGPT is an important issue nowadays. This service is highly controversial because it can threaten a person's job and spread misinformation and bias. This program uses personal data without the consent of the data owner, which will be very detrimental and dangerous for the data owner (McCallum, 2023). Therefore, this paper is interested in analyzing the positive and negative impacts of the ChatGPT service program. ChatGPT users have spread very quickly because this program is very easy to access by the general public. However, ChatGPT has been detrimental so the use of ChatGPT must be stopped immediately. This research aims to identify the amount of ChatGPT user data globally including the advantages and disadvantages of this service system.

II. THE AMOUNT OF CHATGPT USER

ChatGPT is an AI chatbot launched by Open AI on November 30, 2022. ChatGPT set several records of success as five days after its launch, the service program had more than one million users. Another success, in January 2023, this service program will have 100 million users. Then in March 2023, this program had 1.6 billion users, and 1.8 billion users in April 2023 (Nerdynav, 2023). This paragraph explains that the ChatGPT platform has achieved a record as the platform that quickly reached one million users in five days and also reached 100 million users in January 2023. ChatGPT also had a lot of website visits, namely one billion in February, and continued to increase in March by 1.6 billion and in April there were 1.8 billion visitors.

The Effect of GPT Chat on Indonesian and Italian National Security

Table 1. ChatGPT Overview

Activities	Open AI
Number of users	There are 100 million users (five days after its launch, this service program has reached 1 million users) in January 2023
Daily visitors	25 million
Total Website visitors	Users of this system will reach 619 million in January 2023. Increasing to 1 billion in February 2023, 1.6 billion in March 2023
Training method	Reinforcement learning from human feedback (RLHF)
Model	Fine-tuned GPT-3.5 (text-DaVinci-003)
Knowledgebase	Up to 2021
Dataset Size	300 bn words, 570 GB (crawled web, books, Wikipedia)
Queries per day	10 million (estimate)
Infrastructure	Microsoft Azure
Monthly cost to run	3 million USD (estimate)
Cost to users	Free during research preview, $20 for ChatGPT Plus
Predicted Revenue	USD 200 million by end of 2023, USD 1 billion by end of 2024

Source: (Nerdynav, 2023)

The table above illustrates the advantages that ChatGPT has. This advantage certainly gives Open AL pride as the company that created this service program. ChatGPT users reached 100 million and within five days of launch it reached 1 million users in January 2023. ChatGPT has daily visitors of 25 million. There were 619 million visits to the ChatGPT website in January 2023. These visits jumped to one billion in February 2023 and 1.6 billion in March 2023. ChatGPT uses a reinforcement learning training method of human feedback. This chatbot model is finely tuned GPT-3.5 (text-DaVinci-003). The size of the data set that ChatGPT has is 300 billion words, which contains surfed websites, books, and Wikipedia. It is estimated that queries per day reach 10 million. The infrastructure is Microsoft Azure. The monthly costs for implementing the ChatGPT program are estimated at three million USD. Costs for users are free during the research preview except for ChatGPT Plus which is $20. ChatGPT's revenue at the end of 2023 is estimated at USD 200 million. This income will of course continue to increase so that it is estimated that by the end of 2024, it will reach a profit of USD 1 billion.

Table 2. ChatGPT User Statistics

Platform	Time to first 1 million users
ChatGPT	5 days
Facebook	10 months
Instagram	2 months
Spotify	5 months
Netflix	3.5 years

Source: (Nerdynav, 2023)

Table 2 above explains that ChatGPT is the fastest platform to reach one million users in just five days, beating Instagram which took two months to get 100 users.

III. ADVANTAGES AND WEAKNESSES OF CHATGPT
A. Advantages of ChatGPT
1. Copying human conversation
The core features of ChatGPT center on providing human-like conversations based on user-placed queries or commands. The software features of ChatGPT are similar to the virtual assistant technology owned by Apple, namely the Siri system, and Amazon, namely Alexa. However, based on its capabilities, this feature mimics real-life conversations as it is based on advanced supervised learning and reinforcement learning using language models (Ivankov, 2023). This paragraph illustrates that the features contained in ChatGPT are centered on providing human-like conversations. This program is also found in virtual assistant technology owned by Apple and Amazon. The difference is that ChatGPT's ability to imitate real-life conversations is because the learning is further supervised and uses a language model so its scope is different from other smart technologies.
2. Based on Advanced GPT Model
OpenAl as the ChatGPT development company equips this service with an autoregressive language and linguistic prediction model known as GPT-3. This model is an important system in supporting ChatGPT speed. Then, there is also ChatGPT Plus which has greater sophistication because it is based on GPT-4. This program produces text that resembles people's writing (Ivankov, 2023). The GPT used by ChatGPT is GPT-3 which is an autoregressive language prediction model developed by the OpenAI company. This program is one of the largest non-sparse language models and is considered one of the AI systems that has

ever existed in the world. Chat GPT also has a subscription service, namely ChatGPT Plus which is based on GPT-4 which is even more sophisticated than GPT-3. The use of GPT makes ChatGPT have such a good quality of language that it is produced that it is difficult to differentiate its writing from human writing in general.

