NATO Innovation Network Conference - 9 Nov 2021 - Proceedings

Session: OPEN INNOVATION - COGNITIVE WARFARE USE CASE

by Dimitris Moulas and Nana Boateng

Currently, it is widespread knowledge that the growth of technological advancement has surged. There have been diverse fields where innovation takes place; a percentage of them being linked to cognitive warfare. In theory, cognitive warfare is a process where an individual or organization has the ability to defeat their adversaries without any physical destruction. However, their aim is to manipulate and interfere with the cognitive state of these individuals and groups. Subsequently, there can be a change in the way people think and go about their daily lives if such warfare were to profit off them without their knowledge. People who utilize cognitive warfare essentially have the competence of influencing and shaping the opinion of society, without having to use unequivocal force.

During the NATO Open Innovation conference week, a virtual conference took place, hosted by Kristina Soukupova. The topic discussed was the Cognitive Warfare Innovative Approaches. There were 6 representatives on the discussion panel, from academia, industries and NATO. Each speaker presented what their project goals were, how they can implement their innovations and views to the cause, and explain why it is important to take this new domain into consideration.

The 6 representatives on the discussion panel:

Kristina Soukupova - *Defense Security Innovation Hub*

- Cognitive Approaches.

Francois du Cluzel - *NATO ACT HQ*

- Cognitive Warfare; A battle for the brain.

Allison Kuntzman - *US Army Mad Scientist*

- The future of the operational environment & Mad Scientist initiative.

Tomas Vejlupek - *Tovek*

Alexander Rovalino - *Johns Hopkins University*

Seal Guillory - *Booz Allen Hamilton*

The first speaker was Kristina Soukupova, who is the president of Def Sec Innovation Hub from Czech Republic. She introduced the topic of Cognitive Warfare to all the participants in the conference. Kristina Soukupova, stated that they have managed to establish an educational project called NATO Virtual Academy that was presented to International Relations and Diplomacy students. In accordance, DefSec launched the first massive online open course that educated civilian and military staff of NATO about social media security. Additionally, the president informed and introduced the viewers and participants to the topics and projects that DefSec is operating. She further stated that the cognitive warfare field is still relatively new, thus, requiring the organization to constantly look for new answers. With that being said, DefSec is actively looking for experts of this field and many different fields such as humanities, anthropologists, sociologists, and people that can provide potential technical solutions. In addition, they want to approach public debates in order to inform the civilians on the topic, as they can be the ones influenced by such cognitive warfare campaigns.

The DefSec team came up with a new project called HACK THE MIND, that follows the principles of HACKATHON. The event had the intent of collecting ideas related to cognitive warfare issues. It lasted for five months in which they received many applications in different forms. This project helped them create the Cognitive Warfare Dashboard. In this year's event, they are seeking new technical or non-technical ideas and solutions that can answer a variety of questions. Henceforward, DefSec accommodates the idea of communicating their message through comics. Thus, creating 4 heroes and currently expecting 4 more, in order to bring forth a different perspective to cognitive warfare to the general public. After that’s established, the material will be evaluated by academia and NATO. The best results will be presented to NATO and NATO nations.

Next to present was Francois du Cluzel, the keynote speaker. His presentation was titled, “Cognitive Warfare: A battle for the brain.” Francois started the presentation by mentioning that he commissioned two studies, one of them being in cooperation with academia, Johns Hopkins, and a few European Universities which resulted in approximately 200 people contributing to the project. This brought about NATO developing the concept of cognitive warfare, which provided a better understanding of the different technologies and domains that can be a part of such a campaign. Furthermore, cognitive warfare is associated with other forms of action that reach a target audience in a form of cyber warfare or information warfare. A cyber operation domain aims to penetrate computer networks in order to reach adversaries software and disrupt or neutralize their procedures.

