Reichman University

International Institute for Counter-Terrorism (ICT)

With the Support of the Jusidman Foundation

Is the Chatbot a Threat or an Opportunity for Security Organizations?

Colonel (Ret.) Gadi Eshed

June 2023

About the ICT

The International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world. Using a multidisciplinary arpproach, the ICT work to facilitate international cooperation in the global struggle against terrorism.

As an independent think-do-tank, the ICT focuses on themes realted terrorism, counter-terrorism, homeland security, threat vulnerability, risk assessment, intelligence analysis, national security, and defense policy.

Serving as a joint forum for international policymakers and scholars, the ICT draws upon the experiences of a comprehensive and international network of individuals and organizations with unique expertise on terrorism and counter-terrorism research, public policy analysis and education

In addition to publishing research papers, situation reports and academic publications for worldwide distribution, the ICT hosts a number of international seminars, workshops and conferences to discuss and educate followers on global and regional issues of security, defense, and public policy in order to better facilitate the exchange of perspectives, information and proposals for policy action.

Licensing & Distribution

Reichman University International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

ict.org.il
International Institute for Counter-Terrorism, (2023)

Is the Chatbot a Threat or an Opportunity for Security Organizations?

Colonel (Ret.) Gadi Eshed

Abstract

The article explores the benefits, challenges, and potential impact of ChatGPT, an advanced chatbot powered by artificial intelligence. It appears that at this stage, it can be said that large language models (LLMs) and artificial intelligence (AI) models like ChatGPT have achieved a dramatic technological breakthrough in the field of technology. These unique capabilities have the potential to enhance productivity across a wide range of functions.

The article emphasizes the transformative potential of ChatGPT4 in the realm of army, security organizations and police departments. It discusses how this technology can revolutionize operations and leading to enhanced efficiency. The article also notes the increasing investment in artificial intelligence by security agencies, highlighting its critical role in national security.

While acknowledging the enthusiasm surrounding ChatGPT, the article presents also a skeptical perspective by highlighting concerns raised by experts. These include the generation of false information, social biases, and the limitations of the chatbot's lack of contextual understanding and subjectivity. Critics argue that despite its groundbreaking nature, ChatGPT represents a development achievement rather than a revolutionary turning point.

The article addresses the potential risks associated with malicious exploitation of ChatGPT, including the dissemination of disinformation and its impact on electoral systems. It warns about the strategic threats posed to the integrity of elections and the potential for criminal or ideological actors to develop more dangerous innovations using this technology.

However, the article concludes by suggesting that if the reported issues are addressed, ChatGPT can be a valuable tool for the intelligence community and security organizations. It emphasizes the offensive and defensive potential of generative AI and ChatGPT, indicating that organizations failing to adopt and develop these technologies may become irrelevant.

Keywords: Artificial Intelligence (AI); Large Language Models (LLM); Disinformation

Received: 20 June 2023 ■ Accepted: 22 June 2023.

Table of Contents

Introduction

Artificial intelligence (AI) is swiftly becoming an inseparable part of various work processes in the modern era. Tasks that once necessitated the allocation of human resources for extended durations can now be executed within minutes. The applications and advancements of AI are continuously expanding, encompassing a wide array of domains. Artificial intelligence presents remarkable uses and notable advantages. It revolutionizes areas such as self-driving cars, task automation, improved decision-making processes, and the deployment of virtual personal assistants (such as Siri and Alexa) to enhance customer service experiences. Furthermore, AI contributes to the enhancement of cybersecurity systems, enabling the detection of anomalies or patterns indicative of potential threats or attempted attacks. Its capabilities extend to diverse domains, including medical data analysis and recommendations, language translation services, predictive equipment maintenance scheduling, data analysis, and more.

Within the realm of AI, military applications play a crucial and significant role, offering substantial potential to bolster military operations.[1] Certain AI systems are proficient in executing complex tasks with minimal human intervention. Their capabilities encompass data processing, combat simulations, support for combat system operations, decision-making processes, data and research analysis, target identification, threat monitoring, cybersecurity, and beyond.

The field of artificial intelligence encompasses three primary technological channels: machine learning (ML), deep learning, and natural language processing (NLP). NLP particularly focuses on the machine's ability to comprehend human language and speech. These technologies find practical implementation in various contexts, such as advanced search engines, recommendation algorithms, digital assistants, automated spelling and grammar correction, chatbots, and more.

The article explores the realm of artificial intelligence, which, while making significant contributions, also brings forth potential risks and threats. A specific focus is given to the impact of ChatGPT, the chatbot, delving into its advantages and drawbacks. The ramifications of artificial intelligence on security, military operations, criminal activities, and terrorism are thoroughly examined and analyzed.

Unveiling the Dark Side of Artificial Intelligence

As we delve into the realm of artificial intelligence, it becomes apparent that its benefits coexist with certain concerns and potential dangers.[2] One such concern revolves around the issue of bias. Since algorithms are crafted by human hands, they inherently carry the biases intentionally or unintentionally infused by the developers themselves. Whether these biases are embedded during the development process or originate from the biased training data, the inevitable outcome is the propagation of biased results.

[1] "The Most Useful Military Applications of AI in 2023 and Beyond" Sentient Digital, January 2023

[2] Bernard Marr"What Are the Negative Impacts of Artificial Intelligence (AI)?" B. M 2021

As the widespread adoption of artificial intelligence continues, the rise of automation amplifies the risks of job displacement, thus contributing to social and economic disparities. This trajectory paves the way for societal inequality to prevail. Furthermore, the rapid advancement of AI technologies raises crucial questions regarding privacy infringement, as it entails extensive user monitoring and access to their personal information. Additionally, the proliferation of misinformation and disinformation is an area that demands thorough exploration and examination below.[3]

As early as 2018, reports emerged on the exploitation of artificial intelligence for social manipulation, highlighting it as one of its major threats. In an era where politicians rely on technological platforms to promote themselves, examples such as Ferdinand Marcos Jr.'s utilization of TikTok's AI algorithm-powered troll army to influence the 2022 elections underscore the potential ramifications.[4]

Ferdinand Marcos Jr., with an impressive 29.9 million votes, achieved a resounding victory in the Philippine presidential elections. Employing sophisticated campaign strategies, Marcos strategically avoided mainstream media exposure and instead leveraged influencer networks and bloggers, harnessing TikTok's platform for the dissemination of disinformation aimed primarily at the youth demographic, employing a well-crafted social media campaign. The National Union of People's Lawyers in the Philippines expressed genuine concern, stating, "Fact can indeed be stranger than fiction. Or, more accurately, fiction can be repackaged as fact".[5]

Another striking example of the malicious exploitation of artificial intelligence lies in the hands of terrorist organizations that have already amassed a historical record of technological adoption. As part of their modus operandi, they have started employing Unmanned Aerial Vehicles (UAVs), commonly known as drones, equipped with autonomous flight control and artificial intelligence (AI) capabilities. These technologies provide them with offensive capabilities, allowing relatively efficient engagement with security and defense challenges.

