Cognitive Warfare
Problem for the Brain, Opportunity for the Machine

Robin Burda
Joštova 10
Brno, 602 00
CZECHIA

robin.burda@fss.muni.cz

ABSTRACT

Cognitive Warfare (CW) is an emerging concept, but the underlying emphasis on the importance of the human brain in warfare has been here since the very beginning of humankind. The large change came with cyberspace that can provide an attacker with cheap options to influence masses of people. However, it also provides many possibilities for monitoring and subsequent defence against CW thanks to the possible use of artificial intelligence (AI) and machine learning (ML). This paper draws from discussions of SAS-HFM-ET-FE on Early Warning System for Cognitive Warfare, published NATO Science & Technology Organization (STO) reports, and academic literature to offer comprehensive overview of opportunities and challenges of using AI and ML for improvements in CW-related situational awareness and sensemaking.

1.0 INTRODUCTION

Cognitive Warfare (CW) emerged recently as a concept different from previous terms like *propaganda* and *psychological warfare* primarily due to unprecedented advancements in technology and science related to human cognition. The human mind cannot easily wrap itself around the volume of available media and Internet content. It is impossible not to get disoriented, which makes improvements in situational awareness and sensemaking even more critical.

A case demonstrating this was the explosion at al-Ahli Arab Hospital in Gaza on October 17. Hamas promptly accused Israel of bombing a civilian object and killing hundreds [1]. Israeli authorities and numerous open-source intelligence (OSINT) analysts investigated the incident and concluded that it was, in fact, a Palestinian Islamic Jihad's malfunctioning rocket that caused the explosion [2]. Nevertheless, the damage was done and caused harm to diplomatic relations and incited pro-Palestinian rallies around the globe [3]. Navigating through the large quantities of data was impossible for anyone, and damage control was complicated for Israel, which played second fiddle in the cognitive warfare waged by Hamas. Fortunately, while the human brain cannot process and comprehend the sheer volume of data, which is crucial for dealing with CW, *the machine can* – more precisely artificial intelligence (AI) and machine learning (ML) algorithms. Systematically analyzing adversarial communication networks for an operation designated – in this specific case – to damage Israel's image in the international arena might have given more time for decision-making and constructing a counternarrative by offering insight into the situation.

The paper draws from the discussions of SAS-HFM-ET-FE on Early Warning System for Cognitive Warfare, published NATO Science & Technology Organization (STO) reports, and academic literature to provide the best practices and future possibilities for improving situational awareness and sensemaking. The paper's goal is also to give an overview of SAS-HFM-ET-FE findings and inform about the future planned research on the topic by the Research Task Group (RTG) SAS-185 Indicators and Warnings for Cognitive Warfare in Cyberspace. The opportunities and limitations of software solutions for indicators and warnings for CW based on the findings of the discussion of the SAS-HFM-ET-FE team will be presented.

2.0 FROM PROPAGANDA OF OLD TO COGNITIVE WARFARE

While CW is a new concept, it should be noted that various ways of waging war without lethal force have been utilized in the history of humankind. Linebarger claims that one of the earliest cases of psychological warfare (PSYWAR) was Gideon's "use of lamps and pitchers against the Midianites," a story told in the Old Testament [4]. Many such cases were documented in history, and PSYWAR evolved significantly with technological advances. Airborne leaflet campaigns appeared already in 1870, with hot air balloons and planes being used extensively since World War I and playing a significant role in World War II as well [5][6][7].

Shortly after World War II, Jacques Ellul argued that radio and television "permit direct communication with a very large number of persons collectively, while simultaneously addressing each individual in the group" [8]. In fact, with the increased availability of radio and television in the second half of the 20th century, a genuinely interconnected technological society emerged, and influencing people *en masse* became much more accessible. Propaganda became so intertwined with technological society that it is essentially inseparable and needs to be understood as a sociological phenomenon [9].

