THE DEFENCE HORIZON JOURNAL

Aspects Of Cognitive Superiority

SHAPING BELIEFS AND BEHAVIOURS

TIKTOK AND THE RELEVANCE OF THE COGNITIVE WARFARE DOMAIN
Sascha Dov Bachmann

ON COGNITIVE WARFARE: THE ANATOMY OF DISINFORMATION
Peter B.M.J. Pijpers

THE HIGHEST FORM OF FREEDOM AND THE WEST'S BEST WEAPON TO COUNTER COGNITIVE WARFARE
Matthias Wasinger

THE ROLE OF CYBER SECURITY IN COGNITIVE WARFARE
Maria Papadaki

THE RUSSIA-UKRAINE CONFLICT FROM A HYBRID WARFARE COGNITIVE PERSPECTIVE
Josef Schröfl and Sönke Marahrens

NEW PROBLEMS IN HYBRID WARFARE: CYBER MEETS COGNITION
Chris Bronk

FUTURE ELECTIONS AND AI-DRIVEN DISINFORMATION
Gazmend Huskaj

HYBRID THREATS – THE CHINESE FOCUS ON AUSTRALIA
Matthew Warren

AI AND MICROTARGETING DISINFORMATION AS A SECURITY THREAT TO THE PROTECTION OF INTERNATIONAL FORCES
Bernard Siman

Masthead

The Defence Horizon Journal is a professional and academic journal that features essays, reports, and analyses covering geopolitics and law, security- and defence policy, peace and conflict studies, applied military science, as well as developments in weapons technology. The journal aims to inform about procedures, background and trends in the aforementioned topics. The selection of publications is topic- and event-driven.

Disclosure according to §25 (1) Media Law (AUT)

Media owner is the **TMW Horizont Gesellschaft mbH**;
Tenschertstrasse 24/5/3, 1230 Wien

Editor-In-Chief: **Matthias Wasinger, Ph.D.**

Design: **Damir Birsa**

Correspondence: contact@tdhj.org
ISSN: 2960-5687

This special edition of *The Defence Horizon Journal* is produced in collaboration with The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and comprises a synthesis of materials produced for the early October 2023 Cyber Power Symposium on Hybrid Conflict/Warfare held by Hybrid CoE in Helsinki, Finland.

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

THE DEFENCE HORIZON JOURNAL

Disclaimer

TDHJ Special Edition reflects the views of the authors, drawing on prior research and experience in their areas of expertise. The Defence Horizon Journal is a nonpartisan, independent Journal and does not take institutional positions.

Contents

07 → **Sascha Dov Bachmann**

TikTok And The Relevance Of The Cognitive Warfare Domain.

11 → **Peter B.M.J. Pijpers**

On Cognitive Warfare: The Anatomy of Disinformation.

18 → **Matthias Wasinger**

The Highest Form of Freedom and the West's Best Weapon to Counter Cognitive Warfare.

26 → **Maria Papadaki**

The Role Of Cyber Security In Cognitive Warfare.

32 → **Josef Schröfl and Sönke Marahrens**

The Russia-Ukraine Conflict From a Hybrid Warfare Cognitive Perspective.

41 → **Chris Bronk**

New Problems in Hybrid Warfare: Cyber Meets Cognition.

48 → **Gazmend Huskaj**

Future Elections and AI-Driven Disinformation.

60 → **Matthew Warren**

Hybrid Threats – The Chinese Focus On Australia.

65 → **Bernard Siman**

AI And Microtargeting Disinformation As A Security Threat To The Protection Of International Forces.

DR TEIJA TIILIKAINEN
Director
The European Centre of Excellence
for Countering Hybrid Threats

5TH CYBER POWER SYMPOSIUM ON HYBRID CONFLICT/WARFARE: "THE CYBER AND HYBRID ASPECTS OF COGNITIVE WARFARE/SUPERIORITY"

Cyber security and cyber threats are generally considered to be related to physical structures such as ICT systems or critical infrastructures. As a tool and platform for malign hybrid threat operations, the cyber realm seems to provide an ideal space where new technological solutions create unexpected vulnerabilities, and where the attribution of hostilities is extremely difficult.

The cyber realm thus provides an important platform for the ongoing global power competition.

This competition is as much about the detection of vulnerabilities as it is about technological assets and know-how. It deals with the power to set norms – both explicit and visible – as well as implicit norms affecting activities and behaviour. The lack of broadly shared international rules and norms is one of the biggest challenges facing the cyber realm today. This challenge is further compounded by the emergence of new targets for the malign use of cyber tools.

The recent focus on the cognitive dimension addresses a specific target of cyber threats, which may be far more difficult to protect than physical systems or structures. When threats are directed against the cognitive dimension, it is the mental structures, or the human mind in general, that become the target. This is nothing new, as conflicts and war have always included a strong ideational dimension. Apart from physical objectives, political conflicts deal with ideas, ideologies, and narratives. The novelty of current threats to the cognitive dimension is linked to modern technologies and the cyber capabilities they provide to influence and manipulate the human mind. In this way, the cyber and cognitive dimensions become a perilous combination that requires the immediate attention of the security policy community.

When focusing on the cyber and cognitive dimensions, the discussion needs to have a broader focus than that of information operations or the use of disinformation. Modern technologies allow for much more far-reaching influencing of collective thought structures and political identities for hostile purposes. Target societies may therefore become more receptive towards subsequent political operations, or less supportive of the values or policies of their own political regime. Broader mental spaces may be influenced, decision-making processes affected, or public opinion altered. Trust in conventional sources of knowledge and information can be weakened, making the target community susceptible to alternative sources.

Access to big data or AI-based technologies increases the potential for cognitive warfare and creates significant challenges for open, democratic societies to protect themselves.

When opening the 5th Cyber Power Symposium on hybrid conflict and warfare, focusing on the cyber and hybrid aspects of cognitive warfare, I therefore wanted to stress the importance of the topic in the current seriously worsened security policy environment. The goal must be to fully understand the potential that modern technologies provide for malign activities against the cognitive dimension. This understanding will help us identify our own vulnerabilities as open, democratic states and societies. Resilience as a tool must be understood in its broadest sense, covering the resilience of mental structures, and collective and individual identities.

New perspectives and knowledge are needed on the cognitive dimension and how to protect it. I welcome the important collaboration between Hybrid CoE and the EDA in this framework and thank all the experts and participants who took part in the symposium for their valuable contributions to this discussion.

MAJ. GEN. STEFANO CONT
Capability, Armament and Planning Director
European Defense Agency

5TH CYBER POWER SYMPOSIUM ON HYBRID CONFLICT/WARFARE: "THE CYBER AND HYBRID ASPECTS OF COGNITIVE WARFARE/SUPERIORITY"

As part of my keynote speech at the 5th Cyber Power Symposium, I presented some ideas on relevant topics for consideration.

It is quite evident, and would be imprudent not to acknowledge, that the current situation in European defence has changed radically. Political will has been re-ignited, defence budgets have been increased, and collaboration has been bolstered. The reason for this is, of course, the war of aggression waged by Russia at the very borders of the EU.

As we have seen, all conflicts are hybrid conflicts, whether they are attacks on civilian infrastructure, cyber offensive operations targeted at Europe, interference in democratic processes, or many other methods of pursuing and achieving national goals through military operations.

In this vein, the re-ignition of political will came about as a result of three key documents: the Versailles Summit Declaration, the Joint Communication on the Defence Investment Gaps Analysis, to which the EDA contributed, and, of course, the Strategic Compass.

The Compass sets out an ambitious security and defence agenda to improve the EU's ability to act rapidly and robustly whenever a crisis erupts, with partners if possible and alone when necessary.

It also paves the way for advancing on the path of European defence cooperation in the longer term.

However, the operational need, which is directly linked to the ability to act rapidly and robustly, must define how we approach the use of technology.

Without the ability to use technology on the ground in order to obtain a strategic advantage or achieve a goal, technology as such is of no use. The approach to using technology must meet the needs of every one of our soldiers, regardless of the domain, to achieve collectively and individually the end state required. It must also provide the best possible protection to ensure their safety to the greatest extent possible, as well as enable the most rational decisions to be made in the shortest possible time.

This, in my view, is the operational need.

In the cyber domain, the Compass calls for us to step up our ability to prevent, detect, deter and defend against cyberattacks.

To ensure that this operational need is met, the EDA supports the participating Member States (pMS) in identifying capability gaps and in developing solutions to overcome these gaps. This has also been implemented in the area of cyber defence. For example, we recently organised, in conjunction with Hybrid CoE, a training course on the Contribution of Cyber in Hybrid Conflict. The operational need here is to provide training on cyber defence and hybrid threats.
As you probably know, the EU has a relatively new Cyber Defence Policy, which aims to increase cooperation among the EU's cyber defence actors and develop mechanisms to deploy capabilities at the EU level.

We are now working with Member States on an implementation plan for the policy and setting a timeline for each action. The aim is to do more to protect our armed forces and our citizens against cyber threats.

One of the pillars of this Policy is partnering to address common challenges. Indeed, cooperation is deeply ingrained in the DNA of the EDA. The pillar underlines that cooperation with partners remains of the utmost importance for the EU. Building on existing dialogues, the EU will seek to establish tailored partnerships in the area of cyber defence. This is where the cooperation between Hybrid CoE and the EDA will serve to strengthen and foster the development of cyber defence throughout Europe.

By providing opportunities for collaborative cyber defence projects, the EDA can serve as a fulcrum around which research and innovation-driven capability development can lead to greater opportunities to defend citizens.

Future developments in warfare must also be taken into account, which is why the issue of cognitive warfare is taking on greater importance.

In my view, cognitive warfare integrates cyber, information, psychological, and social engineering capabilities to achieve its ends. It exploits the internet and social media to target influential individuals, specific groups, and large numbers of citizens selectively and serially in society. Cognitive warfare therefore means that the human mind becomes a battlefield. The aim is not only to change what people think, but also how they think and act. When waged successfully, cognitive warfare shapes and influences individual and group beliefs and behaviours in favour of the tactical or strategic objectives of the attacker.

We have to find the right answers to how we can strengthen our resilience against cognitive threats, and who we should educate, train and conduct exercises with to enhance our capacity to resist and respond.
This is the challenge that must be met head-on.

Hamas-Israel:
TikTok And The Relevance Of The Cognitive Warfare Domain

SASCHA DOV BACHMANN

Author: Sascha Dov Bachmann is Professor in Law and Co-Convener National Security Hub (University of Canberra), University of Canberra, and a Research Fellow with the Security Institute for Governance and Leadership in Africa, Faculty of Military Science, Stellenbosch University. He is also a Fellow with NATO SHAPE - ACO Office of Legal Affairs, where he works on Hybrid Threats and Lawfare. The views contained in this article are the author's alone.

Abstract: As much as the current Hamas-Israel war occurs on the battlefield, it is being fought in the domain of cognitive warfare. The current conflict highlights the use of cognitive warfare - to influence public support for either side. In cognitive warfare, the human mind becomes the battlefield. The aim is to change what people think and how they think and act. Cognitive warfare as information warfare is what we see again in the current Hamas - Israel conflict: the bombing of the Al-Ahli Arab Hospital in Gaza and the question of attribution and its exploitation have shown the power of both influence operations and dis-information as key elements of cognitive warfare.

Problem statement: How to understand antagonist power's efforts targeting young audiences in the cognitive domain?

So what?: The West is on a trajectory to lose its youth to such malicious foreign influence in the cognitive domain. This undermining of Western resilience will only benefit the new global order of authoritarian regimes and despotism, with the PRC and Russia being the two main geopolitical players. A comprehensive whole of government plus and society approach involving all stakeholders (both public and private) is needed to raise awareness and work towards both deterrence and resilience.

Source: unsplash.com/camilo jimenez

Cognitive Warfare

Disinformation and cognitive warfare operations are being used by both state and non-state actors to influence public opinion. From COVID-19 conspiracy theories to the support of Hamas, the Western public has been and is being targeted in the cognitive domain. Western public has shown its vulnerability to manipulation, highlighted by the extent of anti-COVID activism and now the current pro Hamas/ Free Palestine demonstrations in context of the Hamas - Israel conflict.

The cognitive warfare angle in the context of the current Israel-Hamas conflict aims to influence public support for "for Hamas and Palestinians, and also reignite hatred for Israel. Early signs that this part of Hamas' plan is going well [include] "victory" celebrations… in countries in the Middle East and even in Berlin and New York, with pro-Palestinian groups cheering Hamas' killings and other atrocities."

At a time of heightened tension in the region and globally, an increasing division in civil society regarding the nature and the actors of the Israel-Palestine conflict comes the news of a new TikTok craze: Bin Laden's letter to America.

The current narrative war against the West with its (traditionally) Judaeo-Christian value system and the global rules-based order has many actors and attack vectors. Noteworthy is the formidable collusion between Putin's neo-Soviet Russia and the People's Republic of China (PRC) under President Xi.

Both countries, under their autocratic leaders, see the Western way of life, democracy and the rule of law-based global order as the main obstacle to their vision of a new world order which aims to dismantle the current global governance system. The latter is dominated by institutions created by Western Powers post World War II and is deemed a particular threat to the PRC's growing influence as major power.

Through the exploitation of the cognitive domain by various means of information and disinformation, using technical opportunities available through Mass Social Media, such as TikTok with its

CCP-controlled parent company Byte Dance, the youth in the West has become a main target for disinformation.

Both state and non-state actors are using cognitive warfare operations to influence public opinion. Russia has pitched itself as a junior partner in support of the PRC. Both are opportunistic actors exploiting any geopolitical challenge to the maximum as a chance to weaken the West. Russian and PRC collusion in the current Middle East

Propaganda and Misinformation

crisis highlights these developments. Russia's use of TikTok as a tool for its cognitive warfare approach against the West in connection with the war in Ukraine has gathered significant traction since the spring of 2022. Propaganda and disinformation aimed at Western, mostly young audiences in the information domain, using Facebook, X (formerly Twitter) and, more importantly, TikTok, have boosted Russia's propaganda effort and led to an increased success in influencing young minds in Western democracies as well as on the African continent.

Moscow successfully maintained support among African Union audiences by presenting itself as the moral and legal successor to the Soviet Union, the historical partner of Africa's liberation movements during the era of decolonisation. Similarly, the PRC presents itself as a non-colonial partner in Africa and has successfully ingrained itself in Africa's media sector in addition to its ongoing economic and trade diplomacy on the continent. The PRC's success in Africa is so staggering that a U.S.-led counter-media and information strategy is needed.

Recycling old historical positions and facts regarding colonialism and oppression are part of the new cognitive warfare approach. Adapting historical narratives to new, contemporary realities is highlighted by the current equation of Israel being a coloniser and the Palestinians - including Hamas - being freedom fighters in the narratives of current media TikTok operations by both Russia and China. Targeting Western audiences with anti-Ukraine and anti-Israel content on TikTok is highly sophisticated and shockingly successful. Young Australian and U.S. audiences have become convinced that Israel is a foreign coloniser of indigenous land and is waging a genocidal war against the Palestinians as the land's indigenous people.

It is no surprise that young audiences in both the U.S. and Australia are particularly vulnerable given that both share common conceptions and experiences on indigenous rights, histories of white violence against 'black' people and the role and legacy of coloniser history of the English speaking peoples. Gaza and the Palestinian struggle are being seen as part of a wider struggle for indigenous peoples' rights globally, expressing and reclaiming Palestinian indigenous sovereignty. The theme of indigeneity as resistance against colonialism goes to the heart of the just mentioned Western post-World War II global system as exactly those powers were responsible for colonialism and ignoring their post-colonial role in building the rules-based global order. While reducing Western powers to their historical role and complicity as colonising powers is obviously simplistic and ignorant of the changes these states have gone through in terms identity, culture and ethnic makeups post-decolonisation, it works and is part of the PRC's global war against modern history and Western identity.

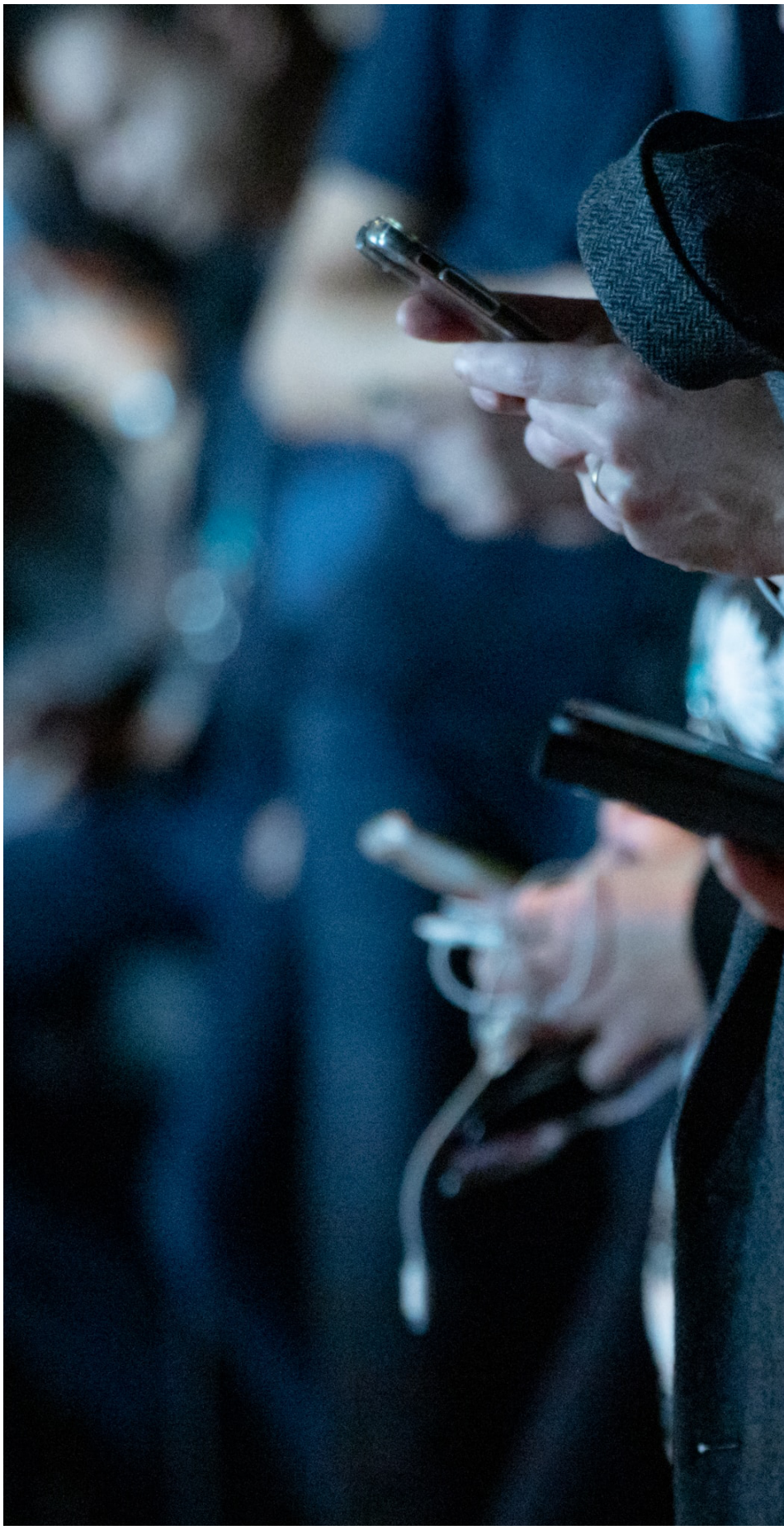
The PRC recently fired a shot across a Western-centric version of history when Chinese 'experts' claimed that the Greek scholar and philosopher Aristotle did not exist and, hence, Western Greek-Roman philosophy was a historical fraught. The PRC attempts to rewrite global cultural identity and heritage. This cultural power competition has to be seen in light of the PRC's increasing use of soft power and as a response to U.S. and Western attempts to limit the PRC's influence via its Confucius institutes, which have been rightly labelled as 'China's Trojan' horse.

