This is how terrorist organizations use AI

written by Elie Klutstein | 07.11.2024

Artificial intelligence (AI) has been one of the most notable technological advancements of the past decade, permeating many aspects of life and serving diverse purposes. Experts predict that as AI progresses, it will open new possibilities for humanity.

AI also plays a crucial role in security and defense. In Israel, it is used extensively for military purposes and in the fight against terrorism. According to various reports, AI technology has helped the IDF identify Hamas targets in Gaza for strikes and is also used to trace terrorist funding. The Israeli intelligence Unit 8200, known for signals intelligence ("SIGINT"), houses an AI center. During Operation Guardian of the Walls in 2021, the center's commander stated that advanced technology enabled the IDF to sift through massive databases to extract information that led to identifying terrorists. One can only imagine the additional uses of these rapidly evolving tools within the IDF, and the entire security establishment.

However, AI's rapid development also risks empowering enemies, terrorists worldwide, international criminals, drug cartels, and more. These advanced tools enhance the operations of such groups, making it easier to execute their agendas.

Rita Katz, head of the open-source intelligence group SITE, emphasized that AI is utilized by a range of extremist groups from Al-Qaeda to neo-Nazi networks. "It's hard to grasp just how much of a gift AI is to terrorists and extremist communities," she said.

Global intelligence agencies share this concern. Mike Burgess, head of Australia's security intelligence organization, warned that "AI will likely make radicalization efforts faster and easier." A UN task force on terrorism and technology reported that extremist networks are already using advanced AI tools for propaganda, manipulating narratives around real-world events, and swaying public opinion in their favor while undermining governments. These tools also assist in the targeted and effective recruitment of terrorists, supporters, and sleeper cells.

As AI capabilities develop, they offer terrorists additional applications. For example, while past technology was limited to basic text messages, AI can now produce images, videos, and audio recordings nearly indistinguishable from authentic content. Imagine a phishing scheme involving a voice message mimicking a loved one, pleading for money. Many would fall victim to such schemes, and it's unclear if authorities could effectively counter these scams on a large scale.

Israel may not yet fully comprehend the scope of AI's reach and its applications. Last June—a lifetime in terms of AI's rapid advancements—State Comptroller Matanyahu Englman warned that "AI could lead to broad technological progress in many fields, but it also poses significant risks, including 'fake news' and misuse by terrorist and criminal elements." Englman announced his intent to examine the government's preparedness on this front and to assess how it safeguards its citizens by restricting harmful AI applications that could endanger the public.

An AI handbook for terrorists

In recent decades, terrorists have quickly adapted to advanced technologies, using them efficiently and lethally for their agendas. They have proven their determination to exploit the internet to further their goals.

Sophisticated AI models, like ChatGPT, incorporate rules preventing users from employing them for harmful purposes, such as learning how to avoid punishment for crimes. Tech giants like Microsoft have pledged to develop "responsible" AI guidelines based on principles of fairness, reliability, safety, privacy, transparency, and accountability. Yet, these guidelines are imperfect, and tech-savvy terrorists will quickly find ways to bypass and overcome these safeguards.

Terrorist organizations recognize the potential of familiarizing supporters with these tools. In February, an Al-Qaeda-linked group announced a virtual workshop on using advanced technological tools. Later, the same group distributed a manual—a lengthy guide for beginners on using "artificial intelligence intelligence tools."

Propaganda is one of the primary ways terrorists use AI. All it takes is a computer, creativity, some talent, and basic knowledge of a few advanced software programs. For example, after the attack on a concert hall near Moscow

last March, in which 140 people were killed by ISIS terrorists, the group released a video showing a news anchor celebrating the attack. The video looked authentic but was generated by AI-powered software.

Locally, Hamas terrorists have already been observed using AI software. Early in the war, Hamas produced fake images purportedly showing Israeli strikes on Gaza or videos of Gazan families combing through the rubble of their bombed homes—intended to evoke sympathy for Hamas and tarnish Israel and the IDF's image. Other AI-generated videos depicted Israeli tanks moving through Gaza neighborhoods.

Using AI software, Hamas members create complex graphics aimed at inciting ideologically driven Palestinians to carry out attacks in its name, especially in the West Bank. Supporters post calls for violence against Israel and pro-Hamas propaganda widely on Telegram and social media, using bot-driven technology to inflame the masses.

Hezbollah, too, reportedly employs AI applications. The advanced drones it sends toward Israel likely incorporate AI. Hezbollah has long used psychological warfare, influence campaigns, and propaganda on social media and the internet, and it's likely that in recent years, it has incorporated AI for these purposes.

The Zelensky effect

AI applications used by terrorists can be divided into "soft" and "hard" tools. The primary soft tool, as mentioned, is propaganda. AI offers numerous ways to quickly and effectively create and distribute content, allowing users to "play" with audience emotions using visuals, background music, and targeted messaging. Not only can advanced, seemingly real content be created, but fake users ("bots") on social media can amplify it. The use of bots makes it harder for social media companies to identify and halt propaganda dissemination.

Propaganda is not only about promoting an organization's ideology but can also involve false information designed to harm the enemy, weaken civilian morale, and mislead enemy commanders. The phenomenon of "deepfakes," for instance, enables overlaying one person's face onto another's body or generating exact voice replicas to convincingly simulate speech, potentially deceiving viewers.

