FALL 2020 COGNITIVE WARFARE

AN ATTACK ON TRUTH AND THOUGHT

NATO OTAN

Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, Olivia Madreperla

JOHNS HOPKINS UNIVERSITY

Table of Contents

Executive Summary

Warfare has shifted dramatically over the past several decades, moving away from the physical threats of conventional warfare. War now moves towards the social and ideological threats brought about by mass media and advances in technology. The advent of this new type of warfare is different from anything we have seen before. Although it takes elements from previous types of hybrid warfare, the reach and level of impact it possesses make it far more dangerous than its predecessors. We have dubbed this new way of war *cognitive warfar*e.

Cognitive warfare, although sharing various similarities to other non-conventional and non-kinetic types of warfare/operations, is ultimately unique in its execution and purpose. In this paper, we examine the origins of non-kinetic warfare by first looking at the Cold War and the use of psychological operations (PsyOps). We follow the evolution of warfare, noting that advancements in technology gave rise to electronic warfare and subsequently cyber warfare. As cyber capabilities continued to develop, intelligence became a growing field and information warfare started to develop. Cognitive warfare, however, goes a step further than just fighting to control the flow of information. Rather, it is the fight to control or alter the way people *react* to information. Cognitive warfare seeks to make enemies destroy themselves from the inside out. We define cognitive warfare as the weaponization of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions.

Destabilization and influence are the fundamental goals of cognitive warfare. These goals work towards the purpose of sowing discontent within a society or encouraging particular beliefs and actions. The 2016 Democratic National Convention (DNC) leaks are a good example of a foreign power exploiting divisions to destabilize a society. Terrorist groups like Al-Qaeda demonstrate how civilians can be influenced and recruited by radical ideologies. Never before has such insidious manipulation been as easy to accomplish as today. Advances in connectivity, digitization, neurology, and psychology have provided society with a great many boons. Yet,

with every new opportunity, a new threat emerges. Today we are faced with the problems that come with social media's ability to broadcast information to billions of willing people in a matter of minutes. We must defend against algorithms that can identify who would be the most susceptible to posted material, and who is most willing to spread it. The present-day ability to fake and manipulate information is unprecedented, and recent advancements in artificial intelligence have now made video and audio suspect as well. People are unsure of what to believe, not even sparing governmental institutions from this lack of faith. Simultaneously, we are revolutionizing what we know about how our brains and emotions function as individuals experiment with different forms of control.

Therefore, it is our belief that NATO must adapt quickly and forcefully to defend against current threats in the sphere of cognitive warfare and work to curtail future threats. While democratic society is both complicated and amazing, it is also vulnerable. To get ahead of these threats, NATO must respond defensively in three ways. First, NATO must work to develop a working definition or framework for cognitive acts of war. This includes a set of criteria for discovering cognitive attacks as they are taking place. Second, the alliance must assess vulnerabilities to cognitive attacks at a national and personal level in hopes of creating and inspiring a more resilient population. Third, NATO must establish organizations to liaise with tech companies and handle the challenges of the future of warfare. An additional final consideration would be an analysis of potential hostile states onto whom we may use cognitive warfare against in an offensive strategy or as deterrent.

The foundation for democracy lies not only in laws and civil order, but also in trust and mutual respect: the trust that we will follow those laws, respect civil institutions, and respect each other and our differing opinions. Trust is now at risk, truth is being attacked, and democracy is being threatened. The time to prepare is now, and the whole world is watching.

Introduction

People have attempted to influence public opinion since the rise of civilization. It is an essential component of the political structures into which we have evolved. However, the *weaponization* of public opinion is a novel, threatening development in how we interact. The advent of the internet and mass media have made possible the large scale manipulation of populations via targeted, accessible, multimodal messaging, which can now exist under the guise of anonymity. In a sea of a billion voices, pinpointing individual sources has become incredibly difficult [1]. An effort that, in some ways, is comparable to the difficulty of identifying who screamed "Fire!" in a crowd. Some will argue that this is intended, contending that anonymity is required for the resources the internet provides. Others, however, fret about the unintended consequences that this lack of accountability might bring about in the long-term [2].

No matter which perspective is correct, it is our opinion that NATO must be aware of the threat that our interconnectedness has wrought. Tactics targeting the public will not fade with time; they will become more efficient. They will aim at broader audiences. Moreover, they will become increasingly convincing. Already, technological advancements have showcased their ability to do exactly this. One does not have to look further than the 2016 DNC information leaks to confirm the rapidity with which information is acquired and spread to the advantage of an opposing party.

Social media, news networks, automation algorithms, artificial intelligence, mental health guidance, and, perhaps, even our own physiology are expected to evolve rapidly in the near future. All of these are working to make us more connected, more data-driven, and more curious. It will be an exciting new era of human interaction. However, the roads in our minds are not one-way streets. Whilst people receive information, they are simultaneously giving away information and data. As it stands, simple lines of codes will one day be able to identify and describe everything about us. Our habits, our friends, our faiths, our cultures, our preferences, and even our vices. For the first time, war will not deal with exposed bodies. It will deal with exposed minds instead. It is this new avenue of war we have dubbed cognitive warfare.

Evolution of Non-Kinetic Warfare

Origins

It starts, as with most things in the nature of modern war, in the Cold War. Mutually assured destruction (MAD) became the accepted global doctrine, rendering total war on the scale of WWII improbable. Proxy warfare became a dinnertime discussion. Subversion and espionage are prevalent in daily international interactions and "plausible deniability" is the term of the time. Thus, the CIA and FBI have expanded far beyond their initial capabilities, and actions in the shadows have become the norm [3]. These new methods have become the "civilized" approach to conflict, clearly better than the "barbarities" of a nuclear holocaust. It is also here where the power of *words* and *ideas*, and *non-kinetic war*, is finally seen in full force. Millions, or even billions, witnessed this when the Soviet Union watched the collapse of the Iron Curtain, unable to fulfill its goal of withstanding the power of "blue jeans and rock and roll." [4]. Democratic nations have always had a "home advantage" in utilizing the voice of the public. Able to tout their messages of individual freedoms and abundant resources, Western democracies have consistently used their words and ideas as ammunition against more authoritative regimes.

Perhaps the proof of the efficacy of such tactics lies in the reactions they have elicited from non-democratic powers. Restrictions, bans, and general censorship have long been the policy of countries such as China, Russia, and, much more drastically, North Korea. The age of the internet has only reinvigorated their concerns. Unsurprisingly, Facebook and other social media platforms face restrictions, if not outright bans, in these and similar countries worldwide [5][6][7]. However, it is these very ideals of free press and free speech that have left Democratic nations vulnerable to powers attempting to control public thought. These nations have been forced to go on the defensive as the protection of resources and individual freedoms no longer hold the same persuasiveness they once did. The global economy has seen both the US and China prosper [8]. The most important change since the Cold War, however, has been the shift in how we communicate and share ideas. We seek to illustrate this change by recounting past shifts

in the way that people have fought over minds and information, concluding with a new era and avenue of war.

Psychological Warfare (PsyOps)

In the United States, PsyOps specifically relates to the use of white, gray, and black products produced by various branches of the military and the CIA or its predecessors. White products are officially identifiable as being sourced from the US, gray products have an ambiguous source element, and black products are meant to seem as if they originate from a hostile source. Operations include the likes of propaganda radio, providing insubordination manuals to the militia, and even encouraging child soldiers to defect to avoid conflict [9][10].

In comparison to cognitive warfare, there are quite a few key differences. First, cognitive warfare deals mostly with gray products. White and black products are either too transparent or too risky to be reliable methods of affecting public opinion. Additionally, there is a certain element of deniability inherent to cognitive warfare that is lost in white products and endangered by black products. Moreover, PsyOps has rarely dealt with large sections of the public in the past. There is an emphasis on military or subversive activity in PsyOps that is not usually the goal of cognitive warfare tactics, which tend to target civilian social infrastructure and governments [9].

Electronic Warfare (EW)

EW is defined by the use of the electromagnetic spectrum to attack the enemy, impede enemy attacks, or identify and scout for specific assets. In some ways, electronic warfare was the precursor to cyberwarfare. Its origins date back to the 1900s with the invention of early wireless communication. Infrared homing, radio communications, and the increasing use of wireless technologies make this an important logistic division inside the armed forces. However, this field deals heavily with instrumentation and tactical advantages. This does not deal with public opinion or even interact heavily with the civilian space outside of impeding household electricity and radio [11][12].

Cyberwarfare

Cyberwarfare is defined as the use of cyberattacks with the intention of causing harm to a nation's assets. Cyberwarfare, and its military classification, is still highly debated [13]. Nevertheless, numerous NATO member states and other countries have invested in developing cyber capabilities, both offensive and defensive [14][15]. Some worry about defining such actions as war because they "only" target computers. However, the global trend towards digitization and the Internet of Things (IoT) has meant that more functions are controlled now by computers than many would imagine. Everything from construction equipment, to financial institutions, to civilian infrastructure, and even to military installations now depend on a complex computer network [16]. The loss of such computer assets can, and already has, cost massive damages not just in terms of time and data loss but in physical damage that can be measured in dollars and lives [17].