TikTok's targeting of Generation 'Z' in the context of the Palestina - Israel conflict highlights the role this generation is being accredited for in going against the political and diplomatic position their governments would take. Squarely aligned with cognitive operations targeting social justice movements like Black Lives Matter and including 'Boycott, diversify and sanction' (BDS) and 'Free Palestine', it is only a question of time before the young generations in the West will have an impact on global policies and diplomacy.

The West's Oppression

Bin Laden's letter to America caused a TikTok craze. In this so-called letter to America, Osama Bin Ladin justifies "Jihad against the aggressors as a form of great worship in our religion" and ties the fight against the West's "oppression" to Israel's occupation and "killing our brothers in Palestine." U.S. TikTok users parroted its message of antisemitism, support of Jihad in general and support for Palestinian terrorism. More significant, though, is the direct undermining of the U.S. "Global War on Terror" post '9/11' and its right to self-defence against the acts of transnational terrorism.

The PRC's and Russia's continuing targeting of young audiences in the cognitive domain while exploiting the asymmetric access to information between the West and the antagonists, information control and limitation is a major threat to the West. With 60 % of TikTok users belonging to the so-called generation 'Z', the continuing targeting of this audience and their manipulation in the cognitive domain is today's greatest 'hybrid' threat. A generation in doubt of their belonging, their identity, their self-worth and their ability to trust their government and even society is the best way to weaken Western societies in terms of national identity, cohesion and ultimately resilience.



On Cognitive Warfare:
The Anatomy of Disinformation

PETER B.M.J. PIJPERS

Author: Dr Peter B.M.J. Pijpers is Associate Professor of Cyber Operations at the Netherlands Defence Academy in Breda and a Researcher at the Amsterdam Centre for International Law (University of Amsterdam).
A Colonel in the Netherlands Army, he has been deployed four times to mission areas, including Iraq and Afghanistan, and was seconded to the European External Action Service for three years. Dr Pijpers has (co-)authored articles on the legal and cognitive dimension of influence operations in cyberspace and how armed forces can manoeuvre in the information environment. See also Orcid ID 0000-0001-9863-5618. The author can be reached at b.m.j.pijpers@uva.nl. The views expressed in this article are solely those of the author.

Abstract: Cognitive warfare entails narrowing down the execution of warfare to the cognitive dimension. While presented as a new notion, cognitive warfare as a concept articulates the essence of warfare, namely changing an opponent's attitude and will - and hence their cognition. Although the concept is not new, the resurgence in attention and relevance is due to the inception of cyberspace (and social media), as well as knowledge of cognitive psychology. This renewed focus is particularly evident in the use of disinformation in influence operations.

Problem statement: How is disinformation used to influence the cognition of other geopolitical actors?

So what?: Societies need to be aware of the dangers of cognitive warfare, and become acquainted with its techniques. However, cognitive warfare alone will not win wars; its effectiveness is maximised in combination with and synchronised with other instruments of state power.

Source: shutterstock.com/metamorworks

"War is thus an act of force to compel our enemy to do our will."[1]

A Notion En Vogue

"Cognitive warfare" appears to be the latest fad in the security realm.[2] Cognitive threats refer to activities directly affecting human cognition without inflicting prior physical force or coercion.

Cognitive warfare can be understood as a part of hybrid warfare – another en vogue notion. Hybrid warfare is the use of all instruments, in all domains, to affect all dimensions (physical, virtual and cognitive). The core challenge in employing hybrid warfare lies in synchronising these capabilities and operations, including cognitive warfare.

The People's Republic of China's (PRC) policy of "three warfares",[3] using public opinion, psychological, and legal means to achieve victory,[4] is a contemporary example of cognitive warfare; in this respect, China's goal is to directly influence its opponent's mind and break its resistance without fighting.

Cognitive threats influence the human mind by using informational means such as words, narratives, and pictures. While influencing human cognition can be benign, using persuasive techniques, it can also be more malign or manipulative in nature. During the Cold War, the Soviets and the US used manipulative cognitive techniques to attain their goals in their respective doctrines of Active Measures and Political Warfare.[5] Fabricated messages, false data, or outright disinformation were often used to evoke human cognitive biases and heuristics, influencing and manipulating deliberation and decision-making processes. Hence, if cognitive warfare – perhaps under a different name – is not new, why is more attention being paid to these activities? Moreover, if disinformation appears to be the weapon of choice to affect human cognition, we have to ask how it works.

Cognitive War or Warfare?

War is an act of force intended to compel an opponent to fulfil one's will. Compelling an opponent can be achieved through military means but could also be inflicted through diplomatic, economic, or informational methods. In fact, Sun Tzu argued that subjugating the enemy's army without fighting is the true pinnacle of excellence.[6]

A distinction can therefore be made between war and warfare. War – especially in the legal sense – is an armed conflict between two states (or state-like entities). Conversely, warfare is the act of subjugating other parties – foe, friend or neutral – by any means available. Forced transnational migration, as witnessed between Belarus and Poland,[7] can be seen as a form of warfare, inducing or coercing a policy change. It follows that cognitive warfare is the art of inducing the other actor to accept one's will, using and focusing on the cognitive dimension.

While all forms of warfare affect the opponent's will, directly or indirectly, following a kinetic attack, cognitive warfare should be set aside from traditional conceptions. Cognitive warfare is not about territory or dominance over resources; it is a conflict between different perceptions, beliefs, or even a clash of civilisations or cultures.

Is Cognitive Warfare a New Phenomenon?

In the cognitive dimension, threats, or even warfare, are not new; nor is the battle over perceptions. This was evident as far back as the Peloponnesian War, and again in the Thirty Years' War, the Spanish Civil War, and more recently during the Cold War. Each of these clashes had a clear cognitive dimension related to clashes in worldviews, belief systems, and religions. However, cognitive threats and warfare are prevalent today due to two developments: first, the emergence of cognitive psychology, magnified by the second development, the inception of cyberspace.[8]

Cyberspace forms part of the information environment, which states have always used in the quest for influence. The inception of cyberspace has not only added new layers to the information space; more importantly, the virtual layers, virtual objects (data), and virtual personas have also unlocked the information environment. Whereas in the past, information and influence operations were executed using cumbersome methods including pamphlets, bribery, or radio broadcasts, they are mainly accomplished today with social media.[9] A tweet or direct message can reach the capillaries of society at the speed of light. Moreover, cyberspace is conducive to creating specific virtual images (deepfakes, virtual reality), memes, virtual personas (Facebook, X [formerly Twitter] or Instagram accounts) or social media communities. It can spread information in an unfiltered, viral, and contagious way that is not limited by national boundaries.

The emergence of academic research in cognitive psychology after the Second World War highlighted the fact that our brain is a neural network governed by heuristics and biases.[10]
It also became apparent that this knowledge could be used as an instrument to influence people. According to the Russian notion of Reflexive Control,[11] humans are prone to respond in a predetermined manner when subjected to specific information in a conditioned environment (time pressure, data overload). Reflexive Control – the primary technique in Active Measures doctrine – aims to find strategic advantages in the information environment by deception, provocation, subversion, and spreading disinformation.[12]

With this mechanism, Russia influences target audiences subconsciously by exploiting cognitive biases, namely the limitations in human information-processing capacity.[13]

The combined developments of cyberspace and cognitive psychology can be misused to influence liberal democracies, which have open societies and rules to protect individual rights and freedoms. Liberal democracies openly discuss problems to find common ground. This openness allows authoritarians to abuse this transparent ecosystem by injecting malign data to incite discord and sow distrust. The very elements that are relevant and essential to liberal democracies (freedom of speech, distribution of power,

independent media) are simultaneously our greatest vulnerability. Moreover, paradoxically, the only way to counter an attack on these core elements appears to be to violate our values. How can we resolve this self-inflicted conundrum?

Malicious actors can exploit these features of cognitive psychology and the internet since social media favours sensationalist content, irrespective of source or factuality. Actors on social media can deliberately manipulate and amplify negative messages by sharing misleading, deceptive or incorrect information that the audience perceives as genuine. Social media actors use algorithms to distribute fake and exaggerated news, and sharing is amplified by automated bots that consistently repeat the news.[14]

Is Cognitive Warfare Effective?

Scholars, including Arquilla, Ronfeldt, Stiennon, and Stone, predicted that the next war would probably be one in which cyberspace and social media activities would support kinetic actions, or even vice versa, in that cyber operations would play the lead role.[15]

This idea gained traction following the interference in the 2016 US presidential election and the 2017 NotPetya attack on the Ukrainian fiscal system, both committed by Russian state(-backed) actors. While the war in Ukraine (or the armed conflict between Israel and Hamas) is not a war in which cyber operations dominate, the persistent conflict in cyberspace is, nonetheless, the largest cyberoperation witnessed so far.[16]

In the war in Ukraine, both Russian and Ukrainian state and non-state actors are engaged in intelligence activities (through cyberspace or otherwise),[17] undermining critical infrastructure via cyberattacks and digital influence operations.[18] Oddly enough, the most effective operations are not the cyberattacks on critical infrastructure but the cognitive activities using cyberspace as a vector. Whereas most cyberattacks during the Russian-Ukrainian war are labelled as mere hindrances,[19] the synchronised effect of digital influence operations is strategically important for both sides. Russian actions influence domestic populations, and pro-Russia narratives sow discord and undermine Ukrainian morale. However, the most effective cognitive activities are Ukrainian operations that influence Western audiences in gaining support for the Ukrainian cause, which is strategically important.[20]

The Anatomy of Disinformation – How Does It Work?

Words have an effect, whether persuasive, coercive or manipulative. Cognitive activities aim to influence human cognition without threatening or imposing kinetic force. The ultimate goal of cognitive warfare is “directly interfering with or subconsciously controlling the enemy’s brain”.[21] This would enable an operator to “induce mental damage, confusion, and hallucinations in the enemy, forcing them to lay down their arms and surrender”.[22]

Not all influence operations employ subconscious methods. Coercive influence operations cut short or circumvent the targeted audience’s deliberate understanding and autonomous decision-making process, forcing them to make an ‘unwilling’ choice consciously. The targeted audience is well aware of the coercive action, leaving them with no other options. Influence operations are not malign per se. Persuasive influence operations aim to change the weighing and number of options available to targeted audiences, so that they make a voluntary (or willing) choice that benefits the influencer. The PRC’s public opinion warfare is an example of a persuasive influence operation using media outlets, including China Global Television Network (CGTN) and the Global Times, to paint a benign but framed picture of the PRC.[23]

While persuasive and coercive influence operations use rational and conscious techniques, manipulative influence operations use subconscious and covert techniques, subverting or usurping the autonomous decision-making process. An often-used technique to deflect target audiences into making reflexive and biased judgements based on cognitive and social heuristics, rather than on rational deliberations, is disinformation.[24]

Disinformation is inherently deceptive; it uses heuristics and biases to lure the target audience away from rational decision-making processes in favour of

what Petty and Cacioppo call the peripheral route.[25] The peripheral route is invoked by luring the target audience towards realistic socially divisive topics (such as poverty, racial issues, or police violence) and then impairing their ability to process incoming data related to that topic by linking the topic to subconscious biases. The information – or rather disinformation – provided to impair the public will be framed and adjusted to the target audience. Groups or individuals will be incapable of verifying or making sense of incoming data due to an overload of data or lack of time. In the 2016 US election, posts were disseminated, targeting religious areas in the US, claiming that candidate Clinton was endorsing gender equality or even stating that she was lesbian herself. Deeply religious people may disapprove of gender equality or same-sex marriage, and hence they would likely anchor Clinton to those negative sentiments. Likewise, posts were shared claiming that the Pope endorses Trump.[26]

Disinformation – in contrast to malinformation (hate speech or trolling) or misinformation (unintended misleading data) – is intentionally misleading information aiming to gain, or contribute to, a strategic intent. Disinformation has different guises. First, it can be deliberately false or fabricated to be deceptive. Second, disinformation can occur when the content and context of a message are not in congruence. Suppose French President Macron were to deliver an official speech in a foreign language or during a Sesame Street broadcast. In that case, the content might be correct, but the message would still be misleading due to the incompatibility with the context. Following this rationale, a commercial or advertisement in which the message is "framed", delivered by a cartoon polar bear or even intentionally misleading, should not be considered disinformation since the context is congruent with the content of the message.

Protection Against Disinformation

Countering disinformation is challenging, not only in practical terms but also in legal and ethical terms. Awareness-raising and digital hygiene are beneficial for augmenting resilience in society, especially when disinformation campaigns are difficult to attribute. There is, however, an underlying tension for open and transparent democratic systems. On the one hand, there is a desire to halt or counter disinformation campaigns by hostile actors such as Russia, while on the other hand, 'maintaining the values that Western democracy is built upon – of freedom of information and expression – is paramount to preserving the legitimacy' of our democratic institutions.[27] Violating these values will be portrayed as an act of hypocrisy and could be further exploited by hostile actors. An example of this is the banning of Russia Today (RT) and Sputnik by the EU in 2022, which sparked protests, first and foremost, by agencies of EU journalists since it violated the foundational principles and freedoms as expressed in international human rights law, such as the European Convention on Human Rights, to which the Russian Federation was also a party.

Hellman and Wagnsson have categorised four avenues for countering Russian information warfare,[28] based on the one hand on the notion of engaging or not, and, on the other hand, on focusing inwards on domestic audiences or outwards on foreign audiences. The resulting avenues are confronting, blocking, naturalising, and ignoring. This template can also be used to assess countering disinformation more generally. Banning RT and Sputnik is an example of blocking the dissemination of disinformation from Russian outlets to promote the pro-Russian war narrative at a time when EU members were expressing support for Ukraine. The PRC's 'block information', part of its confrontational actions,[29] is another example of this avenue. Blocking aims to actively protect one's own population.

A more passive method could be awareness campaigns against malign disinformation on social media, or educational packages for secondary school students. The result would be the ignoring of disinformation. This trend was noticeable during the 2018 mid-term elections and the 2020 US presidential election. After the revelations about Russian interference during the 2016 presidential election, the electorate was no longer naive about the messages being spread on social media platforms.

A state could also focus on the source of the disinformation or what the

receiver perceived as disinformation. A benign option is to amplify the core values of one's own society and persuade other states to adopt these values. Numerous Western states advocate individual human rights in states with collective human rights.[30]

More assertively, one could counter or confront the disinformation directly and fight fire with fire. Covert activities by armed forces, especially the state's intelligence services, could play a role in a confrontational counter-disinformation policy. This implies that state agencies would operate below the threshold of using (armed) force, often within the jurisdiction of another state, which could have legal ramifications since activities may go well beyond traditional espionage.

Paradoxically, many Western states have solid legal and legitimate frameworks for deploying kinetic military forces. However, they are highly reluctant to deploy security forces in the cognitive realm and in areas with effects below the force threshold.

Conclusion and Reflection

While the nature of cognitive warfare is age-old, the development of cognitive psychology and the inception of cyberspace have given cognitive warfare a more comprehensive range and increased its effectiveness. Cognitive warfare can be a useful instrument in the hybrid toolbox of a state or state-like actors. However, strife, competition, or even war – armed conflict between states – can and will only be won if the interplay between kinetic, informational, and cognitive warfare is in unison. These elements must have a unity of purpose and be synchronised. Cognitive warfare alone will not win the war.

Disinformation is an essential technique for waging cognitive warfare, as it directly affects human cognition. Disinformation – as frames, narratives or images with a deliberately misleading context or content – uses subconscious manipulation of the human brain by appealing to heuristics and biases that circumvent the rational decision-making process.
So what? What does this mean for future cognitive warfare and disinformation operations? While numerous developments and challenges come to mind, three stand out:

1. New technologies (such as Artificial Intelligence large language models, including ChatGPT) as generators of disinformation. While the anatomy of disinformation is based on the workings of our neural networks, disinformation can also be produced based on algorithms. Big Data analysis can predict behaviour based on correlations instead of causality, invoking a near-deterministic mode of human behaviour. Future disinformation will not be crafted by cunning humans but by sheer computational power, making it even more powerful but at the same time elusive and uncontrollable.

2. Second, there is an influx of private and non-state actors. If disinformation is a tool to gain strategic advantages, one might assume that state actors will instigate it. While the resources of these actors are almost unlimited, the number of actors is limited, and their actions will also be constrained by legal and ethical boundaries reflecting their ideologies and cultures. With the influx of non-state actors, the number of actors has increased exponentially. If they are willing or able to make use of new technologies, they may become an increasingly large set of actors in conflict and war that are unaffected by international law – examples of which have already been witnessed during Russia's recent campaign in Ukraine.

3. Finally, the threat in the cognitive dimension lies in the asymmetry between worldviews, especially between liberal democratic and authoritarian – between states or even within a state. Diverging worldviews should not be problematic in a healthy society. Their existence should reflect the democratic core values of freedom of expression. They can become problematic, however, if groups in society are locked in social media bubbles that are no longer connected. While war and warfare have been the prerogative of armed forces for eons, perhaps the real conundrum is what kind of role those forces will have in the era of cognitive warfare.