3. Application Utilization

This chatbot can write similar output to a commercial AI copywriter. This program has the advantage of creating works of fiction such as short stories. Another advantage is that this program can compose music. This program can also create an outline so it is very useful for writers and content creators. Chatbots can also summarize and explain large amounts of text. The ChatGPT application can also produce texts containing computer programs (Ivankov, 2023). This paragraph explains the benefits generated by ChatGPT.

4.Plugin Availability for Extensions

ChatGPT can expand functions and features through its plugins to produce an application that is integrated with third-party services. Several plugins allow access to up-to-date information and equip ChatGPT with the same functionality as Microsoft's Bing Chat. Chatbots can control and access third party services through their plugins. ChatGPT has advantages in performance, especially in responding because this service has a complete language model. The space contained in this service can be improved through active training and learning. Then, users also provide responses as feedback via voice (Ivankov, 2023).

B. ChatGPT Weaknesses

1.Inaccuracy and Ambiguity

One of the biggest criticisms and limitations of ChatGPT is that it sometimes produces text that sounds reasonable or convincing but is actually untrue or doesn't make sense. This phenomenon is called hallucination and generally occurs in language models. In addition, the information provided is not accompanied by references or quotations. Therefore, using these chatbots for research and electronic tracking purposes is not recommended (Ivankov, 2023).

2. Limited Knowledge of Current Events

Another weakness of this service is that the information source is not updated because it can only provide information before 2022. This service was launched in 2022 so it does not have information data for that year (Ivankov, 2023). This condition illustrates that this service has limited information if it is not updated, so users must be careful when receiving information from this service program

3.Ethical Issues and Concerns

Another weakness of ChatGPT is that this service program has been the target of scrutiny. Some educational institutions have banned its use. Researchers are concerned about copyright infringement because the output is based on human-generated text. This also raises the question of whether it is ethical to use them as a replacement for services that require human interaction such as customer service representatives and therapeutic counseling (Ivankov, 2023). This prohibition on using ChatGPT is due to copyright issues. Researchers are worried about copyright because ChatGPT uses data and information from the internet that is generated by humans.

4. Possibility of Legal Violations

GPT is created from datasets containing copyrighted material from companies, publishers, authors, or researchers. Criminal activities that occur in cyberspace can use AI-based applications. ChatGPT faces legal uncertainty and potential compliance costs (Ivankov, 2023).

IV. THE IMPACT TO NATIONAL SECURITY

According to Hobbes, critical Security Theory states that the safety and security of the people is the highest law. Hobbes then added that one should not understand security simply as survival under any conditions, but as a happy life forever (Booth, 2012). This statement illustrates that people's safety is the highest legal principle that must be prioritized. The importance of security and safety in society. Security is the main foundation for individual well-being and social stability. In his view, security is not only related to physical protection and survival but also involves psychological aspects such as happiness and overall quality of life. Regarding critical security theory, crime can also occur in cyberspace. Next, we will focus more on cybersecurity.

Cyber security is designed to provide protection and security to computer systems and networks from increasingly sophisticated cyber-attacks. This security also consists of technology that has processes and practices that can protect computer programs and data from illegal access that occurs in cyberspace. Security in cyberspace can only be achieved through technological developments, namely through the creation and development of software engineering techniques. One way is to create security systems in online networks, cryptography in cloud computing and the internet, and maintain privacy in computing (Ghundare, Patil, & Lad, 2020). This method can respond to various crimes that occur in cyberspace because it can prevent and detect attacks. The use of cyber security can help prevent cyber-attacks, data breaches, and identity theft and assist in risk management. When an organization has strong network security and an effective incident response plan, it goes a long way in dealing with these issues.

The Effect of GPT Chat on Indonesian and Italian National Security

For example, User Protection in guarding information against data loss or theft while scanning to detect the computer for malicious code (Seemma, Nandhini, & Sowmiya, 2018).