Additionally, Francois provides visual representation during the conference explaining the differences of the two domains of psychological operation and cognitive warfare. He further elaborates by giving his own definition of what cognitive warfare is, “Cognitive warfare could be called the art of altering and operationalizing cognition.” That being the case, currently within NATO, there is not a commonly agreed definition of the domain of operations. For that reason, it is of high importance for NATO to declare a new domain of operations. Francois du Cluzel, defined the domain of operation as, “The sphere of interest and influence in which activities, functions and operations are undertaken to

accomplish missions and exercise control over the opponent in order to achieve desired effect." Thereby, it needs to be acknowledged in order to protect NATO's personnel and human beings as they are the main vulnerability in such campaigns from adversaries. Lastly, it is highlighted that NATO was late in responding to cognitive warfare challenges, which can result in losing a war. Consequently, NATO is currently building a common understanding for the domain of cognitive warfare, due to the fact that the organization is a defensive alliance, and it is necessary to protect their cognitive abilities before anything else. There were considerable questions that were asked by viewers after the presentation, one of the viewers asked, "If it is mandatory for a NATO member, not only pertaining to the United States, to protect our service members cognitively or does that extend to our populations?" Francois replied by saying, "I think it is a problem that society will face as a whole. Just think of the work culture, I think this is a good example of cognitive warfare, where people think in very different ways than they're used to and it is a long-term process. It goes way beyond our service members, we need to protect our population, and it goes through a wide area of potential solutions, including critical thinking, education and more. It goes way beyond our service members."

After Francois du Cluzel responded to the question that was asked, it was time to move to the third speaker, Allison Kuntzman. Allison is a part of the Army Future Command and Deputy Director of US Army Mad Scientist. The topics covered presented different ways on how they provide support to the army's modernization enterprise. The ideas focus on the years of 2035 to 2050; which means there are probabilities of many possible future endeavors, relating to cognitive warfare. Correspondingly, she analyzed the future components environment (FOE) which is the effort to modernize the NATO and US military. They further provide more information for the components of FOE in AFC Pamphlet 525-2 that was published in 2020. In addition, it is stated that the adversaries are observing the United States strengths and vulnerabilities that will in turn assist them in creating a highly advanced, cutting-edge military. This will be a challenge for the US in the year of 2035, if this trend holds. As of today, opponents have acquired momentum and power, competing with the US for global resources which can result in extremist nations, corporations, and national crime organizations threatening army forces. FOE, will be a complex connected environment with cyberespionage and faster systems that will change the speed of battles. Their assessment is to inform decision makers and other high influencers to modernize the army enterprise.

The second topic presented by Allison, focuses on the Mad Scientist program which is working on the army initiative to explore the operating environment with collaboration with academia, industry and the government. Their team is called the US Army Mad Scientist Initiative that separates the Trade Dock, enforcing their efforts now, till 2035 and the AFC which will cover 2035 till 2050. They use three different ways to collect ideas; which include a storytelling writing contest, their blog, and hosting events which informs the army of modernization priorities, strategies and information advantages. The team also has a podcast for their partners to access all the information given in conferences, writing contests, including twitter. It is worth mentioning that the Mad Scientist group takes part in different

events and works with different partners from universities and organizations from all around the world. Additionally, they participated in an event with the concept of hacking for defense, sponsored by the University of Southern California. After the completion of Allison's presentation, she opened the floor to anyone who had questions. Someone in the audience asked, "In storytelling, do you ever have members or participants provide you input on the way future technologies can look from their own personal libraries? For example, three body problems is a book trilogy set that is based on future possibilities." Kuntzman responded, by saying, "Yes, absolutely. I think something we have done that falls in line with that is writing contests. We had two different sci-fi competitions that had topics and prompts related to future technologies and how they might look on a battlefield. If you have an idea or submission that might not follow in with our writing competition that is taking place, you can always email us, give us a summary about your idea, and we will definitely take a look at it. If there is a way to work it out and make it relevant to a topic we are working on, we will consider it for publications." This concluded Allison Kuntzman's presentation.