Cyberwarfare's relation to cognitive warfare is mostly that they share an avenue of operations. There have been instances of computer viruses spreading themselves through social media by targeting the friends and/or contacts of the afflicted individual. However, these instances are better described as cybercrimes rather than targeted attempts of cyberwarfare. Cognitive warfare utilizes social media networks in a completely different way. Instead of spreading malicious software, agents of cognitive warfare spread malevolent information. Utilizing similar tactics to those used in DDoS attacks, namely botnets, cognitive warfare agents can spread an overwhelming amount of false or misleading information through accounts that look and interact in a human fashion [18]. However, this is only one tactic employed in cognitive warfare and is largely where the similarities with cyberwarfare end.

Information Warfare

Information warfare is the most related, and, thus, the most conflated, type of warfare to cognitive warfare. However, there are key distinctions that make cognitive warfare unique enough to address under its own jurisdiction. As former US Navy Commander Stuart Green described it, "Information operations, the closest existing American doctrinal concept for

cognitive warfare, consists of five 'corps capabilities', or elements. These include electronic warfare, computer network operations, PsyOps, military deception, and operational security." [19]. Succinctly, information warfare works to control the flow of information.

The main distinction between information warfare and cognitive warfare is that the former does not draw a distinction between battlefield tactical information and information aimed toward the public. For example, information warfare deals with DDoS attacks and ghost armies while neither of these falls into the purview of cognitive warfare. Perhaps a sharper delineation is that information warfare seeks to control pure information in all forms and cognitive warfare seeks to control how individuals and populations *react* to presented information [20].

Cognitive Warfare

A recent definition, from December 2019, provided by Oliver Backes and Andrew Swab, of Harvard's Belfer Center defined cognitive warfare thusly: "Cognitive Warfare is a strategy that focuses on altering how a target population thinks – and through that how it acts." [21]. Despite the intentional vagueness of this definition, it serves as a more-than-suitable framework for a further examination of cognitive warfare. Our own research and analysis of past, present, and potential future use cases of the term have allowed us to further segment cognitive warfare into two operational fields. We have also come up with a quick reference list to validate whether or not something falls in the realm of cognitive warfare.

Characteristic	Psychological Warfare	Electronic Warfare	Cyber Warfare	Information Warfare	Cognitive Warfare
Use of mass trends/data			x	x	x
Deals with thoughts and behaviour	x				x
Capacity for extreme public reach			x		x
Interest in circulation of information	x	x		x	x

To summarize, cognitive warfare is the *weaponization of public opinion by an external entity*, for the purpose of **influencing** public and/or governmental policy ***or*** for the purpose of **destabilizing** governmental actions and/or institutions.

Goals of Cognitive Warfare

Cognitive warfare, at its core, can be seen as having the same goal as any type of warfare. As Carl von Clausewitz states, “War [is an] act of force to compel our enemy to do our will.” Cognitive warfare, unlike traditional domains of war, does not primarily operate on a physical plane. Therefore, it does not utilize a physical force in order to compel its enemies. However, it could also be argued that the goal of cognitive warfare is unlike any other type of warfare. Rather than “compel our enemy to do our will,” the goal is get the enemy to destroy himself from within rendering him unable to resist, deter, or deflect our goals.

In either case, the goals of cognitive warfare are achieved through different methods than the goals of conventional warfare. Cognitive warfare has two separate, but complementary, goals: destabilization and influence. While both of these goals can be accomplished separately, to successfully weaponize public opinion, they can also be jointly attained by using one as a means to the other. The targets of cognitive warfare attacks may range from whole populations to individual leaders in politics, the economy, religion, and academics. Further, the role of lesser-known social leaders must not be overlooked. So-called connectors, mavens, and salespeople can be instrumental in the application of cognitive warfare [22].

To better classify cognitive warfare attacks, Figure 1 presents a pair of axes by which events can be characterized. In the following section, we will analyze each goal individually and describe how they are intertwined, generating a new, more dangerous, more pervasive type of warfare. Then, we will detail examples of cognitive warfare battles and skirmishes that have occurred or have the potential to occur in the future. These campaigns will propel cognitive warfare to the global stage. Action must be taken, opposition campaigns created, and defensive measures implemented, to prevent the perpetrators’ success.

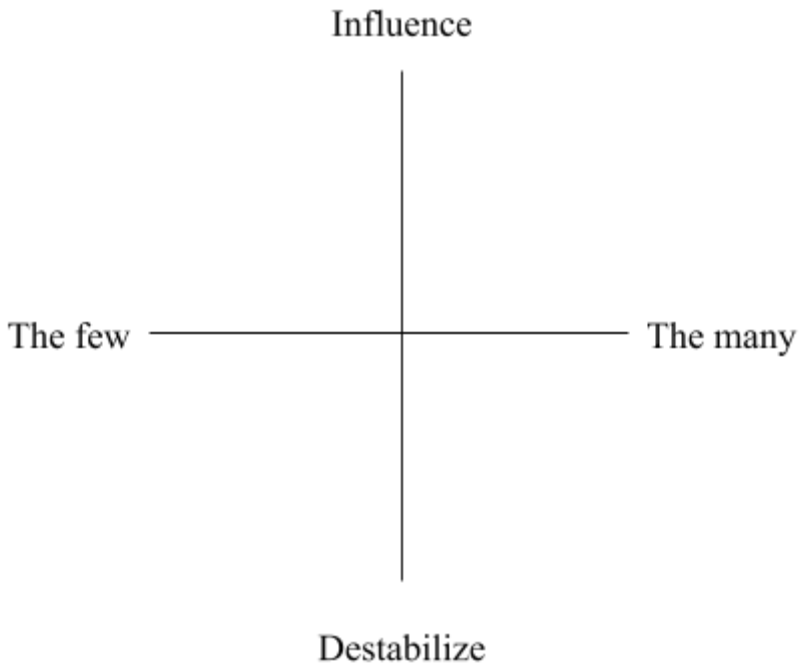

Figure 1. Pair of axes visualizing the characterization of cognitive warfare attacks

Destabilization

The first fundamental goal of cognitive warfare is to destabilize target populations. Destabilization is done by disrupting the organization and unity of a population's systems and people. This results in a drastic drop in productivity and a loss of cooperation as that population is now overwhelmed by internal issues and less focused on reaching common goals. Perpetrators disrupt the organization and unity of their target populations by accelerating pre-existing divisions within groups of the population or introducing new ideas designed to pit different groups against each other and increase polarization.

Leaders can be seen as the targets of destabilization when they become the source of polarizing ideas. Perpetrators can also target the general population of people to randomly introduce divisive ideas that play on previously held beliefs or push false narratives against groups of

people. Some strategies of cognitive warfare that align with the goals of destabilization include, but are not limited to, the following:

- Increase polarization
- Reinvigorate movements/issues
- Delegitimize government/leadership
- Isolate individuals/groups
- Disrupt key economic activities
- Disrupt infrastructure
- Confuse communication

Below are several cases showcasing examples of destabilization as a goal of cognitive warfare and the circumstances surrounding them.

Case 1: Destabilization through Confusion

Cognitive warfare campaigns may strive to destabilize populations of people by causing mass confusion. Chaos is bred when a population no longer knows what is right and who to trust. As a result, civilians may begin to lose faith in the leadership of the nation that is meant to oversee their safety and freedoms. Undermining leadership and generating chaos poses a threat to Western democracies, one of the most recent and glaring examples coming from the outbreak of and early events surrounding COVID-19.

Russia, China, and Iran took the whirlwind of confusion brought about by the virus as an opportunity to initiate a cognitive warfare campaign against the West. It is a multidirectional and multifaceted campaign meant to undermine public confidence in Western states [23]. This campaign started with the outbreak of the virus and confusion surrounding its origin, which is where we began to see cognitive warfare tools, such as disinformation and false narratives, being employed. Chinese foreign minister Lijian Zhao opened up with a barrage of questions in a tweet from early March targeted at the US asking, “When did patient zero begin in the US? How many

people are infected? What are the names of the hospitals? It might be the US Army that brought the epidemic to Wuhan" [24]. He then urged followers to read and spread a conspiracy theory from Global Research, a Canadian website, that stated the virus originated in the US Army Research Medical Research Institute of Infectious Diseases at Fort Derrick, Maryland [24]. The dissemination of these narratives with little to no concrete evidence at such early stages of the virus only functioned to sow doubt in the minds of American citizens and its allies. These tools of cognitive warfare are designed to affect the way people interpret and react to information in a way that makes them doubt their own leadership.