Endnotes

[1] Carl von Clausewitz, On War, ed. Michael Howard and Peter Paret (Princeton University Press, 1989), 75.
[2] Nino Tsikhelashvili, “Cognitive Warfare Through Reflexive Control Strategy In Georgia,” The Defence Horizon Journal, no. September (2023).
[3] Peter Mattis, “China’s ‘Three Warfares’ in Perspective,” War On The Rocks, 2023.
[4] Koichiro Takagi, “The Future of China’s Cognitive Warfare: Lessons from the War in Ukraine,” War on the Rocks, 2022.
[5] Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (London: Profile Books, 2020); Linda Robinson et al., Modern Political Warfare: Current Practices and Possible Responses, 2018.
[6] Ralph D. Sawyer, Sun Tzu: Art of War (Westview Press, 1994).
[7] Shaun Walker, “Beatings, Dog Bites, and Barbed Wire: Life and Death on the Poland-Belarus Border,” The Guardian, 2023, https://www.theguardian.com/world/2023/oct/02/beatings-dog-bites-and-barbed-wire-life-and-death-on-the-poland-belarus-border.
[8] Alicia Wanless and Michael Berk, “The Changing Nature of Propaganda,” in The World Information War: Western Resilience, Campaigning, and Cognitive Effects, ed. T. Clack and R. Johnson, 1st ed, (Routledge, 2021), 66.
[9] Buddhika B. Jayamaha and Jahara Matisek, “Social Media Warriors: Leveraging a New Battlespace,” Parameters 48, no. 4 (2019): 11–23.
[10] Buster Benson, “Cognitive Bias Cheat Sheet,” Better Humans, 2016. See also the Cognitive Bias Codex: https://www.sog.unc.edu/sites/www.sog.unc.edu/files/course_materials/Cognitive%20Biases%20Codex.pdf.
[11] Timothy L. Thomas, “Russia’s Reflexive Control Theory and the Military,” The Journal of Slavic Military Studies 17, no. 2 (2004): 237–56, 238–243.
[12] Andrew Radin, Alyssa Demus, and Krystyna Marcinek, “Understanding Russian Subversion: Patterns, Threats, and Responses,” no. February (2020), 2–3; United States Senate Committee on Intelligence, “Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election – Volume 2: Russia’s Use of Social Media,” vol. 2, 2019, 12–13.
[13] Johan E. Korteling, Anne-Marie Brouwer, and Alexander Toet, “A Neural Network Framework for Cognitive Bias,” Frontiers in Psychology 9 (2018), 2.
[14] Samuel C. Woolley and Philip N. Howard, “Political Communication, Computational Propaganda, and Autonomous Agents: Introduction,” International Journal of Communication 10 (2016), 1.
[15] John Arquilla and David Ronfeldt, “Cyberwar Is Coming,” in In Athena’s Camp: Preparing for Conflict in the Information Age, ed. John Arquilla and David Ronfeldt (RAND, 1997), 79–89; John Stone, “Cyber War Will Take Place!,” Journal of Strategic Studies 36, no. 1 (2013): 101–8; Richard Stiennon, There Will Be Cyberwar (IT-Harvest Press, 2015); Alec Ross, “Will the Next War Be a Cyberwar,” Policy Review, 2019, 16–19.
[16] Digital Security Unit, “Special Report: Ukraine – An Overview of Russia’s Cyberattack Activity in Ukraine,” Microsoft, 2022; Office for Budget Responsibility, Fiscal Risks and Sustainability, 2022, 49–50.
[17] Matthias Schulze and Mika Kerttunen, “Cyber Operations in Russia’s War against Ukraine,” SWP Comments, 2023.
[18] Cyber Peace Institute, “Cyber Dimensions of the Armed Conflict in Ukraine,” 2023.
[19] With the exception of the ViaSat attack on February 23, 2022. It is not stated whether cyberattacks (including wiperware) might have had a strategic impact, but at the time of writing, this does not appear to be the case. See Kraesten L. Arnold et al., “Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russo-Ukrainian War,” in Reflections on the Russian-Ukrainian War, ed. Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (Leiden University Press, 2024) (forthcoming).
[20] Amber Brittain-Hale, “Clausewitzian Theory Of War In The Age,” The Defence Horizon Journal, no. December (2023).
[21] Takagi, “The Future of China’s Cognitive Warfare: Lessons from the War in Ukraine.”
[22] Idem.
[23] Paul Charon and Jean-Baptiste Jeangène Vilmer, “Chinese Influence Operations: A Machiavellian Moment,” 2021, 29–31; Emilio Iasiello, “China’s Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities,” Journal of Strategic Security 9, no. 2 (2016), 52–56.
[24] See e.g., Johan E. Korteling, Maaijke Duistermaat, and Alexander Toet, “Subconscious Manipulation in Psychological Warfare,” 2018; Robert B Cialdini, Influence: The Psychology of Persuasion, Rev. ed. (New York: Harper, 2007).
[25] Richard E. Petty and John T. Cacioppo, “The Elaboration Likelihood Model of Persuasion,” Advances in Experimental Social Psychology 19 (1986), 126.
[26] Renee Diresta et al., “The Tactics & Tropes of the Internet Research Agency,” New Knowledge, 2018.
[27] Aiden Hoyle and Peter B.M.J. Pijpers, “Stemming the Narrative Flow: The Legal and Psychological Grounding for the European Union’s Ban on Russian State-Sponsored Media,” Defence Strategic Communication 11, no. Autum (2022): 51–80, https://doi.org/10.2139/ssrn.4220510.
[28] Maria Hellman and Charlotte Wagnsson, “How Can European States Respond to Russian Information Warfare? An Analytical Framework,” European Security 26, no. 2 (2017): 153–70, 157–158.
[29] Charon and Jeangène Vilmer, “Chinese Influence Operations: A Machiavellian Moment.”
[30] Government of the Netherlands, “Joint Statement on Behalf of 47 Countries in the UN Human Rights Council on the Human Rights Situation in China” (2022); He Zhipeng, “The Chinese Expression of the International Rule of Law,” Social Sciences in China 38, no. 3 (2017): 175–88, 180–181.

The Highest Form of Freedom and the West's Best Weapon to Counter Cognitive Warfare

MATTHIAS WASINGER

Author: Matthias Wasinger is a Colonel (GS) in the Austrian Armed Forces. He holds a Magister in Military Leadership (Theresan Military Academy), a Master's degree in Operational Studies (US Army Command and General Staff College), and a PhD in Interdisciplinary Studies (University of Vienna). He has served both internationally and nationally at all levels of command. He is also the founder and editor-in-chief of The Defence Horizon Journal. Since 2020, he has served at the International Staff/NATO Headquarters in Brussels. The views expressed in this paper are the author's alone.

Abstract: "Our remedies oft in ourselves do lie, which we ascribe to heaven." Shakespeare's timeless words echo throughout history and find validity in contemporary struggles. Modern warfare is, waged in the human domain more than ever, with the human mind becoming the battlefield in cognitive warfare. The aim is to change not only what people think - but how they think and act. Waged successfully, cognitive warfare shapes and influences individual and group beliefs and behaviours to favour one's objectives. Whereas information warfare seeks to control pure information in all its forms, cognitive warfare seeks to control how individuals and populations react to the information presented. Therefore, achieving and preserving cognitive superiority is key. However, this prized end does not justify using all given means.

Problem statement: How to understand the correlation between cognitive warfare and limitations imposed by Western values?

So what?: State actors can achieve cognitive superiority, either inductively through regulations and laws or through educational empowerment. Whereas restrictions might serve as a temporary solution to mitigate immediate risks, only education provides democracies with a sustainable solution. Any total defence approach has to be built on understanding, common values and the educated willingness to fight for the respective identity.

Source: shutterstock.com/Sergei Elagin

A “Great Patriotic War”?

February 24, 2022: The Russian Airborne Forces (Vozdushno-Desantnye Voyska Rossii; VDV) seized the Ukrainian airfield in Hostomel. News of this lightning-swift airborne operation travelled around the world, with reports carrying undertones of Ukraine’s impending collapse. Yet the VDV, despite capturing this vital airport, withdrew without achieving any lasting battlefield success.[1] Mirroring Napoleon’s Old Guard, the VDV was reputedly an elite force, renowned for its consistent success in challenging tasks. In reality, however, the VDV, like the Old Guard, was rarely deployed in demanding missions against an enemy willing to fight. In both cases, the narrative shaped perception. Yet at Waterloo in 1815 and Hostomel in 2022, reality crushed rhetoric.

The Russian Army’s thrust towards Kyiv proved futile. A 64km logistics convoy was transformed from a symbol of imperial might into a soft target for dispersed Ukrainian land and special forces – something all too apparent by March 2, just a week into the invasion.[2] To gloss over the fact that Russia had fielded a Potemkin military in Ukraine, Russian President Vladimir Putin would eventually, during the 2022 Victory Day parades in Moscow, draw parallels between the Great Patriotic War (Russia’s euphemism for the Second World War) and the campaign in Ukraine.[3] What was expected to be a swift, low-risk political decapitation of Ukraine was suddenly transformed verbally into an epic comparable to the Soviet Union’s existential struggle to repel and ultimately defeat invading German forces more than 80 years earlier.

However, we must ask ourselves why Vladimir Putin compared this historical existential threat against all Russians – insinuating the need to unleash the nation’s entire might – with what the Russian state is calling a “Special Military Operation” (SMO) rather than a war.[4] Mere propaganda, balancing the need to mobilise the nation while acknowledging the Russian population’s rejection of the term “war”?[5] Or playing with emotions on all sides?

On February 25, 2022, US Secretary of State Antony Blinken offered to extract the Ukrainian government from the country. Ukrainian President Volodymyr Zelenskyy supposedly – and

in an archetypal American manner - responded, “I don’t need a ride; I need ammunition.”[6] In the months that followed, and while visiting nations that supported Ukraine, such as Germany and the United Kingdom, references were made to Germany’s historical obligation to stand alongside those defending themselves against invading, fascist powers, as well as the UK’s (self-proclaimed) isolation and endurance during the Battle of Britain 1940/1941.[7,8] Mere propaganda and emotional manipulation once again?

The phenomenon is not new, however. Throughout history, states and non-state actors have shaped the perceptions and understanding of their respective target groups. Just as Cato urged the destruction of a Carthage that had already been crippled 50 years prior,[9] Vladimir Putin is trying to spin his failed venture in Ukraine as an existential struggle for Russia. While rejecting the fact that his campaign is a full-fledged war, Putin has euphemistically embraced the term SMO, which he sees as imposed on him by an ever-expanding, imperialistic West. Much like Ernst Moritz Arndt’s Der Gott der Eisen wachsen ließ,[10] written in 1812 to mobilise anti-Napoleonic sentiments in the German states, President Zelenskyy’s communications morally obligate target audiences to support his nation’s cause.

At this point, a distinction must be made between disinformation, misinformation, information warfare, and cognitive warfare. Disinformation and misinformation refer to the dissemination of false or misleading content. Whereas the former is carried out deliberately to gain an advantage over one’s adversaries, the latter happens unintentionally.[11] Both disinformation and misinformation are, among other things, means of information warfare. This is a war fought explicitly with and for information.[12] Cognitive warfare uses information and technology, among other things, to shape and exploit the way information is understood and processed. It is purposefully concerned with exploiting the way in which people comprehend their world in order to achieve cognitive superiority.

In cognitive warfare, belligerents compete for cognitive superiority by leveraging cognitive biases. Whether they are exacerbated, confirmed, rejected or limited by emotions, memories and culture, cognitive biases shape how we understand information. As we live in the information age, the human mind has become more of a battlefield than ever before - and in contemporary war, it might just be the key terrain.

Why People’s Sentiments Matter

War is a social phenomenon. The processes of democratisation and social inclusion have transformed Western states into democratic and sovereign entities, with people playing a crucial role in this phenomenon as both effectors and as target audiences. Wars are waged in, around, for, and by societies, involving members of the armed forces, democratic campaign enablers, and sustainers or influencers in the information realm.[13]

Clausewitz’s classic definition of war as an act of compelling the other to submit to one’s will remains valid. Contrary to Clausewitz’s times, geopolitical actors have a broader range of effectors at hand to achieve their goals in addition to military might. These can be seen in the DIME concept (Diplomacy, Information, Military and Economy). DIME is a commonly accepted minimum set of Instruments of Power (IoP). According to Hybrid CoE in Helsinki, these IoPs target thirteen areas in the democratic ecosystem.[14]

In Western democracies, the democratic ecosystem is built around the needs of the respective society and increases social resilience.[15] To understand the role of society in resilience and resistance, and the armed forces as an integral part thereof,[16] war theory distinguishes between wars with limited and unlimited objectives (versus wars with limited and total means). Whereas nations, thus far, do not fight with unlimited (nuclear) means, they do so for limited or unlimited objectives. Thus, fighting can be aimed at gaining a political bargaining chip to control a region of particular interest, or to force an opposing government to retreat.[17] Actors repeatedly deploy all their available or required IoP below the nuclear threshold in what is known today as hybrid warfare. Conventional, unconventional, sub-conventional, irregular, and even criminal forces and techniques are coordinated and synchronised across all available domains.

They are embedded in and supported by diplomatic and economic efforts. Deception and the infinite power of information are fundamental to this concept.[18]

In this context, the information domain is paramount when it comes to achieving objectives and influencing both intended and unintended effects. Narrative dominance is essential, encompassing the ability to inform, raise reasonable doubts or create plausible deniability. Western democracies ideally strive to perfect their information policies in terms of reliability, accuracy and sourcing. Antagonists, in contrast, seek to achieve superiority by focusing on the speed of information distribution.[19] Both parties have to acknowledge the factual nature of both information and its interpretation. In competing for a target audience's support, actors must balance the quality, quantity, velocity and continuity of information campaigns. Playing by the rules is disadvantageous in this competition since Western values and laws ideally exclude proactive disinformation campaigns.

However, this is just one side of the coin. The question is not solely about who introduces information first, but also about attribution and steering societal understanding to gain public support. The competition for cognitive superiority is vital when in campaign mode.

Superiority in Cognitive Warfare

In cognitive warfare, the human mind is the battlefield. Cognitive warfare aims to change not only what people think but how they think and act. Waged successfully, it shapes and influences individual and group beliefs and behaviours to favour an aggressor's objectives.[20] Whereas information warfare seeks to control pure information in all of its forms, cognitive warfare aims to control how individuals and populations react to the presented information.[21]

Another challenge stems from the fact that using cognitive warfare to achieve cognitive superiority requires an understanding of a vast theoretical and academic field; mastery is therefore complicated. Cognitive warfare calls for competence in the fields of communication studies, anthropology, social science, history and cultural aspects, among others, which may prove to be as crucial as so-called emerging and disruptive technologies. The latter range from Big Data to autonomisation and the Internet of Things.[22] Never before have emerging and disruptive technologies exerted such an influence on the way humans understand and process information. In the information age, automatisation, autonomisation, as well as digitalisation, warfighting, and its preparation rely heavily on cyberspace and the information space. Whereas the former is a human-made space, the latter is an overarching space that is constantly being influenced, whether intentionally or unintentionally.

Cyberspace has essentially facilitated the creation of the vitreous human and – potentially – a transparent society. Digitalisation and the everyday use of cyberspace have turned this artificial domain into a place of real consequence, a diplomatic tool, an economic factor, a military effector, and a social space, satisfying the human need for social connectivity, among other things. Cyberspace has contributed to the democratisation of information, while allowing malign actors to influence target audiences, set and dominate narratives, and exploit information.

Indeed, all these means, including the internet, artificial intelligence, machine learning, and troll factories spreading disinformation and exploiting misinformation, are used to create ambiguity and sow doubt in order to erode societal resilience. Facts are deliberately spun to provide an advantage, question an adversary's legitimacy, and diminish public support for enemies.[23] There is often no need for the Russian government to spread lies (although it regularly does); it is enough to exacerbate eternal fears (the use of nuclear weapons), make false equivalences (Ukraine, Iraq, Afghanistan, Serbia), or reframe the past (Molotov-Ribbentrop Pact). These endeavours, coordinated and synchronised, are supported by trend analyses in social media and widely spread in cyberspace, fuelling the ideas of nihilistic, opportunistic sceptics.

Technology and an understanding of human nature provide geopolitical (and economic) actors with the means to bolster morale, determination and ambition, while diminishing the influence of antagonists on their respective key

target audiences, and weakening an opponent's support base.[24] Hence, achieving and maintaining cognitive superiority is critical. However, sustainable geopolitical success is not merely contingent on technical and analytical mastery.

Soft Power as a Crucial Factor

Western societies draw might and sustainability from democratic legitimacy and legitimation.[25] Sustainability in peace and war is no longer limited by the quality and quantity of armed forces, but by the willingness of the demos to sustain and fight for a social model.[26] Consequently, the demos has become both a kinetic and a non-kinetic objective, a target audience.[27]

In addition, so-called Western values – human dignity, freedom, democracy, equality, the rule of law and adherence to human rights – have empowered societies and created the West's soft power and sustainable wealth.[28] Soft power is significant in this context since the leading antagonist powers lack this kind of social attractivity.[29,30] The fact is that although Vladimir Putin is (surprisingly) still not universally despised given his most recent political deeds,[31] hardly anyone aspires to the Russian way of life. The same applies to the People's Republic of China (PRC). US interventions in Iraq and Afghanistan, which were legally questionable to say the least, as well as the use of Guantanamo Bay as a pseudo-legal detention facility, have hardly affected the attractiveness of the American way of life. On the other hand, the PRC's Belt and Road Initiative (BRI) and Russia's economic support, with immediate effects on the ground, have hardly led to sustainable economic growth and social development in their respective regions.[32] Nor have the PRC and Russia managed to establish themselves as attractive soft powers that trigger economic, social, or political immigration.

Moreover, Western values and liberty pose an existential threat to these illiberal powers. Whereas military containment does indeed create strategic challenges for antagonist states, the proximity of liberal societies endangers their entire governmental system and social model. A military threat perception can be countered by military means; restrictions cannot effectively counter social liberalism, however, as was proven decades ago in a divided Germany with the Berlin Wall.[33]

The Western way of life, its liberties and privileges are what antagonist powers fear the most. This is also reflected in Vladimir Putin's framing of his most recent campaign in Ukraine. Claims such as NATO expansion, Western intrusion into Ukraine, and Russia's vital security requirements do not reflect the apparent military threat to Russia. Modern weapons technology renders these claims illusory. Enhanced connectivity, space and cyber technology, as well as hypersonic and both air defence and missile technology, have marginalised the role of geographical proximity. In addition, stealth technology and long-range weapon systems enable powers to penetrate deep into an adversary's sovereign territory from great distances. The real threat lies in the advance of a liberal social concept that can only be countered by military means. The most recent invasion of Ukraine was not triggered by a military threat posture; rather, it was the consequence of an existential governmental and social danger. Since this line is hard to sell, Putin needed other justifications, such as the aforementioned, to mask his decision. Therefore, promoting an SMO to his own population that draws parallels with the Great Patriotic War, while continuously blaming a so-called NATO expansion, goes far beyond propaganda and disinformation; it is a blatant (and all too often successful) attempt to shape target audiences' understanding. Geopolitical players like Vladimir Putin are well aware of the political and social fault lines and the ever-present scepticism towards the US.[34]

In the face of global competition for cognitive superiority in war and peace, the Western community stands at a crucial inflection point: How to deal with a contested information domain that undermines social cohesion? This decision point offers two apparent options: restriction or education and empowerment.

An Unfair Game

In an immediate response to Russia's most recent invasion of Ukraine and ongoing efforts to dominate the information domain by gaining cognitive superiority, the European Union (EU) banned Russian state-owned media outlets, among others, on 2 March, 2022.[35] Although understandable as an immediate action to counter malign narrative building, shaping and steering, this decision, from a mid- to long-term perspective, undermines Western values and liberty. EU citizens have an inherent right to pick and choose information sources.[36] Like all freedoms, freedom of information is based on the assumption that mature citizens are sufficiently educated. Combined with the media's legal and moral obligations to publish news objectively and truthfully, citizens need to be educated and empowered to decide whether a source is reliable. Indeed, the question arises as to how to deal with external media outlets that are neither bound by nor adhere to good publishing standards. They must be tolerated, however, as failure to do so may pave the way for arbitrary media restrictions. Despite its vulnerabilities, press freedom is one of democracy's crucial pillars.