The United Nations Security Council's Counter-Terrorism Committee warned that Unmanned Aerial Systems (UAS) are identified as one of the primary terrorist threats.[6] The report establishes that governments worldwide will need to grapple with significant security challenges arising from the use of these systems by terrorist organizations. The threat intensifies with the possibility of arming UAVs.

Non-state actors, including Hamas, Hezbollah, Boko Haram, and ISIS, have already

[3] "Negative effects of Artificial Intelligence", October 3, 2022, https://masaar.net/en/negative-effects-of-artificial-intelligence/

[4] Mike Thomas" 8 Risks and Dangers of Artificial Intelligence to Know" Build in, Jan 25, 2023

[5] Karen Lema "Philippines election winner Marcos tells world to judge him by actions, not family's past", Reuters, May 10, 2022

[6] Christina Schori Liang," Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies", Geneva Centre for Security Policy, 15 March 2023

utilized drones, which have the potential to carry chemical, biological, and radiological materials. As an illustrative example, in 2015, a drone armed with a radioactive substance targeted the office of the Japanese Prime Minister.

The UAVs have emerged as potent tools for terrorists and criminal organizations, enabling them to carry out targeted assassinations and attacks. This mode of operation is predominantly employed by state-sponsored actors. Notable instances include the unsuccessful assassination attempt on the President of Venezuela, Nicolás Maduro, in August 2018, and a similar assassination attempt on the Prime Minister of Iraq, Mustafa al-Kadhimi, in 2021.

Louisiana State University published an article on the construction of a radio-controlled GPS-guided UAV, capable of carrying payloads weighing up to 4.5 kilograms for a duration of 10 minutes, with a cost of less than $2,000. Additionally, online instructions on 3D printing small-scale aerial platforms facilitate the production of low-cost UAVs, requiring the procurement of engines and computer components. The ease and affordability of these manufacturing processes make them ideal systems for low-cost terror attacks.

Open-source software allows for the enhancement of UAV capabilities, eliminating the need for GPS guidance or radio control through alternative control mechanisms such as inertial systems that track surface orientation or equations-based navigation. These opportunities create dangerous avenues for exploitation by terrorist organizations and criminal elements.[7]

In 2016, ISIS executed its first successful UAV attack in northern Iraq, further solidifying its reputation as an organization adept at leveraging sophisticated technologies. A year later, it announced the establishment of its "Unmanned Aircraft of the Mujahideen". The threat lies in the potential of AI-powered UAVs transforming into deadly autonomous killing machines. The deployment of such UAVs by terrorists holds the alarming prospect of enabling large-scale and highly perilous acts of mass destruction.

The utilization of UAVs as tools of terror presents a significant challenge to global security. Terrorists can exploit AI systems, which are commercially available, in several ways. For example, they can utilize autonomous vehicles to transport explosives and carry out attacks, ensuring that the perpetrators remain distant from the targets both temporally and geographically. Concerning the deadly autonomous weapon, it has been referred to as the "third revolution in warfare," following the advent of gunpowder and nuclear weapons.[8]

A survey conducted by the UN Counter-Terrorism Centre (UNCCT) among 27 experts representing governments, industry, academia, and international and regional organizations

[7] Thomas G. Pledger "The Role of Drones in Future Terrorist Attacks" THE ASSOCIATION OF THE UNITED STATES ARMY, LAND WARFARE PAPER 137 / FEBRUARY 2021

[8] Jacob Ware "Terrorist Groups, Artificial Intelligence, and Killer Drones" Special Series - AI and National Security, WAR ON THE ROCKS, September 24, 2019

yielded worrisome findings. 44% considered the malicious use of AI for terrorist purposes as "very likely," while 56% deemed it "somewhat likely." None of the respondents claimed that the malicious use of AI was "unlikely."[9] The experts identified four significant factors contributing to the potential malevolent exploitation of AI for terrorist purposes.

Democratization" of new technologies: The "democratization" of new technologies, such as AI, has significantly reduced barriers to entry for malicious actors. This concept refers to the transformation of previously exclusive technologies, accessible only to a limited community with unique resources and expertise, into widely available tools that can be utilized with minimal investment or technical background.

In this era, most popular algorithms are open-source and do not require high levels of expertise. The democratization of technology serves as a catalyst for development, but it also expands the risk of malicious use. These capabilities can be exploited by negative actors through external market manipulation, functioning as a criminal business model within a digital underground economy involving a variety of cybercrime commercial services.

AI Scalability: Generally, scalability refers to the ability to scale up the utilization of a technology. Given the potential for widespread adoption of artificial intelligence, defense systems against malicious use of AI need to adapt to the increasing volume and intensity of attacks. An example of this is the threat posed by remotely operated and autonomously flying UAV attacks.

The Inherent Asymmetry in the Fight Against Terrorism: The asymmetry in the challenges posed by terrorism lies in the fact that counterterrorism entities, when adopting AI tools, grapple with the legislative challenges while navigating between security needs, human rights, and freedoms, whereas terrorist actors are exempt from such dilemmas and would eagerly adopt and exploit any development or means to further their ideologies.

Societal Dependency on Data and Technology: Society is becoming increasingly reliant on the completeness and availability of the internet and the credibility of data for its ongoing functioning. Artificial intelligence is integrated into daily life through smart devices and smart cities, including critical infrastructures such as healthcare providers, energy suppliers, and biological and nuclear facilities. While enjoying tremendous advantages, all of these entities are equally exposed to cyber-attacks and severe threats that can disrupt daily life.

It is important to reiterate that artificial intelligence contributes immensely to modern life, but we cannot ignore the existence of certain threats, one of which is referred to as "black box algorithms". Since one of the goals of artificial intelligence systems is sometimes to make predictions, highly complex algorithms are required. The problem is that often even their creators cannot explain how the integrated variables lead to the

[9] "ALGORITHMS AND TERRORISM" United Nations Interregional Crime and Justice Research Institute (UNICRI), 2021

obtained prediction. Due to this lack of transparency, some algorithms are referred to as "black box".[10]

When the danger of lack of transparency merges with the complex task of combating disinformation dissemination, addressing these threats becomes increasingly arduous. With the emergence of deep learning-based systems like Chat GPT, which utilize advanced algorithms and models, impressive technological advancements are accompanied by the threat arising from the lack of transparency, commonly referred to as the "black box" of artificial intelligence.