Russia reacted in a similarly malicious way through its government-owned news agency, Sputnik. It released propaganda in over thirty languages in line with many of the narratives coming out of China, that argued the virus originated in the U.S. or that the U.S. developed and released the virus as a bioweapon intended to weaken China's economy [24]. The constant stream of false narratives varied from somewhat plausible stories to outlandish accusations targeted at Western states and government organizations. Herein lies the danger of cognitive campaigns: it becomes increasingly difficult to differentiate between credible and non-credible stories, especially when they originate from government-backed news sites like Sputnik. The Kremlin can send out thousands of different stories with various levels of credibility and plausibility and see what sticks. This strategy quickly results in the undermining of Western governments in what the population might see as a lack of honesty towards its people regarding the virus or the inability to protect them from it.

Iran is the third major player conducting its own cognitive warfare campaign against the citizens of Western states. News stories emerging from Tehran contained themes similar to the stories coming out of Beijing and Moscow. Press TV is an English and French news network associated with the Islamic Republic of Iran Broadcasting, which released numerous pieces tying the Coronavirus outbreak to the U.S. military [24]. The commander of the Islamic Revolutionary

Guard Corps, Hossein Salami, has gone so far as to proclaim that COVID-19 is the spearhead of a U.S. biological invasion [24].

The cognitive campaigns of China, Russia, and Iran surrounding the outbreak of the Coronavirus are all targeted against Western states and contain nearly identical messaging. The danger in these campaigns is their tremendous reach and support from government leaders and institutions. Similar stories are released in dozens of languages all over the world and either come directly out of state-controlled news sites or government-supported media outlets [24]. But that is just the origin, with tens of thousands of independent sites and users spreading the same narratives to undermine the credibility of Western societies, whether intentionally or not. Americans are finding these stories over and over and encouraged to believe their government is hiding information from them. Or they are overwhelmed with stories that make them doubt the nation's ability to protect them from serious threats to their safety and personal liberties. The threat is not only in the information that is being spread but in the destabilizing reactions and beliefs of those receiving them.

Case 2: Destabilization by Sowing Division

Cognitive warfare often seeks to divide a population and increase polarization. Pre-existing divisions along political party lines may seem to be the most obvious to exploit. However, this is not always the case as cognitive campaigns can be aimed at sowing internal divisions within a group. We see a strong example of this in the case of the 2016 DNC email leaks.

Russia had been training its cyber capabilities for several decades, experimenting on countries in Europe, such as Ukraine, to test its impact in elections. As the director of the National Security Organization and commander of US Cyber Command, Adm. Michael Rogers stated, "this was not something that was done by chance, this was not a target that was selected purely arbitrarily. This was a conscious effort by a nation-state to achieve a specific effect" [25]. And it did have a profound effect on the DNC and the Democratic party at large.

In April of 2016, Russian cyber units gained access to the DNC's internal servers, allowing them to steal confidential emails and documents. Several months later, these communications were leaked on WikiLeaks. It was at this point that the operation turned from typical espionage to political sabotage. Campaigns were being uprooted and division began to grow within the party. It was revealed that the DNC was favoring Hillary Clinton in the time leading up to the selection of an official presidential candidate. This turned progressive Democrats and moderate Democrats against each other. The rift within the democratic party resulted in a shift in the candidates' support. Instead of focusing on the Russian attack itself, political figures were much more concerned with the content and what it might mean for their careers [26]. Voters began shifting due to the issues brought out by these new documents and released statements of discontent. Hillary Clinton's campaign admitted that this attack had a significant effect on the outcome of the overall election [23]. And this is not to say there wasn't a further polarizing impact along party lines as well. President Trump's campaign turned towards the content of the hacks as well, rather than the Russian attack itself. In a time when the country could not afford to react in a partisan way, the two major parties turned on each other and themselves, resulting in one of the most polarized stages in American politics.

The Russian attack goes far beyond an act of cyberwarfare. The cyber capabilities and lack of appropriate security were merely the tools and opportunities that made the attack possible. The attack itself, however, was aimed at a much larger end, one accomplished with flying colors. American politics were thrown into disarray and Russia now has influence in two of the most important institutions in American democracy: elections and independent media [25]. The divisions created and escalated by this event destabilized politics and the election process. Unfortunately, the media was nothing but excited to cover the content that was being released, with WikiLeaks being the most searched political term for the month of October in 2016 [25]. This was precisely the reaction that Russia had hoped for. Their cognitive campaign was perfectly targeted at exploiting the divisions of American politics and resulted in a state of blame and uncertainty.

Case 3: Destabilization as a Means to Influence

Perpetrators of cognitive warfare may cause destabilization in order to influence members of a population, convincing them that their government cannot provide for them. Historically, economic power has always been a significant source of leverage for nations seeking to extort struggling nations. Such economic superiority can be exploited through the use of sanctions. Per the Destabilization and Insensitivity of Sanction theory, sanctions are the "manipulation of economic relations for political objectives designed to threaten or execute economic punishment in order to coerce a society to change its policy or its government." There are two types of sanctions according to this theory: coercive and manipulative. In this case, we will further examine manipulative sanctions directed at the society of a target country. The goal of such sanctions is to "alienate the public from the leaders to such a degree that the latter lose their powerful positions." The result is a change in policy or government as a result of a burdened population. Instances in the recent past involving the sanctioning of other states have been attributed to the destabilization of not only a nation's economy but their social and political situation as well [27].

Take for example, the Allende regime in Chile. American public opinion was against an overt use of force against the Chilean government. It was quickly decided that the best way to overthrow the Chilean government would be to place the blame of a deteriorating nation on inferior socialist policy. The American government took a two-pronged approach to destabilizing the government in Chile by attacking both the Chilean economy and society. The economic onslaught involved a multitude of factors. The American government terminated all private American investments, new and old. Additionally, the American government used their unprecedented power on the world stage to keep international financial institutions from funding any Chilean operations. This had a critical effect on Chilean life as Chile's primary industry, copper, was dominated by American multinational corporations [27].

While these changes did have a detrimental effect on the Chilean economy, a major economic downturn cannot destabilize a nation's standing on its own. Take Cuba, for example. The US implemented a similarly stringent economic policy to combat Castro and his socialist regime. However, simply leveraging economic dependence is not enough to destabilize an entire government, as proven by Cuba's persistence through America's economic endeavors. Cubans at the time were accustomed to slim resources and repressive economic policy. Contrastingly, Chile had a well-established middle class that depended upon a consumer culture to maintain their standard of living. Allende recognized the standards of the middle class as well as their dependence on the United States in far more areas than simply economics and attempted to cater to the requests of the middle class. However, he soon found it difficult to maintain the middle class' standards due to American economic retaliation, and the standard of living plummeted. Soon, the Chilean people were convinced their current government was not competent in the leadership of their country. Thus, the demise of the Chilean government was not the result of economic pressure placed by the United States, but rather the social implications of the subsequent economic decline[27].

Essentially, the United States destabilized an economic system in order to influence a population to believe their government could not provide them the same opportunity. As a result of such influence, the Chilean government was overthrown by a capitalist regime without blame ever being turned on American officials. By implementing damaging economic policy, America changed the thought processes of an entire population while barely lifting a finger. The sanctions created doubt, the doubt festered within the Chilean people, and the doubt turned to retaliation. It is this silent sewing of distrust, through manipulation and the weaponization of public opinion, that defines cognitive warfare.

In addition to portraying the effects of destabilization as a means of influence, this case also highlights the necessity of understanding the ins and outs of the target population. Without a full understanding of the quarry in question, it is impossible to enact an effective attack. Although a similar strategy was used against Cuba, it didn't have the desired effect because the US did not

take the lack of the middle class into account. Offensively, it is essential to understand your target. Defensively, it is necessary to know how your population might be exploited.

With the advent of the internet, a perpetrator's ability to understand a population has only grown stronger. With a few clicks, someone can find all there is to know about a place and its people. This unlimited access will result in similar threats occurring on an even larger scale. When Nixon enacted this economic policy, he didn't have access to the information that would tell him that it would function in Chile but not Cuba. Now, with extensive historical data bases, internet search engines, and, most importantly, hackers, information about any target population can be easily obtained and exploited. For example, if the United States wanted to target a nation similar to Chile, it would prove effortless to gather intel on the size of the middle class and whether it was large enough to ensure an effective rebellion. Before the internet, the only way to know would have been to travel to Chile and experience the culture which would have looked suspicious from the start. Now, a US intelligence representative can simply run a search on Chile's economic demographic distribution, and they will have the information they need to conduct an effective attack.

Influence

The second fundamental goal of cognitive warfare is to influence target populations. The goal to influence is accomplished by manipulating a target's interpretation and understanding of the world around them. Perpetrators can subsequently guide their target's actions in a way that benefits the perpetrator's cause. The goal to influence differs from the goal of destabilization in that the ultimate intent is for a target group to be like-minded about an issue. At their greatest potential, perpetrators aim to generate consensus among a population with enough power to effect a paradigm shift, turning their targets against the fundamental ideas they were raised on.