In view of Russia's attack on Ukraine, the immediate ban on Russian state-owned media outlets was a necessary, well-discussed, and considered decision. Nevertheless, it seeded conspiracy theories among some about Western narrative control in favour of Ukraine. Those minorities who felt misled and misinformed following the Covid pandemic saw this as further proof of conspiracy.[37] Unfortunately, due to the complexity of the information space, the longer such media remain restricted, the easier it becomes for antagonists to sow doubt about the legitimacy and legality of such actions, and to promote a self-proclaimed truth that is "obscured" by the mainstream. Malign actors can argue that such actions exist to suppress freedom of thought and enable social control. Thus, restrictions become tools of cognitive warfare as a theoretical (but not logical) plausibility starts to drive alternative narratives.

There is also a tendency in politics to prioritise short-term needs over long-term threats.[38] Although the imposed restrictions represent a short-term requirement, they are neither sustainable from a democratic perspective nor conducive to countering Russia's cognitive efforts. The longer these restrictions are maintained, the clearer another critical shortfall becomes: society's lack of education.

Social conduct can be understood and influenced by attitudes and behaviour.[39,40] In the short term, regulations and limitations may serve to shape behaviour in such a way that it complies with the outlined requirements. However, only a change in attitude will lead to sustained compliance with a state's needs.[41] Attitudes can be developed through the cultivation of a common understanding. Consequently, and particularly from a democratic standpoint, long-term educational empowerment is a whole-of-society tool for countering cognitive warfare and preserving a democratic identity.

In this regard, a major challenge in the coming years will be malign actors' activities in the cognitive arena that will lead us to undermine our own core values. Western democracies must resist the temptation to restrict transparency and freedom of information in an effort to dominate the cognitive domain. Contrary to the given logic, fighting the beast must not lead to becoming the beast ourselves. Cognitive warfare is an unfair game, and certain aspects should be accepted. Self-imposed discipline within a liberal society may ultimately be the most efficient way to counter cognitive warfare; after all, personal self-discipline is the highest form of freedom.

State actors can achieve cognitive superiority, either inductively through regulations and laws or through educational empowerment. Whereas restrictions might temporarily mitigate immediate risks, thus treating the symptoms, education alone treats the cause by teaching people how to understand when they are the target of malign manipulation. Vladimir Putin might complain about NATO expansion and promote a Great Patriotic War; however, as we have seen time and time again, educated citizens across the world see Putin's words for what they are: Lies.

In today's information-centric world, many autocratic powers exhibit great military strength. Nevertheless, the attractive way of life in liberal

societies, adequately protected by robust, sustainable armed forces, remains a threat to such regimes, and one that cannot easily be defeated. In Machiavelli's words, "Fear is a very stable foundation for a relationship".[42] If there is one thing that antagonist powers fear the most, it is Western values, namely our liberty, equality, and dignity. Education is the key to effectively countering malign actors' deeds while maintaining our identity. Moreover, societal education levels are a precondition for a more prosperous society. This ultimately leads to even more soft power for our societies.

Endnotes

[1] Dermot Nolan, "When Lightning Fails to Strike: Russia's Failure to Secure Decisive Victory in Ukraine," The Defence Horizon Journal, 2022, last accessed October 19, 2023, https://www.thedefencehorizon.org/post/russia-failure-victory-ukraine.
[2] Eric Beech, "Russian Military Convoy North of Kyiv Stretches for 40 Miles," 2022, last accessed October 20, 2023, https://www.reuters.com/world/europe/russian-military-convoy-north-kyiv-stretches-40-miles-maxar-2022-03-01/.
[3] Guy Faulconbridge, "Putin Touts 'Sacred' Battle with West in Ukraine as Russia Marks Pared Back Victory Day," 2023, last accessed October 20, 2023, https://www.reuters.com/world/europe/russia-hold-victory-day-parade-amid-tight-security-after-drone-attacks-2023-05-08/.
[4] Lawrence Freedman, COMMAND: The Politics of Military Operations from Korea to Afghanistan. [S.l.]: ALLEN LANE, 2022, 395-399.
[5] Timothy Frye, Weak Strongman: The Limits of Power in Putin's Russia. Princeton: Princeton University Press, 2021, 145-148.
[6] Glenn Kessler, "Zelensky's Famous Quote of 'Need Ammo, Not a Ride' Not Easily Confirmed," The Washington Post, 2022, last accessed October 20, 2023, https://www.washingtonpost.com/politics/2022/03/06/zelenskys-famous-quote-need-ammo-not-ride-not-easily-confirmed/.
[7] President of Ukraine, "Address by President of Ukraine Volodymyr Zelenskyy to the Bundestag," last accessed October 20, 2023, https://www.president.gov.ua/en/news/promova-prezidenta-ukrayini-volodimira-zelenskogo-u-bundesta-73621.
[8] President of Ukraine, "Address by the President of Ukraine to the Parliament of the United Kingdom," last accessed October 20, 2023, https://www.president.gov.ua/en/news/zvernennya-prezidenta-ukrayini-volodimira-zelenskogo-do-parl-73441.
[9] Andrew D. Lambert, Seapower States: Maritime Culture, Continental Empires and the Conflict That Made the Modern World, New Haven: Yale University Press, 2019, 86-87.
[10] Ernst Moritz Arndt wrote this patriotic poem (Song to the Fatherland) in 1812, denouncing the fact that several German states fought on Napoleon's side against German nations. "The god who made iron grow, Did not want slaves; Therefore he gave sabre, sword and spear, To man in his right hand; Therefore he gave him bold courage, The rage of free speech, So that he would prevail to the last drop of blood, Even unto death, in the struggle."
[11] Shaping Europe's digital future, "Tackling Online Disinformation," last accessed October 29, 2023, https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.
[12] TDHJ, "How to Set a Theater from an Information Warfare Perspective," last accessed October 29, 2023, https://www.thedefencehorizon.org/post/information-warfare-theater-setting.
[13] Rupert Smith, The Utility of Force: The Art of War in the Modern World. New York: Vintage Books, 2007, 7-9.
[14] European Commission, Joint Research Centre, "HYBRID THREATS: A COMPREHENSIVE RESILIENCE ECOSYSTEM," last accessed October 19, 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf, 8.
[15] Ibid., 7-9.
[16] Samuel P. Huntington, The Soldier and the State: The Theory and Politics of Civil-Military Relations. Renewed ed. Cambridge, Mass., London: Belknap Press, 1985, 80-97.
[17] Donald J. Stoker, Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present. Cambridge United Kingdom, New York NY USA: Cambridge University Press, 2019, 4-19.
[18] Vladimir Slipchenko and M. A. Gareev, Budushchaí á Voĭna. Moskva: OGI, 2005, 11-28.
[19] Barbie Zelizer, "The Disinformation Ecosystem," last accessed October 28, 2023, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf, 1-3.

[20] North Atlantic Treaty Organization. “Countering Cognitive Warfare: Awareness and Resilience,” last accessed October 19, 2023, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.
[21] Megan Burns, “Information Warfare: What and How?,” last accessed October 19, 2023, http://www.cs.cmu.edu/~burnsm/InfoWarfare.html.
[22] Bernhard Schulyok, Lukas Grangl, and Markus Guber, “A Primer on the Functional Trinity of the Information Environment,” The Defence Horizon Journal, 2023, last accessed October 19, 2023, https://www.thedefencehorizon.org/post/trinity-information-environment.
[23] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare, First edition, New York NY: W. W. Norton & Company, 2021, 68-76.
[24] Bernhard Schulyok, Lukas Grangl, and Markus Guber, “A Primer on the Functional Trinity of the Information Environment,” The Defence Horizon Journal, 2023, last accessed October 19, 2023, https://www.thedefencehorizon.org/post/trinity-information-environment.
[25] Andreas Stupka, Militärwissenschaften: Ihre Grundlagen Und Ihr System, Schriftenreihe der Landesverteidigungsakademie Wien Sonderpublikation 2011,1, Wien: Republik Österreich, Bundesminister für Landesverteidigung und Sport, 2011, 81.
[26] Morris Janowitz, The Professional Soldier: A Social and Political Portrait, Free Press trade paperback edition, New York: Free Press, 1960, 395-397.
[27] United States, The Petraeus Doctrine: The Field Manual on Counterinsurgency Operations, Joint Chiefs of Staff joint publication 3-24, [Washington, D.C.]: Joint Chiefs of Staff; Aquitaine Media Corps, 2009, VI-2.
[28] Daron Acemoglu and James A. Robinson, Why Nations Fail: The Origins of Power, Prosperity, and Poverty, Pbk edition. London: Profile Books, 2013, 428-462.
[29] Jonathan E. Hillman, The Emperor’s New Road: China and the Project of the Century, New Haven, London: Yale University Press, 2020, 9-15.
[30] Timothy Frye, Weak Strongman: The Limits of Power in Putin’s Russia. Princeton: Princeton University Press, 2021, 38-40.
[31] Janakee Chavda and Moira Fagan, “Large Shares See Russia and Putin in Negative Light, While Views of Zelenskyy More Mixed,” last accessed October 29, 2023, 195Z, https://www.pewresearch.org/global/2023/07/10/large-shares-see-russia-and-putin-in-negative-light-while-views-of-zelensky-more-mixed/.
[32] Daron Acemoglu and James A. Robinson, Why Nations Fail: The Origins of Power, Prosperity, and Poverty, Pbk edition. London: Profile Books, 2013, 428-462.
[33] Timothy Frye, Weak Strongman: The Limits of Power in Putin’s Russia. Princeton: Princeton University Press, 2021, 44-47.
[34] Beshay and Moira Fagan, “Poles and Hungarians Differ over Views of Russia and the U.S,” accessed October 29, 2023.739Z, https://www.pewresearch.org/global/2023/10/02/poles-and-hungarians-differ-over-views-of-russia-and-the-us/.
[35] “EU Imposes Sanctions on State-Owned Outlets RT/Russia Today and Sputnik’s Broadcasting in the EU,” last accessed October 28, 2023, https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/.
[36] European Union Agency for Fundamental Rights, “Article 11 - Freedom of Expression and Information,” last accessed October 28, 2023, https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information.
[37] Kai Bohme, Marcela Mader Furtado, Marita Topitsidou, Sabine Zillmer, Sebastian Hans, Dea Hrelja, Alessandro Valenza, and Arianna Mori, “Research for REGI Committee: The Impact of the COVID-19 Pandemic and the War in Ukraine on EU Cohesion, Part II: Overview and Outlook,” last accessed October 28, 2023, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733095/IPOL_STU(2022)733095_EN.pdf, 36-68.
[38] David M. Edelstein, Over the Horizon: Time, Uncertainty, and the Rise of Great Powers, 1st paperback printing, Ithaca, London: Cornell University Press, 2020, 16-17.
[39] United States, The Petraeus Doctrine: The Field Manual on Counterinsurgency Operations, Joint Chiefs of Staff joint publication 3-24, [Washington, D.C.]: Joint Chiefs of Staff; Aquitaine Media Corps, 2009, VI-2, VIII-8-VIII-12.
[40] David Kilcullen, Out of the Mountains: The Coming Age of the Urban Guerrilla, London: Hurst & Company, 2015, 17.
[41] Niccolò Machiavelli, “Discourses on Livy,” last accessed October 28, 2023, https://identityhunters.files.wordpress.com/2017/07/niccolo-machiavelli-discourses-of-livy.pdf, 8.
[42] Niccolò Machiavelli, The Prince, Penguin classics, London: Penguin Classics, an imprint of Penguin Books, 2014, 66-67.

The Role Of Cyber Security In Cognitive Warfare

MARIA PAPADAKI

Author: Dr Maria Papadaki is an Associate Professor in Cyber Security at the Data Science Research Centre, University of Derby, UK. She has been an active researcher in the cyber security field for more than 15 years, focusing on incident response, threat intelligence, maritime cybersecurity, and human-centred security. Her research outputs include 70+ international peer-reviewed publications in this area. Dr Papadaki holds a PhD in Network Attack Classification and Automated Response, an MSc in Networks Engineering, a BSc in Software Engineering, and professional certifications in intrusion analysis and penetration testing. The views contained in this article are the author's alone and do not represent those of the University of Derby.

Abstract: Cognitive warfare has taken advantage of the 21st century's technological advances to evolve and alter the way humans think, react, and make decisions. Several stages utilise cyber security technological infrastructure, especially in the initial stages of content creation, amplification and dissemination. In fact, evidence points to the use of cognitive threats as a means of inciting wider cyberattacks and vice versa. The war in Ukraine has accounted for 60% of observed cognitive incidents, with Russia being the main actor in this context. The DISARM framework outlines the two nations' prominent Tactics, Techniques and Procedures (TTPs) as the development of image-based and video-based content, the impersonation of legitimate entities, degrading adversaries, and the use of formal diplomatic channels. Combining the DISARM and ATT&CK frameworks could enhance the analysis and exchange of threat intelligence information.

Problem statement: How to analyse the relationship between cyber security and cognitive warfare and what lessons can we learn from the war in Ukraine?

So what?: Although the DISARM framework is still in the early stages of its development, it provides an invaluable step towards opening up the dialogue on and understanding of FIMI behaviours across the community. Adopting cyber security concepts for the rapid build-up of capacity and resilience in the cognitive domain would be beneficial. In parallel, educating a multi-disciplinary workforce (and society as a whole) against combined scenarios of cognitive warfare and cyberattacks would help to improve their resilience.

Source: shutterstock.com/Skorzewiak

Marking a Step in an Ever-Evolving World

While militarisation continued to decrease across the globe for 15 years prior to 2022, the world has not become more peaceful. According to the 2022 Global Peace Index, 70% of countries have reported a decline in peace over the past 15 years, with discourse, polarisation, social division, violent demonstrations, and conflict affecting societies globally.[1] The prevalence of misinformation and disinformation is considered to be the most significant catalyst. The underlying aim of the two is ostensibly rooted in destabilising trust in information and political processes among the masses. Misinformation and disinformation are also seen as potentially posing a more severe threat than a hot conflict or weapons of mass destruction over the next ten years. At the same time, cyberattacks consistently remain among the top 10 risks in global risk rankings, and their significant impact highlights the need to boost our level of preparedness across the globe.[2]

Relating the Concepts

As a first step towards investigating the relationship between cybersecurity and cognitive warfare, it is important to consider relevant terms. Due to the dynamic nature of the threats in question, terminology may vary depending on the source or the time of publication. In other words, the terms below, including disinformation and FIMI (explained below), are not mutually exclusive semantically. This suggests the need to review such overlaps by adopting an interdisciplinary approach and perspective. It is also important to recognise that conventional warfare is expanding into cyberspace and the information space, where FIMI threats are expected to play a significant role (e.g., using cyber-infrastructure to dismiss or distort information on casualties or the impact of conventional warfare operations).

Term	Description
Misinformation	"false or misleading information *shared without harmful intent*, although the effects can be still harmful."
Disinformation	"verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security."
Foreign Information Manipulation and Interference (FIMI)	"a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory."
Cognitive Warfare (CogWar)	"CogWar is not necessarily new but has emerged as a product of the integration and confluence of many technological advances and as availability and access to information and technology has increased. CogWar takes well-known methods within warfare to a new level by attempting to alter and shape the way humans think, react, and make decisions. CogWar has emerged replete with security challenges due to its invasive, intrusive, and invisible nature and *where the goal is to exploit facets of cognition to disrupt, undermine, influence, or modify human decisions*. CogWar represents the convergence of a wide range of advanced technologies along with human factors and systems, such as Artificial Intelligence (AI), Machine Learning (ML), Information Communication Technologies (ICT), neuroscience, biotechnology and human enhancement that NATO's adversaries are deliberately using in the 21st-century battlespace. CogWar presents a significant risk to global defence and security at every level, including economic, geopolitical, social, cultural, and threatening human decision-making."

Describing terminology; Source: EEAS.

Based on the definitions above, there are many similarities between misinformation and disinformation, but also between FIMI and cognitive warfare. According to the 1st European External Action Service (EEAS) Report on Foreign Information Manipulation and Interference Threats (FIMI) and the EEAS Strategic Communications (STRATCOM) Activity Report, both misinformation and disinformation are defined as fake content, but disinformation is distinguished by the intentional creation and sharing of false information. The same report introduces FIMI threats, which are characterised by their intentional nature and coordinated manner, and which also have actors, intentions and features in common with cognitive warfare.[3,4] The NATO Science and Technological Organization (STO) Human Factors and Medicine (HFM) Exploratory Team (ET) 356 describe Cognitive Warfare (CogWar) in greater depth and highlight its reliance on human factors and technology, such as ICT, AI, neuroscience, biotechnology and human enhancement.[5]

Professor Seumas Miller also recognises that cognitive warfare focuses on altering how a target population thinks, and hence how it acts by weaponising public opinion to influence public and governmental policy and destabilise public institutions. Furthermore, he identifies the origins of cyber warfare in psychological operations (PSYOP) and information warfare, noting its

heavy reliance on new ICT technologies, social media platforms, cybertechnologies (e.g., bots) and, notably, AI. He also pinpoints disinformation and sophisticated psychological manipulation techniques as key features of cognitive warfare.[6]

The definition of cyber security has also evolved to reflect its ubiquity, pervasiveness, and rapidly evolving nature. The latest ISO/IEC TS 27100:2020 standard defines it as "safeguarding of people, society, organisations and nations from cyber risks. Safeguarding means keeping cyber risk at a tolerable level". Cyber risk is defined as "[the] effect of uncertainty on objectives of entities in cyberspace, where cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace". In turn, cyberspace is defined as "[an] interconnected digital environment of networks, services, systems, people, processes, organisations, and that which resides on the digital environment or traverses through it".[7]

Cyber Security for Representing and Understanding FIMI Threats

One example of interdisciplinary collaboration within the FIMI defender community is the creation of the DISARM (DISinformation Analysis & Risk Management) framework, designed to represent a knowledge base and taxonomy of known FIMI adversarial behaviours, as well as defences against them.[8,9] It is inspired by MITRE ATT&CK®, a curated knowledge base and model for cyber adversary behaviour from the cyber security domain. Both frameworks are open source, aiming to fight cyber and FIMI threats respectively by sharing threat intelligence data, conducting analyses, and coordinating effective actions. The DISARM Red framework represents Tactics, Techniques and Procedures (TTPs) of incident creator FIMI behaviours, whereas DISARM Blue describes potential response options.