The Rise of Chatbots

As previously mentioned, we live in an era where artificial intelligence technology has infiltrated various domains of our daily lives. The recent interactive breakthrough came with the introduction of chatbots, particularly ChatGPT, an automated chat based on artificial intelligence developed by OpenAI. It was first released on November 30, 2022, and is designed to facilitate conversational interactions.

A chatbot is computer software that simulates human conversation to assist in communication using artificial intelligence. The software generates responses similar to human replies through voice commands or text-based messaging services.

The application has rapidly gained popularity. Within five days of its launch, it reached one million users. By December 2022, it expanded to 57 million users, and by January 2023, it reached 100 million users. The app's development has garnered immense popularity due to its ability to provide complex answers quickly, applicable to a wide range of topics.

The application enables users to ask questions, perform tasks such as writing articles, emails, essays, poems, or writing and checking code in various programming languages. The app's capabilities significantly enhance software development speed and innovation, which have already been adopted by businesses and organizations worldwide.[11] However, in totalitarian countries such as Russia, China, Syria, Cuba, Iran, and North Korea, where the use of powerful and open informational tools is restricted, the application is blocked as part of internet censorship.[12]

The tool relies on an impressive data system comprising over 175 billion machine learning parameters. For comparison, the previously largest trained language model, Microsoft's Turing Natural Language Generation (NLG), had merely 10 billion parameters.[13] Leveraging deep learning algorithms, the application can identify, summarize, translate, visualize, and generate text and other content based on acquired

[10] Philip McKeown "What Are the Risks of Artificial Intelligence"? Audit Board. April 28, 2021

[11] "ChatGPT: Unlocking the Potential of Large Language Models" CREDIT SUISSE, 2023, pp.4-5.

[12] Divya Bhati" Viral AI chatbot ChatGPT is banned in many countries, but why? Full list of countries" India today, Apr 5, 2023

[13] Ben Lutkevich, Ronald Schmelzer, " GPT-3", TechTarget, March 2023

knowledge from vast data systems. The system has the ability to comprehend a wide range of disciplines, create text-based graphics, and even enable users to engage in "human-like" conversations, as it can identify patterns and generate new outputs based on its understanding.

In an attempt to showcase its relevance and technological innovation, the US Pentagon, for instance, utilized ChatGPT on February 8, 2023, to draft a press release about the establishment of Task Force 39 for dealing with drones, with the emphasis that [14] "the article that follows was generated by OpenAI's ChatGPT. The use of AI to generate this story emphasizes U.S. Army Central's commitment to using emerging technologies and innovation in a challenging and ever-changing operational environment. The team is focused on countering the threat of small Unmanned Aerial Systems and developing innovative solutions to other security challenges".

The Dilemma

ChatGPT provides numerous benefits and opportunities for the general public, businesses, research institutions, and various organizations, including security agencies. The ongoing and evolving dilemma revolves around the assessment of the advantages and drawbacks of this technological development. To address these concerns, the research laboratory OpenAI has implemented protective mechanisms in an attempt to mitigate potential harmful uses. These mechanisms include data encryption, permission verification, access control, and the utilization of machine learning algorithms to identify and prevent negative activities. The system also incorporates inherent defense measures against malicious bots, making it seemingly difficult for malicious actors to exploit the system for inappropriate purposes. Nevertheless, these measures can still be circumvented, thus presenting a potential risk of exploitation for nefarious individuals and entities, including terrorist organizations.[15]

The technological breakthrough poses a new challenge for security authorities and law enforcement. While the information sources used by ChatGPT may be freely available on the internet, the ability to utilize the model itself for complex queries and tasks means that malicious actors find it considerably easier to understand, penetrate, exploit, and commit various types of crimes. These crimes include identifying potential attack targets, disseminating disinformation, and cybercrimes. The primary concern is that ChatGPT lowers the entry barrier for malicious actors.

ChatGPT is one of several natural language processing and artificial intelligence (AI) tools available to the public. Shortly after its launch in November 2022, cybercriminals on dark web forums began showing great interest in exploiting it for the creation of

[14] DoD's Defense Visual Information Distribution Service (DVIDS), U.S. Army Central Prioritizes Innovation with Task Force 39 https://www.dvidshub.net/search?q=counter-drone+task+force&view=grid

[15] Whitney Chavez" Understanding How ChatGPT is Changing Law Enforcement" Homeland Security Digital Library at NPS, Mar 29, 2023

malicious software, learning, and exploiting cyber vulnerabilities and weaknesses. This implies a dangerous potential where individuals with limited technical knowledge and without advanced coding skills can develop malicious tools using real-time examples and guidance.

Alongside its advantages, there are also risks associated not necessarily with what the program outputs, but rather with what users input into it. It has been revealed that users sometimes share data with ChatGPT as part of their conversation with the system, in order to refine and clarify their queries. While this data contributes to the improvement of the program's artificial intelligence, it is primarily public. In fact, the shared data, including sensitive information, is not restricted and may be shared with other service consumers according to OpenAI's data usage policies.

A study conducted by the cybersecurity company Cyberhaven, analyzing 1.6 million employees using ChatGPT, uncovered concerning data. It was found that 6.5% of them exposed company data in ChatGPT, and 3.1% copied and pasted sensitive data into the program. For instance, two software developers of Samsung's Korea-based semiconductor business plugged lines of confidential code into ChatGPT and requested the AI to check for any issues and make corrections.[16]

In the new era, traditional cybersecurity solutions cannot prevent users from pasting sensitive text into the ChatGPT browser, which poses a problem for organizations as it hinders their ability to assess the extent of potential problems and damages.

In response to these potential threats, companies such as JP Morgan, a multinational banking corporation considered the largest bank in the United States, decided to restrict their employees' usage of ChatGPT due to concerns about jeopardizing their information security and protection.[17]

JP Morgan is not the only company that prohibited the use of the tool. Amazon also took a similar step, along with the telecommunications company Verizon, the consulting firm Accenture,[18] as well as several Wall Street companies such as Bank of America and Goldman Sachs Group.[19]

In addition to these major corporations taking precautionary measures, Italy became the first Western country in March 2023 to ban the use of the application due to concerns about its negative potential. The local regulator pointed out a data breach in OpenAI that allowed the exposure of chat headlines between users and the chatbot. The regulator emphasized that the system lacks a legal backup for the collection and processing of personal data, leaving the algorithms to perform their tasks without clear regulations.

