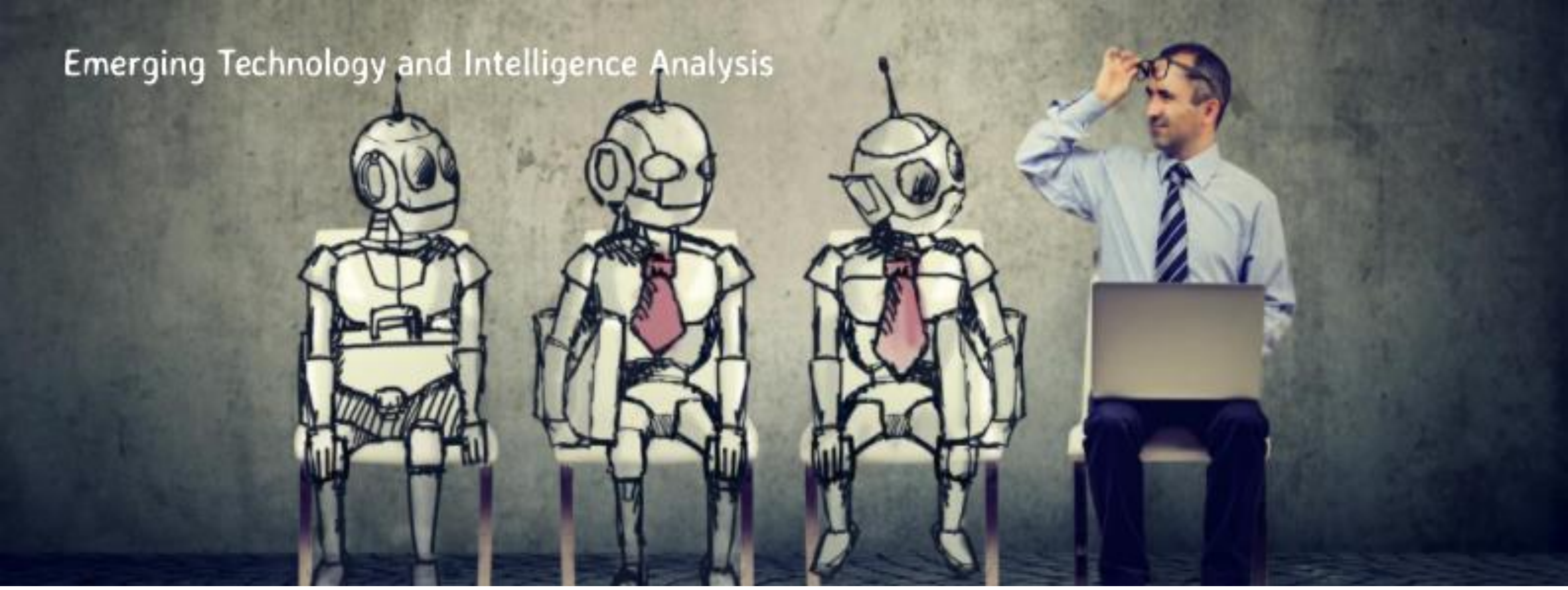


Emerging Technology and Intelligence Analysis

Introduction

Major inventions have regularly upended the intelligence gathering mechanisms of security professionals. Adapting to these advanced technologies is critical for analysts and protectors. Going back only to the 18th century, during the US Civil War, hot air balloons enabled "balloonists" to hover over battles and telegram "real time" information back down to the ground. The transatlantic telegram was also a major technological innovation that significantly advanced Signals Intelligence (SIGINT) by allowing great powers like the UK to tap the lines.

A similar innovation in SIGINT occurred when the internet became used globally. Allowing the NSA, UK's GCHQ, and other security agencies to harvest data directly from fiberoptic cables. The internet also radically changed Open-Source Intelligence (OSINT) because analysts can now access online the type of information that previously had to be manually collected from local and regional newspapers or by listening to radio stations. These types of emerging technologies radically changed intelligence each time, and now in the 21st century technological advances will mean that intelligence will change again.

The physical-cyber convergence is an important issue for the security profession, and there are varying perspectives about how the changing nature of the digital world will impact protectors. Emerging technologies that intelligence analysts need to understand include artificial intelligence tools, large language models, the metaverse, and drones. Each of these offer novel capabilities and insights for intelligence analysts that can make their work more efficient and therefore produce better results for their clients.

