## Imperialism K Aff

### 1NC – Cognitive Warfare

#### Cognitive warfare is necessary to combat foreign disinformation.

Reding & Wells ’22 (Dale Redings, Office of Chief Scientist, NATO Headquarters, Bryan Wells, Office of Chief Scientist, NATO headquarters, “Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies” <https://link.springer.com/chapter/10.1007/978-3-030-94825-2_2>)

As NATO moves towards the future, it finds itself confronting the challenges of a changing world. As noted in the NATO2030 process (Maizière et al., 2020; NATO, 2021a), NATO will need to address a host of returning and emergent challenges such as Russia’s aggressive actions, the threat of terrorism, cyber-attacks, emerging and disruptive technologies, the security impact of climate change, and the rise of China. The solutions to these challenges require a delicate blend of political and military action married with the deep collective wisdom contained within the Alliance. Within the three core missions specified by NATO’s 2010 strategic concept (collective defence, crisis management and cooperative security) (NATO, 2020d), the Alliance is focused on five operational imperatives: cognitive superiority, layered resilience, influence and power projection, cross-domain command, and integrated multi-domain defence (NATO, 2021c). These imperatives and the overarching challenges outlined in NATO2030 have led NATO to expand its operational domains from three (air, land, sea) to include cyber (NATO, 2019) and space (NATO, 2021b). However, a school of thought exists that has strongly advocated that the cognitive domain should be given equal importance and noting that it is an area where Alliance nations are particularly vulnerable (Cole & Le Guyader, 2020). Recent examples of the ever-growing threat presented by disinformation, misinformation, and propaganda, including actions taken during the COVID-19 crisis, would support such an assertion. It is worthwhile at this point to clarify the definitions necessary to consider conflict in the cognitive domain. First, misinformation may be taken to mean the creation and dissemination of false and/or manipulated information, without malicious intent. Similarly,weaponised misinformation, otherwise known as disinformation, is defined by NATO as “the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead” (NATO, 2020b). The key distinguishing difference between the two is that disseminating disinformation is an act conducted with malice and forethought. The organised dissemination of disinformation is often called a disinformation campaign, which may also mix in selected facts so as to obscure or confuse. On the other hand, propaganda disseminates information or narratives that may be factual, false, highly selected or manipulated in nature but are intended to put a country or social group in a particular light (positive or negative) or influence opinion. More succinctly, it is information with an agenda (DiResta, 2018). The more insidious modern form, computational propaganda, is defined as “the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion” (Woolley, 2016). The employment of computational disinformation has meant that the costs of creating a disruptive disinformation campaign have significantly been reduced, along with a dramatic increase in effectiveness, focus and agility. Information warfare has always been part of organized conflict (e.g., Tzu, 2018). Nevertheless, a more modern definition, drawn from Russian doctrine, definesinformation warfare (or operations) “[as the] conscious employment of information to enable the user to achieve his political, economic, military, or other goals … [to be] conducted constantly, in peacetime, in the period of threats … and in wartime … [by] committing all available forces and software and hardware potentialities to impact the opponent’s information capabilities and protect our own against similar actions by the opponent” (Ball, 2017). Information warfare is not about armed forces, equipment or infrastructure in the physical domain but rather a part of a strategic campaign to influence, affect perceptions, and validate realities that support national power agendas (Carr, 2019). In US doctrine information warfare consists of five aspects: electronic warfare, computer network operations, PsyOps (psychological operations), military deception, and operational security (Bernal et al., 2020). More concisely, “information warfare works to control the flow of information” (Bernal et al., 2020; Cluzel, 2020). One of the critical challenges of defensive information warfare is to recognise when an attack is occurring (Nimmo, 2016) and to act accordingly. In addition, defensive information warfare may also be used as a means of developing a narrative to inoculate one’s citizens against an actual or perceived information attack (Dumitrescu, 2019). Narratives are stories about stories (Verdon, 2019). Beliefs, history, information, disinformation, misinformation, propaganda and mythmaking are all part of the development of a strategic narrative defined as “a means for political actors to construct a shared meaning of the past, present, and future of international politics to shape the behaviour of domestic and international actors. Strategic narratives are a tool for political actors to extend their influence, manage expectations, and change the discursive environment in which they operate. They are narratives about bothstates and the system itself, both about who we are and what kind of order we want. The point of strategic narratives is to influence the behaviour of others” (O’Loughlin et al., 2013). Strategic narratives are a double-edged sword, playing a role in societies as tools for defensive information warfare (potentially based on disinformation) or as a means of increasing social resilience to cognitive conflict (Dumitrescu, 2019). Cognitive warfare is a generalisation and extension of information warfare beyond the battlefield. It is best defined as an attack on knowledge, or more clearly, it is a means of conflict designed to impact how individuals, groups or nations think about an issue, event or situation. Ultimately, “destabilisation and influence are the fundamental goals of cognitive warfare” (Cluzel, 2020). The difference between information and cognitive warfare is significant (Bienvenue et al., 2018). It lies in the process of turning information into knowledge, as per the first two steps of the OODA loop (Osinga, 2005). In cognitive warfare, the weapon is information, but the domain of