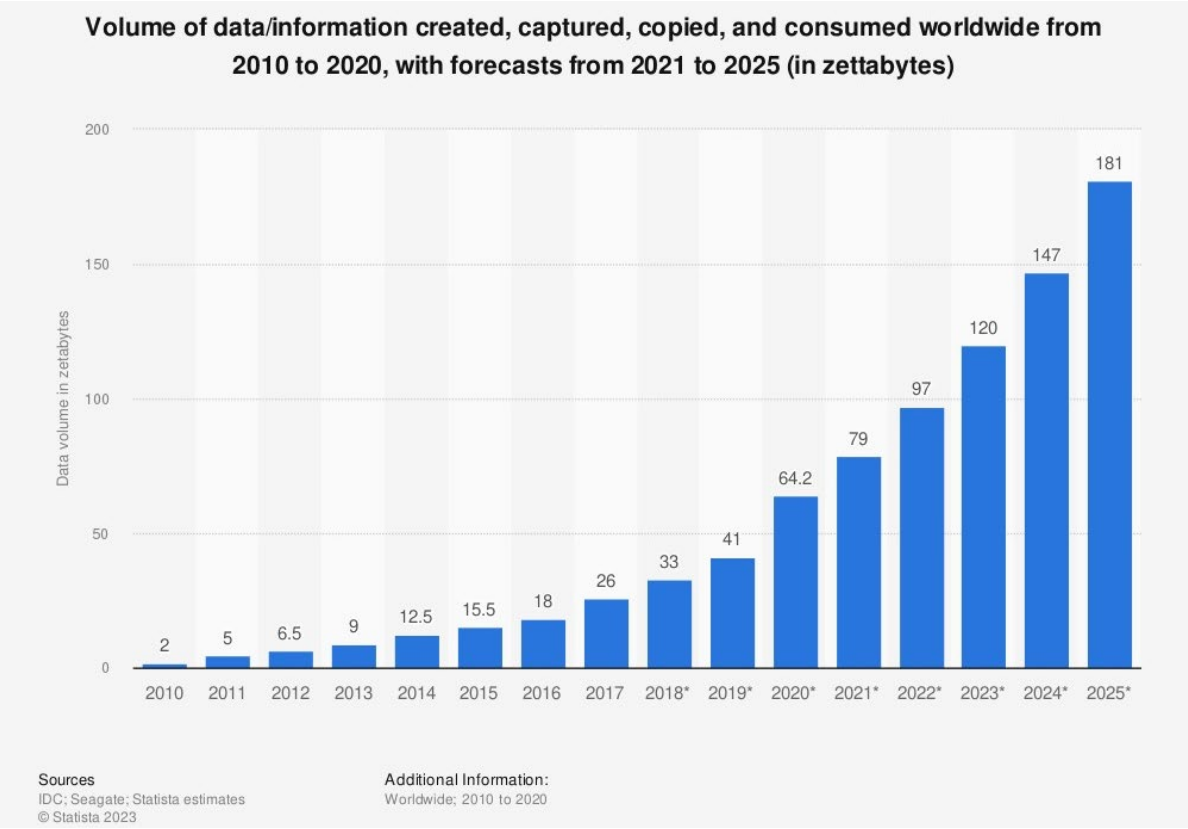


Figure 1. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes) [10].

With the arrival of the Internet and its quickly increasing availability, a new channel for masses of people appeared. However, with Web 1.0, propaganda and other forms of information warfare were still more similar to mass media. While more people could be reached – with personal computers and laptops ever more easily as well – communication was still a one-way street. One actor disseminated the information, and the other consumed it and potentially spread it to a limited audience close to them.

The most significant change came with the so-called Web 2.0, a term referring to slightly varying concepts that have in common a notion that the Internet changed from primarily an information provision system to a communication platform [11]. This development constitutes the crucial turning point in the war for the human mind, which is now starting to be called *Cognitive Warfare*. Without the participatory nature of Web 2.0 and the emergence of social media platforms, the Internet would be merely a new tool for the same old propaganda and communication techniques. Wanless and Berk describe a new concept called participatory propaganda, which moves from a "unidirectional 'one-to-many' form of communication, to a 'one-to-many-to-many more' form where each 'target' of influence" [12].

With new ways of inter-human communication, a significant difference can also be observed in the consumption of news. Based on the Reuters Institute Digital News Report, social media are currently the main source of information for citizens in some countries like Thailand or Chile, but also in countries like the UK the percentage is over 40% [13]. Spreading information to large audiences is relatively easy and cost-effective, which makes CW even more dangerous. The sheer volume of data generated and consumed by internet users makes the matter even more complicated – see Figure 1. For illustrative purposes, if we consider an average movie to be around 2 gigabytes, then one zettabyte is equivalent to roughly 500 billion movies.

3.0 COGNITIVE WARFARE – MACHINE-ENABLED THREAT

New technologies offer a wide range of possibilities for manipulating information to influence the target audience. One such example could be so-called *deepfakes,* referring to photos or even videos created by deep learning algorithms, which can be virtually unrecognizable from actual images. However, while such tools constitute yet another technology that can be easily exploited, humans are generally strongly influenced by the huge proliferation of electronic devices. The online world can easily be accessed via mobile phones, and nearly anyone can take photos or stream video in real time, radically changing individuals and societies [14].

An argument can be made that, despite the apparent technological advancements, the nature of war is the same for the most part. As Linebarger demonstrated in an example of Gideon, psychological warfare has been there for a long time [1]. However, it may not be the nature of war that changed – but humans did. CW constitutes a novel concept largely due to unavoidable changes in the human brain. A research paper by Firth et al. suggests that there are several crucial areas where the human brain changed with the Internet [15]:

> *a) the multifaceted stream of incoming information encouraging us to engage in attentional-switching and "multi-tasking", rather than sustained focus;*
>
> *b) the ubiquitous and rapid access to online factual information outcompeting previous transactive systems, and potentially even internal memory processes;*
>
> *c) the online social world paralleling "real world" cognitive processes, and becoming meshed with our offline sociality, introducing the possibility for the special properties of social media to impact on "real life" in unforeseen ways.*

The nature of what has been called *psychological warfare* since the 1920s [16] changed dramatically, and the human brain has, indeed, become a "battlefield of the 21st century" [17][18].

Cognitive Warfare is, essentially, a threat enabled by machines and big data, which are currently omnipresent. Not only does the Internet allow fast transfer of information around the globe using personal computers and smartphones, but crucially – with the recent boom of the Internet of Things (IoT) and 5G technologies – humans and machines are increasingly intertwined [19][20]. This allows for even more possibilities for exploitation and manipulation [19][20].