Next to present was Tomas Vejlupek, President of TOVEK, informing viewers that his company's mission is to provide solutions, create models of reality which can be used to achieve goals, solve problems, or get a competitive advantage. TOVEK platform supports analysts, police and judges; aiding them to find efficient and effective answers to their questions from various data sources. Their platform operates in their own built in code that uses artificial intelligence and machine learning for recognition of entities in text and multimedia. This is achieved with rules and dictionaries that exist in the code, resulting in hybrid data fusion that unify multiple source data search and analysis. Their platform offers a variety of data analysis tools. It recognizes photographs of entities, and analyzes the objects in them. Indexing videos that can scan and detect different objects, voice data that can index output of speech to text recognition, and an identifying document application that verifies if signs and stamps are authentic. Furthermore, they have other concepts such as active knowledge maps that create and distribute comprehension. This way, they can create smart questions and maps in order to find knowledge; for example, "Who is the leader of a terrorist group?"

At last, TOVEK has a visualization platform with all the data collected that allows them to check links, sections and locations. This model operates as a decision support system, using artificial intelligence in order to summarize and synthesize large volumes of data, while giving answers for specific questions. Such as where the data is collected, the reason it was marked, when the data was stored, and why the particular data was retrieved. In conclusion, the platform can support analysts to save time connecting all the dots to provide useful insight, for decision makers to get valid and clear answers, for teams to share information and human knowledge securely. A viewer asked, "Intelligence is never precise, so how to fuse precise and imprecise information to meet decision making goals?" Tomas Vejlupek responded by saying, "Of course, when we administer some information sources, we always give it evaluation, we know that some sources are more reliable and some not. It is a general practice in intelligence so it is used to help analysts make some assumptions. They check which sources the parts are collected from, so they can validate the results. It is satisfying

when one makes the final picture to link the original sources, so it can be made known how they found certain facts and verified them. Thus, it is very important that no information is lost, while verifying and checking the data, due to it being a very important concept of our solution."

The next speaker to present was Alexander Rovalino, a third year biomedical engineering student at Johns Hopkins University. The Klark Scholar and his team are trying to find solutions for the broad question of what cognitive warfare is. They ended up finding that in this new domain of cognitive warfare, the target is always the mind. They addressed that it is known that cognitive warfare involves disinformation and misinformation, however, there are other techniques employed within cognitive warfare. As a result, they expand to a new domain with cyber warfare, informational warfare, psychological warfare, and social engineering. These techniques have a main goal, which is to influence people's minds and affect societal opinions. This can be observed in modern society using social media and digital interconnectivity systems that uncover cognitive weaknesses. An easily observed weakness is the filter bubbles effect that appears in social media, where people tend to follow sources that agree and coincide with their beliefs and preconceptions. This normally results in confirmation bias, social proofing, and recency bias. Those weaknesses can be used by adversaries in the cognitive domain to manipulate society. Henceforward, they developed a matrix that was focused on the leaks of the 2016 United States and United Kingdom elections. This prompted the team to find that warfare attacks on the web can be both successful and unsuccessful. Likewise, the team is developing a prototype user interface by acquiring data by articles, network trees, different accounts and keywords to track, monitor, predict and respond to cognitive attacks across the world. Correspondingly, a study from MIT found that a strong indicator of fake news virality is the emotional content, the surprise and anticipation of the post instead of whether or not it originates from a bot. It has been found that a fake post doubles every 15 minutes and it reaches 16 million people in around 6 hours. This led them to create a tool to identify fake news and to trigger a circuit breaker in order to slow down the spread. By applying this tool the spread will be decreased by doubling every 30 minutes. With such a decrease in 6 hours it will reach only 4 thousand people. Additionally, NATO is focusing on the biophysical, behavioral, biochemical and genetic aspects of people's cognitive ability and behavior. The aim is to find a way to modify them in order to improve cognitive ability especially for soldiers within NATO. An example of that is the prosthetics hands that use sensors to provide sensation to a person's brain although they are missing the limb, which is a cutting-edge technology. This can allow in the future for more advanced sensory perception. Lastly, they are researching capabilities that can be imparted in a user in order to disrupt people's cognitive or physiological abilities for them to defend against cognitive attacks by strengthening their minds.

https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Why Cognitive Warfare? | Innovation Hub