To influence how entire populations or segments of populations think, perpetrators may target political, economic, academic, or social leaders as vectors to reach a greater audience. Alternatively, perpetrators may simply release information, casting a wide net in hopes of

reaching enough people to provoke change. Situations where cognitive warfare techniques may be used to influence include, but are not limited to, the following:

- Promote extremist ideologies
- Manipulate civilian beliefs
- Control key economic activities
- Regulate government actions
- Sway or delegitimize elections
- Recruit civilians to marginal groups
- Quell dissent

Below are several cases demonstrating how cognitive warfare may be waged to influence populations and the conditions surrounding each case.

Case 1: Influencing to Recruit

Cognitive warfare campaigns may be launched for the purpose of recruiting civilians to a cause, as may be seen in the case of terrorist groups. The concept of an "ideological engine" describes a cognitive warfare strategy in which "abstract, motivating factors converge to produce violent ideologies" [21]. This model has been used by the terrorist group Al-Qaeda in the Middle East. The model is propelled by so-called "identity entrepreneurs": social leaders who don't necessarily have great influence in political or economic institutions but are able to empathize and connect with ordinary members of their target society. Identity entrepreneurs are able to recruit civilians to extremist ideologies by presenting a narrative in which constituents are designated as protagonists who will improve society. These leaders may target civilians in poor living conditions, convincing them that they are not alone, they are not to blame for their poverty, and that there is a tangible oppressor to blame. In the case of Al-Qaeda, the selected narrative told the story of Islam's fall from greatness and deemed recruits to be the ones who would restore their land to its original prosperity. Consistent with most other cognitive warfare strategies, the ideological engine is most effective when it is fueled by *pre-existing* sentiments against the perceived oppressor.

Identity entrepreneurs lay the groundwork for violent actors, setting the stage for an attack on the identified oppressor. Strategically, the terrorists select the target of the violent attack to be an institution likely to overreact and use excessive force in retaliation. Such a reaction allows the insurgents to frame the perceived oppressor in a negative light, justify their cause to civilians, force polarization, and morally isolate the perceived oppressor. Al-Qaeda accomplished this step by provoking the US through violent acts such as bombings of US embassies and the September 11 attacks. Hence followed a decades-long "war on terror" that has resulted in significant civilian casualties, providing insurgents with an opportunity to vilify the West.

In the final stages of such campaigns, the terrorists shift the framing of their struggle to the context of national, cultural, or religious duty. Thus, an individual's failure to join the resistance against the perceived oppressor is viewed as a betrayal of societal values. Societies continue to fight not for material benefit, as they may have initially done, but to defend an ideology. Once the ideological engine reaches this stage, constituents have been successfully indoctrinated into the identity entrepreneurs' ideology.

As technologies advance and the internet's reach grows, the ideological engine will only grow stronger. The interconnectedness of societies will allow terrorist organizations to create global networks and expand beyond national borders. As stated by Stuart Green, founder of the ideological engine model, "Insurgent campaigns have shifted from military campaigns supported by information operations to strategic communications campaigns supported by guerilla and terrorist operations" [19]. In this new era of warfare, the physical plane is no longer the dominant domain by which perpetrators compel their targets to act according to their will. Instead, physical violence is used to prop ideologies and support battles in the latest domain for war: the minds of every target.

Case 2: Influencing Policy Enactment

Cognitive warfare methods have great potential to be used in influencing policy. An ambitious nation, seeking to grow its influence globally would benefit from a world superpower, such as the US, adopting an isolationist foreign policy. For example, in recent months, China has pursued an expansionist foreign policy, as demonstrated in its hostility at the China-India border and in the South-China Sea [28]. In order to act more aggressively without retaliation, a perpetrator sponsored by China could target the general public of the US with the goal of manipulating civilians to pressure their elected representatives to turn their focus inwards and reduce foreign engagement.

This type of interference in another country's politics would require the target to be the public rather than politicians because, although politicians have power, civilians must approve of their representatives' actions. As previously established, the goal of cognitive warfare is to change how targets perceive reality. Even if politicians were coerced into passing legislation or making decisions to benefit a foreign power, there would be public uproar in any functioning representative democracy if civilians did not believe in such a cause. Such a campaign would be particularly insidious as the perpetrator would be bypassing international organizations and typical diplomatic communications, targeting citizens directly.

For this type of cognitive warfare campaign to succeed, there must be pre-existing isolationist sentiments to exploit. A cognitive warfare attack would be more effective if, for example, the target nation had a history of failed foreign policy or a recent national embarrassment on the global stage. Emphasis is placed on this condition as cognitive warfare capitalizes and thrives on existing biases and views. It is significantly more difficult for a perpetrator to plant a seed of an idea in millions of heads than it is to cultivate and grow deep-rooted sentiments. Although China, Iran, and other regional powers may not have cognitive warfare capabilities and resources like Russia's, it is likely that they are developing them. It would be dangerous to underestimate other nations as contenders in the cognitive domain.

Case 3: Influencing as a Means to Destabilize

Influence may be used as a means of destabilization when certain population sectors are encouraged or coerced to take on and promote specific views, particularly against those of other groups within the population. A prominent example of cognitive warfare is that of Russian interference in foreign elections. Such attacks are part of a larger campaign to diminish trust in democratic nations globally, weakening the West. First occurring in the Baltic states—Estonia, Latvia, and Lithuania—there have since been accusations and warnings of Russia extending its efforts to Western powers such as the United States, the United Kingdom, and Germany. Russia's ultimate goal is assumed to be the incapacitation of its adversaries, allowing it to extend its global reach. By distracting and polarizing the public on the homefront of Western superpowers, Western states are forced to turn inwards to remediate the disarray produced by accusations of foreign interference or collusion in their elections. With their attention elsewhere, such states may lose authority on the global stage or be rendered unable to defend themselves or their allies from Russian aggression. To accomplish such a goal, Moscow must convince the people of democratic nations that their governments and election systems are untrustworthy and illegitimate. Thus, destabilizing by means of influence.

The Baltic states were particularly vulnerable to Russia's cognitive warfare efforts due to several factors. Estonia, Latvia, and Lithuania are unique due to their geographic proximity to Russia, historical ties to the nation, Russian ethnic populations, and residents' access to Russian state-controlled media. Taking advantage of these factors, Russia has launched information operations against the Baltic states since their independence was restored in the 1990s. Moscow concentrated on times of vulnerability, particularly elections, during which Russian media sources espoused three messages: Baltic governments were fascist and Nazi sympathizers; Baltic governments were ineffective at governance; and Baltic states were discriminatory towards ethnic Russians [21]. Such framing turned significant populations of ethnic Russians living in the Baltic states against other citizens. Utilizing Russian state-sponsored media and Russian trolls on social media, Moscow has been able to disseminate disinformation, inflammatory information,

and propaganda. By capitalizing on existing biases, Moscow has exacerbated tensions and further polarized the general publics of Estonia, Latvia, and Lithuania. Although Western nations do not have the same conditions and vulnerabilities as the Baltic states, they have vulnerabilities, nonetheless. With experience exploiting foreign divisions to influence how citizens think—and vote—Russia would be able to use similarly insidious tactics against Western nations.

Considering the definition of cognitive warfare, we have put forth, Russia's actions meet the conditions of such an attack. The perpetrator is identified to be the Russian government and the target to be the general American public. This case is classified as destabilization by means of influence because Moscow is attempting to convince people not of certain political opinions, but of two divisive notions: fellow citizens of an opposing political party are dangerous and election integrity cannot be guaranteed. Such sentiments have experienced an upsurge in recent years. Voters on both sides of the political spectrum have become increasingly polarized, perpetuating an "us vs. them" mentality. There already exist both Democrats and Republicans who believe the other party betrays the ideals of the nation. Russian internet trolls and bots have only widened the chasm.

The concept of Democrats and Republicans becoming increasingly polarized has been termed "tribalism" [29]. Voters have begun treating politics like a team sport, prioritizing party loyalty over policy. Voters are more prone to escalate disagreements into arguments and circulate the belief that any idea not beneficial to one's party must be an attack on them. Russia is believed to have exploited these divisions between Democrats and Republicans in the past.