Critical Security Theory provides a detailed framework for understanding the ontological (reality), epistemological (knowledge), and security. This framework includes an understanding of how security is not only related to states and military power but also involves social, economic, political, and environmental aspects. Critical Security Theory encourages critical reflection on the domination, inequality, and injustice that may occur in the development of security policies and voices the need for new alternatives that are more inclusive and just (Booth, 2012). Cyber security theory includes principles, concepts, and frameworks that guide understanding and practice in securing digital systems, networks, and data from cyber threats. Theory involves the study of the motivations, tactics, and techniques used by criminals as well as the development of strategies to defend systems against such attacks. Some key aspects in cyber security theory include confidentiality, integrity, availability, authentication, authorization, risk management, incident response, and defense in security. These principles drive the implementation of measures such as encryption, access control, data classification, detection of data modification or manipulation, and effective risk management. Cyber security theory continues to evolve as threats change and technology develops to meet new challenges and ensure the protection of digital systems and information.

ChatGPT threat to cyber security i.e. ChatGPT is used to write convincing messages and create malicious code; ChatGPT can be asked to write medical advice articles in a doctor's style or create legal documents that appear legitimate (but are not written by lawyers); ChatGPT can also imitate the writing style of famous figures; ChatGPT can generate code that works for crimes, ransomware attacks, and other exploits when given a simple English prompt. This program can be misused by potential hackers through the program information obtained because these hackers can carry out data theft through dark web malware scripts and encryption tools. Experts predict that there will be greater cybercrime by the end of 2023 with the help of ChatGPT (Nerdynav, 2023). This paragraph explains several ChatGPT threats to cyber security are described. ChatGPT has many impacts and threats that will affect the cyber world. Threats can include fraud, impersonation of professionals or famous figures, and hacking.

Technology is developing rapidly and making a big contribution to making human life easier. However, apart from having a positive impact, technology also has a negative impact that can threaten the security of every human being. The chairman of the Italian Data Protection Authority (DPA) took firm action against one of Open AI's products, namely ChatGPT, for serious violations of European law on the processing and protection of personal data (De Angelis et al., 2023). This action is the Italian government's way of dealing with the negative impacts caused by rapid and difficult-to-control technological developments. Technology products that start to conflict with the values and laws of a country deserve to be dealt with firmly. Based on the ChatGPT case which resulted in the blocking of Open AI in Italy, it is hoped that it can maintain cyber security, especially in protecting personal data.

Based on an interview conducted by the BBC with OpenAI said that ChatGPT complies with privacy laws, however, the Data Protection Authority (DPA) stated that there were privacy issues related to the LLMs created by the company (McCallum, 2023). LLMs are artificial intelligence tasked with collecting and studying large amounts of data. LLMs are becoming a product of advanced modern technology. LLMs have very large and numerous amounts of information that are collected and then distributed based on the results of artificial intelligence processing. ChatGPT is a Large Language Models (LLMs) developed by the OpenAI company or an artificial intelligence research and distribution company. LLMs on ChatGPT are developed very sophisticatedly by optimizing dialogue in messages that are very responsive in interacting and conversing like humans. Based on data, since the day ChatGPT was released, it reached one million users in five days (De Angelis et al., 2023). This product was welcomed enthusiastically because it greatly facilitates human work in obtaining information. However, the presence of ChatGPT was then considered very dangerous and raised concerns about security threats.

A mistake that artificial intelligence (AI) may make is the spread of incorrect or biased information. One of the leading figures from the world of technology, Elon Musk, then called for applications using this AI system to be suspended because there were concerns that many parties were competing to develop it out of control (McCallum, 2023). The potential for ChatGPT to have a negative impact is greater than its positive impact, making it a new security issue, especially in cyber security. The concern from big figures in technology about this type of AI system should make countries in the world prepare themselves for more serious cyber threats. Therefore, action is needed from the government and cyber security policymakers to immediately create policies regarding this matter.

Italy has paid increasing attention to cyber security in recent years. Several measures and policies have been implemented to protect the country's information technology infrastructure and its citizens from cyber threats. One of the institutions responsible for cyber security policy in Italy is the Personal Data Protection Authority (*Garante per la protezione dei dati personali*). These authorities have taken strict steps to block ChatGPT. Then, these authorities will investigate ChatGPT's compliance with general data protection regulations. The Personal Data Protection Authority said that there is no legal basis to justify the mass collection and storage of personal data to train the algorithms underlying the operation of the platforms. The app also has no way to verify the user's age and has exposed minors to answers that are completely inappropriate compared to their level of development and awareness (McCallum, 2023). This step taken by *Garante per la protezione dei dati personali* shows that the Italian government is

The Effect of GPT Chat on Indonesian and Italian National Security

aware of the dangers that can be caused by the uncontrolled use of ChatGPT. *Garante per la protezione dei dati personali* has played an important role in regulating the use of personal data preventing possible privacy violations due to cyber-attacks and overseeing privacy policies and personal data protection in Italy.