Artificial Intelligence

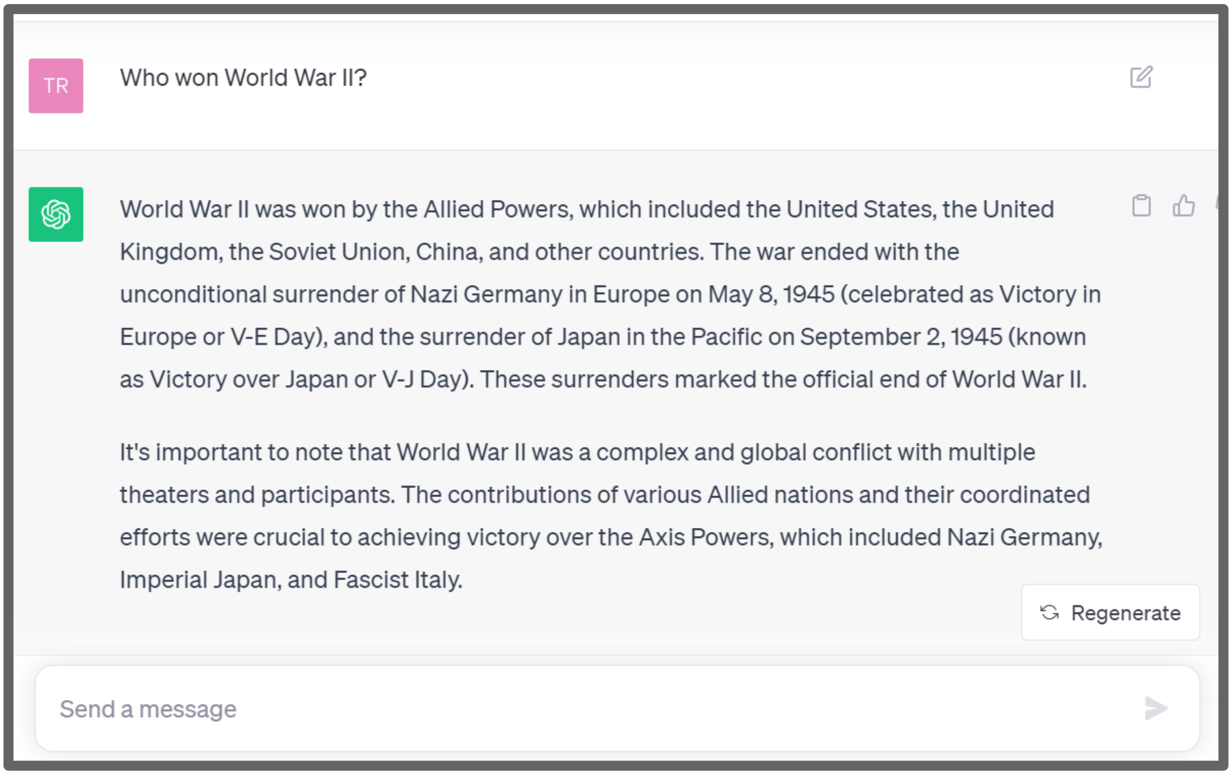
Artificial intelligence (AI) is the term we give to programs that perform specific tasks while learning to perform those tasks more effectively. There are different versions of AI from the incredibly simple (rules engines) to the massively complex (machine and deep learning), but all of them are tools that help researchers, workers, and even analysts. National security organizations have brought in AI to help intelligence analysts for years (see research here and here on the subject), but corporate security intelligence has lagged behind their use. Many free tools are available to help analysts save time and effort.

To start, analysts often find the collection of information and data to be a tedious process that detracts from the actual analysis part of their jobs. That is a critical area where AI tools will be essential for analysts. For example, web scrapers can help gather requisite information so that analysts do not have to spend hours upon hours collecting and collating the information before getting to the risk or impact analysis. Exceptionally useful for intelligence analysts is the role AI plays in translating languages. Google has significantly advanced its image searches so that in a reverse image search the program will translate languages in the picture. No need to type out phrases one sees in pictures or struggle if it’s a non-Latin script.