In the 2016 election, Moscow waged its most ambitious cognitive warfare attack yet. The Kremlin's interference in the 2016 election was complex and insidious, targeting multiple aspects of American politics, as seen in *Case 2* of *Destabilization*. As aforementioned, American intelligence agencies determined that Russian president Vladimir Putin had ordered private emails from the Clinton campaign to be leaked and social media bots to be created to propagate extremist views and divisive news. After nearly three years, on August 18, 2020, the US Senate

released a report stating, “the Committee found that the Russian government engaged in an aggressive, multifaceted effort to influence, or attempt to influence, the outcome of the 2016 presidential election” [30]

There were three main factors that contributed to this attack’s success. First, then-Republican-nominee Donald Trump did not condemn Putin when asked for his thoughts on the possibility of Russian interference in the 2016 election. Prior to Trump, mainstream American politicians had consistently and definitively deemed Russia a threat to America. Conversely, Trump emphasized the content of the leaked documents from the Democratic National Convention over the fact that an American political institution had been attacked by a foreign power. Second, Moscow had access to the leaked emails prior to Hillary Clinton’s nomination as the Democratic candidate. Had a different candidate been nominated, the leaks may not have been as effective. Third, President Obama, a Democrat, had been hesitant to reveal the intelligence or strike back without Republican endorsement. The Obama administration was concerned that releasing such intelligence to the public shortly before the election would seem partisan, as if it was trying to manipulate the election themselves. Thus, the conditions of the 2016 presidential election created the perfect storm for a calculated cognitive warfare attack to instate an American president not adamantly opposed to Russian interference, generate a chaotic distraction within the political scene, and divide Americans along partisan lines.

To underscore the gravity of this situation: investigations have proven that the Kremlin ordered a cyberattack on an American political organization to steal internal documents and communications with the intention of using them to weaponize public opinion against that organization’s party. In the preceding months before a major presidential election, the Kremlin went on to leak the stolen documents to the public, providing a divisive talking point and sowing doubt in the minds of Americans regarding the integrity of their political institutions. Furthermore, Russia undertook efforts to spread divisive rhetoric, buying ads on social media platforms, creating social media accounts, and crafting narratives to polarize voters. Moscow has found a method of exploiting the very basis of a functioning democracy: the discourse between a

diverse range of opinions. New technologies have made this campaign possible as armies of Russian internet trolls inflame voters on both sides of the political spectrum, battalions of Russian bots broadcast disinformation and inflammatory news, and legions of Russian hackers obtain and release damning material.

Future Threats

Looking Ahead

Thus far, we have described a few instances of when Western nations and institutions have come under cognitive attack. Cognitive warfare is dangerous in its current form, but the true threat lies in its future potential. Neuroscience, psychology, and sociology are in their infancies in the grand scheme of human innovation. All of these sciences have benefitted from advancements in computational power and the ability to simulate large numbers of connections and scenarios. Sociology has particularly faced a revolution in the advent of social media. Social media itself has proven to be extremely adaptable and rapid in its evolution. The past ten years have seen the rise and fall of over five different social media platforms each with hundreds of millions, if not billions, of users. As scientists get closer and closer to truly understanding how we think, how we interact with each other, how we get motivated, and ultimately who we are as humans, we become increasingly vulnerable to those seeking to exploit these insights.

Furthermore, we have provided evidence that NATO's adversaries are more than willing and able to employ these methods. They have also showcased that they have the capability to leverage these resources and advancements. Ultimately, we believe it will not be non-state actors that lead cognitive warfare campaigns, but state actors. While non-state actors may be able to use cognitive warfare techniques, they do not have the resources to sustain a campaign that may last generations. An example of such a campaign was described by Soviet defector Yuri Besmenov in a 1984 interview, who stated that ideological subversion is the process of "[changing] the perception of reality of every American that—despite the abundance of information—no one is able to come to sensible conclusions in the interest of defending themselves, their families, their community, and their country" [31]. Bezmenov went on to detail how the first stage of ideological subversion—demoralization—takes 15 to 20 years to complete. These decades-long campaigns could now be shortened to a few years due to advances in social technology. They

have become easier to plan, execute, and conceal. If NATO plans to preserve reality itself, it must prepare and retaliate against perpetrators of cognitive warfare.

One needs to think no further than the 2020 American presidential election to see the potential for disaster. In the months leading up to the election, there have already been internal accusations from both sides of the aisle as to the legitimacy of the upcoming election.

Current President Donald Trump has expressed his worry that the mail-in voter system, championed by the Democratic party, might cause "election rigging." When asked if he would respect the results of 2020 elections in the case he lost, he responded with "I have to see. No, I'm not going to just say yes. I'm not going to say no," stating the above concerns as a reason for his trepidation [32]. Outcry over these statements, led by the Democratic party, have accused him of attempting to undermine the democratic process.

On the other side, Democrats, both public and officials, have criticized the American electoral process that led to Trump's election as president in 2016. Specifically, this criticism has been levied at the electoral college, which gave Trump the presidency despite his loss in the popular vote. These criticisms have provoked Republican party members, who argue for the value of the electoral college in the American election system and the power it affords smaller states.

Regardless of which party's nominee is elected, the defeated nominee's party can utilize this confusion and distrust to call the validity of the voting process into question. It is these pre-existing divisions Moscow can exploit. In circulating disinformation and fanning the flames of America's political divide, Russia has provided each party with ammunition and they are likely to use it.

Already, major technology companies, such as Facebook, have identified "highly-sophisticated" Russian and Iranian election interference operations. On October 21, 2019, Facebook announced that it had removed four "networks of accounts, Pages, and Groups" from the social media

platform, having identified three to be of Iranian origins and one of Russian origin. Inauthentic users in these networks masquerade as locals in the areas they are targeting and spread disinformation and propaganda [33]. As the election quickly approaches, these efforts will be expanded. To further defend against cognitive warfare efforts, information security must be strengthened, foreign bots and trolls must not be given a platform, and trust in the democratic system must be reinforced. Below are some of the threats our team perceives as up-and-coming in the future of cognitive warfare. This is not meant to be an exhaustive list but rather a representation of how cognitive warfare agents could go about achieving the goals described in previous sections. It will also provide a framework for areas which NATO will have to address moving forward in the fight against cognitive warfare.

Threat 1: Ease of Selection and Virality

The recent success of TikTok has been attributed to its amazing algorithmic abilities. Each video is presented to users most likely to "engage" with the content via commenting, liking, sharing, or just viewing. The main goal of such an algorithm is, of course, to maximize watch time and ad revenue [34]. However, it has had unprecedented success. TikTok itself has to insert notices reminding viewers to periodically sleep or log off from the service [35]. It has also created an environment where users can share content, and organize, with like-minded individuals at blazing speed. In just days, TikTok can foster subcommunities that band together to push reform, raise money for causes, or even organize and plan protest activity [36].

This is not to say that TikTok presents a unique or unreproducible capacity. The reality is that every single existing social media is attempting to improve their algorithmic recommendations, and all have seen recent success. If not TikTok, another social media platform would simply stumble upon similar levels of algorithmic technology eventually. Algorithmic recommendations, however, are not the only way to produce "viral" content. Recent research into pandemic spread patterns have gleaned more insight into the "friendship paradox" or "superuser effect". Epidemiological studies have consistently shown that the spread of information, or a virus, is actually mostly attributed to a much smaller number of vital "nodes".

Turns out, in all networks of human connection there are a few, for lack of a better term, popular individuals who serve as an anchoring point for a lot of other individuals who have a much more limited social circle. These “superusers” have been shown to have an unprecedented level of control over the spread of information and diseases [37]. China, particularly, has already placed resources in identifying and figuring out how to connect to these individuals [38].

Ultimately, as these networks become easier to identify and utilize, there is a real threat of outside forces targeting at-risk communities that now have the tools to quickly organize. This can be dangerous, such as in the case of targeting disenfranchised political groups. It can be worse, such as in the case of targeting the familial unit of the military-enlisted individuals, especially those who are younger or have other risk factors. Or it can also be critical, such as in the case of targeting individuals with existing mental health disorders. Especially those of the delusional or paranoid inclination. There is a saying online that “internet time” runs faster than real world time due to how quickly information spreads and trends rise and fall. For example, one week in the real world may seem like a year on the internet. As the spread rates of viral information increases, there will be less warning for authorities. A predictive warning system is desperately needed to respond to these incredibly fast targeted campaigns.

Threat 2: A New Age of Truth

There has been an increasing interest in the ability to produce content that can be passed off as true. This can be seen in the fake articles that have been propagating for some time now on social media networks. However, the next generation of this fake content is much more worrying. “Deepfakes” are videos which seek to create the illusion of an individual doing or saying something with face-transplant technology. These videos can be very convincing, and the technology is only improving as time goes on. Bloomberg and PBS have both published examples in the last two years showcasing how the technology is accelerating at a rapid pace [39][40]. Additionally, audio-only versions of this same faking technology, such as the so-called “Lyrebird” AI application, are also seeing further development [41]. Social media networks such as Facebook and TikTok have already launched campaigns to ban deepfake content [42].

However, this solution is only a bandage to the symptoms of a larger problem. A worry is that even if fake content is revoked or removed, corrections and reversals do not reach everyone who viewed the original content as they lack the same "viral momentum." As these technologies develop, there must be a consolidated effort to develop accurate detection algorithms or some other form of defense which we must apply, quickly.