When examining the cognitive warfare operations in the war in Ukraine, one can identify numerous examples of FIMI threats that the DISARM framework can shed light on. According to the 1st EEAS Report on FIMI threats, the war in Ukraine accounted for 60% of observed incidents.[10] In the context of the invasion, incidents have sought to distort the narrative and shift the blame onto other actors, such as Ukraine or the EU. Russia is the main actor, utilising a plethora of techniques, the most prominent of which are outlined by the DISARM framework as follows:

- Develop image-based and video-based content (T0086, T0087)
- Impersonate legitimate entities (T0099)
- Degrade adversaries (T0066)
- Use formal diplomatic channels (T0110)

The development of fabricated images and video content was used to distort facts by reframing events, degrading an adversary's image or ability to act, and discrediting credible sources. Aiming to reach a wider audience, the content was translated into multiple languages. Observed incidents featured at least 30 languages, 16 of which were EU-based. Formal diplomatic channels were used to deliver content, distort facts by reframing the context of events, and degrade adversaries. Fabricated content was then amplified and distributed by cross-posting across multiple groups and platforms, which propagated it to new communities among the target audiences or to new target audiences.[11]

Russia's cognitive warfare operations in Ukraine are evidently designed to:

- Dismiss allegations: e.g., claiming that Kyiv staged the Bucha massacre to discredit the Russian army.
- Distort the narrative and twist the framing: e.g., the alleged discovery of U.S. biolabs in Ukraine to justify the "special military operation".
- Distract attention and shift the blame onto a different actor or narrative by "scapegoating": e.g., claiming that the West demonises Vladimir Putin and hinders negotiations.
- Dismay to threaten and frighten opponents: e.g., intimidating Russia's political opponents.
- Divide to generate conflict and widen divisions within communities: e.g., spreading the hoax that a Ukrainian court had ordered the demolition of an Orthodox church.

According to the 1st EEAS Report on FIMI threats, the war in Ukraine has also provided evidence of alignment and support between Russia and the People's Republic of China (PRC), with some content (such as the alleged U.S. military biolabs in Ukraine) being amplified by PRC-controlled media and official social media channels. There were also instances of providing a platform for sanctioned Russian media outlets.[13]

FIMI threats utilise cyber security technological infrastructure, especially in the initial stages of content creation, amplification, and dissemination. In fact, specific cyberattacks could be considered a precursor to FIMI incidents and vice versa, which further supports the case for using both the DISARM and ATT&CK frameworks in combination. For instance, cyberattacks could be used to obtain information that could later become the basis for fake content creation in information operations. Similarly, stealing voter registration data could support and develop specific narratives, whereas obtaining personal email addresses could be used to disseminate content. Fake accounts could be created, existing accounts compromised to establish legitimacy, and websites hacked to display fake content.[14]

Finally, one example which illustrates that FIMI incidents serve as a precursor to cyberattacks would be the March-October 2022 incidents, where content was routinely posted by a hacker group through Telegram, and systematically amplified by Russian state-controlled outlets to incentivise with cryptocurrencies any cyberattacks against Westerners "lying" about the Ukrainian invasion.[15]

It is also important to consider the effect that FIMI threats could have on the cyber security domain. As the emergence of deepfakes and "disinformation-for-hire" services could lead to novel, highly sophisticated and successful impersonation attacks and deception techniques, understanding FIMI adversarial behaviours would also help build our resilience against them and maintain our security posture.[16]

Although the DISARM framework is still in the early stages of its development, it marks an invaluable step towards facilitating the dialogue on, and understanding of, FIMI behaviours across the community. It paves the way for improving the analytical maturity of FIMI threats and standardising threat intelligence information exchange. Moreover, it exemplifies the benefits of adopting cyber security concepts in the cognitive warfare domain, illustrating that cyber security could contribute to the rapid build-up of capacity and resilience in the cognitive domain.

Thoughts on Countering Cognitive Threats

Western communities' level of preparedness for cognitive threats is continuously improving, with threat intelligence communities monitoring, analysing, and preparing defences against such pervasive threats. Having the infrastructure in place to detect, model, study and communicate the evolution of cognitive threats is key to devising effective defence strategies. The strong links and relationships between cognitive warfare and cyber security could be hugely beneficial.

However, technology alone will not suffice; education, simulation, and gamified learning could be useful to support awareness-raising and information literacy campaigns, eventually aiming to improve the resilience of a multi-disciplinary workforce against combined scenarios of cognitive warfare and cyberattacks. Recognising the importance of positive security to support the transition from awareness to a security culture, in which secure behaviour is integrated and becomes the default option, will be key.[17]

Endnotes

[1] Institute for Economics and Peace (IEP), “Global Peace Index 2022: Measuring peace in a complex world,” June 2022, https://www.visionofhumanity.org/wp-content/uploads/2022/06/GPI-2022-web.pdf.
[2] World Economic Forum, “The Global Risks Report 2023: 18th Edition Insight Report,” January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.
[3] European External Action Service (EEAS), “1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence,” February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.
[4] European External Action Service (EEAS), “2021 STRATCOM Activity Report: Strategic Communication Task Forces and Information Analysis Division (SG.STRAT.2),” 2021, https://www.eeas.europa.eu/sites/default/files/documents/Report Stratcom activities 2021.pdf.
[5] Yvonne Masakowsi, and Janet Blatny, “Mitigating and responding to cognitive warfare,” NATO Science and Technical Organization, March 2023, https://apps.dtic.mil/sti/citations/trecms/AD1200226.
[6] Seumas Miller, “Cognitive warfare: an ethical analysis,” Ethics Inf Technol 25, 46 (September 2023), https://doi.org/10.1007/s10676-023-09717-7.
[7] ISO/IEC 2700, “Information Technology - Cybersecurity - Overview and concepts” (2020).
[8] “DISARM Framework Explorer,” DISARM Frameworks, last modified November 2023, https://disarmframework.herokuapp.com/.
[9] Erika Magonara, Apostolos Malatras, “Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape,” ENISA, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape/.
[10] European External Action Service (EEAS), “1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence,” February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.
[11] Idem.
[12] Nicolas Hénin, “FIMI: Towards a European redefinition of Foreign Interference,” EU Disinfo Lab, April 2023, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/.
[13] European External Action Service (EEAS), “1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence,” February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.
[14] Erika Magonara, Apostolos Malatras, “Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape,” ENISA, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape/.
[15] European External Action Service (EEAS), “1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence,” February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.
[16] Joseph Buckley, and Stina Connor, “Cyber Threats: Living with Disruption,” Control Risks and AirMic, October 12, 2021, https://www.controlrisks.com/our-thinking/insights/reports/cyber-threats-living-with-disruption.
[17] Sidney Dekker, Just Culture: Restoring Trust and Accountability in Your Organization (Third Edition, CRC Press, 2016).

The Russia-Ukraine Conflict From a Hybrid Warfare Cognitive Perspective

JOSEF SCHRÖFL SÖNKE MARAHRENS

Author: Josef Schröfl started his career in the Austrian Armed Forces in 1982 and worked since then in various areas of the military, including several military operations/UN tours, e.g., to Syria. Since 2006 he served in the Austrian MoD, heading: “Comprehensive Approach”, “Hybrid threats”, and “Cyber Security/Cyber Defence”.

He holds a B.A. in Computer Technology, an M.A. in International Relations from the University of Delaware/US, and a PhD in International Politics from the University of Vienna. Several publications/books on Asymmetric/Cyber/Hybrid threats, crisis, conflict and warfare. Peer Board member/reviewer of/from several magazines, e.g., “The Defence Horizon Journal”. Current position: Deputy Director for CoI Strategy & Defence at the hybrid CoE in Helsinki/Finland, leading the Cyber-workstrand there.

Sönke Marahrens, Colonel i.G. (GER AF), Dipl. Inform (univ), MPA, Director, COI Strategy & Defence. He is a career Air Force officer, previously serving as head of research for Strategy and Armed Forces at the German Institute for Defence and Strategic Studies in Hamburg. As well as a Full Diploma in Computer Science, he holds a master’s degree from the Royal Military College in Kingston, Canada, and another from the University of the Federal Armed Forces in Hamburg. He was deployed with NATO to Bosnia and Kosovo, and in 2020 served as Branch Head for Transition at HQ Resolute Support in Kabul, Afghanistan.

The views expressed in this article are solely those of the authors and do not represent the views of Hybrid CoE, or the Austrian and/or the German Federal Armed Forces.

Abstract: Russia’s invasion of Ukraine has had major global consequences, ranging from a humanitarian crisis resulting in millions of refugees, to food crises in the Near East and Africa, followed by a worldwide energy crisis with economic shocks triggering geopolitical realignments, ultimately affecting all military domains, including cyberspace. Specifically, since the Russian invasion on 24 February 2022, Moscow has tried to bring Kyiv to its knees in the cyberspace domain. Accordingly, this paper analyses how hybrid and non-hybrid, cyber and information warfare have worked in Russia’s favour, and where these tools and techniques might have failed. It highlights how the electromagnetic spectrum cannot be fully separated from the cyber and information spaces.

Problem statement: How to analyse the relationship between cyber security and cognitive warfare and what lessons can we learn from the war in Ukraine?

So what?: Whoever has the edge in cyberspace has the ability to shape what people and societies perceive as the truth, as well as control the narrative about what is happening physically on the ground. Lessons from the war in Ukraine call for a coordinated and comprehensive strategy from Western states to strengthen defences against the full range of cyber-destructive acts, espionage, and influence operations.

Source: shutterstock.com/Marco Iacobucci

The Hybridity of Russia's Attack on Ukraine

On the morning of 24 February 2022, Russia's attack on Ukraine suddenly catapulted the West into a reality that it had not acknowledged until then. Since then, the larger Western states have been forced to abandon the self-cultivated state of self-deception that they had been labouring under. Western military strategists have coined the acronym 'VUCA' – volatility, uncertainty, complexity and ambiguity – to describe the characteristics of the future operational environment, or, more pessimistically, 'BANI', which stands for brittle, anxious, nonlinear, and incomprehensible. It can be said that the Russians have been highly dynamic in creating - either intentionally or unintentionally - VUCA or BANI conditions for the West with near-perfect precision.

The invasion of Ukraine cannot be understood without taking into account Russian President Vladimir Putin's view of history. In his view, Russia has had to assert itself against enemies from the West for 1,000 years to achieve its strength – most recently in the Second World War. Putin accuses the West of denying Russia's world power status since 1990,[1] a worldview that results in a permanent sense of threat. Accordingly, to pursue his goals, Putin has merely reactivated the old methods from the KGB junk room. The "old" Soviet instruments included:

- Disinformation and misinformation: Fake news must be spread on all channels. In recent years, the Kremlin has also built up its own media industry with RT and Sputnik in order to influence opinions abroad. A speciality of both Soviet as well as current Russian disinformation is the reinterpretation of real or historical events.

- Sabotage: The goal is to confuse the enemy and destabilise the enemy population's trust in its government's ability to provide the basic necessities of life. State actors work closely with organised crime, a general feature of Russian warfare.

In contrast to the Soviet era, however, new and additional "digital fire accelerators" are available through the internet and social networks.

Hybrid war is, therefore, a perpetually evolving phenomenon. Hybrid warfare (based on hybrid threats carried out with military means in particular) is still an interim term for the phenomenon. In the Hegelian sense, "hybrid war" can be seen as the antithesis of war

in a world that situated war in international humanitarian law and finally prohibited it by making all nations sign the UN Charter. However, the synthesis is still missing. According to Hybrid CoE,[2] four characteristics of hybrid threat activity (encapsulating threats and warfare) can be distinguished:

1. It is not a single event.
2. It needs a malign intent/actor.
3. It is conducted within authoritarian systems, challenging democratic rule-based systems.
4. The grey zone is created by the defender, not the attacker; the latter is merely exploiting the defender's unwillingness to protect red lines. The antagonist exploits either the unwillingness of the rule enforcer to defend the rules or the complexity of created laws and rules, which provides the malign actor with the opportunity to either misuse those rules or create dilemmas through the application of those rules.

Russia's War in Ukraine Through a Hybrid War Lens

Russia's hybrid threat campaign against Ukraine and its surroundings before 24 February 2022 was a strategic masterpiece of thought. Neither the US, NATO, nor the EU were sure what was happening, and the hybrid threat activities instilled fear (or pragmatism about survival) in the Baltic states, Sweden, and Finland.[3] The hybrid threat campaign was highly agile, constantly scanning for weak points in the West and addressing them almost immediately with legal, information, disinformation, and diplomatic means. These efforts were accompanied by a rather lengthy military show of force around Ukraine, adding to the overall uncertainty.

The less successful unfolding of military events after 24 February 2022, whereby the Russian forces could not exploit their assumed tactical agility, may have been accompanied by a strategic meltdown within Putin's inner circle. The moment the Russian President started humiliating some of his senior leaders publicly, including the head of his intelligence service, Sergey Naryshkin, and later, his Chief of Defence, General Valery Gerasimov, the necessary organisational trust may have been broken. The organisation was reset into a less proactive "just follow orders" mode to avoid further humiliation, which reduced military efficiency and the effectiveness of ongoing hybrid threat activities against the West.

Lack of Electronic Warfare: Problems Due to Russia's Own Communications?

After the intensive use of electronic warfare capabilities (e.g., jamming frequencies or disturbing electronic devices like GPS equipment) during the last eight years by the Russian military in the Donbas/Luhansk region, the Western definition of the military cyber domain was recently expanded to incorporate electronic warfare. Hence, Western military experts assumed that Russian military operations in Ukraine would be accompanied by the heavy electronic warfare activities that had already been demonstrated. This did not happen, however. Western experts have different explanations for the absence or lack of electronic warfare activities. This means that Russia is conducting an ever more intense cyber and information war, including the electromagnetic spectrum: The systematic distribution of psychologically and ideologically grounded material of a provocative nature can generate psychosis. If this is also combined with partly truthful and false information, accompanied by attacks on critical infrastructure, it is not hard to imagine how despair and a mood of doom may undermine confidence in the government and armed forces. Such measures serve a nihilistic ideology of pure power.

It looks as if Russia has been struggling with the problem of the tradeoff between jamming frequencies and the necessity to maintain command and control of its troops by using those frequencies. Further, it is confronted with the so-called "last mile" problem of supporting mobile forward-deployed forces with digital data. The Russian forces have apparently bypassed this problem by using Ukrainian communication networks.[4]

Ukrainian intelligence sources published numerous Russian military communications intercepted via internet connections through Ukrainian networks, which, of course, prevents Russian commanders from giving orders to shut down those networks using electronic warfare. The electromagnetic spectrum has been used to interfere with and/or disrupt the adversary's flow of information. Russia attempted to cut off cyberspace within Ukraine by shutting down their server and mobile connections, such as 3G/4G band, to disrupt their national command and control systems so that the Ukrainian departments responsible for monitoring these systems would not be able to counter Russian disinformation.[5]

Other parts of cyberspace are adding new dimensions to this conflict. Cyber, including IT and the information domain, has become as hard a power as military power. On the Western and international front in particular, it looks as if Ukraine is winning the war of social media memes and narratives against Russia. However, it is still difficult to evaluate the extent to which the Russian population, influenced as it is by fake narratives about "denazification"[6] and "preventing a genocide", can be reached or influenced by the Ukrainian counter-narratives. Furthermore, the Western media see a kind of applied "hybrid" thinking in the clandestine use of Russian military forces against targets in Belarus, and presumably in Luhansk, to foster Belarusian and separatist support. It is too early to evaluate the impact of the IT hacking activities. After Ukraine amassed an "army of 30,000" hackers and Anonymous took Ukraine's side,[7] it is not entirely clear what is going on in the networks. There is intense activity in the cyber domain. However, it is difficult to assess whether Ukraine has consolidated its IT security sufficiently due to being under constant attack, whether Russian troops still need access to the internet as a primary means of communication, or whether Anonymous is neutralising Russian troll factories.

A Hybrid War Gone Rogue

Today, Russia's invasion of Ukraine or, as the Kremlin calls it, the "Special Military Operation", has to be understood as a hybrid war that went rogue. However, after the initial failure in late February 2022, Russia's activities must also be analysed and addressed as part of conventional war theory rather than merely "hybrid war" theory. One of the main intents of Russian propaganda activities is to "dehumanise" the other side. Targeted means of influencing serve as part of psychological warfare, a common method in times of war. From now on, these narratives will determine how and what the West should think about a crisis/war and what judgment should be made. Many political scientists agree that Ukraine's conflict with Russia – an established cyber superpower that does not hesitate to flex its muscle aggressively – could test the rules of war in new and unexpected ways. Some say it already has.[8]

The cyber domain is the new battlefield, and its means, such as information operations, could be as effective as conventional military means, although NATO, the EU and their member states have yet to fully grasp this. Is it a new comprehensive domain, or is it better to regard its elements separately? The same could be said about the electromagnetic spectrum. The electromagnetic spectrum, the information space, and cyberspace reside within the physical dimensions of the information environment and can be used as sites of warfare, equivalent and akin to the domains of land, air, sea, and space.

From the authors' perspective, these domains are of equal value. Moreover, it must always be considered that one can influence the other and that information or electromagnetic attacks cannot be that successful without using cyberspace. The connection can also be summarised with an analogy: It is a threaded pipe in which water flows. The thread is the electromagnetic spectrum, the pipe is cyberspace, and the water represents the information flowing through it. Therefore, the electromagnetic spectrum cannot be fully separated from cyberspace and the information space.

The operations of the Russian Armed Forces, and especially their warfighting tactics, have often failed to meet even basic international standards such as International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC), which adds an organisational or systemic dimension to the file of observed war crimes committed by individual soldiers.[9]

Russia's War in Ukraine Through a Hybrid War Lens

Vladimir Putin's information-space army of trolls and cyber criminals has been unleashing its destructive power on the Western world for years. Their cyber-attacks have interfered in countless elections and referendums, with Brexit and the 2016 US election being the best-known examples. They hacked Western computer systems, spread viruses like NotPetya (one of the most disruptive cyberattacks in history) in Ukraine in 2017, and attacked Western critical infrastructures such as SolarWinds in 2020 and Colonial Pipeline in 2021. Moreover, they also fuelled conspiracy theorists and right-wing hardliners, as in the stories about Q-Anon or Western coronavirus vaccines.

However, when the time came to oversee Putin's most ambitious and probably most important operation, the information-space army failed on all fronts. The goal has been to spread false information and manipulate society to push for actions that can destabilise Ukraine during the war. However, rather than establishing in the minds of Europeans the narrative of Russia as the Eastern leader fighting Nazis in Ukraine and protecting all ethnic Russians, Ukraine has thus far dominated this online battle for the hearts of Westerners.[10] Furthermore, it is now very difficult for Russia to change the narrative. When the initial hybrid-threat approach of using land forces to coerce the Ukrainian government failed within the first ten days, the Russian Armed Forces regrouped, even (mis-) using safe Belarusian territory.

To the utmost surprise of Western observers, they chose a style of attack reminiscent of the First and Second World Wars, with mass artillery fighting rather than 21st-century doctrinal Western-based modern warfare, which relies on precision-guided munitions to reduce civilian casualties. This has increased the brutality of the Russian operations, causing heavy military casualties among the Ukrainian Armed Forces, as well as civilian casualties.

Besides the brutal and excessive use of military force under the statute of a military strategy described by experts as "Terror", the Community of Interest for Strategy and Defence at the European Centre of Excellence for Countering Hybrid Threats also observed overt applications in Ukraine of military methods attributed to the arsenal of hybrid warfare in sub-threshold environments: targeting and attacking systemic vulnerabilities to influence decision-making or undermine and terrorise Ukrainian society.