[16] Susan Miller "ChatGPT's other risk: Oversharing confidential data" Government Computer News, April 20, 2023

[17] Adlan Chaykin," How ChatGPT is lowering the entry barrier to cybercrime" Control Risks, Analysis, 09 Mar 2023

[18] Ben Wodecki" JPMorgan Joins Other Companies in Banning ChatGPT", AI Business
February 24, 2023

[19] Jo Constantz " Nearly Half of Firms Are Drafting Policies on ChatGPT Use", Bloomberg, 20.03 .2023

The regulator also highlighted the problematic nature of the system, such as the absence of age restrictions and the chatbot's ability to provide inaccurate information, thereby disseminating misinformation. The Italian response highlighted a broader problem of lacking concrete regulations in the field, as it occurred while European Union member states were in the midst of an effort to develop rules and regulations for artificial intelligence.[20]

After a few weeks, Italy decided to remove the restrictions on ChatGPT, following the lead of other countries, while still maintaining certain regulatory requirements. However, the core issue remains, as there is a lack of acknowledgment that chat outputs do not provide links and transparency regarding their sources.[21] The company's response primarily involved adding information to its website about data collection and usage for algorithm training, creating a new form for users in European Union countries to opt-out of using their data for training, and incorporating age verification tools during registration.

According to a report by NordVPN, a provider of virtual private network (VPN) services, on March 14, 2023, the volume of posts related to ChatGPT in dark web forums increased by 145% from January 13 to February 13. A few of these posts delved into the sophisticated natural language processing (NLP) abilities of the chatbot, employed for spear-phishing campaigns or the crafting of social engineering methods. These techniques possess the potential to dupe even security personnel and manipulate unsuspecting employees, thereby revealing confidential data, infiltrating harmful software, and executing other malicious activities by generating text and voice exchanges that convincingly emulate human interactions.

Marijus Briedis, a cybersecurity expert at NordVPN, argued that for cybercriminals, revolutionary artificial intelligence and ChatGPT can fill the missing piece in their criminal puzzle. He pointed out the potential for unauthorized access to organizational information through the chatbot, which could lead to data theft, identity theft, fraud, and other malicious activities.

The potential distribution of malicious software and viruses can also enable data theft by bypassing authentication and authorization systems. This is primarily achieved through social engineering, a process that involves manipulating the target object to click on a malicious link or download malicious software via email, text messages, or online chats. Such a process usually takes considerable time for attackers. However, clever exploitation of the advantages of bots provides them with a tool to perform these tasks in a faster and more efficient manner.[22]

[20] Ryan Browne "Italy became the first Western country to ban ChatGPT. Here's what other countries are doing", CNBC, Apr 4, 2023

[21] Kelvin Chan "ChatGPT is back in Italy after OpenAI met regulators' privacy demands before a big deadline" Fortune, April 28, 2023

[22] David Rame "Hacking ChatGPT: 'The Dark Web's Hottest Topic" Virtualization, 03/14/2023

In response to the dilemmas accompanying the new era, Vice President of the United States, Kamala Harris, addressed the topic of technological advancements, emphasizing that alongside opportunities, they also present risks, and creative artificial intelligence is no exception. She highlighted that AI is one of the most powerful technologies of our time, with the potential to improve people's lives while tackling some of the greatest social challenges. However, it also has the potential to significantly increase security threats, compromise privacy and civil rights, and undermine public trust in democracy.[23]

Against the backdrop of these concerns, a meeting took place at the White House on May 4, 2023, with the objective "to share concerns about the risks associated with AI." It was attended by the Vice President and CEOs from leading companies such as Anthropic, OpenAI, Microsoft, and Alphabet (Google).[24] Additionally, nine high-ranking government officials, including Jacob "Jake" Sullivan, the National Security Advisor, participated in the session. At a certain point, President Biden also joined them to emphasize, as stated in the press release, that companies have a fundamental responsibility to ensure the safety and security of their products before they are released to the public.

During the meeting, three main areas were discussed: the need for companies to be more transparent with policymakers, the public, and others regarding their AI systems; the importance of assessing, verifying, and ensuring the safety, security, and efficiency of AI systems; and the need to protect AI systems from attacks and malicious actors.

The Security Aspect

It appears that at this stage, it can be said that large language models (LLMs) and artificial intelligence (AI) models like ChatGPT have achieved a dramatic technological breakthrough in the field of technology. These unique capabilities have the potential to enhance productivity across a wide range of functions. In a study conducted by two doctoral candidates at MIT, 444 employees were required to perform tasks related to marketing copywriting, grant analysis, data analysis, and human resource findings. They were divided into two groups, one using ChatGPT and the other using conventional tools. After 20-30 minutes of work, their output was evaluated by professional editors in the field. The speed and quality of the products they produced were examined. The contribution of ChatGPT was assessed, whether it served as an effective substitute or disrupted the workflow. The results were impressive. The group that used the application completed tasks 37% faster (17 minutes compared to 27 minutes) and achieved similar quality scores as the second group. As the employees repeated their tasks to improve the quality of their output, the ChatGPT group continued to show significant improvement.[25]

[23] "Statement from Vice President Harris after Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation" The White House. May 04, 2023

[24] "Readout of White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation""The White House. May 04, 2023

[25] josh Bersin" New MIT Research Shows Spectacular Increase in White Collar Productivity from ChatGPT", Insights on Corporate Talent, Learning, and HR Technology, March 7, 2023

The question arises whether intelligence and security organizations can also benefit from this level of productivity. How can these technological solutions, for example, develop arguments? This is a complex and significant area involving a comprehensive review of vast amounts of information to build a response. Dr. J. Keith Dunbar conducted experiments on these issues and asked ChatGPT to review China's space capabilities over the past 10 years, based on the assessment of threats by the Office of the Director for National Intelligence of the US, involving hypothesis, counterarguments, supporting evidence, and assumptions. ChatGPT provided a detailed response within 10 seconds, including the option for a graphical representation of the argument. The application also identified the need for additional data collection to turn assumptions into evidence.[26]

As an illustrative example, in the chapter on foundational assumptions, it is determined that China's space capabilities are part of a broader effort to challenge US military dominance and exert greater influence in global affairs. China may be willing to use its space capabilities to achieve strategic goals, even if doing so risks conflict with the US and its allies. Assessments over the past 10 years suggest that China's space capabilities have rapidly advanced and could pose a significant threat to US national security. While the full extent of this threat remains uncertain, it is clear that the US must take steps to monitor and mitigate potential risks posed by China's space program.

When examining the product in several dimensions, such as structure, logic, clarity, and recommendations received within seconds, it can be seen that there is significant potential. The problem that existed and remains alongside the impressive findings is that the product does not reflect important data, both for academic purposes and, of course, for intelligence and security purposes. It is necessary to transparently disclose the sources on which it is based. In fact, without this disclosure, the reliability of the product cannot be determined. This may, at least at this stage, deter the deepening use of these factors. It appears that, at least for security entities, part of the solution may involve reliance on closed databases.