operation is cognitive. Cognitive warfare is part of the larger concepts of grey zone or hybrid warfare. Grey zone warfare describes conflict conducted below the level of engagement that could initiate traditional military actions. “The Gray Zone is characterised by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war” (Votel et al., 2016), with the Cold War being the quintessential example. NATO considers hybrid warfare as “a wide range of overt and covert military, paramilitary, and civilian measures … employed in a highly integrated design” (Hoffman, 2018). This definition describes the use of mixed military-political tools of conflict used within the grey zone of operations. NATO nations have recognised the threat of hybrid and grey zone conflict. At the 2018 Brussels Summit, heads of state noted that “We face hybrid challenges, including disinformation campaigns and malicious cyber activities.” This was followed up in 2019 at the London Summit with heads of state noting that NATO will be “strengthening [its] ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies”, a point reinforced once again at the 2021 NATO summit in Brussels. In the intervening years, NATO has developed a clear strategy to counter disinformation based on promulgating factual narratives. Disinformation is countered by offering a counter-narrative built on refuting, debunking, providing relevant facts and sources, and supporting the actions of a free press. Alliance nations share best practices, approaches, lessons learned, and insights among themselves and partners such as the EU and UN. This counter disinformation strategy includes continued research in disinformation methods and grey-zone tactics. NATO S&T has played a vital role in supporting NATO efforts to understand better and counter disinformation, whether through the Science for Peace and Security Program, working with partner nations, or through the collaborative efforts of the Science and Technology Organization. The COVID-19 pandemic is not a consequence of geostrategic conflict. Nevertheless, the pandemic has had a direct and adverse effect on all Alliance nations, particularly their medical, political, and economic systems. Exploiting this crisis, several countries and groups with partisan agendas attempted to create a watershed moment in global security by undermining Alliance cohesion and national resolve. As noted by the World Health Organization’s (WHO) Director-General at the 2020 Munich Security Conference, “We’re not just fighting an epidemic; we’re fighting an infodemic” (Zarocostas, 2020). The COVID-19 pandemic presented an information exploitation opportunity for some strategic actors as part of existing grey zone conflicts. At the same time, this has raised awareness of the enduring challenge of countering misinformation, disinformation and outright propaganda. These attacks can, and have, imposed considerable costs to the nations and has needlessly increased the death rate from COVID-19. However, in any complex crisis, such as that experienced during pandemics, information transparency and open communication builds trust and ultimately saves lives. Over the initial phases of the COVID-19 crises, Russian disinformation campaigns focused on stories such as (EEAS, 2021): COVID-19 was developed in NATO laboratories, global elites are imposing tyranny, and the EU is disintegrating. As time went on, these attacks expanded to include those designed to increase doubt on vaccine efficacy, safety and availability, accusing countries of genocide for not using the Russian vaccine (Sputnik V), suggesting that migrants (or NATO) have been spreading the virus across Europe, as well as implying that degenerate geopolitical and commercial interests were over-riding the interests of European and North American citizens. While some of these attacks are homegrown, there has also been a trend towards amplifying attacks from secondary sources (e.g., right & left-wing groups, Iran, ISIS, China, anti-vaxxers, etc.). This approach maintains a veneer of plausible deniability and evades responsibility for accurate reporting. At the same time, these efforts have presented an inflated narrative of Russian (and to some extent Chinese) generosity and scientific, military and societal strength. This narrative was supported by logistics and medical support provided to groups with deep historical and linguistic ties to Russia or Kremlin-friendly forces (Ozawa, 2020). In late April of 2020, Russia launched three harmonised disinformation attacks on NATO (NATO, 2020b). First, a fake letter was published, purportedly from Jen Stoltenberg, NATO’s Secretary-General, to Raimundus Karoblis, Lithuania’s Minister of Defence. The letter noted that NATO had decided to withdraw its multinational battlegroup from Lithuania due to rising COVID-19 infections. The letters were posted on blogs in English and Lithuanian and were later picked up by various websites and social media platforms. Fake accounts, created days before, were used to spread the disinformation further. Following this, an edited YouTube video was released suggesting that COVID-19 within the multinational battlegroup was the single agenda item for a recent NATO Defence Ministers meeting. Finally, the letter was sent directly to NATO Headquarters via a spoofed NATO e-mail address. Surprisingly, given the care taken to orchestrate this attack, the letter contained many formatting, structural and grammatical mistakes, and was recognized quickly as a fake. Ultimately the attack was a failure and died out quickly. NATO responded rapidly to discredit the story, as did the Lithuanian Defence Ministry. Early identification (understand) and rapid reaction (engage) nullified the attack. As noted by the Secretary-General, “They have not been successful because, first of all, it has been clearly revealed that this is a fake letter; secondly, we’ve seen that NATO allies remain committed, remain united, and are actually helping each other in the midst of the coronavirus crisis” (NATO, 2020b). Disinformation has been a constant threat to the Alliance since its inception. Nevertheless, with the increased use of asymmetric (hybrid) warfare and the attendant growth of social media, disinformation and its institutional twin of propaganda have significantly increased in volume and precision. Moreover, these efforts are part of more significant military and geopolitical trends, such as those presented by hybrid or grey zone warfare, where success is defined through operations in the cognitive sphere.