Threat 3: Cyber-induced Institutional Discomfort and Distrust

NATO countries are extremely productive, as is to be expected of those with some of the most complex social systems in the world. Every single day citizens rely on economic, medical, and judicial institutions to work effectively to preserve order and comfort. Thus, to disrupt this order and comfort, cyberattacks tend to target these very institutions in ostentatious fashion. A hospital's incentive to recover their digital data and computer power is much more urgent than those of the typical private company [43]. However, there is an alternate scenario where these cyberattacks have the same targets but are more insidious in their methods and goals.

There are claims already that these societal institutions discriminate against individuals based on socioeconomic status, race, religion, and other factors. One could easily use the cyber world to reinforce these beliefs. Perhaps a targeted subsection of the population experiences glitches: nothing too critical, but annoying and concerning. These small mistakes could be alarming due to their proximity to vital information. A lost document or payment, incorrect data, perhaps even alarming notes, or directives, which could mean something more. Research already shows that once information becomes tainted, people lose trust in the entire document or system [44]. One can see how these effects could be amplified if supporting fake news reports claim these glitches to be deliberate subversion attempts by the government. The distrust can spread from hospitals, to banks, and even to the courts system. If the target population is chosen carefully, this could quickly destabilize the already precarious faith that people have in government influenced institutions.

Threat 4: Biological and Therapeutic Emotional Manipulation

Mental health guidance and treatment have recently achieved a spotlight on the international stage. There are various exciting developments in the field which might revolutionize how we view and treat mental health ailments. For example, transcranial magnetic stimulation (TMS) is a method of utilizing magnetic fields to stimulate nerve cells in the effort to treat symptoms of depression [45]. Transcranial direct current stimulation (TDCS) is a related field which applies an electric current to the scalp in the hope of stimulating nerve cells close to the skull, another method being developed to treat depression [46]. Therapists and psychiatrists are also working alongside app developers in order to come up with therapy tool apps to tackle ADD, PTSD, depression, and anxiety. Some of these are already out on the market with favourable reviews [47].

Despite this, there are many worries regarding the speed at which some of these technologies are being developed, especially the rate at which they are being commercialized. TDCS in particular is relatively lightweight in its construction and operation. Various products already exist in the market, see the Muse [48], and the parts required are such that some adolescents on the social media site Reddit have already managed to make their own at-home versions. It is this last aspect which is particularly disconcerting. TDCS is still actively under research and development, especially as it relates to the brain function of minors. Various scientists and researchers have expressed worry about this development and urged more strict regulations on commercial ventures. Some first-person reports of increased irritation, confusion, and anger have already spawned from these at-home versions and commercial ventures [46]. Similarly, while some therapy apps are sponsored by board certified mental health professionals, the space is far from regulated.

This is all to say that more direct methods of changing cognitive persuasion and mood are available on the market in such a way that they can be easily intercepted. These direct methods also tend to deal with at-risk populations such as veterans with PTSD using therapy apps or

impressionable adolescents creating at-home TDCS kits. A foreign power could easily fill a therapy app with “bad” advice in very dangerous ways, or they could upload slightly “off” TDCS manuals and directions on Reddit. While not necessarily potent in their own right, this can be followed up by a targeted cognitive warfare attack to take advantage of the altered state. If someone truly understood what they were doing, the results could be notable and terrifying.

Threat 5: Enhanced Recruitment of Agents

Public opinion is difficult to predict and manage. The systems that connect people to each other can be extremely complex. However, we’ve already showcased that some of the people in these vast networks have more influence than others. In fact, to see the influence of some of these individuals, you need only to open your Twitter application. There are various forms of influencers which now have closer connections to the public than ever before. Educational, economic, cultural, religious, and political leaders have recently been given platforms to the public in sizes which would have been unthinkable only a decade ago. In a lot of ways, this has also made influencing public opinion much easier than ever before, reducing the number of targets one has to compromise in order to affect mass thought.

Individual-specific cognitive warfare deals with the attempt to “recruit,” or compromise, these individuals in an effort to weaponize the public opinion of their audiences. The Church of Scientology, classified as a dangerous cult by some NATO members, has already shown the importance that recruiting elites and celebrities can have in propagating and legitimizing certain ideas and beliefs [49][50]. The new threat in this small number of targets lies in the fact that direct mind control is becoming an increasingly dangerous prospect.

There are indirect methods of achieving this. Synthetic designer drugs are more popular than ever, and they can be made to be incredibly addicting [51]. Hooking a celebrity on a drug makes for a compelling incentive. A more direct method would be to implant electrical or optogenetics stimulators in the brain. Although known research of this direct method is still in extreme infancy, the results in animal testing have been incredibly compelling. For example, scientists

have been able to create false fear memories in mice. Scientists will place a mouse in box A. They will then remove the mouse but mark the memory space through imaging. They will then place it in box B and give it a shock, while at the same time stimulating the neurons mapped to box A through an optogenetic receptor. When the mouse is placed back in box A, it will freeze in fear, having the false impression that it was already shocked inside box A. A false memory has now been created [52]. The usefulness, impact, and danger of this technology in cognitive warfare campaigns cannot be overstated. Of course, implanting electrodes or optogenetic receptors in the brain is not a small task, especially if one needs to achieve it covertly and accurately. However, the direct nature of this manipulation makes it a risk worth monitoring extremely closely in the field of cognitive warfare.

Strategy Recommendations

As stated above, attempting to influence the public is not new. Politicians, generals, market leaders, and other influencers have been using rhetoric, propaganda, and messaging to manipulate public opinion for years. What is new are the tools for doing so, and subsequently the reach that can be achieved. The internet, social media, and the 24-hour news cycle allow for constant flows of information making it easier than ever to influence the human mind, and the freedoms afforded to citizens of NATO member countries make it easier to do so. Liberal, western democracies are not only lacking in their understanding of cognitive warfare, they are also more susceptible to, and unprepared in dealing with the rapidly evolving threat. In order to turn the tide of this battle, NATO should work at various levels in the alliance to define and measure cognitive threats, assess the vulnerabilities of its members, and task key groups with initiatives to mitigate and respond to cognitive campaigns against the organization.

Threat Recognition Framework and Criteria

The first question NATO must ask when dealing with cognitive warfare is, how do we know when we are being attacked? There are two steps that must be taken to answer this: first, adding cognitive warfare to the larger international framework for warfare, and second, developing a set of criteria to ascertain when a cognitive attack is actually taking place.

Current international definitions of warfare stem from post-World War II era doctrines, namely the U.N. charter. There are two main sections within the charter that define the limits of warfare and are now the causes of confusion. Article 2(4) prohibits the "threat or use of force against the territorial integrity or political independence of any state"; Article 51 allows for "self-defense if an armed attack occurs against a Member of the United Nations." [53]. The articles were written at a time when lethal-kinetics were the main instruments of war [54]. Since then, the advances and reliance on computational power and the internet have allowed for the emergence of large scale cognitive warfare, leaving terms such as "use of force" and an "armed attack" unsuitable to

encapsulate the threat. Other military doctrines also pulled into question are those of distinction and proportionality: how one should distinguish between civilian and military actors and how one should respond proportionally to a cognitive attack, respectively [55]. The confusion behind how governing bodies define modern warfare have allowed enemies to threaten the security and stability of NATO member countries. For this reason, NATO must work to develop a set of rules or framework so that acts of non-kinetic warfare can be defined, and appropriately responded to. One of the better attempts at doing so comes from the Schmitt framework, which is an attempt to separate cybercrimes from cyber acts of war [56]. A framework such as this one could be adapted to develop legal definitions and metrics for cognitive acts of war.

The second part of this problem is figuring out when an act of cognitive warfare is actually taking place. One of the biggest differences between cognitive warfare and other forms of non-kinetic warfare is that these other methods often require an enemy to push information onto a population. With cognitive warfare, not only will people come across “attacks” posed innocuously as random posts or tweets, they will then begin to actively seek out information that affirms their beliefs. This is similar to the difference between push and pull marketing. With AI and machine learning, tech companies have created algorithms dedicated to holding our attention. Now, hostile actors have broken the code, and are able to craft narratives and stories using data to manipulate large masses of population, all without the knowledge of the reader. Before NATO can take steps toward combating the effects of cognitive warfare, it must take a proactive approach to unearth the attacks and develop a framework for differentiating a random online opinion from a larger, more insidious cognitive campaign.

Risk Assessment

The next question for NATO to answer is, how vulnerable is the alliance? This will require taking a deeper dive into not just NATO itself, but each of its member countries. Starting with the alliance, NATO should look towards any divisions or factions which an enemy could exploit to potentially weaken, or even break up, the alliance. After this, NATO should analyze each of its member countries and partners to see if any upcoming events and existing divides could be

targets and tools for a cognitive attack, respectively. By understanding the state of member countries in the alliance, NATO can proactively work towards identifying threats, designing mitigation strategies, and crafting counter narratives in hopes of preventing large scale chaos before it begins.