The Military Aspect

In addition to the aspects explored in the intelligence research field, ChatGPT has potential, mainly in the future, to fulfill a role in a wide range of military applications by leveraging its advanced language processing capabilities. [27] This includes the ability to develop techniques and algorithms for analyzing intelligence material, fusion, and management of large volumes of data. It can also perform terrain analysis, extracting topographic information, analyzing images or other types of data, and identifying details such as height, slope, and obstacles for detailed topographic mapping. It can locate information about potential targets, such as their size, shape, location, and movements.

ChatGPT may assist in creating investigative reports and summaries, automated target identification, robotics, system testing, modeling and simulations of virtual and augmented

[26] J. Keith Dunbar " ChatGPT: Friend or Foe to the Intelligence Community", FEDLEARN, April 3, 2023

[27] Som Biswas "Prospective Role of Chat GPT in the Military: According to ChatGPT" Qeios, Feb 27, 2023

reality, simulations of various types of combat, and the development of materials with simulations to enhance realism and the challenges of training, as well as military records tracking and logistics. These tools also have the potential to be used offensively against enemy artificial intelligence systems. They can be applied to autonomous vehicles and weapon systems, network security and communication, autonomous flight control of drones, aircraft, and more.

When the system overcomes its limitations, the GPT (Generative Pre-trained Transformer) AI could completely transform the geopolitics of the battlefield. For example, there is an expected significant expansion of AI-guided military operations. The Pentagon is already experimenting with AI robots for flying F-16 fighter jets, Russia is testing autonomous tank-like vehicles, and China is deploying its own AI systems. According to retired U.S. Air Force Gen. Charles Wald, AI-driven programs can reduce the decision-making window from hours or days to merely minutes. On the other hand, decision-makers may become dependent on strategic and tactical assessments made by artificial intelligence, which could also extend to nuclear threats.[28]

Recent developments are fueling the race for artificial intelligence. The U.S. Department of Defense declared, "rapid advances in AI – along with robotics, autonomy, big data and increased collaboration with industry – will define the next generation of warfare[29]". As ChatGPT overcomes its weaknesses, its potential for upgrading decision-making processes by utilizing its understanding, responsiveness, and communication abilities with humans, along with its unique capabilities, makes it an ideal tool for various applications.

Another important aspect is in the defensive sector. The system can be used to analyze natural language data, such as email content and text messages, to identify and extract relevant information for cybersecurity against malicious software. It can automatically analyze and process massive network traffic, log data, and other information to identify anomalies that may indicate a cyber-attack.

Another important channel is the ability to generate and test potential passwords and crack encrypted databases by creating secure encryption keys. Analysis and identification of patterns in data that can be used to create optimal secure keys, including the development of steganography techniques for hiding data within other data in a way that no one else can see or know about their existence. Another important aspect is the exploitation of the ChatGPT's ability to quickly understand, through expert analysis, the current trend of attacks, the tools and capabilities used Tactics, Techniques, and Procedures (TTPs), and to prioritize the optimal response.

[28] Michael Hirsh "How AI Will Revolutionize Warfare, the new arms race in technology has no rules and few guardrails." Foreign Policy April 11, 2023

[29] Exploring the Possibilities of ChatGPT in Rugged Military AI Applications, Systel ,February 8, 2023 https://systelusa.com/blog/exploring-the-possibilities-of-chatgpt-in-rugged-military-ai-applications/

An example of the military and security exploitation of the integration of artificial intelligence and the ChatGPT tool from OpenAI with Google's speech function was demonstrated with the robotic dog from Boston Dynamics, which allows complex data to be transformed into content understandable by humans. The development enables operators to ask the robot about the collected information, and the robot updates its operators about the mission. The integration with ChatGPT allows for the expansion of communication between humans and robotic tools.

At the end of the mission, robots accumulate a vast amount of data. Since querying the data is usually not a simple task, the upgrade using ChatGPT shows operators the configuration files and mission results. In experiments, for example, a voice command was given instructing the robot to stop scanning. Subsequently, it could be investigated when combining speech-to-text capabilities, allowing the robot to provide voice-based answers. For instance, updating the operators about the latest mission and where it has been and whether it was successful or not.[30]

On the other hand, alongside the enthusiasm for the enormous potential of artificial intelligence for military purposes, in his book[31], Brigadier-General Y., the commander of unit 8200[32], emphasizes that a machine can use Big Data to generate better information than humans. However, the machine cannot understand context, lacks emotions or ethics, and cannot think "outside the box". Therefore, instead of choosing between humans and machines, he recommends creating a team that integrates artificial and human intelligence, resulting in "super-cognition".[33] Another conclusion is that military and security systems will not rely on an open capability but will build internal capabilities with maximum effort to defend against cyber-attacks.

Disinformation

In the modern era, part of the toolkit includes information warfare. ChatGPT can be trained to monitor social media platforms and extract information about public opinion. It can be used to generate propaganda such as news articles, posts, or speeches that align with specific agendas or messages. Psychological manipulations, including social engineering techniques like creating "Deepfake" with convincing and realistic videos, impersonating political figures or military leaders, and disseminating disinformation on communication and social media platforms, can also be carried out.

In these contexts, experts in cybersecurity and artificial intelligence have pointed out that ChatGPT can be rapidly and efficiently exploited for the dissemination of disinformation

[30] Vilius Petkauskas "ChatGPT injected into Boston Dynamics' Spot", Cyber news, 26 April 2023

[31] The Human-Machine Team: How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World, May 5, 2021

[32] An Israeli Central Collection Intelligence Corps responsible for clandestine operation, collecting signal intelligence (SIGINT) and code decryption, counterintelligence, cyberwarfare, military intelligence, and surveillance.

[33] Amos Harel - Interpretation | Artificial Intelligence to Take the Place of Intelligence Personnel: The Future According to Unit 8200 Commander" - Haaretz, October 1, 2021

and manipulation on social media, employing armies of trolls and massive volumes of activity. Such activities previously required significant allocation of resources, time, and human effort.

Research conducted by Georgetown University[34] has established that advanced language processing systems like ChatGPT are capable of influencing actions by operating fake accounts and spreading deceptive information on social media. The document highlights the potential of language models to compete with human-generated content at low cost. These models have the potential to offer clear advantages to malicious actors who utilize them. Tools that broaden access for a greater number of players would enable new tactics of influence, making campaigns more tailored, efficient, and dangerous. The amount of misleading information, deceptive content, and persuasive quality could increase, complicating message detection for regular internet users as part of disinformation campaigns.