With the human-machine inseparable relationship, the whole society is under imminent threat of CW, which cannot be stopped by means of censorship or physical borders. While restricting communication

channels towards the population can slow CW down, a multitude of tools and circumventions can be exploited both by the adversary and the target audience itself. It is possible to shut down websites, as was the case of Russian Sputnik News after the 2022 invasion [21], but the restriction of social media and other online sources is a much more complex task. Even an authoritarian regime like China is not fully successful in restricting information flow among its population [22]. With that in mind, how can democratic regimes – that have their proverbial hands much more tied due to free speech [23][24] – ever hope to deal with CW?

4.0 MACHINES AS MEANS OF DEFENCE

All warfare – CW included – requires going through an observe-orient-decide-act (OODA) loop. The concept was coined by Boyd and can be explained as follows [25]:

> *OODA loop suggests that success in war depends on the ability to out-pace and out-think the opponent, or put differently, on the ability to go through the OODA cycle more rapidly than the opponent.*

The contemporary world is fast-paced, information spreads almost instantly, and the consequences are far-reaching for the OODA loop. The global environment has become highly complex, and analyzing all necessary data for making the correct decision to tackle CW is impossible solely by the human brain, which makes situational awareness and sensemaking ever more critical and simultaneously more dependent on machines. Brooks goes as far as to argue the following [26]:

> *The current state of the art systems prove that it is very possible to build automated systems that can perform automated vulnerability detection, exploit generation and software patching in binary software without human intervention.*

The aforementioned increase in reliance on machines to analyze data and assist in decision-making can be considered a weakness. However, I would argue that – while the weakness is a very relevant aspect – there is, first and foremost, no way around using machines to deal with CW. The final report of HFM-ET-356 *Mitigating and Responding to Cognitive Warfare* deals with situational awareness and sensemaking extensively[1], and the authors argue that "technologies equipped with AI and adaptive ML algorithms have the potential to support sensemaking capabilities for enhanced SA in the future security environment" [19]. I would go as far as to argue that ML and AI are not only potentially beneficial but *necessary* tools for battling CW.

The purpose of ML and AI for defense against CW is to reduce the complex environment into more graspable and understandable parts for human decision-makers. The complexity of tasks related to defense against CW can be split into several levels, each with more abstract and complicated answers for solutions. Treverton works with three levels of questions – puzzles, mysteries, and complexities (see Table 1) [27]. As CW is a complex concept and targets the whole population, it is necessary not to reduce the complexity by simple "educated guesses." Even methods like PESTLE[2] or SWOT[3] would not be helpful, as they require a lot of time and effort from skilled analysts and simplify the environment too much. Some situations can spin out of control in a matter of minutes, such as demonstrated in the disinformation operation of Hamas regarding the explosion at al-Ahli Arab Hospital in Gaza on October 17. Therefore, time is a luxury in matters related to CW, which only underlines the need for AI and ML algorithms to speed up the OODA loop by shortening the *observe* and *orient* parts.

[1] Situational awareness and sensemaking are an integral part of the house model created by the HFM-ET-356 team.

[2] Political, Economic, Social, Technological, Legal, Environment

[3] Strong, Weak, Opportunity, Threat

Table 1. Puzzles, mysteries, and complexities based on Treverton [27].

Type of Issue	Description	Intelligence Product
Puzzle	Answer exists but may not be known	*The* solution
Mystery	Answer contingent, cannot be known, but key variables can, along with sense for how they combine	Best forecast, perhaps with scenarios or excursions
Complexity	Many actors responding to changing circumstances, not repeating any established pattern	"Sensemaking"? Perhaps done orally, intense interaction of intelligence and policy

