TECHNOLOGY

As Artificial Intelligence Evolves, So Does Its Criminal Potential

By JOHN MARKOFF  OCT. 23, 2016

Imagine receiving a phone call from your aging mother seeking your help because she has forgotten her banking password.

Except it’s not your mother. The voice on the other end of the phone call just sounds deceptively like her.

It is actually a computer-synthesized voice, a tour-de-force of artificial intelligence technology that has been crafted to make it possible for someone to masquerade via the telephone.

Such a situation is still science fiction — but just barely. It is also the future of crime.

The software components necessary to make such masking technology widely accessible are advancing rapidly. Recently, for example, DeepMind, the Alphabet subsidiary known for a program that has bested some of the top human players in the board game Go, announced that it had designed a program that “mimics any human voice and which sounds more natural than the best existing text-to-speech systems, reducing the gap with human performance by over 50 percent.”

The irony, of course, is that this year the computer security industry, with $75 billion in annual revenue, has started to talk about how machine learning and pattern recognition techniques will improve the woeful state of computer security.

But there is a downside.
“The thing people don’t get is that cybercrime is becoming automated and it is scaling exponentially,” said Marc Goodman, a law enforcement agency adviser and the author of “Future Crimes.” He added, “This is not about Matthew Broderick hacking from his basement,” a reference to the 1983 movie “War Games.”

The alarm about malevolent use of advanced artificial intelligence technologies was sounded earlier this year by James R. Clapper, the director of National Intelligence. In his annual review of security, Mr. Clapper underscored the point that while A.I. systems would make some things easier, they would also expand the vulnerabilities of the online world.

The growing sophistication of computer criminals can be seen in the evolution of attack tools like the widely used malicious program known as Blackshades, according to Mr. Goodman. The author of the program, a Swedish national, was convicted last year in the United States.

The system, which was sold widely in the computer underground, functioned as a “criminal franchise in a box,” Mr. Goodman said. It allowed users without technical skills to deploy computer ransomware or perform video or audio eavesdropping with a mouse click.

The next generation of these tools will add machine learning capabilities that have been pioneered by artificial intelligence researchers to improve the quality of machine vision, speech understanding, speech synthesis and natural language understanding. Some computer security researchers believe that digital criminals have been experimenting with the use of A.I. technologies for more than half a decade.

That can be seen in efforts to subvert the internet’s omnipresent Captcha — Completely Automated Public Turing test to tell Computers and Humans Apart — the challenge-and-response puzzle invented in 2003 by Carnegie Mellon University researchers to block automated programs from stealing online accounts.

Both “white hat” artificial intelligence researchers and “black hat” criminals have been deploying machine vision software to subvert Captchas for more than half a decade, said Stefan Savage, a computer security researcher at the University of California, San Diego.
“If you don’t change your Captcha for two years, you will be owned by some machine vision algorithm,” he said.

Surprisingly, one thing that has slowed the development of malicious A.I. has been the ready availability of either low-cost or free human labor. For example, some cybercriminals have farmed out Captcha-breaking schemes to electronic sweatshops where humans are used to decode the puzzles for a tiny fee.

Even more inventive computer crooks have used online pornography as a reward for human web surfers who break the Captcha, Mr. Goodman said. Free labor is a commodity that A.I. software won’t be able to compete with any time soon.

So what’s next?

Criminals, for starters, can piggyback on new tech developments. Voice-recognition technology like Apple’s Siri and Microsoft’s Cortana are now used extensively to interact with computers. And Amazon’s Echo voice-controlled speaker and Facebook’s Messenger chatbot platform are rapidly becoming conduits for online commerce and customer support. As is often the case, whenever a communication advancement like voice recognition starts to go mainstream, criminals looking to take advantage of it aren’t far behind.

“I would argue that companies that offer customer support via chatbots are unwittingly making themselves liable to social engineering,” said Brian Krebs, an investigative reporter who publishes at krebsonsecurity.com.

Social engineering, which refers to the practice of manipulating people into performing actions or divulging information, is widely seen as the weakest link in the computer security chain. Cybercriminals already exploit the best qualities in humans — trust and willingness to help others — to steal and spy. The ability to create artificial intelligence avatars that can fool people online will only make the problem worse.

This can already be seen in efforts by state governments and political campaigns who are using chatbot technology widely for political propaganda.

Researchers have coined the term “computational propaganda” to describe the
explosion of deceptive social media campaigns on services like Facebook and Twitter.

In a recent research paper, Philip N. Howard, a sociologist at the Oxford Internet Institute, and Bence Kollanyi, a researcher at Corvinus University of Budapest, described how political chatbots had a “small but strategic role” in shaping the online conversation during the run-up to the “Brexit” referendum.

It is only a matter of time before such software is put to criminal use.

“There’s a lot of cleverness in designing social engineering attacks, but as far as I know, nobody has yet started using machine learning to find the highest quality suckers,” said Mark Seiden, an independent computer security specialist. He paused and added, “I should have replied: ‘I’m sorry, Dave, I can’t answer that question right now.’”

A version of this article appears in print on October 24, 2016, on page B3 of the New York edition with the headline: As Artificial Intelligence Evolves, So Does Its Criminal Potential.