In addition to military targets, Russian forces and their proxies have started to strike Ukraine's societal system-relevant targets, conducting deliberate and repeated attacks on important railway infrastructure and power grid nodes. These attacks fit the hybrid definition and the definition of cross-domain effects in the Western Multi-Domain Operations terminology.[11] In sum, Russia has applied an overall systems-thinking approach to its warfare capabilities, allowing for more complex military operations.

While the Ukrainian railway system proved resilient,[12] the Ukrainian power system, presumably due to its size and need for essential infrastructure and critical spare parts, has regularly been severely affected by missile strikes with longer-lasting power outages.[13]

Russian disinformation experts have tried to influence the Ukrainian population through "targeted messaging" over the years. However, their efforts fell flat in light of the war crimes committed by Russian troops (e.g., in Bucha). Nevertheless, Russian propaganda concerning the "evil Ukrainians" continues to resonate among the Russian population, with internet polls still showing a total lack of Russian empathy or sympathy for Ukrainians.[14]

Although many Western observers have been surprised by the way in which Russia conducts its military operations, all of these examples are deeply interconnected and rooted in Russia's theoretical military and strategic thinking. However, for the first time, the Russian idea of reflexive control theory is being applied simultaneously and in parallel in sub-threshold hybrid warfare environments and real war environments; whether by accident or design can only be ascertained after the war.

Reflexive Control

"Reflexive control is an activity which influences the adversary's decision-making processes with a specifically altered piece of information in a prepared information campaign. The primary goal of such doctored information is to induce the other side to make decisions that are, in fact, predetermined by the producer of the doctored information."[15]

The concept of reflexive control has a long history in Russian military strategy. Taught in military schools and academies, it is also codified in the Russian National Security Strategy. Its elements include:

- Power pressure (provocation and deterrence);
- Measures to present false information about the situation (deception, distraction, and paralysis);
- Influencing the enemy's decision-making algorithm (exhaustion, divisions, and suggestion);
- Altering the decision-making time (pacification and overload).[16]

The foundations of Russian reflexive control, dating back more than 200 years, are rooted in the ideas of General Peter Rumyantsev and Alexander Suvorov.[17] Overall, reflexive control loosely aligns with the concept underpinning Chinese General Sun Tzu's commandments of war: "The supreme art of war is to subdue the enemy without fighting".

The concept was updated in the late 20th century in line with:

- Evgeny Messner's ideas on subversion-war an activity that is intended to erode an adversary's socio-cultural and military cohesion;
- Alexander Dugin's network-centric war more in a virtual dimension, establishing control over networks, more political than military, and not to be confused with Western ideas of Network-Centric Warfare; and
- Igor Panarin's information warfare, handling psychological and specifically informational aspects.

Accordingly, all information means are used to target decision-making processes by manipulating international and domestic public opinion.[18]

The Use of Modern Technologies with a Hybrid Character

Since the dawn of humankind, war has been a relentless innovator. Russia's war against Ukraine is no exception to this rule.

Cyber

The cyberspace war began long before the first Russian troops crossed the border into Ukraine. Since 2014, Ukraine has registered more than 5,000 cyberattacks on state institutions and critical infrastructure.[19]

By mid-2021, Russian hackers had begun targeting digital service providers, logistics providers and supply chains in Ukraine and abroad to gain further access to Ukrainian systems and those of NATO member states.[20] When all diplomatic efforts to de-escalate the conflict failed in early 2022, and the Russian military began to complete its troop deployment along the border with Ukraine, cyberattacks intensified rapidly. Hackers were also increasingly using wiper malware, which erases hard drives and data, against Ukrainian institutions.

On the one hand, Ukrainian IT systems are subject to constant Russian attacks. Cyberattacks do not cease during a conventional war. On the other hand, so-called spill-over or domino effects of offensive cyber operations – as predicted by Western experts as an argument against the use of offensive military cyber operations – have not yet been observed. Finally, critical infrastructures must be identified early, protected, and defended in the physical and cyber domains simultaneously.

Hybrid Threats and Warfare Around Ukraine

Russia has carried out extensive hybrid activities during the war in Ukraine, applying almost all of the above means and methods in other operations around the world:

- Russian Private Military Companies (PMCs) acted just as brutally in Africa as they did in Ukraine, but with almost no international reaction. The killing of 300 Malian civilians by Wagner mercenaries and Malian Army units drew almost no international condemnation;[21]
- Constant Russian disinformation campaigns through pre-established networks throughout Europe and the Americas;
- The use of so-called "useful idiots" and influencers in almost all Western societies;
- Unattributed or denied attacks on pipelines and critical infrastructures all over Europe; and
- Cyberattacks on Western political leaders, especially those who have publicly spoken out against Russia.

Fighting Value = Capabilities x Motivation

Both Western and Putin's experts mainly discuss technology as the driving force behind military might or power. However, military leaders are already taught at a very early stage of their careers that the fighting value of their troops must be seen as a function of their capability (technical means/weapons) to conduct a mission multiplied by their motivation squared.[22]

Normally, this is only seen at the individual force level, but Russia's war in Ukraine demonstrates that this must also be considered at a force-wide level. It would explain why the Ukrainian military and their "army of volunteers" can successfully take on the mighty battle-hardened Russian military, as the Ukrainian Armed Forces called it.

Poor mental preparation by the Russian ground forces, leading to deserters and abandoned equipment, can also be interpreted as a sign that the Russian military leadership, in particular, might have seen waging war as the only possible option within the overall hybrid threat campaign against Ukraine, and hence they failed to plan adequately. The Russian Armed Forces masked their initial main attack thrust axes into Ukraine – Kyiv from the North, Donbas/Luhansk from the East and Mariupol from the South – by deploying battalion task groups without any logistical or communications support, creating problems for Western intelligence services attempting to assess Russian intentions.

Fortunately for Ukraine, the deployment did not go as planned. The Russian forces have suffered from gaps in their communications and logistical setup in particular. The low morale of the troops should also be factored in, as reports from Belarus before the attack indicated that Russian units had cleared forestland for firewood and bought food with their own money.[23]

What Are the Implications of Russia's War in Ukraine for Hybrid Warfare and Hybrid Threats?

The Russian military forces, Secret Services, and PMCs are willing to engage in inhuman brutality and violence, even in the public eye. Hence, Western assumptions that covert operations, where attribution is almost impossible, would not be conducted by Russia or Russian operatives due to concerns about morale should be dismissed.

The authors are highly sceptical of the possibility that Western militaries, such as NATO Allies, with their ongoing and floating ideas of a "Cognitive Warfare Concept", will develop a concept that can cope with Russia's reflexive control theory. Copying it will be a value-based subset only, which cannot replicate the Russians' outreach. Moreover, Russia has implemented systems thinking into hybrid and conventional military thinking. It is conducting military operations and targeting accordingly. This fosters the need for rapid implementation of Multi-Domain Operations and a re-thinking of defence as total defence by integrating non-military security providers and striving for societal resilience.

Over the past year, pundits have constantly analysed and discussed possible scenarios for the outcome of Russia's war in Ukraine. One of the constants in all scenarios was that hybrid threats and warfare would continue due to their cheap and, unfortunately, effective and flexible nature. The unexpectedly high conventional losses of Russian military personnel and materiel amplify the risks of hybrid threats in a post-war setting. Regardless of whether Russia wins the

war, hybrid threats and warfare will be Moscow's first and cheapest choice to bridge the gap until it regains sufficient conventional military power, especially in the European geopolitical sphere.

What Should NATO and the EU Expect in the Future?

The West will likely be prepared for a protracted, mostly low-intensity war. Putin already perceives the imposition of sanctions almost as a declaration of war. For Russia, the means of retaliation could be cyber and disinformation operations. In its November 2023 report, Microsoft warned of increased Russian military offensive cyber operations (wiper malware) against European critical infrastructure in the coming months. These attacks began in February 2022, targeting Ukrainian government agencies and IT service providers. Collective Western efforts towards cyber resilience at national, EU, and NATO level urgently need to be accelerated.

The cyber threat landscape is evolving at a rapid pace. Europe must now prepare for ongoing grey-area conflicts. Through anticipation, risk mitigation, and creativity, the West can shift the balance of power in cyberspace in favour of the defenders of an unfragmented, safe, and free internet.

EU and NATO countries should develop satellite capabilities to provide internet coverage and connectivity. This would become part of a global doctrine to encourage open information provision in conflict zones and to counter authoritarian internet shutdowns. The logic should follow that of Cold War shortwave radio.

Whoever wins in the cyberspace domain decides what people and societies believe, what the truth looks like, and what is happening physically on the ground. Whoever loses the battle for information also loses the moment to act and win the physical war.

Endnotes

[1] Fiona Hill, “Putin kämpft den Krieg seines Vaters,” Die Zeit, Mai 06, 2015, https://www.zeit.de/politik/ausland/2015-05/gedenken-zweiter-weltkrieg-wladimir-putin-tag-des-sieges.
[2] European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats/.
[3] Finnish Ministry of Defence, “Russian attack on Ukraine and Finland’s support to Ukraine,” last accessed December 29, 2023, https://www.defmin.fi/en/topical/russian_attack_on_ukraine_and_finlands_support_to_ukraine#744487d3.
[4] “Ukraine conflict: Russian forces attack from three sides,” BBC, last accessed 29 December, 2023, https://www.bbc.com/news/world-europe-60503037.
[5] Idem.
[6] Patrick Gensing, Andrej Reisin und Carla Reveland, ““Entnazifizierung” als Vorwand,” Tagesschau, Feber 25, 2022, https://www.tagesschau.de/faktenfinder/russland-propaganda-ukraine-101.html.
[7] IT Army of Ukraine, https://itarmy.com.ua/.
[8] Vladimir Putin, “Article by Vladimir Putin ‘On the Historical Unity of Russians and Ukrainians’,” http://en.kremlin.ru/events/president/news/66181.
[9] Lonas Lexy, “Here are Russia’s alleged war crimes in the Ukraine invasion,” The Hill, https://thehill.com/policy/international/3262626-here-are-russias-alleged-was-crimes-in-the-ukraine-invasion/.
[10] The Guardian, https://www.theguardian.com/world/series/ukraine-live.
[11] Stephen Russell, Tarek Abdelzaher and Niranjan Suri, “Multi-Domain Effects and the Internet of Battlefield Things,” IEEE, https://ieeexplore.ieee.org/abstract/document/9020925.
[12] Jack Peat, “War-torn Ukraine running more reliable train service than TransPennine Express,” January 06, 2023, https://www.thelondoneconomic.com/news/war-torn-ukraine-running-more-reliable-train-service-than-transpennine-express-342002/.
[13] Claire Parker, “Russia and Syria conducted dozens of illegal ‘double tap’ strikes, report says,” The Washington Post, https://www.washingtonpost.com/world/2022/07/21/syria-russia-double-tap-airstrikes-report-war-crimes/.
[14] Lew Gudkov, “Interview Conducted by Christina Hebel in Moscow,” Der Spiegel, https://www.spiegel.de/international/world/opinion-researcher-lev-gudkov-russians-have-little-compassion-for-the-ukrainians-a-066c08c6-60f4-48e1-853a-d2b3d67bd6b8.
[15] “Seeing Red,” Hybrid CoE 8th Research Report, Jukka Aukia & Lucjan Kubica, March 2023, 34.
[16] Former Research Director of Hybrid CoE, Dr Hanna Smith, in a paper not publicly available, August 12, 2022.
[17] Idem.
[18] Idem.
[19] “The unfolding cyberwar in Ukraine,” Vision of Humanity, https://www.visionofhumanity.org/ukraine-cyberattacks-2022/.
[20] Office of Budget Responsibility, “Cyber Attacks During the Russian Invasion of Ukraine,” last accessed December 29, 2023, https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/.
[21] Emmanuel Akinwotu, “Russian mercenaries and Mali army accused of killing 300 civilians,” The Guardian, April 05, 2022, https://www.theguardian.com/world/2022/apr/05/russian-mercenaries-and-mali-army-accused-of-killing-300-civilians.
[22] Allan R. Millett, Williamson Murray and Kenneth H. Watman, “The Effectiveness of Military Organizations,” International Security 11, no. 1 (1986): 37-71, https://doi.org/10.2307/2538875.
[23] ISW, “Ukraine Conflict Updates,” ISW Press, last accessed December 29, 2023, https://www.understandingwar.org/backgrounder/ukraine-conflict-updates.

New Problems in Hybrid Warfare: Cyber Meets Cognition

CHRIS BRONK

Author: Chris Bronk is an associate professor at the University of Houston and director of its cybersecurity graduate program. He has conducted research on the politics and diplomacy of cyberspace; critical infrastructure protection; propaganda and disinformation; counter-terrorism; and cybersecurity. He has served as both a Foreign Service Officer and Senior Advisor at the U.S. Department of State. The views expressed in this article are the author's alone and do not represent those of the University of Houston nor the State of Texas.

Abstract: Hybrid warfare encompasses the area of adversarial relations between war and peace. In this space, questions have emerged about how cyber action, which involves the subversion of confidentiality, integrity, and availability of data, intersects with information operations (also known as propaganda or influence). While definitions of these phenomena remain imprecise and emergent, terms such as social and cognitive cyber security are gaining currency amongst scholars and practitioners.

Problem statement: How are cyber techniques used to disseminate information designed to influence publics, elites, and leaders?

So what?: The most open societies are likely the most vulnerable to data manipulation and information operations. The community of democratic states, namely those populating the OECD or the NATO alliance and its Pacific analogues, must erect defences against malign information influence delivered through cyberspace.

Source: shutterstock.com/Gorodenkoff

Conflict in Cyberspace

Strategic thinkers have been pondering conflict in cyberspace for three decades. In the 1990s, Arquilla and Ronfeldt argued that "Information is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labour have been in the industrial age".[1] Since then, the militaries of the United States and its Western allies have cashed in a peace dividend at the Cold War's end, waged a war on terror in the aftermath of 9/11, and have now entered a renewed period of great power competition, primarily marked by the rise of the People's Republic of China (PRC). Through all this, scholars and practitioners have debated the role of information and computing technologies in the calculus of power.[2]

Writing on power a decade ago, Joseph Nye described it as resting on three legs: military, economic, and soft power.[3] This is not far removed from where Carr rested his pillars of power in 1939, substituting "power over opinion" for Nye's more recently coined "soft power" term.[4] For all this consistency over time on what power is, Western societies have a tough time identifying and measuring this third leg of power.

The Cyber-Information Nexus

If there is an unanticipated externality of the rise of massively networked computing to the global scale, it is cybersecurity - the security of cyberspace, a construct of science fiction[5] and a theoretical vehicle of the earliest thinkers on robotics and forms of machine intelligence.[6] An interconnected, worldwide computational infrastructure, cyberspace can be a vehicle for both malicious behaviours undertaken through it, and attacks made upon it.[7] Cybersecurity is a desired end state. The National Institute of Standards and Technology, an agency of the U.S. Commerce Department, defines cybersecurity as:

> Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications

> services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[8]

For this work, cybersecurity is a socio-technical activity in which computer systems are protected from subversion or manipulation; activities often labelled as "hacking".[9] In the last thirty years, it has morphed from a curiosity into a significant area of military activity, described by the U.S. Department of Defense (DoD) as a conflict domain alongside land, sea, air, and space. The field has enormous taxonomies of vulnerabilities, attacks, defences, and other related phenomena. It is the intersection of computing and illicit, criminal, belligerent, and militarily hostile behaviour.[10]

Cybersecurity is largely a product of technological innovation for both offence and defence. The field is heavily preoccupied with attacks, which have definitional beginnings stemming more from intellectual contributions in cryptography and computing than international security.[11] Every attempt to subvert a system, or violate the five terms in NIST's definition above, is considered an attack. As time passes, practitioners are learning that cyberattacks are seldom decisive.[12] On their own, they can be - but rarely are - a form of coercive action.[13] Consider two cases, the first involving a cyber-kinetic hack and the second involving multiple incidents of data confidentiality compromise coupled with disinformation campaigns.

The first case, well-known and subject to much revisionist re-evaluation, is the Stuxnet cyberattack on the Industrial Control System (ICS) for Iran's nuclear enrichment infrastructure.[14] As best we can tell, in 2007, when the George W. Bush administration considered options for dealing with Iran's advancing effort to construct a nuclear weapon, diplomatic efforts were considered insufficient, while air strikes by Israel and the US appeared too risky.[15] Cyberattacks on Iran's centrifuges were weighed as a third option and eventually employed (along with covert action against Iran's nuclear scientists and engineers).[16] Four years after Stuxnet became public information, Iran agreed to curtail its nuclear programme, agreeing to a Joint Comprehensive Plan of Action (JCPOA) in July 2015.[17] The cyberattack against Iran's nuclear programme demonstrated technical superiority but was very narrow in scope. Stuxnet made enriching uranium harder for Iran by sowing some degree of chaos in the machines doing that job.[18] It did not deliver the JCPOA, but it certainly demonstrated a degree of technical sophistication not found elsewhere in achieving a major military-diplomatic goal.

Russia undertook a very different cyber campaign during the 2016 US presidential election.[19] While systems were subverted, email accounts "hacked", and information purloined from servers, cyber security was a component of a broader online influence campaign.[20] Cyberattacks against the Democratic National Committee and the Clinton campaign hardly matched the technical novelty of Stuxnet, but still had impact.[21] Emails purloined from the campaign and its chief of staff's personal email account were made public by a false leaker, Guccifer 2.0, acting as a stand-in for elements of Russian intelligence services.[22] Guccifer was not alone in doing this work. The leaks were a small part of a larger influence campaign to disrupt the 2016 election.[23] Representative Jackie Speier summarised the events in a hearing: "We basically have the brightest minds of our tech community here, and Russia was able to weaponise your platforms to divide us, to dupe us and to discredit democracy."[24] A combination of leaked information and social media advertisements damaged the Clinton campaign.[25] As with the JCPOA, the cyber actions undertaken by Russia in the 2016 election may not have been definitive in producing the outcome, but they likely shaped it to a degree.

To summarise, various forms of cyberattack diminished Iran's nuclear enrichment programme and the Clinton campaign. They both exposed how computerised tools and information resources could be subverted to produce an unexpected outcome. They are cases in which forms of information power (or smart power) influenced the outcome of events.

While we have narrow definitions of cyber security and cyberattack, the broader set of phenomena involving cyberattacks must also be considered. A cyberattack is an accepted tool in the repertoire of covert action.[26] Iran's centrifuges were tampered with by malicious software, but agents or operatives

of foreign powers also assassinated some of its nuclear scientists.[27] That targeted violence may also have influenced government decision-making in Tehran. Similarly, the cyberattacks on the Clinton campaign no doubt mattered, but so did Russian propagandists' words and advertising buys, which formed part of an information strategy designed to affect opinion.

Today, we are contending with both narrow and broad cyber securities. Consider attacks on cyberspace as well as those delivered through cyberspace again. An attack on cyberspace may be anything from denial-of-service to a kinetic attack by a process control computer. One coming through cyberspace may deliver messages that delegitimise politicians, purloin sensitive data, or confuse citizens. In narrow cyber security, there is a generally accepted offence-dominant bias in favour of the attacker.[28] We do not know whether this offence-dominant bias exists for broader forms of action undertaken through cyberspace.