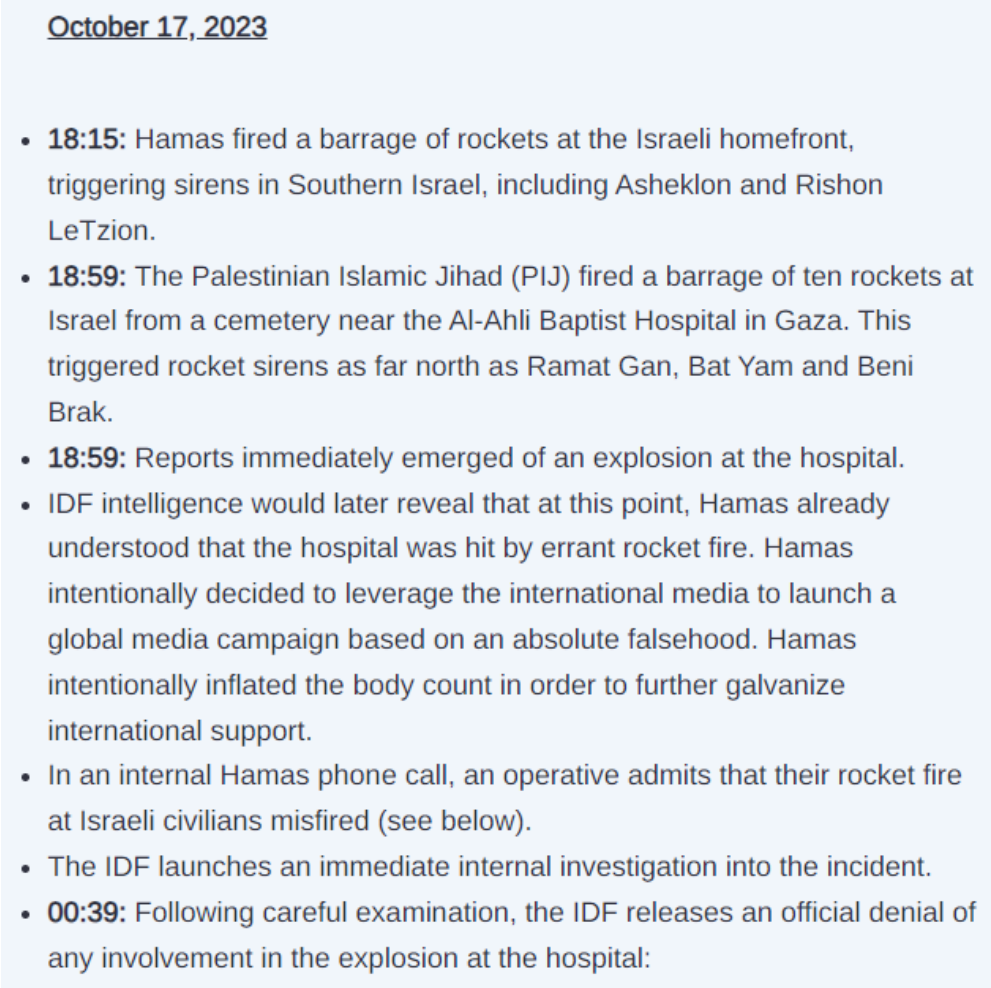
ML and AI should be utilized in situational awareness and sensemaking related to CW to reduce complexities to mysteries and, potentially, mysteries to puzzles. To be put more plainly, the environment can be analyzed and "understood" by artificial intelligence and reduce the "complexities" to a set of "mysteries," which can later be – using another AI algorithm – deconstructed into "puzzles" that have a definite answer [27]. This is, naturally, an ideal example that will inherently be full of pitfalls in the AI and ML tools, as well as the humans interpreting the information and acting upon it. The question is *how exactly* could AI and ML be utilized?

Let us, once again, use the explosion at al-Ahli Arab Hospital in Gaza as a model example. After the terrorist attack of Hamas from the Gaza Strip on October 7, 2023, that resulted in at least 1,400 Israeli deaths, Israel announced a complete siege of Gaza and proceeded with widespread aerial bombardment [28]. On October 17, 2023, an explosion at al-Ahli Arab Hospital in Gaza happened, which was immediately attributed to the Israeli airstrikes by Hamas on Telegram merely three minutes after they launched a barrage of rockets on Israel (see Figure 2) [29]. This claim was quickly shared by established Western news outlets such as the New York Times, Reuters, AP News, and Politico [30], and naturally by pro-Palestinian media like Al-Jazeera and Al-Arabiya. Israel's initial reaction was "painfully slow (to the point of incompetence in political warfare)" [31]. Despite later evidence provided by Israel that the attack was likely a result of a failed rocket strike by Palestinian Islamic Jihad, the damage has been done, and convincing the world that the initial reporting was false will not be an easy task [31].

Figure 2. Telegram excerpt as shared and described by AP News [29].

Israel's failure was in the slow reaction (see Figure 3), where the full OODA loop took too long to diminish the negative effects of Hamas' CW. In this case, AI implemented to gather real-time data from social media platforms like Telegram and performing initial automated content analysis could have given Israelis a warning that there is an event not related to known flight paths and bomb runs (which might also be available to the AI), where the Israeli Airforce is accused of killing hundreds of civilians. The information could be used in another AI model that would quickly share a short official announcement to pre-emptively counter the narrative or at least form the environment for future steps. In the meantime, relevant decision-makers would be automatically alerted and given structured information regarding the incident. The *observe* part of the OODA loop would essentially be skipped, and the *orient* part made significantly shorter. This would buy extra time and enable dictating the narrative by being the first to comment on the incident to international media that would not have to resort to creating politically and diplomatically damaging sensational stories for Israel from Hamas' CW.

It is apparent that with the increased use of information technologies, the decision-making process itself is not straightforward, and focusing solely on the human element is problematic, as with the combination of human and machine elements, failure – and success – can happen on *human-human*, *human-machine*, and even *machine-machine* interaction lines [33]. Essentially, machines are both the root cause of CW's dangerousness and the basis for tools used for defense against it.