AI programs are limited, though, and they will focus on completing the assigned task even if doing so does not follow human logic. When OpenAI was training their reinforcement learning systems on the game CoastRunners (a boat racing game), the AI ignored the human idea of finishing the race and instead focused on getting a high score by staying in a lagoon to constantly hit targets. When using specific tools, analysts must be careful to match the need with the right program. Analysts cannot expect AI tools to go beyond their specific function or they may run into the problem of the lagoon.

Large Language Models

One of the most significant revolutions in the past year has been a highly improved version of ChatGPT. For those uninitiated, ChatGPT is a large language-model chatbot (LLMs) that produces realistic answers to queries that the user has. Even simple questions can produce useful responses (see below for an example). This is absolutely a useful tool for analysts, but it is critical for them to understand how to use the LLM as a tool rather than a replacement for analysis. One way that ChatGPT is helpful is in summarizing a series of articles, which could save analysts hours of work when trying to produce background on a topic. Simply copy and paste the relevant text into the prompt and command ChatGPT to summarize the articles. Another useful approach is asking ChatGPT to produce scenarios for political or geopolitical events. This can help analysts think of possible alternatives to do better forecasting. For example, when asked to list scenarios for the Russo-Ukrainian War, ChatGPT produced seven possible outcomes. An analyst could take those, determine probabilities, and assess indicators and impacts.



TR

Who won World War II?

World War II was won by the Allied Powers, which included the United States, the United Kingdom, the Soviet Union, China, and other countries. The war ended with the unconditional surrender of Nazi Germany in Europe on May 8, 1945 (celebrated as Victory in Europe or V-E Day), and the surrender of Japan in the Pacific on September 2, 1945 (known as Victory over Japan or V-J Day). These surrenders marked the official end of World War II.

It's important to note that World War II was a complex and global conflict with multiple theaters and participants. The contributions of various Allied nations and their coordinated efforts were crucial to achieving victory over the Axis Powers, which included Nazi Germany, Imperial Japan, and Fascist Italy.

Figure 1: Example from ChatGPT

Of course, there are limitations to the use of ChatGPT and other LLMs. To start, they have a tendency to lie, or more accurately, as an AI, it will follow its protocols and produce answers even if those answers are not accurate. For example, a lawyer was sanctioned in June because he had used ChatGPT for legal research, and the LLM made up fake court cases to support his queries. The editor of Oxford Review also told the story of ChatGPT making up fake academic references when his students used the model. Besides making up facts and references, ChatGPT also has a political bias. According to researchers at the Technical University of Munich and the University of Hamburg, ChatGPT has a "pro-environmental, left-libertarian orientation." Political bias is not inherently wrong (we all have it), but analysts must always strive for objectivity, and if they take the responses by ChatGPT wholesale, then they will incorporate bias into their analysis.

Metaverse

In their "fictional intelligence" book *Burn-In*, Peter W. Singer and August Cole describe a fascinating scenario where terrorists organize their violence through anonymous avatars in the metaverse. Although the current metaverse is nowhere near that quality (we are far away from a *Ready Player One-type* situation), over the next five years the metaverse is highly likely to take on a more sophisticated role for consumers and businesses. Intelligence analysts need to start preparing a strategy to handle information gathering in this new online space.

Sock puppets in particular will be an issue to resolve. Currently, most OSINT analysts and red teamers have sock puppet accounts (i.e., fake online personas) to gather information on social media and elsewhere. Such accounts are important because analysts must practice operational security and prevent as much as possible threat actors learning they are being targeted for observation. A separate phone, VPNs, and virtual machines are typical tradecraft for sock puppet accounts, but it is entirely plausible the metaverse will have fundamentally different requirements. Social media only requires a phone number to get started on Twitter, Facebook, Snapchat, or the like.

