Cybersecurity expert weighs in on AI benefits and risks

January 5 2024, by Brooke Kleiboer

Credit: Pixabay/CC0 Public Domain

Artificial intelligence has been taking the world by storm as the powers of tools such as ChatGPT and others have become available to the

public.

A security researcher, Dr. Natalia Stakhanova (Ph.D.) is the Canada Research Chair in Security and Privacy and an associate professor of computer science in the USask College of Arts and Science, whose research work has been focused on practical security solutions to everyday problems. One of them is making computer systems secure. She has published numerous articles on software and network security and more recently on how to leverage AI in security. She is the holder of four patents in the field of computer security and is a member of the Canadian Cross-Cultural Roundtable on Security (CCRS).

As the public continues to gain an interest and adopts AI into everyday use, Stakhanova said it's important to recognize that AI technology has been around for a long time. Now, it is embedded in our daily lives, even though it is not always recognized.

"For example, banks' phone support is often powered by AI which helps you navigate through various options and provide answers you're looking for," said Stakhanova. "Something like this is a simple use of AI."

AI has also been under scrutiny in the cybersecurity world for a wide range of applications in which it could possibly contribute to issues surrounding cybercrime.

In a world where data collection and exploitation are becoming increasing threats as digital products that store personal and financial information—such as social media platforms—have taken over the world, safety and understanding of AI is paramount to combating fears of its use.

"From a security standpoint, there are two ways to look at AI," said Stakhanova. "On the one hand, AI seems to enable more efficient

exploitation of data and users. However, on the other side, AI has a great potential to be used for defense."

When people store data through a social media account, this data becomes stored on the company's computer systems, most of which are designed to be secure. But most of these computer systems are not immune to clever hacks that could put data security at risk.

If AI can be used to find ways to attack secure systems on one side, the opposite should also be true—that AI can potentially provide a way for individuals or companies to test and defend the security of their computer systems.

"The question is, how effective are your defenses against AI?" she said. "I can envision in the future we would use AI to both attack a system and defend a system, taking the human out of the picture completely."

Stakhanova said that the ability of AI to build and test security systems can be great news for those who work in the field of creating a more secure cyberspace, where important data and information are exchanged billions of times per day around the planet.

"Somehow we tend to think of the negatives, but we should also think of the positives," she said. "If AI is leveraged by cyber criminals to attack, the defenders can also use it to continuously test the security of their systems. This provides us with a significant advantage allowing to test at scale impossible for a human and test for threats that may seem infeasible now, but potentially quite realistic in a very near future."

Although there are benefits to what AI can accomplish—such as searching for information, writing coherent communications, creating code, providing information, and analyzing data at a pace impossible for humans—there are still limitations that restrict its usefulness and

reliability that should be considered when using an AI tool.

"AI has limited capabilities for complex reasoning," said Stakhanova. "There are a lot of limitations when we're talking about the chain of thought that humans can generate easily and make conclusions based on. It's not just our immediate knowledge, but also the experiences, the 'baggage' we have and something that we've seen or read [that can influence our actions], and AI is still not able to use that chain of thought effectively."

There is much hesitancy around introducing AI capabilities in workplaces, schools, and other locales that could potentially change job structures and workflows.

"This is understandable. Right now, it's a Wild West and really there's almost no regulations in place," she said. Even with limitations, the rise of AI is an innovation that Stakhanova thinks is worth embracing. "I believe AI adoption will continue and probably more rapidly than we would like it to happen," she said.

Stakhanova has been involved in creating educational resources for youth about cybersecurity and staying safe online. In her opinion, cybersecurity is an important subject to bring up to kids who are growing up in a largely digital world.

The important next steps will be to develop safety guidelines and recommendations around AI and its use to help protect people and guide usage as much as possible.

"Having conversations around AI is a good first step but we are definitely behind regulating this technology. [Using] AI will bring us huge benefits but without controls, it can also be destructive."