October 17, 2023

- **18:15:** Hamas fired a barrage of rockets at the Israeli homefront, triggering sirens in Southern Israel, including Asheklon and Rishon LeTzion.
- **18:59:** The Palestinian Islamic Jihad (PIJ) fired a barrage of ten rockets at Israel from a cemetery near the Al-Ahli Baptist Hospital in Gaza. This triggered rocket sirens as far north as Ramat Gan, Bat Yam and Beni Brak.
- **18:59:** Reports immediately emerged of an explosion at the hospital.
- IDF intelligence would later reveal that at this point, Hamas already understood that the hospital was hit by errant rocket fire. Hamas intentionally decided to leverage the international media to launch a global media campaign based on an absolute falsehood. Hamas intentionally inflated the body count in order to further galvanize international support.
- In an internal Hamas phone call, an operative admits that their rocket fire at Israeli civilians misfired (see below).
- The IDF launches an immediate internal investigation into the incident.
- **00:39:** Following careful examination, the IDF releases an official denial of any involvement in the explosion at the hospital:

Figure 3. Timeline of the Al-Ahli explosion based on the Israel Defence Forces' (IDF) initial report [32]. Note the first response of the IDF took more than five hours.

5.0 CHALLENGES FOR CW-RELATED AI AND ML SOLUTIONS

Automated solutions for CW situational awareness and sensemaking are a necessity to enable an effective decision-making process. Nonetheless, there are several key areas that can be visualized on two axes – (1) understanding and (2) awareness – forming a well-known graph (see Figure 4). Theoretical knowledge is necessary for any practical tools, and by far, not everything is mapped entirely regarding the emerging concept of CW, forming a significant area of *unknowns*.

However, the awareness axis is potentially even more crucial. Cybersecurity has been dealing with *zero-day vulnerabilities*, referring to unknown system vulnerabilities, since the beginning. Researchers even attempted to create new metrics to assess susceptibility to zero-day vulnerabilities [34]. As CW is strongly interrelated with cyberspace, zero-day vulnerabilities can also be exploited for psychological impact. There is, therefore, a natural pressure toward identifying theoretical and practical issues for situational awareness and sensemaking related to CW operations. This chapter draws from discussions of SAS-HFM-ET-FE team.

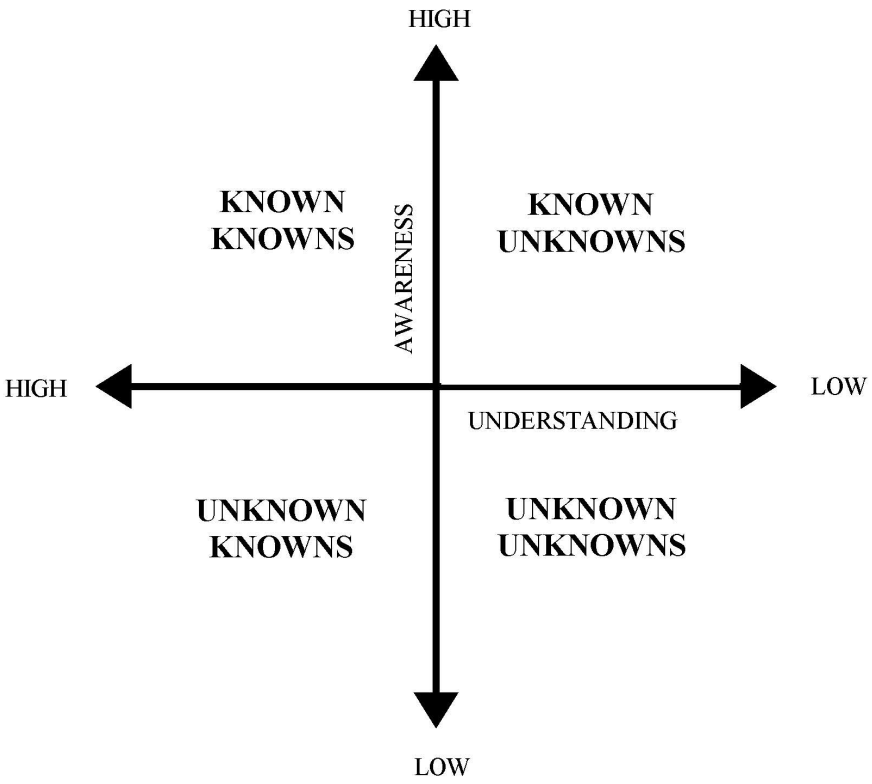


Figure 4. Awareness-Understanding matrix of knowns and unknowns.

5.1 Known-Knowns

It is hard to imagine that known-knowns might pose a significant problem for defense against CW. However, numerous already-known limitations exist to any use of AI and ML algorithms for situational awareness and sensemaking regarding CW. First and foremost, the core referential object that needs to be defended is NATO, which consists almost entirely of liberal democracies. While democracy is a core value for NATO members, it is also quite limiting in many aspects due to necessary adherence to human rights and international law [23][24]. A long list of things must be considered in designing any automated solution for monitoring CW-related adversarial activities, such as general data protection regulation (GDPR), international law, freedom of speech, and ethical aspects of gathering large amounts of personal information. Furthermore, the "maneuvering space" is shrinking even more with regulations imposed by the EU and national states.

Any ML or AI solution requires big data to work, which also needs to be sustainably and continuously gathered to keep the system up-to-date and working. However, the significant data pool collected daily in cyberspace would inherently contain much personal data, which could potentially be used against individuals and groups to increase security and battle CW. This creates a typical Hobessian dilemma with *freedom* on one side and *security* on the other.