Concerns about this type of activity were raised by the Senate Intelligence Committee as early as 2019 when it was determined that a deceptive campaign was launched prior to the 2016 US elections. Thousands of Twitter, Facebook, Instagram and YouTube accounts created by the St Petersburg-based Internet Research Agency focused on harming Hillary Clinton's campaign and supporting Donald Trump[35]. The real concern is that future elections will have to contend with a deluge of manipulated information originating from highly advanced technological systems, such as ChatGPT.

It seems that security agencies are not equipped to deal with the issue of disinformation, even before the use of AI. This includes dealing with external enemies such as foreign states or terrorist organizations, alongside internal political factors that employ bots and generate fake news. At this stage, this is one of the main risks of ChatGPT. When masses of information consumers treat manipulations, speculations, facts, conclusions, personal opinions, lies, and fabrications as a single obstacle without the desire to understand what the truth is.

Fertile ground has been created for the exploitation of this tool. In the not-so-distant past, for example, personal information was transferred from Facebook to Cambridge Analytica. a data analysis company that worked with Donald Trump's election campaign and the Brexit campaign in the UK. Millions of Facebook profiles were leaked and exploited to build powerful software that predicted behaviors and attitudes, in order to tailor personalized political content and influence choices at the ballot box.[36] This new invention has the potential to upgrade malicious capabilities and pose a much more

[34] Josh A. Goldstein Girish Sastry, Micah Musser Renée DiResta, Matthew Gentzel, and Katerina Sedova "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations "Georgetown University, January 2023

[35] David Silverberg "Could AI swamp social media with fake accounts?" B.B.C News, 14 February 2023

[36] Carole Cadwalladr and Emma Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" Guardian, 17 Mar 2018

significant threat.

In July 2018, Elizabeth Denham, the person in charge of enforcing the UK's laws on data protection, revealed that in 2014 and 2015, the Facebook platform allowed Cambridge Analytica to harvest 87 million profiles of users worldwide for the US presidential campaign in 2016 and the Brexit campaign in the UK.[37] The rationale behind this method was a research conducted by the Psychology Department of the University of Cambridge, which claimed it could build a 'psychographics' model of voters based on their Facebook interests, predicting traits like their openness, conscientiousness, extraversion, agreeableness and neuroticism and thus tailor influential messages accordingly.

A similar lawsuit was filed in the federal court in California against the Israeli digital intelligence company Voyager Labs, which allegedly collected massive amounts of data from user accounts on social media platforms, including Facebook, Instagram, Twitter, YouTube, and Telegram, for commercial purposes.[38] The company created 38,000 fake accounts through which it gathered public information about hundreds of thousands of users using a technique called "Web Data Scarping". This technique automatically scans content from websites and processes it to display it on another website. The algorithm that performs the "Scraping" usually includes some form of artificial intelligence that separates different pieces of information, allowing each type of data to be entered into a separate field in the external database without the users' knowledge.[39] As mentioned earlier, with the ChatGPT, the threat of malicious exploitation is increasing, and the danger of disseminating disinformation is worsening.

Another problem with artificial intelligence, such as ChatGPT, is its "generative" capability. It not only generates new texts, code, or images but also invents products, and this flaw necessitates a thorough correction. In a test conducted by the I-Team, the chatbot was asked to write an article describing the activities of Michael Bloomberg since he ended his tenure as mayor of New York City. The text generated by ChatGPT seemed like a persuasive summary of his philanthropic activities and included a quote attributed to him. However, when attempts were made to verify the quote, no documentation was found that he ever said those things. The document also included completely fabricated quotes from anonymous sources that vilified him and attributed the use of his wealth to influence public policy.[40]

Therefore, at this stage, intelligence agencies such as the CIA and the Department of State, despite their interest in these developments, need to exercise caution and skepticism regarding the outputs and the use of such technology. Regarding these concerns, Lt. Gen. (ret.) Jack Shanahan, the founding director of the Pentagon's Joint

[37] James Ball "The real story of Cambridge Analytica and Brexit" The spectator, 11 October 2020.

[38] Omer Kabir "Meta Sues Israeli Voyager Labs: Gathered Information on 600,000 Users through Fake Accounts" Calcalist, January 13, 2023

[39] https://www.mrcoral.co.il/web-data-scraping/

[40] Chris Glorioso "Fake News? ChatGPT Has a Knack for Making Up Phony Anonymous Sources" 4 NEW YORK, February 23, 2023

Artificial Intelligence Center (JAIC) from 2018 to 2020, acknowledged his excitement and regular use of ChatGPT, but to his knowledge, no intelligence analyst utilizes these systems. His successor at JAIC, Marine Corps Lt. Gen. (ret.) Michael Groen, agreed with these statements and added that they could experiment with them, but he estimated that implementation would take years. [41].

As mentioned, alongside the clear advantages, the system also includes inherent drawbacks that will require further development. It remains uncertain whether it will be possible to neutralize all of them, as malicious actors will make every effort to exploit the full potential of these technologies. The concern is that the proliferation of possibilities, such as information warfare tasks and manipulations by terrorist organizations and criminal actors, poses a significant potential risk. Additionally, from a military perspective, at least at this stage, it is not certain whether the application has the capability to understand the context of specific military tasks or situations, which could lead to inaccurate responses and recommendations.

It should be noted that the operating framework is trained on text data, and if adversaries succeed in infiltrating the data used for training the model, the output of the model could be compromised. Since the performance of the application is linked to the quality and quantity of the data on which it was trained, if the model is not trained on a reliable, diverse, and representative dataset, it is likely that it will not perform the required tasks adequately.

ChatGPT and Terrorism

Terrorists and jihadists are known as avid adopters of advanced technologies. The leader of al-Qaeda, Osama bin Laden, utilized email for the transfer of plans related to the September 11 attacks. Al-Qaeda ideologue Anwar al-Awlaki used YouTube for propaganda purposes and recruited a generation of followers and ideological admirers in the West. Over the years, it has been common practice for al-Qaeda to recruit technologically skilled experts. Even the Islamic State utilized Twitter as part of its caliphate-building project.[42]

Terrorists have been using the internet and social media for years, searching for ways to maximize their online activities for planning attacks. Artificial intelligence (AI) and ChatGPT have immense potential to serve as a dangerous platform for advancing their ideological goals.

As early as December 6, 2022, a user on the Rocket.Chat server operated by ISIS, publicly announced that they were already using the free AI ChatGPT software for advising on upgrading support for the caliphate. They stated that the software was more advanced than the majority of operatives, offering precise guidelines for identifying and enlisting a

[41] Sydney J. Freedberg," Pentagon should experiment with AIs like ChatGPT but don't trust them yet: DoD's ex-AI chiefs", Breaking Defense, April 06, 2023

[42] Steven Stalinsky "Terrorists Love New Technologies. What Will They Do With AI? "NEWSWEEK, 3/14/23

"core group of supporters," formulating a "political and ideological strategy," garnering backing from "the Muslim community," capturing "territory," establishing "institutions and governmental structures," and advocating for and safeguarding the new caliphate.