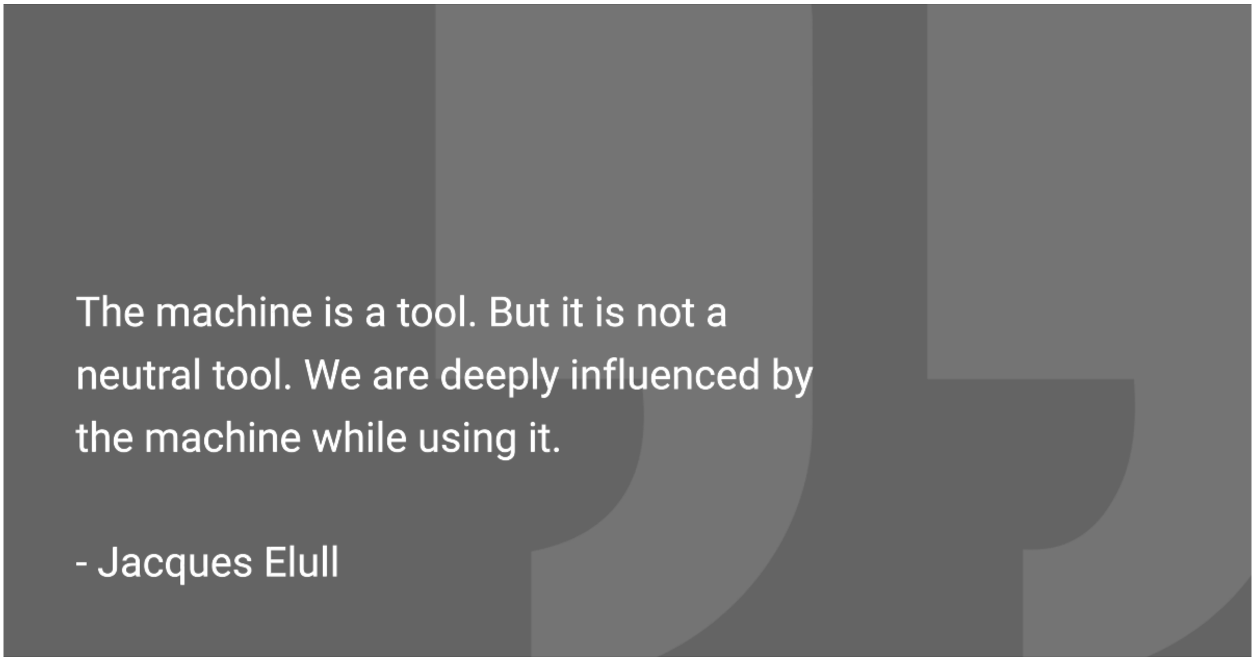
There are highly likely to be two alternatives to this issue: strong identification requirements through something like blockchain or the ability for complete anonymity in which identity is purely malleable. Neither of these will be good for intelligence collection. If it is the former, then it will be significantly more difficult for analysts to create sock puppets and surreptitiously gather intelligence on individuals and groups. If it is the latter, then it will be significantly more difficult to find and identify persons or groups of interest. Understanding that the metaverse is coming can help prepare analysts to engage in such a world. They should actively be learning how AR/VR will develop and what possible tools will be available for their use.

Drones

Drones are no longer emerging technology. Sometimes called unmanned aerial vehicles (UAVs), drones have been around for decades, and they are now commercially available for incredibly cheap prices. What do drones have to do with emerging technology and intelligence? Most analysts engage in real-time analysis through OSINT or SOCMINT, but drones should be an important augmentation of intelligence gathering for security professionals in the private sector, especially during events like protests or monitoring principals in high-risk situations. Having more direct observational power will help analysts provide intelligence support to security professionals on the ground.

There are several contemporary examples of drones being used by civilians and amateurs for such purposes. Ukrainian soldiers and civilians have already demonstrated the capabilities of low-cost drones used by novices to gather intelligence. DJI drones are specifically designed for filmmakers and photographers, and they are relatively easy to use. Outside of conflict zones, law enforcement agencies have already used drones to monitor protests that had the potential to turn violent. In the UK, police used drones to monitor protests of both left-wing and right-wing extremists. In France, police used drones to monitor protests on May Day (one of the more raucous protest days each year). Such real time intelligence can be critical for protectors, and intelligence analysts should learn how to gather information with drones and analyze the images.

Concerns remain over FAA regulations, safety issues, and privacy laws, but all of that is manageable for security professionals. Proper standard operating procedures that follow municipal, state, and federal regulations along with guiding principles can protect safety and privacy.



The machine is a tool. But it is not a neutral tool. We are deeply influenced by the machine while using it.

- Jacques Elull

It is critical for intelligence and other security professionals to understand both the capabilities and limitations of the emerging technologies that will impact the evolving nature of intelligence. Used effectively, technology will streamline processes, save time, and make better intelligence products that enable better decisions. Used poorly, tech can become just a set of expensive toys that do not really add value, or worse, harm credibility.