Cyber Warfare 2023: AI, ChatGPT, and Coming Battle of the AI

Cyber Security Summit Webinar Series

May 30th, 2023

Speaker: Micki Boland, CTO, Checkpoint

Moderator: Sean Costigan, Director of Cyber Policy; Professor at George C. Marshall

European Center for Security Studies

Report Author: Alex Kemp, Intern, Cyber Security Summit

Speaker Bio: Micki Boland holds the Office of the CTO Architect and Evangelist at Check Point Software Technologies. A company dedicated to offering multilevel security architecture to over 100,000 customers to defend cloud, network, and mobile devices. Micki is also a Cybersecurity warrior and CISSP with over twenty years of Information Technology domain experience. She graduated University of Texas at Austin with a Master of Science in Technology Commercialization IC2 McCombs School of Business. She has also received her MBA with Global Security concentration. U.S. Army veteran. U.S. Army Information Systems Command. Long time IEEE member.

Introduction: The plentiful benefits and applications that innovations such as AI provide are never without an equal volume of dangers and nefarious uses. Our defenses must be constantly evolving in a similar manner to the technology it is protecting. Not just our defenses require constant maintenance, but our regulations and legislation as well. All AI should exist for the human to use, not the AI to use the human. The latter becomes more and more plausible the longer it goes without proper understanding and regulation.

Cyber Warfare 2022 year in review: DeepFakes, automated bots, generative AI: Three human impersonation softwares have become increasingly prevalent within the last year. Which, like all modern day luxuries provide their intended aids but can be used as tools to meet a malevolent end. The first being DeepFake technology, an artificial intelligence that can be used to create images, audio, and video. After continual feeding of training data, it becomes more and more difficult to perceive the fake. We've seen it used to help a highschool Valedictorian with speech difficulty deliver her graduation speech, but also generate fraudulent video of the Ukrainian President in an effort to get the Ukrainian people to halt their defense efforts under the false pretenses of a cease fire. The growing accessibility to automated bots allows online healthcare platforms to attend to a greater number of patients than ever before possible, but also allows for the rapid spread of fake news or extreme views with ease. Without proper security and regulation generative AI can become rather dangerous. Because the same sources

that allow us to create audio, visual, text, and code in order to revolutionize our healthcare, economy, and everyday lives can also be used to attack them.

2023:ChapGPT (openAI) risk reward tradeoff: On one hand, ChatGPT is capable of generating responses quickly and efficiently offering significant time savings to the user. In the form of chatbots on websites it allows businesses to process high volumes of customer inquiries and complete other trivial tasks. This frees human employees to complete more executive duties. On the other, bias is impossible to avoid seeing as these AIs require initial training from a human. This bias can be perpetuated further the more it is utilized. Safety concerns can also arise if used to make decisions in a healthcare situation. Diagnosis and courses of treatments should always receive a second opinion from a professional. Being a machine run off algorithms, Ais are incapable of providing sympathy or empathy. The lack of empathy can lead to unsatisfied customers. Generating responses to significant tragedies can result in those affected feeling slighted and unhappy. While some safeguards do exist they act largely as a glass wall, due to them being easily bypassed. They are taught not to divulge certain information or provide responses to certain questions. Yet there are workarounds which easily nullify those restrictions.

Call to action for cybersecurity, GRC, and data protection and privacy professionals: If these generative AI sources are used by a company, data privacy should be a top priority. A business account should be had in order to protect private information and remove outside bias. Yet, ChatGpt was hacked twice and business accounts were targeted. Releasing payment info and protected prompts. In addition to using a business account to protect private information ChatGPT 4, which sandboxes and destroys data should be used. Together, a good wall of security is realized.

Conclusion: While overtly useful Deep Fakes, automated bots, and generative AI are not without their faults. Technical understanding is paramount to proper regulation and security necessary for safe and beneficial usage.