Two weeks later, on December 21, supporters of ISIS expressed interest in the Perplexity Ask platform, used for generating jihadist propaganda content. One of the participants shared their findings in a discussion, and the respondents agreed that artificial intelligence could be used to assist the global jihadist movement. In another discussion among the same groups in mid-January 2023, again on Rocket.Chat, it was emphasized that ISIS supporters need to recognize the importance of understanding technology. Learning crucial coding for cyber warfare and developing cyber security skills were deemed "necessary for fighters to cope with the enemy's military infrastructure"[43].

For now, it seems that ChatGPT has the capability to support terrorist organizations by simplifying procedures and schedules when it comes to planning missions, spreading information, recruiting individuals, and propagating their ideologies.

The Criminal Aspect

The cybersecurity risks of ChatGPT can generally be classified into four categories:[44]

Phishing

This type of malicious software involves the attacker creating deceptive emails, posing as legitimate entities, to manipulate recipients into performing harmful actions. These actions can include clicking on unsecured links, opening malicious attachments, providing sensitive information, or transferring funds to specific accounts. Phishing scams are the most common type of malicious software.

Data Theft

Unauthorized access and retrieval of confidential data on the network. It involves attempts to obtain personal information, passwords, or even software codes that can be used for extortion or other malicious purposes.

Malware

A comprehensive term encompassing various types of software designed to harm users in some way. It can be utilized to breach private servers, steal information, or simply destroy data.

Botnet Attacks

These are targeted cyber-attacks in which the attacker infiltrates and "enslaves" devices connected to the internet. Botnet attacks are carried out to gain control over a collection

[43] Steven Stalinsky "Terrorists Love New Technologies. What Will They Do With AI? "NEWSWEEK, 3/14/23

[44] "The Cyber Security Risks of ChatGPT and How to Safeguard Against It" Sangfor Technologies 17 Jan 2023

of computers, servers, and other networks for a range of malicious objectives.

The Innovation Lab of Europol[45] conducted several workshops involving different content experts to examine how criminals can exploit developments in artificial intelligence, with a specific focus on ChatGPT. The findings of these workshops revealed that if a potential criminal lacks knowledge in a specific criminal domain, ChatGPT can significantly assist them in the learning process, including the four aforementioned threats.

Therefore, ChatGPT can be utilized to specialize in various potential criminal domains without prior knowledge. This includes engaging in online fraud through phishing, data theft, developing malicious software, executing botnet attacks, and even learning how to carry out activities such as breaking into homes, engaging in pedophilia, terrorism, and money laundering. As all the information provided by ChatGPT is freely available online, the model can be employed to facilitate specific stages of criminal activities, offering contextualized responses and enabling malicious actors to better understand diverse areas of criminality and carry out different types of offenses. [46]

In the past, basic phishing scams were relatively easy to identify due to grammatical and linguistic errors. However, it is now possible to create more realistic impersonations of organizations or individuals, even with only a basic understanding of the English language. The model can provide new opportunities for criminals, particularly in crimes related to social engineering, as it can respond to messages in the appropriate context and adopt specific writing styles. Additionally, it can be exploited for various forms of online fraud, such as creating fictitious engagement on social media platforms, including promoting fraudulent investment proposals.

ChatGPT can also be used to generate spam messages to distribute malicious software to a large number of users. In the pre-model era, perpetrating fraud and creating deceptive communication involved processes that criminals had to generate themselves. With the assistance of ChatGPT, various types of online fraud can now be generated rapidly, authentically, and on a large scale.

The new technology can also increase the risk of hybrid attacks,[47] such as password cracking. These attacks include methods like Brute Force[48], where the attacker attempts to discover the target's password by running combinations of passwords, and Dictionary Attack[49], where the attacker tries to uncover the password by downloading a password file and running it. Hybrid attacks create a crossbreed attack where the computational power required to crack the password is significant, and the time dimension plays a

[45] "Europol" European Union Agency for Law Enforcement Cooperation helps national law enforcement authorities fight serious international crime and terrorism.

[46] "ChatGPT-The impact of Large Language Models on Law Enforcement" Europol Innovation Lab, 27/03/2023

[47] Passwords Attacks https://www.israelclouds.com/article/types-cyber-attacks

[48] A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

[49] A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password.

crucial role in password exposure.

Another concern is the exploitation of ChatGPT's capabilities in code development, a potential that improves over time. The latest version of GPT-4 can assist cybercriminals in understanding the context of the code, correcting error messages, and programming mistakes. For a criminal with limited technical knowledge, this becomes a valuable resource, while for more advanced cybercriminals; the potential to exploit improved versions will enhance their hacking tools, including the automation of sophisticated and more dangerous modus operandi.[50]

In the face of these criminal threats, there are also opportunities. The rapid advancement of Artificial Intelligence (AI) and Machine Learning (ML) technologies has led to innovative solutions that can assist law enforcement agencies. For instance, ChatGPT-4 has the potential to revolutionize the way police departments operate. by serving as a cautious predictive tool for criminal activities and enhancing organizational efficiency.[51]

Intelligent exploitation of such tools that harness Natural Language Processing (NLP) algorithms and machine learning enables the analysis of vast amounts of data from various sources, integrating them into fusion centers for efficient information flow, insights, and recommendations. However, optimal utilization of these tools in law enforcement domain requires their deployment in non-open data bases, necessitating internal development and relying on internal capabilities.

Part of the potential lies in identifying patterns, trends, and behaviors that may indicate potential criminal activities. The outcomes will enable proactive law enforcement actions. The use of ChatGPT-4 can rapidly identify potential hotspots for criminal activities, facilitating the efficient deployment of law enforcement resources.

Furthermore, ChatGPT-4 can assist in criminal investigations by analyzing large volumes of data and identifying connections between fragments of information, leading to new investigative directions and the identification of potential suspects. The integration of artificial intelligence systems can aid in scanning and analyzing extensive CCTV footage from past incidents, surveillance videos, and observations.

The new technology, as a natural language processing tool (NLP), can also scan and analyze email messages to detect suspicious language patterns and identify anomalies that may indicate fraud. It can compare email text with previous communication sent by the same user to determine if the language used is consistent. Financial institutions, like law enforcement authorities, will need to strengthen their detection and prevention systems using biometrics and advanced authentication methods to identify customers and reduce the risk of fraud, money laundering, and terrorist financing.