Interdependencies Between Cyberspace and Information

Some years ago, I wrote "[C]yberspace is a reflection of the human condition".[29] This claim stands at odds with the military doctrinaires who see cyberspace as the first human-made domain in which forces fight wars.[30] This contention, in turn, is hard to square with Neal Stephenson's reference to cyberspace as a consensual hallucination.[31] Applying a comprehensive definition to cyberspace remains challenging. It is science fiction that became technological fact. Even the once fanciful concept of a noosphere appears to be more tangible.[32]

The linkages between the global digital infrastructure we call cyberspace and the information space of news, microblogs, short videos, and all manner of other images and text seem inextricable at this point. All the information that we consider news comes in packets. Flows of such information are subject to disruption in cyberspace. A decade ago, the website of The New York Times was knocked offline when the paper's domain name registrar was compromised by malicious hackers calling themselves the Syrian Electronic Army (SEA).[33] This disruption came at a critical point in Syria's civil war, after the Assad regime used nerve agent chemical weapons against domestic insurgents. Days before the hack, SEA reputedly compromised the Twitter account of the Associated Press and then sent a tweet: "Breaking: Two explosions in the White House and Barack Obama is injured[.]"[34] An ancillary result of the latter action was the $136 billion "flash crash" on the New York Stock Exchange. From that knee-jerk reaction, we learned the significant degree to which automated securities trading algorithms were linked to social media.[35]

It is reasonable to argue that cyberspace and the information space are largely intertwined. For this reason, the U.S. Department of Defense's labelling of cyberspace as a warfighting "domain" and information as an "environment" might have been a hasty decision.[36] However, there is more. Emergent concerns in cyber security mention AI and even neurocognitive hacking.[37] We remain concerned with the hacking of information resources, but must also accept forms of cyber information influence activity that are designed to alter human processing of information resources, denying, disrupting, or otherwise manipulating them. So much of the information we consume, guided by internet searches or social media prompts, will be computer-controlled or mediated. That can be hacked too.

The Cyber-Information-Influence Nexus

Put into print more than 80 years ago, E.H. Carr's conceptualisation of information power has advanced from delivery of international propaganda by the mass media of his time to tailored messages delivered via cyberspace today.[38] We see exemplars of information power in the operations to subvert democratic elections, spread disinformation, and incite violence against different ethnic or political groups. Cyberspace is the de facto medium of transmission for contemporary information operations.

What has arisen in the last decade are information and cyber operations from a set of states increasingly hostile to Western democracies. These nations, which include the People's Republic of China, Russia, North Korea, and Iran

(CRNKI), utilise information and computing technologies (ICTs) for espionage, political influence, economic destabilisation, and industrial sabotage. Western powers also use ICTs for espionage and covert action; differences arise in information controls.

The CRNKI states have created enormous infrastructure for information controls. They exchange technology and tradecraft for isolating themselves from the rest of the world's information ecosystem.[39] The rest of the world varies widely on online information controls. The U.S. and the Organization of Economic Co-operation and Development (OECD) countries largely embrace freedom of speech for online activity. This is not a universal norm, as more than 50 countries have either convicted or incarcerated citizens for their speech online.[40] States reside on a continuum of information and internet freedoms, and those with the greatest degree of freedom may be the most vulnerable to the malign influence of information.

A framework of understanding for cyber-information-influence may be found in contemporary advertising. While ads were once distributed in print publications or broadcast to wide audiences in television and radio programming, their transmission has been revolutionised by the internet. Facebook and Google, rebranded Meta and Alphabet, respectively, have generated enormous profits from the capacity of their platforms to issue precisely targeted advertisements to individuals based on their interests and online activity.

The messages pushed to individuals' devices, including televisions, personal computers, mobile telephones, and wristwatches, can be designed to influence beliefs. The aspiration to convince people to believe particular ideas is nothing new, but the Dick Tracy wristwatch is. This global constellation of internet devices, the äppärät for most of humanity, attracts an enormous amount of human attention.[41] Communicating ideas to äppärät is at the centre of a cyber-information-influence strategy. Returning to the relentless drive for advertising as a vehicle for Silicon Valley revenue, there is a certain irony that one of the two most popular mobile phone operating systems is largely designed to facilitate Google's Adwords mobile advertising software.

Our technical understanding of protocols, software, and hardware for delivering messages to computerised devices is relatively solid. Much remains to be learned when it comes to the efficacy and dynamics of the human-machine interface, however.[42] How do we know what ideas will take hold with individuals? Which individuals will influence their peers to believe such ideas? To what extent is a cyber-information-influence campaign effective at drawing societal attention and gaining acceptance among a large audience? The answer may be found in research programmes in cognitive warfare, for which multiple views are emerging.

"Cognitive warfare is … an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder action, with negative effects, both at the individual and collective levels."[43] Similarly, a pair of researchers posit that "Cognitive warfare is specific to the domestic information environments of … states … and takes as its overarching goal to undermine or shape domestic political processes by changing mindsets".[44] Both of these point to Carr's third leg of power, that over opinion. There may be a historical record of how propaganda and hybrid warfare have worked together, but what is relatively new is the computerisation of information. "Cognitive warfare is not new. Weaker parties in an asymmetric conflict have manipulated information and ideas to convince stronger opponents to not fight … What is new is the extent to which technologies enable cognitive warfare - resulting in the delegitimization of governments by sowing discord and creating division in order to compel acceptance of political will."[45]

At the beginning of the Intifada in 1987, Palestinians shifted their methods from violent terrorist activity to futile acts of stone-throwing against well-armed Israeli soldiers and police. The First Intifada's stone- throwers represent asymmetric victories of the (somewhat) non-violent or the ideologically driven, attempting to find support for their cause in a display of weakness. The application of overwhelming force employed by Israel's security forces has only served to generate greater sympathy for the Palestinians.

Conversely, the terror bombings of the Second Intifada are antithetical to the sympathy created by the futile resistance of its predecessor. These were both insurgencies tied to traditional media, especially television. The tableau of contemporary media is electronic, computerised, and persistent. Mobile devices, social media, and constant connection likely alter human cognition.[46] They change the methods of cognitive warfare, but the aim is still the same: to change how others think and feel about a particular people, cause, or issue.

At hand is how computing may change the discovery, presentation, and exchange of information in politics. A preferable term to cognitive warfare may be computerised political-cognitive influence (computational propaganda is also useful). What is important to recognise is that this exercise of power largely falls inside Carr's "power over opinion" category or Nye's "soft power".

The questions our discipline needs to ask now are: Do cognitive techniques work in statecraft, and how may we measure their effectiveness? Answers may be found in the areas of information and neuroscience, as well as psychology and computing.[47] Obviously, the more we learn about how digital devices affect our minds and perceptions, the more we know about how ICTs can influence beliefs and opinions.

The Cyber-Information-Influence Nexus

In Western democracies, an enormous amount of effort is expended in the media and news on offering opinions and exercising persuasion. It is puzzling why some groups or states resist, often at great cost, while others may capitulate with relative ease. Why has Ukraine stood fast against the most recent Russian invasion since February 2022?[48] How come the Afghan government left behind by the US-led international force there collapsed in days? [49] What can either of those examples tell us about a war over Taiwan? In understanding hybrid conflict involving information and cognition, we seek to know which tools of information power may produce the desired outcomes for those who wield them. In understanding the linkage between computing, information, and influence, we remain in the earliest of days. Hacking systems remains relatively easy. Hacking publics, states, and even alliances are far more challenging tasks. Cyber-information-influence tools that are simple in their employment and predictable in their effects are most likely quite a way off. That may not be all bad.

Note: This paper is a synthesis of materials produced for the early October 2023 Cyber Power Symposium on Hybrid Conflict/Warfare held by the European Centre of Excellence for Countering Hybrid Threats. An earlier draft was presented at the International Studies Association sub-conference at the US Air Force Academy in late October 2023.

Endnotes

[1] John Arquilla and David Ronfeldt, "Cyberwar is coming!," Comparative Strategy 12, no. 2 (1993): 141-165.
[2] James Der Derian, "The question of information technology in international relations," Millennium 32, no. 3 (2003): 441-456.
[3] Joseph S. Nye Jr, The future of power, PublicAffairs, 2011.
[4] E. H. Carr, The twenty years' crisis, 1919-1939: Reissued with a new preface from Michael Cox. Springer.
[5] Katie Hafner and John Markoff, Cyberpunk: outlaws and hackers on the computer frontier, revised. Simon and Schuster, 1995.
[6] Norbert Wiener, Cybernetics or Control and Communication in the Animal and the Machine, MIT press, 2019.
[7] Ronald J. Deibert and Rafal Rohozinski, "Risking security: Policies and paradoxes of cyberspace security," International Political Sociology 4, no. 1 (2010): 15-32.
[8] Cybersecurity, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/cybersecurity.
[9] Ben Buchanan, The cybersecurity dilemma: Hacking, trust, and fear between nations, Oxford University Press, 2016.
[10] Chris Bronk, "Cybersecurity," in: David J. Galbreath and John R. Deni, eds. Routledge Handbook of Defence Studies, London, New York: Routledge, 2018.
[11] Willis Ware, Security controls for computer systems, Rand Corp. Tech. Rep, 1970.
[12] Thomas Rid, Cyber war will not take place, Oxford University Press, USA, 2013.
[13] Brandon Valeriano, Benjamin M. Jensen and Ryan C. Maness, Cyber strategy: The evolving character of power and coercion, Oxford University Press, 2018.
[14] Erik Gartzke, "The myth of cyberwar: bringing war in cyberspace back down to earth," International Security 38, no. 2 (2013): 41-73.
[15] Kim Zetter, Countdown to zero day: Stuxnet

and the launch of the world's first digital weapon, Crown, 2015.
[16] William Tobey, "Nuclear scientists as assassination targets," Bulletin of the Atomic Scientists 68, no. 1 (2012): 61-69.
[17] Ardavan Khoshnood, "The Attack on Natanz and the JCPOA," BESA Center Perspectives Paper 1,997 (2021).
[18] Ralph Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security & Privacy 9, no. 3 (2011): 49-51.
[19] Andy Greenberg, Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers, Anchor, 2019.
[20] Siyu Lei, Silviu Maniu, Luyi Mo, Reynold Cheng and Pierre Senellart, "Online influence maximization," in: Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 645-654. 2015.
[21] Andy Greenberg, Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers, Anchor, 2019.
[22] Eric Lipton, David E. Sanger and Scott Shane, "The perfect weapon: How Russian cyberpower invaded the US," The New York Times 13 (2016).
[23] Michael Buratowski, "The DNC server breach: who did it and what does it mean?," Network Security 2016, no. 10 (2016): 5-7.
[24] https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.
[25] Gabi Siboni and David Siman-Tov, The superpower cyber war and the US elections, Institute for National Security Studies (INSS), 2016.
[26] Chris Bronk, "Getting creative on what will do: cyber espionage, conflict and covert action," Conflict and Covert Action (2016).
[27] Sharon Weinberger, "Murders unlikely to slow Iran's nuclear efforts: experts say international sanctions are the best way to stall the weapons programme," Nature 481, no. 7381 (2012): 249-250.
[28] Rebecca Slayton, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," International Security 41, no. 3 (2016): 72-109.
[29] Chris Bronk, Cyber threat: The rise of information geopolitics in U.S. national security, Bloomsbury Publishing USA, 2016.
[30] Glenn Alexander Crowther, "The cyber domain," The Cyber Defense Review 2, no. 3 (2017): 63-78.
[31] William Gibson, Burning chrome, Hachette UK, 2017.
[32] Teilhard De Chardin, The future of man, Image, 2004.
[33] Christine Haughney and Nicole Perlroth, "Times Site Is Disrupted in Attack by Hackers," The New York Times, August 27, 2013.
[34] Max Fisher, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?," The Washington Post, April 23, 2013.
[35] Ilya Zheludev, Robert Smith and Tomaso Aste, "When can social media lead financial markets?," Scientific reports 4, no. 1 (2014): 4213.
[36] Gian Piero Siroli, "Considerations on the cyber domain as the new worldwide battlefield," The International Spectator 53, no. 2 (2018): 111-123.
[37] Kim Hartmann and Christoph Steup, "Hacking the AI - the next generation of hijacked systems," in: 2020 12th International Conference on Cyber Conflict (CyCon), vol. 1300, 327-349. IEEE, 2020 and John J. Heslen, "Neurocognitive hacking: A new capability in cyber conflict?," Politics and the Life Sciences 39, no. 1 (2020): 87-100.
[38] Edward Hallett Carr, The twenty years' crisis, 1919-1939: Reissued with a new preface from Michael Cox, Springer, 2016.
[39] Andrea Kendall-Taylor and David Shullman, Navigating the deepening Russia-China partnership, Center for a New American Security, 2021.
[40] Adrian Shahbaz and Allie Funk, Freedom of the Net: The Global Drive to Control Big Tech, Freedom House, 2021.
[41] Gary Shteyngart, Super sad true love story: A novel, Random House Trade Paperbacks, 2011.
[42] Ben Shneiderman, Software psychology: Human factors in computer and information systems (Winthrop computer systems series), Winthrop Publishers, 1980.
[43] B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel, "Cognitive Warfare: The Future of Cognitive Dominance," in: First NATO scientific meeting on Cognitive Warfare (France)-21 June, 2022-03, 2021.
[44] Oliver Backes and Andrew Swab, "Cognitive Warfare," The Russian Threat to Election Integrity in the Baltic States, Cambridge: Belfer Center for Science and International Affairs(2019).
[45] Laurie Fenstermacher, David Uzcha, Katie Larson, Christine Vitiello and Steve Shellman, "New perspectives on cognitive warfare," in: Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII, vol. 12547, 162-177. SPIE, 2023.
[46] Henry H. Wilmer, Lauren E. Sherman and Jason M. Chein, "Smartphones and cognition: A review of research exploring the links between mobile technology habits and cognitive functioning," Frontiers in psychology 8 (2017): 605.
[47] Andreea Stoian-Karadeli and Daniel-Gabriel Dinu, "Securing the Mind: The Emerging Landscape of Cognitive Warfare," Redefining Community in Intercultural Context (2023): 26.
[48] Timothy Snyder, "Ukraine holds the future: The war between democracy and nihilism," Foreign Affairs. 101 (2022): 124.
[49] Jennifer Bick Murtazashvili, "The collapse of Afghanistan," Journal of Democracy 33, no. 1 (2022): 40-54.

Future Elections and AI-Driven Disinformation

GAZMEND HUSKAJ

Author: Gazmend is the Head of Cyber Security at the Geneva Centre for Security Policy (GCSP) and a doctoral candidate focusing on offensive cyberspace operations at the Department of Computer and Systems Sciences, Stockholm University. Previously, he was a full-time doctoral student at the Swedish Defence University, and before that, he served as the Director of Intelligence for Cyber-related issues in the Swedish Armed Forces. He is a military and UN veteran with over five years of field experience in conflict and post-conflict areas. At the GCSP, his focus areas include Executive Education, Diplomatic Dialogue, and Policy Research & Analysis. The views expressed in this article are the author's alone and do not represent those of the Geneva Centre for Security Policy (GCSP) nor DSV.

Abstract: This paper conceptualises the impact of Artificial Intelligence (AI) on disinformation campaigns, contrasting AI-driven operations with traditional human-operated methods. Utilising a Human Intelligence Collector Operations (HUMINT) and Offensive Cyberspace Operations (OCO) framework, the research analyses the advancements in AI technology in terms of speed, efficiency, content generation, and adaptability. The findings reveal that AI-driven operations, particularly those with billions of tokens, significantly outperform human-operated disinformation campaigns in speed and efficiency, demonstrating an ability to process vast datasets and complex scenarios almost instantaneously.

Problem statement: How to understand the need to develop AI-driven strategies to protect democratic processes against disinformation campaigns?

So what?: Governments, tech companies, and academic researchers must collaborate on advanced AI countermeasures to combat AI-driven disinformation campaigns.

Source: shutterstock.ozrimoz

AI – A Blessing or a Curse?

The 2016 US presidential election serves as an example of how disinformation can influence public opinion and electoral outcomes. The computational propaganda research project has reviewed several case studies on how social media was used to manipulate public opinion: first, how bots were used as tools to spread disinformation in the presidential election in the States in 2016[1], and later, between 2015 and 2017, in Brazil, Canada, the People's Republic of China (PRC), Germany, Poland, Taiwan, Russia, Ukraine, and the US. Threat actors purposefully distributed misleading information over social media networks by exploiting algorithms, automation, and human curation. It was noted that the most potent forms of computational propaganda involved algorithmic distribution and human curation using bots and trolls in combination.[2]

The Cambridge Analytica (CA) case highlights the use of both algorithmic and human means to exert influence. Cambridge Analytica's activities are emblematic of the political importance of the massive amounts of data that humans produce in today's interconnected world. CA provided services for many different political actors, analysing the political campaigns they were supporting.[3,4] Part of their success was due to scraping user data from popular social media sites and pairing it with individual psychological profiles.[5,6]

Recent research has significantly advanced our understanding of digital behaviour analysis. For instance, the study "Computer-based personality judgments are more accurate than those made by humans" provides evidence that algorithmic assessments can surpass human accuracy in personality judgment.[7] This is further complemented by the findings of the study "Mining Big Data to Extract Patterns and Predict Real-Life Outcomes",[8] which demonstrates the potential of big data in uncovering behavioural patterns and forecasting real-life events. In addition, "Psychological targeting as an effective approach to digital mass persuasion"[9] offers insights into how digital platforms can be used for tailored persuasive communication. Taken together, these studies underscore the growing capabilities of digital tools in understanding and influencing human behaviour.

These capabilities to influence human behaviour also have significant implications, particularly in the context of electoral scenarios. As mentioned, this was exemplified by the US presidential election in 2016 and other global cases, where a combination of algorithmic and human interventions played a notable role. These instances underscore the urgency of understanding and anticipating the impacts of more sophisticated AI-driven disinformation campaigns in future elections. As AI technology advances, its capabilities to manipulate information, target specific demographics, and influence public perception are expected to become more pronounced. This evolution could lead to increasingly disruptive effects.[10]

Research Methodology

At the outset of this research, it is important to disclose the utilisation of ChatGPT4, a Large Language Model (LLM), as a research assistant and language editor. This disclosure aligns with the ethical guidelines established by Nature and Springer Nature journals,[11] ensuring transparency in the research process.

In the initial step, the human intelligence collector approaches were identified.[12] Next, ChatGPT4 was asked to map disinformation / influence cyber operations to HUMINT approaches, developing a HUMINT-OCO framework.

HUMINT operators use various approaches, including psychological techniques and verbal trickery, to collect information from human sources successfully.[12] An example is the "Emotional Love Approach", which exploits a target's love for something, such as patriotism, by focusing on the anxiety the target feels about a particular issue.

Similarly, Offensive Cyberspace Operations (OCO) may leverage psychological insights to achieve their objectives through cyberspace. These operations employ offensive methods to targets in cyberspace.[13] For example, OCO might involve altering the content of a web page to include disinformation that exploits human psychological traits, like patriotism, in a manner akin to techniques used in HUMINT.