5.2 Known-Unknowns

From the theoretical point of view, the known issues are constituted primarily by known research gaps. In CW-related research, such gaps can be empirical – i.e., some crucial actors and their operations have not yet been addressed. However, there are also conceptual gaps related to the novelty of the term CW as understood by NATO. Furthermore, concepts can get politicized, which, based on an understanding of some researchers,

happened to hybrid warfare. Raitasalo goes so far as to say that "[c]rying 'hybrid warfare' easily gets one's security-related argument heard" [35]. It is essential to avoid this faith with CW – strong conceptualization is one of the core theoretical gaps. Other broad areas that require further research include issues of bot detection on social media [36] or natural language processing models for languages like Arabic.

One example from practice, albeit not related to CW, is the extensive use of cheap drones against armored targets, including main battle tanks. While the awareness of such a threat was there, experts several years ago concluded that the consequences of current-generation drone proliferation for interstate war are *low* [37]. However, the War in Ukraine showed extensive use of drones, which resulted in the use of welded cages dubbed "cope cages" or "emotional support armor" due to their ineffectiveness [38]. The known threat of drones was not understood well enough by armies, as demonstrated in the War in Ukraine and recently even Hamas's successful disabling of an Israeli Merkava tank [39].

5.3 Unknown-Knowns

One of the largest potential pitfalls for automated solutions for CW-related situational awareness and sensemaking is not knowing what is known, which can be a result of a mere lack of such knowledge or intentional ignorance. Usually, solving the unknown knowns and moving them to known knowns would be a result of a literature review. However, any review will inherently be incomplete due to the amount of data on most research topics. Furthermore, knowledge can be classified by state and non-state actors, limiting the researcher. What can pose a much larger problem is *willingly* omitting known knowns for selfish reasons, like coming up with seemingly "novel" ideas or solutions. There is a considerable difference between the aforementioned reasons for insufficient handling of unknown knowns, but the result is the same – time and effort are invested in research or development of already existing technologies and solutions.

5.4 Unknown-Unknowns

The most dangerous issues are the unknown unknowns. It is complicated to deal with those; one cannot just list them out and prepare, and the existing defense might be toothless against unknown threats. What can happen in CW that would be a total surprise? Naturally, that is hard to predict, but with the fast advancements in technology, things like the exploitation of social media algorithms on a large scale, leaps forward in deepfakes are among the threats that might soon materialize. However, the largest unknowns are likely tied to the use of quantum computing with its impact on cryptography [40], but crucially also on cognitive sciences [44]. The impact of new knowledge of the human brain that will be gathered thanks to the power of quantum computing is unpredictable and could potentially change the shape of CW.

6.0 WHERE TO GO FROM HERE?

6.1 Strong Conceptualization

Both researchers and practitioners should beware of the politicization of CW. It is understandable and necessary to promote the need for research and active measures against CW, but the well-known fairytale of the boy who cried wolf from Aesop's Fables demonstrates that repetitive use of a threat can result in becoming numb to it. The concept of CW needs to be well-established but also sufficiently bounded to ensure that everything is not automatically labeled as *Cognitive Warfare* for the sake of argument. STO has already done much work to ensure the concept is developed well, but the danger of CW politicization remains.

6.2 Quantitative Research

While qualitative research of CW is beneficial, there is a strong argument for quantitative research in this area. AI and ML algorithms are necessary enablers for automated solutions for situational awareness and

sensemaking, as demonstrated in chapter 4.0, which require numeric inputs. Furthermore, quantitative indicators for CW in cyberspace could bring much-needed information to the decision-making process by aggregating large datasets, offering insights into the complex environment. Research should focus on both language-independent and dependent indicators.

Zhou and Zafarani offer an overview of various language-dependent and independent attribute types of *fake news* features grouped under types like sentiment, complexity, or subjectivity [41]. Such attributes can help analyze cyberspace content and probe for CW operations. Some concrete examples include the *percentage of subjective verbs*, the *percentage of negative words, lexical diversity: unique words or terms (%),* and many others [41]. A different example – mainly language independent – can be social network analysis (SNA). SNA can be used to visualize relationships between actors, including on social media platforms like Facebook or X, which play crucial roles in areas like disaster management [42], but crucially also CW. Quantitative research of disinformation, fake news, propaganda, social media, marketing, and many other areas can be built upon to improve knowledge on CW and help with improvements of situational awareness and sensemaking.

6.3 SAS-185 on Indicators and Warnings for Cognitive Warfare in Cyberspace

In 2022, the SAS-HFM-ET-FE exploratory team on *Early Warning Systems for Cognitive Warfare in Cyberspace* started its work, resulting in a technical activity proposal approved in August 2023. The research task group SAS-185 began its work on the Indicators and Warnings for Cognitive Warfare in Cyberspace project in September 2023. The team's goal is to develop quantitative indicators for CW and prepare requirements for a future software solution for monitoring cyberspace for CW operations. Quantitative indicators are crucial for any software solutions dealing with large quantities of data hiding adversarial CW operations. They essentially constitute *enablers* for both practical tools used for improving situational awareness and sensemaking and further steps in the decision-making process. In the end, there can be no successful defense strategy if the threat is not identified in time.