Organizations already utilize behavioral biometrics tools, where each click acts as a

[50] Chris Smith"3 ways ChatGPT can help criminals take advantage of you", YAHOO, March 28, 2023

[51] Marcin Frackiewicz "ChatGPT-4 for Smart Policing: AI-powered Crime Prediction and Prevention"TS2 SPACE, 9 April 2023

unique personal fingerprint. Accumulated findings of typing speed, mouse movement patterns, and other digital behaviors form an individual profile. Machine learning identifies human behavioral patterns using behavioral biometrics and converts the data into insights on the level of verification or risk associated with that behavior. Through technologies that analyze digital behavioral intelligence, it becomes easier to distinguish between genuine users and impostors [52].

The benefits of artificial intelligence and ChatGPT are immense, but as emphasized, there is also a concerning potential for exploitation by malicious actors. Technological developments necessitate constant updates and require the army, law enforcement and security agencies to continuously learn, train, and equip their personnel to be relevant and prepared to harness the benefits offered by these systems while also being capable of effectively addressing the threats they will inevitably face, which are continuously evolving and growing.

Conclusion

ChatGPT provides numerous benefits and opportunities for the general public, businesses, research institutions, and various organizations, including security agencies. However, the accompanying dilemma, present from its early stages, lies in the deliberation between adopting its benefits and addressing the inherent concerns.

When examining, for example, the output of the chatbot in the experiment that analyzed the Chinese space program in terms of structure, logic, clarity, and the received recommendations within seconds, one can be impressed by its potential. Yet, these capabilities still require upgrading and customization to military needs, both in defensive and offensive aspects, including counterterrorism and combating criminal activities. Naturally, one cannot ignore the troubling issue of the system's tendency to invent answers and utilize unreliable information and sources, a flaw that was well reflected in the results of the experiment involving misinformation about Michael Bloomberg. It is a significant flaw that necessitates thorough correction.

Among the advantages of ChatGPT4, for instance, is the potential to revolutionize the operations of security organizations in general and police departments in particular. It is a technology that can assist in forecasting and upgrading organizational efficiency. Intelligent exploitation of such tools will enable the analysis of vast amounts of data from various sources, integrating them into fusion centers for efficient information flow, insights, and recommendations.

Part of the potential within police departments lies in the identification of patterns, trends, and behaviors that may serve as indicators of criminal activities. The outcomes will enable proactive law enforcement actions, and the use of ChatGPT-4 can facilitate the efficient deployment of law enforcement resources. Furthermore, it can assist in criminal investigations by analyzing large volumes of data and identifying connections

[52] Iain Swaine "Can ChatGPT help fight cybercrime?" IBS Intelligence, March 23, 2023

between fragments of information, leading to new investigative directions and the identification of potential suspects.

We are currently in an era where the implementation process of ChatGPT is deepening, as part of an arms race of artificial intelligence. Jake Sullivan, the United States National Security Advisor, has argued that selected technologies such as artificial intelligence and information systems are of immense importance in the coming decade, and that leadership in these key technologies is crucial for national security.[53] Already, some security organizations are investing significant resources in artificial intelligence and emerging technologies. For example, the public expenditure on artificial intelligence in the U.S. Department of Defense increased from over USD 600 million in 2016 to USD 2.5 billion in 2021. This budget has been used in 685 artificial intelligence projects, including several related to major weapon systems, launched in early 2021.[54]

There are already indications that artificial intelligence, in general, will play a prominent role in how countries operate on the international stage. A report by the U.S. National Security Council on artificial intelligence highlighted that this technology will be a tremendous source of power for companies and nations that adopt it. While there is no historical perspective to fully assess its impact, it represents a transformation on a large scale, similar to Thomas Edison's description of the electricity revolution, rather than just a technological breakthrough.[55]

However, amidst the enthusiasm and praise, [56] there is also a more skeptical approach to the recent development. Arthur Holland Michel, a senior fellow at the Carnegie Council for Ethics in International Affairs, has raised concerns about negative aspects of ChatGPT, such as its tendency to generate false information and reflect social biases. Regarding its future, he sees it as a non-revolutionary trend. He claims that it is a regular process that often occurs with emerging technologies, where there is initial enthusiasm and efforts to find ways to use them. However, the reality is often that a new technology will, sooner or later, reveal itself to be poorly suited to most of those imagined applications.

Additional criticism was voiced by Professor Michael Ahn from the University of Massachusetts, Boston, who argued that areas requiring more subjectivity still necessitate human intervention. This statement echoes the opinion of the Unit 8200 commander, who claimed that ChatGPT cannot understand contexts because it lacks emotions or ethics, and therefore cannot think "outside the box". Michael Ahn argued that while it is indeed a groundbreaking technology, he did not see ChatGPT as a dramatic turning

[53] Yojana Sharma," ChatGPT shakes up the AI research landscape – but who is ahead? "University World News ,30 March 2023

[54] Colin Demarest "ChatGPT can make short work of Pentagon tasks, Air Force CIO says"C4ISRNet, Wednesday, Mar 1

[55] Kiko Llaneras, Andrea Rizzi, José A. Álvarez "ChatGPT is just the beginning: Artificial intelligence is ready to transform the world", EL PAIS Jan 31, 2023

[56] Stephanie Kanowitz " ChatGPT for state and local agencies? Not so fast." Government Computer News, March 27, 2023

point on the scale of the electricity revolution, but rather as a development achievement reminiscent of the impact of the invention of 3D printers.

Given the malicious exploitation of ChatGPT by criminal or ideological actors, responsible for providing cyber defense to facilities, they may initially find themselves under a wave of attacks, with the main challenge primarily related to the scope rather than dramatic innovations. On the other hand, in the long run, ChatGPT could be utilized by malicious parties from the criminal or ideological domains (such as terrorists) with technological backgrounds and skills to develop more dangerous and threatening innovations.

A significant and menacing aspect of the chatbot is its contribution to the dissemination of disinformation and fake news for the purpose of deceiving consumers, but primarily its potential influence on electoral systems in democratic countries, which could pose a strategic threat to the integrity of elections.

Although Chatbots, as mentioned, poses threats in various aspects, some of which are highly significant, if the reported issues are addressed, particularly the lack of transparency and guidance regarding the sources on which its findings are based, while neutralizing the option of producing false outputs and biases, this technological development can also be a valuable tool for the intelligence community and security organizations. It can provide them with an advantage against entities and organizations that fail to adopt and develop it. When generative AI and ChatGPT become more accurate and reliable, surpassing their inherent limitations, their deployment in these technologies has immense offensive and defensive potential for army, law enforcement and security units. Organizations that are not present and do not undergo ongoing adjustments and updates may become irrelevant.