For example, Russian-affiliated actors released a video of Ukrainian President

Volodymyr Zelensky, urging his fighters to lay down their arms. Zelensky's face was overlaid on the speaking figure, and his voice featured in the video. However, the speaking body remained static, exposing the deception. But imagine a group of fighters crowded around a phone in a tense battlefield moment—would they notice such subtle details? How would such a video affect them? And how would Israelis react if Hamas used such videos to simulate hostages speaking for them?

Such campaigns can particularly influence targeted audiences, such as children and adolescents who spend significant time online and may be more susceptible to extreme indoctrination due to their young age.

Another way AI capabilities are used is for recruiting terrorists. Advanced AI-driven bots can interact with potential recruits, provide them with information tailored to their character, and assess their suitability for the organization. In Afghanistan, ISIS's Khorasan Province operatives have tried using online connections with young Europeans to encourage them to join and carry out attacks in their home countries.

AI programs can also be used to raise funds. An Israeli study found that advanced platforms complied with researchers' requests to assist in "fundraising for the Islamic State," providing detailed instructions on managing a fundraising campaign and what to post on social media for success.

Alongside these, AI technology provides terrorists with "hard" tools as well. These include capabilities to transmit encrypted messages or obtain classified information through sophisticated means. As the British Home Secretary stated, advanced tools allow terrorists to plan more efficient and lethal attacks. One example is the ability to use simulators to plan drone flight paths for targeted attacks.

In general, the use of drones and other autonomous tools is rapidly advancing with the aid of AI. This allows terrorists to strike an enemy's weak points and execute efficient attacks without risking their lives. The UN discussed this threat several years ago. According to experts, autonomous weapons that make split-second shooting decisions based on sensor data are becoming increasingly common on the battlefield. These tools can rely on AI for planning routes, navigation, advanced target recognition, and more. One major fear is the potential use of AI-driven vehicles loaded with explosives, programmed to target

and “suicide bomb” enemies—similar to the IDF’s use of old armored vehicles in Gaza. Reports indicate that ISIS is working on developing such vehicles.

Another “heavy” AI application is conducting sophisticated cyberattacks, tasks that humans would struggle to perform in a short time. Such attacks can cause damage independently and serve as a kind of “preemptive strike”—a means of softening and confusing the enemy before physical attacks.

Shortly after the outbreak of the COVID-19 pandemic, UN Secretary-General António Guterres warned that terrorists might mimic the virus’s “success” by using AI and biotechnological developments to create lethal viruses targeting specific population groups based on their genetics to increase lethality. Although highly complex, this possibility, though still theoretical, remains feasible.

Influence on US elections

Iran’s Supreme Leader Ali Khamenei has also recognized the advantages of the latest technological development, marking AI as a key target for Iran.

“We must master all aspects of AI technology before an international regulatory body like the IAEA is established, and we have to ask permission… In some matters, they will not give us permission,” Khamenei said last month in a speech posted on his website. “AI is advancing at an incredible pace today. It’s amazing to see the technology’s global impact and rapid progress. Our different sectors—security and military—use AI, but we must not make the mistake of only being end-users,” he added.

Khamenei’s mention of the IAEA was likely intentional. In his view, AI advancements might become a game-changing weapon, similar to a nuclear bomb. His remarks are part of a broader Iranian initiative to advance AI technology, which began during former President Ebrahim Raisi’s tenure. Iran discussed introducing digital currencies into its economy, helping it circumvent Western sanctions.

In July, Tehran launched the National AI Organization, aiming to position Iran among the world’s top ten AI leaders, specifically in governance, digital economy, and entrepreneurship. To achieve this, Iran has developed a detailed AI strategy document now being implemented. Reports indicate that Tehran already uses similar technology to monitor and suppress women’s rights. Simultaneously,

OpenAI, developer of ChatGPT, noted that Iranian organizations have used its software to sway American public opinion ahead of the US presidential elections.

Once Iran attains expertise in AI, it will likely explore all relevant applications in security, missile development, influence operations, and even nuclear science, which stands to gain significantly from AI advancements. Iran is also expected to share AI-based knowledge and developments with its affiliates across the Middle East, similar to other weaponry provided to the Houthis or Hezbollah. This means that Hamas, for instance, will gain the know-how to best use advanced software—a significant challenge for Israel.

Israel must examine ways to leverage the AI tools in its arsenal—an area where it is considered a global leader—not only for offense but also for counterterrorism. In September, it was reported that Israel would join dozens of nations in signing an international AI treaty, ensuring transparency, privacy, and equality. Understandably, this treaty does not cover AI's use in national security; otherwise, Israel likely would not have signed it.

Looking ahead, Israel must consider regulatory measures to manage AI applications that support terrorism, but without limiting the security establishment's use of similar tools. It might also explore creating specialized working groups with its allies to share intelligence and expertise in specific cases to prevent harm to innocent civilians.

At the same time, Israel must maintain its qualitative edge in AI, explore innovations for its needs, and train the next generation of experts to support its security forces in using these applications offensively, defensively, and in safeguarding the Jewish people in their homeland.

Published in Israel Hayom, November 7, 2024.