While the group is at the beginning of its task, several crucial conclusions were drawn in the exploratory phase, implicitly shaping this paper's chapter on *pitfalls of automated solutions for CW sensemaking*. STO should continue CW-related research and bolster cross-panel cooperation, as CW is in and of itself a multifaceted threat that requires knowledge from social and technical sciences. It is crucial to understand that large AI models can be used for indicators and warnings for CW to improve sensemaking and situational awareness, but even more straightforward quantitative features in combination may offer enough information. A concept of *ensemble learning* can be useful for future CW monitoring tools, as it combines multiple algorithms or methods with a simulated democratic vote at the end to reach more precise conclusions without necessarily deploying costly neural networks [43].

7.0 CONCLUSION

Cognitive Warfare poses a problem and an imminent threat to the human brain. However, with how reliant CW is on cyberspace, big data, and modern technologies in general, there is a significant opportunity for defense when the very same machines used for malicious influence are used as a means of defense. I demonstrated in a recent example of Hamas' CW that without utilizing AI and ML, defending against the threat of CW will not be possible. However, as of now, there are numerous challenges ahead, with few knowns and many unknowns. These need to be continuously tackled by NATO and its allies to ensure timely reactions to adversarial operations.

However, what also needs to be considered is the nature of the threat – CW is inseparable from contemporary society, and addressing it is not a matter of constructing a "Cognitive Maginot Line" – a whole-of-society approach is needed instead [24]. One can even liken CW to a virus, similar to the approach of Filipec in regard to disinformation [45]. In line with this argument, it could be argued that CW cannot be

rooted out entirely from any society by any known measures. The defense needs to be based on a long-term and continuous defensive fight to ensure minimal impact of CW on societies and – in the case of NATO and its allies – democracy itself.

8.0 REFERENCES

[1] A. Ackerman, "What We Know About the Gaza Hospital Blast." The Wall Street Journal, [Online]. Available: https://www.wsj.com/world/middle-east/what-we-know-about-the-gaza-hospital-blast-b238a40d

[2] M. Biesecker, "AP visual analysis: Rocket from Gaza appeared to go astray, likely caused deadly hospital explosion." AP News, 2023, [Online]. Available: https://apnews.com/article/israel-palestinians-hamas-war-hospital-rocket-gaza-e0fa550faa4678f024797b72132452e3

[3] S. Jones, "Angry protests flare up across Middle East after Gaza hospital blast." The Guardian, 2023, [Online]. Available: https://www.theguardian.com/world/2023/oct/18/gaza-hospital-al-ahli-al-arabi-blast-explosion-protests-demonstrations-middle-east

[4] P. Linebarger, Psychological Warfare. Washington, DC: Infantry Journal Press, 1948.

[5] H. M. Baus and W. B. Ross, Politics Battle Plan. 1968.

[6] O. Oyen and M. L. De Fleur, "The spatial diffusion of an airborne leaflet message," Am. J. Sociol., vol. 59, no. 2, pp. 144–149, 1953.

[7] D. Lerner, Sykewar: Psychological Warfare Against Germany, D-Day to VE-Day. GW Stewart, 1949.

[8] J. Ellul, The Technological Society. Vintage, 1964.

[9] J. Ellul, Propaganda: The Formation of Men's Attitudes. Vintage, 1973.

[10] P. Taylor, "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025." Statista, 2023, [Online]. Available: https://www.statista.com/statistics/871513/worldwide-data-created/

[11] C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval, Internet and surveillance: The challenges of Web 2.0 and social media, vol. 16. Routledge New York, 2012.

[12] A. Wanless and M. Berk, "The audience is the amplifier: Participatory propaganda," in The Sage handbook of propaganda, P. Baines, N. O'Shaughnessy, and N. Snow, Eds. Sage, 2019, pp. 85–104.

[13] N. Newman, R. Fletcher, K. Eddy, C. T. Robertson, and R. K. Nielsen, "Reuters Institute digital news report 2023," Reuters Inst. study Journal., 2023, [Online]. Available: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf

[14] C. Montag and S. Diefenbach, "Towards homo digitalis: important research issues for psychology and the neurosciences at the dawn of the internet of things and the digital society," Sustainability, vol. 10, no. 2, p. 415, 2018.

[15] J. Firth et al., "The 'online brain': how the Internet may be changing our cognition.," World Psychiatry, vol. 18, no. 2, pp. 119–129, Jun. 2019. doi: 10.1002/wps.20617

[16] S. Narula, "Psychological operations (PSYOPs): A conceptual overview," Strateg. Anal., vol. 28, no. 1, pp. 177–192, 2004.

[17] Modern War Institute. MWI Video: The Brain is the Battlefield of the Future – Dr. James Giordano [video]. YouTube. Available: https://youtu.be/N02SK9yd60s?si=xT0T-kgYbxkBpYJz

[18] F. du Cluzel, "Cognitive warfare," Innov. Hub, NATO ACT, June--November, 2020, [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW Final.pdf

[19] Y. R. Masakowski and J. M. Blatny, "Mitigating and Responding to Cognitive Warfare," 2023.

[20] D. Pappalardo, "Win the war before the war?": A French perspective on cognitive warfare," War Rocks, vol. 1, 2022.

[21] L. Kayali, "EU to ban Russia's RT, Sputnik media outlets, von der Leyen says," Politico, February 27, 2022.