A smaller, tangential part of this risk assessment must take place at a personal level. Technology, specifically the internet, is ubiquitous with the 21st century. While usage and mastery of these technologies have increased, education on the dangers has not. For this reason, NATO should encourage citizens within the alliance to build their own personal resilience towards cognitive attacks. The first step in this effort could be through the creation of a spotlight study informing citizens of the importance or dangers of relevant topics, including, but not limited to, bias in media, fact checking, threats of echo chambers, online privacy, and information security. By increasing awareness towards these possible dangers, citizens would ideally take steps to shield themselves from future threats and attacks that come from the connectivity brought about by our reliance on technology.

Organizational Implementations

The third question for NATO to answer is, who should be tasked with managing and addressing the challenges of cognitive warfare? Technology, psychology, and neuroscience have all started to shape the future of warfare; NATO and its member countries' administrations must reorganize accordingly if they are to lead their citizens into a safe and secure future. The first step in this is finding a home for cognitive warfare challenges within NATO, whether as a unit in the Emerging Security Challenges Division, or something larger [57]. Beyond that, NATO and its allies should establish cognitive organizations as part of their law enforcement and military organizations with communication channels operating across the alliance, branches of the military, and between the government and local law enforcement. Responsibilities for these units should be threefold: first, to establish the alliance's current state in dealing with cognitive attacks by developing attack frameworks and completing a vulnerability assessment of NATO and its members; second, to prepare for anticipated cognitive attacks prior to important events such as

elections and nationwide protests; and last, to investigate cognitive attacks to ascertain the perpetrator and craft an appropriate response. This last responsibility can be shared with NATO's public diplomacy division to reveal the attacks to the public in hopes of creating a more cognitively-resilient population [58]. In addition to this endeavor, the public diplomacy division should work on crafting media and spotlight studies focused on personal vulnerability and mitigating cognitive attacks against oneself.

Another tangential challenge that has been brought up throughout this paper is that of NATO's and its member countries' growing tech illiteracy. Governments can no longer pretend that they are knowledgeable and up to date on opportunities and threats presented by the evolution of technology, and they can no longer afford to alienate large tech conglomerates as they continue to gain power and control over markets and media. The government must find a way to cooperate with the Facebooks, Googles, and Microsofts of the world. To do this, member countries can either follow in the footsteps of Denmark and create an office of tech diplomacy, or establish an overarching post or office tasked with liaising with the silicon valleys of the world [59]. For example, one of the responsibilities of this organization would be in establishing jurisdiction when dealing with misinformation on social media platforms. Currently, the regulation of social media in the Western world is split between the government and media companies with few lines being defined. Although this may work for the time being, technology is constantly evolving, and tech companies are growing in power and influence. Allowing them sole regulation of specific posts on media sites may set a dangerous precedent for the future. For these reasons, tech liaisons should work with media conglomerates to establish rules and jurisdictions over specific cases, especially when the spread of information can potentially threaten human health as seen across the world with the spread of false Coronavirus treatments and conspiracy theories.

Offensive Considerations

All of the measures above deal with preparation and defense against cognitive attacks, but there is still an offensive side to consider. There are certain factors which can be used to create a framework to guide the development of offensive strategies. The first of these is understanding the type of war that is taking place. If it is a hybrid war in which cognitive warfare is a smaller part of a larger offensive strategy, cognitive methods may not be the best methods of combat, and nations may wish to look towards other strategies such as cyber and lethal-kinetics if absolutely necessary. If the war taking place is largely that of cognition, the first step in determining strategy is to understand the goals of the campaign, as defined in the *Goals of Cognitive Warfare* section of this paper. Once the goals are understood, possible vectors become clearer. Another portion of the strategy is gaining an understanding of the geopolitical state of the enemy to find pressure points for targeting. Important factors here may include the centers of wealth and power, the structure of infrastructural systems, industry layout and leaders of media sources, major factions within the nation, and legal loopholes. By better understanding these key pressure points, strategies and tactics may reveal themselves and help to level the playing field in wars of cognition.

Closing Thoughts

In his remarks at the launch of NATO 2030, Secretary General Jens Stoltenberg affirmed “As we continue to compete in a more competitive world, we must keep our democracies strong.” [60]. When dealing with the day-to-day challenges of new forms of warfare, whether it be cyber or cognitive, NATO must not lose sight of the endgame. So far, the West, namely the US has adopted a doctrine of “defense forward” [61]. This means preemptively preventing and proactively searching for attacks without going on the offensive. The reasoning: NATO and the US feel they must remain within international laws and regulations to keep in high diplomatic standing and prevent infringing on freedoms and democracy across the world [61].

NATO’s enemies are currently less concerned with their international standing. Their goals are to show that democracy is not a plausible solution to the world’s problems. If the West habitually defaults to a defensive posture, it could lead to a ‘cat and mouse’ game in which NATO and its members become trapped. Thus, NATO must answer the following question: how can we not only prevent, but deter, cognitive attacks of the future while remaining an unwavering example of freedom and democracy for the rest of the world? This will likely be NATO’s primary military and diplomatic challenge of the 21st century.

Bibliography

[1] Greenemeier, Larry. “Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers.” *Scientific American*, 11 June 2011, www.scientificamerican.com/article/tracking-cyber-hackers/.

[2] Torbet, Georgina. “3 Undeniable Reasons Why You Need Online Anonymity.” *MakeUseOf*, 3 Apr. 2020, www.makeuseof.com/tag/3-undeniable-reasons-need-online-anonymity/.

[3] “The Evolution of the U.S. Intelligence Community-An Historical Overview.” *FAS*, Federation of American Scientists, 23 Feb. 1996, fas.org/irp/offdocs/int022.html.

[4] McCarthy, Brigid. “How Rock and Roll Brought the Soviet Union Down.” Edited by Lisa Mullins, *The World from PRX*, Public Radio International, 19 May 2011, www.pri.org/stories/2011-05-19/how-rock-and-roll-brought-soviet-union-down.

[5] Zucchi, Kristina. “Why Facebook Is Banned in China & How to Access It.” *Investopedia*, 22 Oct. 2019, www.investopedia.com/articles/investing/042915/why-facebook-banned-china.asp.

[6] Talmadge, Eric. “North Korea Blocks Facebook, Twitter and YouTube.” *Global News*, The Associated Press, 4 Apr. 2016, globalnews.ca/news/2616449/north-korea-blacks-facebook-twitter-and-youtube/.

[7] Somin, Ilya. “Facebook Should Stop Cooperating with Russian Government Censorship.” *The Washington Post*, WP Company, 21 Dec. 2014, www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/21/facebook-should-stop-cooperating-with-russian-government-censorship/.

[8] Morrison, Wayne M. “China's Economic Rise: History, Trends, Challenges, and Implications for the United States.” *EveryCRSReport*, Congressional Research Service, 25 June 2019, www.everycrsreport.com/reports/RL33534.html.

[9] “Psychological Operations: Air Force Doctrine 2-5.3.” Edited by Timothy A. Kinnan, *Iwar*, United States Air Force, 27 Aug. 1999, www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf.

[10] Seligman, Lara. “The Child Soldier Crisis: 'Kids Are Cheap'.” *Foreign Policy*, 8 Nov. 2019, foreignpolicy.com/2019/11/08/child-soldier-crisis-kids-are-cheap-yemen-isis-my-star-sky/.

[11] Rambo. “History of Electronic Warfare.” *Blogspot*, 7 Dec. 2009, ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html.

[12] “Electronic Warfare: Joint Publication 3-13.1.” Edited by William E Gortney, *FAS*, Joint Chiefs of Staff, 8 Feb. 2012, fas.org/irp/doddir/dod/jp3-13-1.pdf.

[13] “Cyberwar - Does It Exist?” *NATO Review*, NATO, 13 June 2013, www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.

[14] Grenoble, Ryan. “Trump Reverses Obama-Era Rules On Cyberattacks.” *HuffPost*, 17 Aug. 2018, www.huffpost.com/entry/trump-cyberattack-directive-20_n_5b758f76e4b0df9b093d1b06.

[15] “The UK Is a Global Cyber Power, Says Director GCHQ.” Edited by Jeremy Fleming, *GCHQ*, 25 Feb. 2019, www.gchq.gov.uk/news/the-uk-is-a-global-cyber-power--says-director-gchq.

[16] Low, Vincent. “The Trend Towards Digitisation.” *Sg.Canon*, Canon, 2020, sg.canon/en/campaign/business-insight/ambassador/the-trend-towards-digitisation.

[17] Brenner, Susan W, and Leo L Clarke. “CIVILIANS IN CYBERWARFARE: CASUALTIES .” *Law.UPenn*, University of Pennsylvania Carey Law School, July 2010, www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/BrennerClarke.pdf.

[18] Costa-Roberts, Daniel. “Here's How to Spot a Russian Bot.” *Mother Jones*, 1 Aug. 2018, www.motherjones.com/media/2018/08/how-to-identify-russian-bots-twitter/.