#### The AFF has misconstrued cognitive warfare, cognitive warfare is both necessary and useful.

Reding & Wells ’22 (Dale Redings, Office of Chief Scientist, NATO Headquarters, Bryan Wells, Office of Chief Scientist, NATO headquarters, “Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies” <https://link.springer.com/chapter/10.1007/978-3-030-94825-2_2>)

NATO has shown that we remain ready and able to defend our nations, that allies and partners are supporting each other, and that investing in our Armed Forces is an investment in the strength and resilience of our societies. This readiness was demonstrated in no uncertain terms by our Alliance’s vital role in fighting this deadly pandemic. This capacity stretches across the maritime, land, air, cyber, and space domains, as well as the information or cognitive sphere. Taken together, this will help us build the resilience of our societies, and building resilience in our communities requires a whole-of-society approach. Everyone has a role to play; the media, the private sector, academia, civil society, of course, the whole-of-government. But it also includes all the relevant groups in our communities to ensure that our institutions and citizens are equipped for today’s digital realities. Beyond the nations that make up the Alliance, we must work in concert with our partners to strengthen our collective ability to prevent crisis and address challenges. It is clear that no nation alone, no continent alone, can cope with the magnitude of the challenges we are now facing as democratic societies. NATO is about security, but it’s also about values, shared values, and shared interests. This Alliance is about freedom, and I think our nations, especially those coming from behind the Iron Curtain, appreciate that strong narrative. To ensure our success and resilience in the face of adversity, we must unambiguously and proactively communicate our core narrative, intent and actions to our publics, our potential rivals, and adversaries. But the pandemic also showed us that resilience is a whole-of-society concern. But to correctly assess this societal resilience, we need better to understand the nature, diffusion and power of disinformation. With this understanding, we may define even more precise indicators, metrics, and analytics to help Allied nations cope. Leveraging modern research in social and information sciences will support this work. This book will play a small but essential part in building such resilience, representing a whole-of-society perspective including academia, industry, and NATO scientists. But it also crucial to understand that the speed of innovation and technology implementation and how this might change operations across the operational domains, including the information sphere. Understanding how current and future developments of emerging disruptive technologies (EDTs) will impact these domains of operation will be essential to our operational success. We will need to harness the research, technological and analytical talent in our societies. Bring our universities together, bring our scientists together, bring our top experts, and embed our values and ethical and moral code in our technologies. If we succeed, and I’m very confident that we will, we will maintain our edge and keep our societies safe and resilient. And that is the concept of NATO. It is not only strong together dedicated to looking forward, introducing innovation, understanding the realities and technologies of today, countering disinformation and propaganda, bringing together the best of our scientific and technological base. I think all our citizens are and will continue to be safer because of that. This book captures and contributes to the collaborative effort of the nations which make up the Alliance and its partners. It promotes a shared understanding of the information sphere, outlines the attempts to undermine the Alliance during the COVID-19 pandemic, and contextualizes the hazards of disinformation and propaganda. It will guide our travels through and competition for ideas within the information sphere as we evolve as an Alliance.