The Italian government's policy of immediately responding by blocking ChatGPT because there were no specific regulations regarding this application did not make the Indonesian government do the same. The Indonesian government has not yet responded to this matter. According to experts from the Center for Indonesian Policy Studies (CIPS), the use of ChatGPT does not need to be officially regulated by the government or at the national level. CIPS experts also stated that restrictions could be carried out in two ways, first, restrictions on the use of technology, and second, restrictions on each sector (Alamsyah, 2023). CIPS expert Ajisatria said that there is already quite a lot of use of artificial intelligence in various fields, for example, biometric technology for facial recognition. Technology such as biometrics for facial recognition can be used in several sectors, one of which is law enforcement. However, if it is used for surveillance purposes, the advice given is that its use is limited or prohibited. Regarding personal data protection policies, the Indonesian government has created the Personal Data Protection Law (UU PDP). However, regarding the use of Chat GPT, especially in the education sector, Ajisatria said that regulations in this sector can still be explained or regulated further regarding activities or programs that are permitted and not permitted so that later they can be regulated at the national level or a policy can be created (Alamsyah, 2023). Based on the response issued by the Center for Indonesian Policy Studies (CIPS), the policy regarding the use of ChatGPT in Indonesia, which has not yet been regulated, means that this application will not be blocked soon. In contrast to the Italian government, Indonesia sees positive impacts as more dominant than negative impacts as feared by the Italian government.

V. CONCLUSIONS

ChatGPT still has many shortcomings that can threaten security. ChatGPT still has the potential to spread misinformation, has the potential to spread pornography, and other negative content that can damage people's morals and mental health, still lacks control over the use of user data so that personal data can leak, and this service can also be used by irresponsible parties to carrying out cyber-attacks and violating national security. Meanwhile, the Italian and Indonesian governments have different policies regarding ChatGPT. The Italian government views this service program as a threat to the country, so it requires the protection of digital systems and information by issuing an operational ban on ChatGPT. Meanwhile, the Indonesian government does not see that this service program will have an impact on social, economic, political, and environmental aspects, so the Indonesian government has not issued a ban on the use of this service.

REFERENCES

1) Alamsyah, I. E. (2023). CIPS: Pemerintah Tak Perlu Meregulasi Penggunaan Chat GPT (CIPS: The government does not need to regulate the use of GPT chat). Retrieved 5 November 2023, from
https://news.republika.co.id/berita/rs28oq349/cips-pemerintah-tak-perlu-meregulasi-penggunaan-chat-gpt

2) Booth, K. (2012). *Theory of World Security* (First). London, UK: Cambridge University Press.
https://doi.org/https://doi.org/10.1017/CBO9780511840210

3) De Angelis, L., Baglivo, F., Arzilli, G., Privitera, G. P., Ferragina, P., Tozzi, A. E., & Rizzo, C. (2023). ChatGPT and The Rise of Large Language Models : The New AI-Driven Infodemic Threat in Public Health. *Frontiers*, (April), 1–8. https://doi.org/10.3389/fpubh.2023.1166120

4) Ghundare, S., Patil, A., & Lad, R. (2020). Importance of cyber security. *International Journal of Engineering Research & Technology (IJERT)*, *8*(05), 1–3. Retrieved from https://www.ijert.org/research/importance-of-cyber-security-IJERTCONV8IS05036.pdf

5) Ivankov, A. (2023). Advantages and Disadvantages of ChatGPT. Retrieved 1 November 2023, from
https://www.profolus.com/topics/advantages-and-disadvantages-of-chatgpt/

6) McCallum, S. (2023). ChatGPT banned in Italy over privacy concerns. Retrieved 3 June 2023, from
https://www.bbc.com/news/technology-65139406

7) Nerdynav. (2023). 107 Up-to-Date ChatGPT Statistics & User Numbers. Retrieved 12 November 2023, from
https://nerdynav.com/chatgpt-statistics/

8) Romana, F. (2023). Risiko Keamanan Data, Italia Larang ChatGPT (Data Security Risk, Italy Bans ChatGPT). Retrieved 2 November 2023, from https://www.kompas.id/baca/internasional/2023/04/01/risiko-keamanan-data-italia-larang-chatgpt

9) Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering (Ijarcce)*, *7*(11), 125–128. https://doi.org/10.17148/ijarcce.2018.71127