[19] Green, Stuart A. “Cognitive Warfare.” *The Augean Stables*, Joint Military Intelligence College, July 2008, www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare.pdf.

[20] Burns, Megan. “Information Warfare: What and How?” *CS.CMU*, Carnegie Mellon University, 1999, www.cs.cmu.edu/~burnsm/InfoWarfare.html.

[21] Backes, Oliver and Andrew Swab. “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019.

[22] Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Abacus, 2000.

[23] Epstein, Diana, and John D. Graham. “Polarized Politics and Policy Consequences.” *RAND*, RAND Corporation, 26 Aug. 2007, www.rand.org/pubs/occasional_papers/OP197.html.

[24] Mshvidobadze, Khatuna. “Trio Pandemic Propaganda: How China, Russia and Iran Are Targeting the West.” *GFSIS*, Rondeli Foundation, 23 Apr. 2020, www.gfsis.org/blog/view/1067.

[25] Lipton, Eric, et al. “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.” *Nytimes*, The New York Times, 13 Dec. 2016, www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[26] Yuhas, Alan. “Hillary Clinton Campaign Blames Leaked DNC Emails about Sanders on Russia.” *The Guardian*, Guardian News and Media, 24 July 2016, www.theguardian.com/us-news/2016/jul/24/clinton-campaign-blames-russia-wikileaks-sanders-dnc-emails.

[27] Merom, Gil. “Democracy, Dependency, and Destabilization: The Shaking of Allende's Regime.” *Political Science Quarterly*, vol. 105, no. 1, 1990, pp. 75–95., doi:10.2307/2151226.

[28] Chellaney, Brahma. “China's Expansionism Enters Dangerous Phase.” *The Hill*, 25 Aug. 2020, thehill.com/opinion/international/513574-chinas-expansionism-enters-dangerous-phase.

[29] Packer, George, et al. “A New Report Offers Insights Into Tribalism in the Age of Trump.” *Newyoker*, The New Yorker, 13 Oct. 2018, www.newyorker.com/news/daily-comment/a-new-report-offers-insights-into-tribalism-in-the-age-of-trump.

[30] “REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION.” *Intelligence.senate.gov*, The Senate, 2020, www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

[31] Griffin, Edward G, and Yuri Bezmenov. “Soviet Subversion of the Free World Press.” Accessed 1984.

[32] Wallace, Chris. “Transcript: 'Fox News Sunday' Interview with President Trump.” *FoxNews*, FOX News Network, 19 July 2020, www.foxnews.com/politics/transcript-fox-news-sunday-interview-with-president-trump.

[33] Rosen, Guy. “Helping to Protect the 2020 US Elections.” *About Facebook*, Facebook, 21 Oct. 2019, about.fb.com/news/2019/10/update-on-election-integrity-efforts/.

[34] Matsakis, Louise. “How TikTok's 'For You' Algorithm Actually Works.” *Wired*, 18 June 2020, www.wired.com/story/tiktok-finally-explains-for-you-algorithm-works/.

[35] Burke, Caroline. “TikTok's New Screen Time Prompts Remind Users To Take A Breather.” *Bustle*, 19 Feb. 2020, www.bustle.com/p/tiktoks-new-screen-time-prompts-remind-users-to-take-a-breather-21816527.

[36] Herrman, John. “TikTok Is Shaping Politics. But How?” *Nytimes*, The New York Times, 28 June 2020, www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z.

[37] Christakis, Nicholas A., and James H. Fowler. “Social Network Sensors for Early Detection of Contagious Outbreaks.” *PLoS ONE*, vol. 5, no. 9, Sept. 2010, pp. 1–8. *EBSCOhost*, doi:10.1371/journal.pone.0012948.

[38] Huang, Joyce. “China's Virus Tracking Technology Sparks Privacy Concerns.” *Voanews*, Voice of America, 22 June 2020, www.voanews.com/covid-19-pandemic/chinas-virus-tracking-technology-sparks-privacy-concerns.

[39] Turton, William, and Andrew Martin. “How Deepfakes Make Disinformation More Real Than Ever: QuickTake.” *Bloomberg*, 7 Jan. 2020, www.bloomberg.com/news/articles/2020-01-06/how-deepfakes-make-disinformation-more-real-than-ever-quicktake.

[40] O'Brien, Miles. “Why 'Deepfake' Videos Are Becoming More Difficult to Detect.” *PBS*, Public Broadcasting Service, 12 June 2019, www.pbs.org/newshour/show/why-deepfake-videos-are-becoming-more-difficult-to-detect.

[41] *Lyrebird*, 2020, www.descript.com/lyrebird.

[42] Shead, Sam. “Facebook to Ban 'Deepfakes'.” *BBC*, British Broadcasting Corporation, 7 Jan. 2020, www.bbc.com/news/technology-51018758.

[43] “Cyber Attacks: In the Healthcare Sector.” *CISSecurity*, Center for Internet Security, 27 Sept. 2019, www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/.

[44] Bernal, Alonso, and Jennifer Ockerman. “Principal Cognitive Systems Engineer at Johns Hopkins University Applied Physics Laboratory.” 20 July 2020.

[45] “Transcranial Magnetic Stimulation.” *Mayo Clinic*, Mayo Foundation for Medical Education and Research, 27 Nov. 2018, www.mayoclinic.org/tests-procedures/transcranial-magnetic-stimulation/about/pac-20384625.

[46] Anita Jwa, Early adopters of the magical thinking cap: a study on do-it-yourself (DIY) transcranial direct current stimulation (tDCS) user community, *Journal of Law and the Biosciences*, Volume 2, Issue 2, July 2015, Pages 292–335, https://doi-org.proxy1.library.jhu.edu/10.1093/jlb/lsv017

[47] Truschel, Jessica. “Top 25 Mental Health Apps for 2020: An Alternative to Therapy?” *Psycom*, 13 Aug. 2020, www.psycom.net/25-best-mental-health-apps.

[48] “Meditation Made Easy.” *Muse*, 24 Aug. 2020, choosemuse.com/.

[49] Sappell, Joel, and Robert W Welkos. “Courting the Power Brokers.” *Latimes*, Los Angeles Times, 27 June 1990, www.latimes.com/local/la-scientology062790a-story.html.

[50] McMaster, Geoff. “Once Thriving Church of Scientology Faces Extinction, Says Cult Tracker.” *Folio*, 11 Jan. 2018, www.folio.ca/once-thriving-church-of-scientology-faces-extinction-says-cult-tracker/.

[51] “An Expanding Synthetic Drugs Market.” *Unodc*, United Nations Office on Drugs and Crime, 23 Mar. 2020, www.unodc.org/documents/scientific/Global_SMART_23_web2.pdf.

[52] Noonan, David. “Meet the Two Scientists Who Implanted a False Memory Into a Mouse.” *Smithsonianmag*, Smithsonian Institution, 1 Nov. 2014, www.smithsonianmag.com/innovation/meet-two-scientists-who-implanted-false-memory-mouse-180953045/.

[53] “UN Charter.” *Un*, United Nations, 26 June 1945, www.un.org/en/sections/un-charter/un-charter-full-text/.

[54] Bienvenue, Emily, et al. “Cognitive Warfare.” *Cove.army*, The Cove, 19 Sept. 2018, cove.army.gov.au/article/cognitive-warfare.

[55] “BASIC PRINCIPLES OF THE LAW OF WAR AND THEIR TARGETING IMPLICATIONS.” *Doctrine.af.mil*, Curtis E. Lemay Center, 15 Mar. 2019, www.doctrine.af.mil/Portals/61/documents/Annex_3-60/3-60-D33-Target-LOAC.pdf.

[56] Foltz, Andrew C. “Stuxnet, Schmitt Analysis, and the Cyber ‘Use-of-Force’ Debate.” *Ndupress.ndu*, National Defense University Press, 2012, ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

[57] Nato. “New NATO Division to Deal with Emerging Security Challenges.” *Nato.int*, NATO, 4 Aug. 2010, www.nato.int/cps/en/natolive/news_65107.htm.

[58] “NATO Public Diplomacy Division's Co-Sponsorship Grants.” *Nato.int*, NATO, 6 Dec. 2018, www.nato.int/cps/en/natohq/63610.htm.

[59] *Office of Denmark's Tech Ambassador*, 2020, techamb.um.dk/.

[60] Stoltenberg, Jens. “Remarks by NATO Secretary General Jens Stoltenberg on Launching #NATO2030 - Strengthening the Alliance in an Increasingly Competitive World.” *Nato.int*, NATO, 8 June 2020, www.nato.int/cps/en/natohq/opinions_176197.htm?selectedLocale=en.

[61] Sulmeyer, Michael, and Paul M Nakasone. “How to Compete in Cyberspace.” *Foreign Affairs*, 25 Aug. 2020, www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.