[22] B. Xu and E. Albert, "Media censorship in China," Counc. Foreign Relations, vol. 25, p. 243, 2014.

[23] L. Boswinkel, N. B. Finlayson, J. Michaelis, and M. Rademaker, "Weapons of mass influence," The Hague Centre for Strategic Studies, 2022. [Online]. Available: https://hcss.nl/wp-content/uploads/2022/04/Weapons-of-Mass-Influence-Information-Warfare-HCSS-2022-V2.pdf

[24] R. Burda, "Cognitive Warfare as Part of Society," The Hague Centre for Strategic Studies. The Hague Centre for Strategic Studies, 2023, [Online]. Available: https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf

[25] R. Zager and J. Zager, "OODA loops in cyberspace: A new cyber-defense model," Small Wars J., vol. 20, no. 11, 2017.

[26] T. N. Brooks, "Survey of automated vulnerability detection and exploit generation techniques in cyber reasoning systems," in Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2, 2019, pp. 1083–1102.

[27] G. F. Treverton, Addressing" Complexities" in Homeland Security. Center for Asymmetric Threat Studies (CATS), National Defence College, 2009.

[28] A. Martínez, E. Bubola, and M. Pronczuk, "What We Know About the Hamas Attack and Israel's Response." The New York Times, 2023, [Online]. Available: https://www.nytimes.com/article/israel-gaza-hamas-what-we-know.html

[29] M. Biesecker, "AP visual analysis: Rocket from Gaza appeared to go astray, likely caused deadly hospital explosion." AP News, 2023, [Online]. Available: https://apnews.com/article/israel-palestinians-hamas-war-hospital-rocket-gaza-e0fa550faa4678f024797b72132452e3

[30] M. Berg, "NYT admits error in Gaza hospital report." Politico, 2023, [Online]. Available: https://www.politico.com/news/2023/10/23/gaza-hospital-new-york-times-00122986

[31] A. H. Cordesman, "The Hospital Attack and the Gaza War." Center for Strategic & International Studies, 2023, [Online]. Available: https://www.csis.org/analysis/hospital-attack-and-gaza-war

[32] Israel Defence Forces, "Gaza Hospital Blast: Initial IDF Al-Ahli Report." [Online]. Available: https://www.idf.il/en/mini-sites/hamas-israel-war-articles-videos-and-more/al-ahli-al-ma-amadani-hospital-initial-idf-aftermath-report-october-18-2023/

[33] P. M. Salmon, G. H. Walker, and N. A. Stanton, "Pilot error versus sociotechnical systems failure: a distributed situation awareness analysis of Air France 447," Theor. Issues Ergon. Sci., vol. 17, no. 1, pp. 64–79, 2016.

[34] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities," IEEE Trans. Dependable Secur. Comput., vol. 11, no. 1, pp. 30–44, 2013.

[35] J. Raitasalo, "Getting a Grip on the So-Called 'Hybrid Warfare,'" ASPJ Africa Francoph., vol. 8, no. 3, pp. 20–39, 2017.

[36] M. Aljabri, R. Zagrouba, A. Shaahid, F. Alnasser, A. Saleh, and D. M. Alomari, "Machine learning-based social media bot detection: A comprehensive literature review," Soc. Netw. Anal. Min., vol. 13, no. 1, p. 20, 2023.

[37] M. C. Horowitz, S. E. Kreps, and M. Fuhrmann, "Separating fact from fiction in the debate over drone proliferation," Int. Secur., vol. 41, no. 2, pp. 7–42, 2016.

[38] The Economist, "Russian tanks in Ukraine are sprouting cages." The Economist, 2022, [Online]. Available: https://www.economist.com/science-and-technology/russian-tanks-in-ukraine-are-sprouting-cages/21808191.

[39] O. Yaron, "Hamas Drone Assault Surprised Israel, Using Russia-Ukraine War Tactics." Haaretz, 2023, [Online]. Available: https://www.haaretz.com/israel-news/security-aviation/2023-10-09/ty-article/.premium/hamas-drone-assault-surprised-israel-using-russia-ukraine-war-tactics/0000018b-155d-d2fc-a59f-d55d05eb0000.

[40] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.

[41] X. Zhou and R. Zafarani, "Fake news: A survey of research, detection methods, and opportunities," arXiv Prepr. arXiv1812.00315, vol. 2, 2018.

[42] J. Kim and M. Hastak, "Social network analysis: Characteristics of online social networks after a disaster," Int. J. Inf. Manage., vol. 38, no. 1, pp. 86–96, 2018.

[43] I. D. Mienye and Y. Sun, "A survey of ensemble learning: Concepts, algorithms, applications, and prospects," IEEE Access, vol. 10, pp. 99129–99149, 2022.

[44] M. Lewis, "Quantum computing and cognitive simulation," in Quantum Computing in the Arts and Humanities: An Introduction to Core Concepts, Theory and Applications, Springer, 2022, pp. 53–105.

[45] O. Filipec, "Towards a disinformation resilient society?: The experience of the Czech republic," Cosmop. Civ. Soc. an Interdiscip. J., vol. 11, no. 1, pp. 1–26, 2019.