In addition, OCO can be used to exfiltrate sensitive information from a target, such as an email server, and post the exfiltrated information (emails) on a third party (such as WikiLeaks). The intent would be to increase doubt and embarrassment for the target. This parallel demonstrates how psychological manipulation is a common denominator in both the physical world and in cyberspace.

Furthermore, the purpose was also to identify those approaches that do not map to OCO because they require direct interaction with the target, while a cyber operation has remote access to the target. The large language model was fed all 19 human intelligence collector approaches and was provided with the following prompt:

"Map disinformation / influence cyber operations to the HUMINT approaches. For example, 'Using disinformation to exacerbate discord on topics like race, immigration, and gun rights' is mapped to the Emotional Hate Approach tactic. The purpose is to create a generalised framework for mapping cyber operations related to disinformation/influence to the HUMINT approaches. Can you do this? (it is likely that some cyber operations cannot be mapped to some HUMINT approaches because these approaches require physical contact; in those cases, just put N/A)."

The output was 19 approaches, with 10 approaches marked as N/A, meaning those approaches required direct access to the target. Hence, they were discarded, and only nine remained as part of the HUMINT-OCO framework. The nine approaches are listed below:

1. Emotional Love: This involves promoting content that fosters strong affinity, loyalty, or patriotism towards a cause or group. It often involves positive disinformation, creating a sense of connection or allegiance.

2. Emotional Hate: This strategy focuses on inciting hate or anger towards specific groups, races, or nations. It includes spreading false information to exacerbate racial tensions or create animosity.

3. Emotional Fear-Up: This approach is about disseminating false information that induces fear or panic. Examples include rumours about exaggerated threats or fabricated crises to create a sense of urgency or dread.
4. Emotional-Pride and Ego-Up: This involves cyber campaigns that flatter or inflate the ego of a target group. Disinformation is used to make a group feel superior, manipulating perceptions and actions.

5. Emotional-Pride and Ego-Down: Contrary to the previous approach, this one aims to undermine the confidence or self-esteem of a target group. It often involves spreading false narratives that belittle or shame them.

6. Emotional-Futility: This approach spreads disinformation to make a

target audience feel that resistance or dissent is futile. It fosters feelings of hopelessness or apathy towards certain issues or actions.

7. Repetition (Interrogation): This tactic involves repeatedly spreading the same false information or narrative across various platforms. The repetition reinforces its acceptance as truth.

8. Rapid Fire (Interrogation): This method quickly bombards an audience with a high volume of disinformation. The goal is to overwhelm and confuse, preventing critical analysis and response.

9. False Flag (Interrogation): This involves conducting cyber operations while masquerading as a different entity or group. The aim is to mislead about the source of the information or to discredit the entity being impersonated.

The next step was to apply the framework to the case of Russian disinformation and influence operations during the 2016 US election, including the cyberattacks on the Democratic National Committee (DNC). The aim was to demonstrate the framework's applicability in a real-world case. Furthermore, the framework was applied to a hypothetical scenario involving a fictional country's election in 2016, executed by an AI with millions of tokens, and compared to the human-conducted Russian operations. This comparison explored the differences between AI-conducted and human-conducted disinformation and influence operations. To explore the differences, the following questions were asked, generated in collaboration with the LLM:

1. How would the scale and precision of disinformation campaigns differ between human-operated Russian interference and an AI-driven operation? Would the AI be able to target individuals more effectively based on their online behaviour and psychological profiles?

2. How would the speed and adaptability of the AI's operations compare to the alleged Russian operations? Could the AI respond and adjust its strategies in real time based on emerging trends and countermeasures?

3. In what ways might the content created by AI differ in terms of sophistication, believability, and variety from that created by human agents? Could the AI generate more convincing fake news, deepfakes, or other forms of misleading content?

4. How might the impact on public opinion and trust in democratic institutions differ between the two scenarios? Would an AI's ability to personalise and optimise messages lead to more profound societal divisions?

5. How might the use of AI in such operations affect global politics and international relations? Would it lead to an escalation in cyber warfare tactics among nations?

First, the basis for calculating the complexity of a model is tokens, which are the basic units for calculating the length of a text.[14] For example, in English, one word is approximately 1.3 tokens, while in Spanish and in French, one word is approximately two tokens. GPT-3.5 can "memorise" 4,096 tokens,[15] which, in English, would be approximately 3,000 words.[16] On November 6, 2023, OpenAI released GPT-4 Turbo, which can "memorise" 128,000 tokens, approximately 93,750 words (the equivalent of more than 300 pages[17]).

The idea of using an AI model with millions of tokens stemmed from the Russian cyber-enabled disinformation campaign targeting the US election in 2016. The entire campaign likely consisted of thousands and thousands of social media posts, including the OCO targeting and exfiltrating emails from the Democratic National Committee (DNC). Consequently, the total sum of words is believed to be in the millions.

A similar rationale was applied to assess the AI model with billions of tokens: by assessing how many tokens the human brain was likely to hold. Various estimates exist.[18,19]

Research Limitations

Several limitations should be acknowledged when conceptualising insights into the impact of AI advancements on disinformation campaigns. The paper primarily uses a large language model to map disinformation strategies to

human intelligence collector operation approaches. While the model is sophisticated, the analysis is likely to be limited by inherent biases and the scope of data on which it was trained. Another limitation is the use of hypothetical scenarios. There is no empirical data available on real-world events. Therefore, the results should be interpreted as indicative rather than conclusive.
Furthermore, technology is rapidly changing in both cyber operations and AI; hence, some conclusions are drawn on the current state of technology, which does not account for future developments in these areas. Finally, the results are limited in their generalisability because even though the case of the US 2016 election was used, the structure of the system in the US is quite binary and (largely) composed of two parties, Republicans and Democrats.

Results

Scale and Precision of Operations

How would the scale and precision of disinformation campaigns differ between human-operated Russian interference and an AI-driven operation? Would an AI be able to target individuals more effectively based on their online behaviour and psychological profiles?

Scale: Human-operated Russian interference operates on a large scale but is inherently limited by human resources, constraining the number of campaigns and the extent of topics covered. In contrast, AI-driven operations, particularly those utilising millions of tokens, achieve a significantly larger scale due to automation, managing more campaigns and covering a wider range of topics. This scale is further amplified in AI operations with billions of tokens, which can run numerous diversified campaigns concurrently, surpassing human capabilities and less sophisticated AI systems.

Precision: The precision of human-operated campaigns is moderate, relying on human understanding of social and political contexts, but often lacks deep personalisation. AI-driven operations with millions of tokens offer more precision by analysing large datasets to identify trends and effectively tailor messages to specific groups. Precision reaches an exceptional level with billions of AI tokens, demonstrating a nuanced understanding of complex behaviours and trends, and generating deeply resonant content. Overall, AI-driven operations provide greater precision in content creation, with the most sophisticated AI achieving the highest level of nuanced content.
Targeting: Human operations typically target broader demographic and psychographic profiles, which are less effective in hyper-personalisation. AI-driven operations with millions of tokens improve targeting by analysing online behaviour and psychological profiles. With billions of tokens, the most advanced AI excels in individual targeting, utilising advanced algorithms for highly personalised content creation. Both AI systems outperform human operations in targeting, with the more advanced AI being particularly adept at crafting highly personalised messages.

As the sophistication of AI in disinformation campaigns increases, there is a corresponding increase in the scale, precision, and effectiveness of these operations, particularly in their ability to target individuals based on their online behaviour and psychological profiles.

Speed and Adaptability

How would the speed and adaptability of AI operations compare to the alleged Russian operations? Could the AI respond and adjust its strategies in real time based on emerging trends and countermeasures?

1. Adaptability and Strategy Modification: Human-operated campaigns adapt more slowly to new information and changing circumstances, often employing more rigid and less dynamic strategies. AI-driven operations with millions of tokens are more adaptable and capable of modifying strategies based on data trends. However, they may not fully capture human behavioural complexities. With billions of tokens, the most advanced AI is highly adaptable and capable of real-time strategy modification based on a comprehensive analysis of emerging trends and nuanced human behaviours.

2. Targeting and Personalisation: Human-operated campaigns rely on human intuition and available data for targeting, which may be less

precise. AI-driven operations with millions of tokens improve targeting capabilities using data-driven approaches, but they may lack deep personalisation. In contrast, AI with billions of tokens excels in targeting and personalisation, being able to tailor content and strategies to individual preferences and behaviours at a granular level.

3. Response to Countermeasures: Human campaigns are slower at identifying and responding to countermeasures, often reacting after the fact. AI-driven operations with millions of tokens are quicker to identify countermeasures than humans. However, their responses may not always be optimally effective. The most sophisticated AI, with billions of tokens, is highly efficient in identifying, anticipating, and countering measures, often in a proactive manner.

In summary, AI-driven operations, especially those with billions of tokens, offer significant advantages over human-operated campaigns in terms of speed, efficiency, adaptability, and sophistication, with potential implications for democratic processes and international relations.

Content Creation and Variation

How might the content created by an AI differ in terms of sophistication, believability, and variety from that created by human agents? Could the AI generate more convincing fake news, deepfakes, or other forms of misleading content?

1. Sophistication: While capable of understanding nuanced human emotions and cultural contexts, human agents are limited by individual knowledge and biases, and may lack speed and volume in content creation. AI-driven operations with millions of tokens can analyse and process large datasets, identify patterns, and generate coherent, contextually relevant content. Still, they are limited in understanding nuanced human emotions and complex scenarios. In contrast, AI with billions of tokens exhibits high sophistication, particularly in understanding and mimicking human expressions and complex scenarios, and is adept at creating content that closely resembles human thought and speech.

2. Believability: Human agents can create believable content, but their output is limited by individual knowledge and time constraints. AI-driven operations with millions of tokens can generate believable content more rapidly than humans, although they may occasionally lack human-like nuances, especially in complex or emotional contexts. However, AI with billions of tokens excels at creating highly believable content, with an advanced understanding of language and subtleties, making it difficult to distinguish from human-generated content.

3. Variety: Human agents produce diverse content, but individual capabilities and perspectives limit their output. AI-driven operations with millions of tokens can generate a wide variety of content, surpassing individual human capabilities, but may exhibit certain patterns or limitations. However, AI with billions of tokens offers immense variety, easily adapting styles, tones, and perspectives. It can mimic a range of human authors, making its content highly diverse and adaptable.

4. Potential for Misleading Content: While human agents can produce misleading content, AI-driven operations, especially with millions of tokens, can generate convincing fake news and disinformation, albeit less tailored and targeted compared to more advanced AI. AI with billions of tokens is more adept at creating highly tailored and targeted misleading content, including convincing deepfakes, making it more effective at spreading disinformation. Consequently, AI with billions of tokens poses a greater risk of spreading misleading content, including more convincing deepfakes, compared to less advanced AI and human agents.

While both AIs would surpass human capabilities in content creation in terms of speed and volume, the AI with billions of tokens would be particularly more advanced in terms of creating sophisticated, believable, and varied content. Such a tool has the potential for creating and spreading compelling fake news, deepfakes, and disinformation, with significant implications for society and politics.

Impact on Public Opinion and Trust

How might the impact on public opinion and trust in democratic institutions differ between the two scenarios? Would an AI's ability to personalise and optimise messages lead to more profound societal divisions?

1. Impact Level: AI-driven operations with millions of tokens can generate convincing and personalised content, significantly influencing public opinion, especially when it comes to polarising societal divisions. However, they are somewhat limited in understanding complex socio-political contexts or nuanced human emotions. In contrast, AI with billions of tokens creates highly sophisticated, contextually accurate, and profoundly personalised content. It more convincingly mimics human behaviour and speech, profoundly and widely influencing public opinion. The advanced capabilities of AI with billions of tokens result in a more profound impact on public opinion due to the sophistication in creating personalised content.

2. Trust in Institutions: The spread of disinformation by AI with millions of tokens could lead to increased scepticism and erosion of trust in democratic institutions, but still allow some resilience against complete erosion of trust. However, AI with billions of tokens crafts messages that resonate deeply with individual beliefs and biases, leading to a more significant erosion of trust in democratic institutions. The difficulty in distinguishing AI-generated content exacerbates the spread of disinformation. Consequently, AI with billions of tokens poses a greater risk to trust in institutions due to its ability to create more convincing and resonant disinformation.

3. Societal Divisions: While AI with millions of tokens influences public opinion, it might lack depth and nuance, somewhat limiting its potential to deepen societal divisions. On the other hand, AI with billions of tokens tailors messages to exploit specific societal fractures, potentially deepening divisions. It adapts content based on real-time feedback, effectively exacerbating tensions. Therefore, AI with billions of tokens is more effective at deepening societal divisions due to its precision and adaptability regarding content creation.

4. Personalisation and Optimisation: AI with millions of tokens can personalise content based on user data, but with less precision and subtlety compared to more advanced AI with billions of tokens. The latter leads to more effective echo chambers and further polarisation of public opinion. With superior personalisation and optimisation capabilities, AI utilising billions of tokens contributes significantly to this effect.

While both AIs would have a significant impact on public opinion and trust in democratic institutions, the AI with billions of tokens would likely be more effective in terms of personalising and optimising messages. This could lead to more profound societal divisions, as it would be more capable of subtly reinforcing and exploiting existing societal fractures and tensions.

Global Implications

How might the use of AI in such operations affect global politics and international relations? Would it lead to an escalation in cyber warfare among nations?

1. Global Politics: AI-driven operations with millions of tokens can influence public opinion and interfere in nations' internal affairs, potentially leading to strained diplomatic relations. Such operations are particularly effective at targeting countries with less sophisticated digital disinformation countermeasures. However, AI with billions of tokens has a more profound impact, with the ability to manipulate public opinion, destabilise nations, or influence election outcomes, becoming a major bone of contention in international

politics. Advanced AI would have a significant and destabilising impact on global politics, with the potential to sway elections and national stability.

2. International Relations: Deploying AI with millions of tokens might prompt discussions on cyber norms and AI regulation in information warfare. However, detection and attribution challenges could hinder international consensus. In contrast, deploying AI with billions of tokens could lead to an escalation in cyber warfare tactics and trigger an AI arms race, with nations striving to develop or acquire comparable capabilities. The use of more advanced AI intensifies international relations, leading to potential AI arms races and heightened discussions on cyber norms.

3. Cyber Warfare: The increase in cyber tactics as a facet of geopolitical strategies is evident in AI-driven operations utilising millions of tokens. Nations might invest more in offensive and defensive cyber capabilities, including counter-AI strategies. However, AI with billions of tokens necessitates advanced countermeasures. Nations might engage in aggressive cyber operations for defence and pre-emptive disruption, signalling a new era of digital espionage and counter-espionage. AI with billions of tokens would lead to more advanced and aggressive cyber warfare tactics, necessitating sophisticated countermeasures and potentially changing the landscape of international cyber operations.

4. Escalation in Cyber Warfare: AI-driven operations with millions of tokens contribute to escalating cyber warfare tactics. However, the utilisation of AI with billions of tokens represents a significant leap in capability, leading to more aggressive and widespread use of cyber operations. This advanced AI poses a greater risk of escalating cyber warfare tactics, with the potential for heightened aggression and wider impact.

The use of AI in disinformation campaigns, whether with millions or billions of tokens, could have a major impact on global politics and international relations. It could lead to an escalation in cyber warfare, potentially triggering an AI arms race among nations.[20,21] The AI with billions of tokens, in particular, could represent a substantial shift in offensive cyberspace operations.

Equipped with an understanding of the differences between human-generated operations, and AI with operations generated by millions and billions of tokens respectively, the following three tables show how these were manifested in 1) the Russian interference operations targeting the US election in 2016, 2) a fictional scenario concerning an election in 2024, and 3) a fictional scenario regarding an election in 2030 with technologies such as 5G and 6G.

Table 1 illustrates how the tactics used in the alleged Russian operations during the 2016 US presidential election can be mapped to traditional HUMINT approaches, adapted to the informational digital age and the context of cyber warfare and information manipulation.

HUMINT Approach	Application in 2016 US Election (Alleged Russian Operations)
Emotional Love	Pro-Russian or pro-Trump narratives to build a positive image among US voter segments, including spreading positive disinformation or selectively presenting information favourably.
Emotional Hate	Disseminating disinformation to incite hate or anger towards Hillary Clinton, the Democratic Party, or other perceived adversaries of Trump, highlighting or fabricating negative aspects.
Emotional Fear-Up	Spreading false information to induce fear about Hillary Clinton's potential presidency, exaggerating threats related to wars, gun control, or economic policies.
Emotional-Pride and Ego-Up	Cyber operations flattering American nationalist sentiments, promoting US superiority or the need to "make America great again", aligning with Trump's campaign rhetoric.
Emotional-Pride and Ego-Down	Efforts to undermine the confidence or self-esteem of opposing groups, such as spreading narratives belittling the Democratic Party, its supporters, or policies.
Emotional-Futility	Spreading disinformation suggesting that voting for Hillary Clinton or the Democrats was futile or that the political system was corrupt, aiming to decrease voter turnout for the opposition.
Repetition (Interrogation)	Continuously pushing the same narratives (e.g., Clinton's email scandal, the DNC's alleged bias against Bernie Sanders) to reinforce their acceptance and impact on voter perceptions.
Rapid Fire (Interrogation)	Rapid release and promotion of different pieces of damaging information, especially through social media, creating a sense of overwhelming scandal around the DNC and the Clinton campaign.
False Flag (Interrogation)	The DNC hack, attributed to Russian actors, was seen as a false flag operation where the true perpetrators conducted the operation but left trails implying someone else was responsible.

Table 1. Disinformation operations conducted by humans; Source: Author.

Table 2 illustrates the application of HUMINT approaches within a hypothetical scenario where an AI, equipped with millions of tokens and operating at current broadband speeds, impacts a fictional country's election in 2024 through disinformation and influence operations.

HUMINT Approach	AI-Driven Operations in 2030 Fictional Scenario
Emotional Love	Creating highly personalised content that endears political figures or ideologies to specific demographics, leveraging deep data analysis to resonate with individual values and desires.
Emotional Hate	Identifying and amplifying societal divisions, generating content that exacerbates animosity or contempt towards certain groups or ideologies, using sophisticated targeting based on online behaviour and psychological profiles.
Emotional Fear-Up	Crafting and disseminating scenarios that instil heightened fear about specific outcomes (e.g., national security threats, economic collapse) associated with certain political choices.
Emotional-Pride and Ego-Up	Generating content that boosts the ego of targeted individuals or groups, affirming their beliefs and making them more confident in their political choices aligned with the AI's objectives.
Emotional-Pride and Ego-Down	Subtly undermining the confidence of targeted individuals or groups in their political choices, using tailored content to make them question their decisions or the capabilities of their preferred candidates.
Emotional-Futility	Creating a narrative of inevitability around certain political outcomes, leading to helplessness or apathy among the opposition, reducing their motivation to vote or engage politically.
Repetition (Interrogation)	Repeatedly exposing individuals to specific messages across various platforms reinforces these messages to enhance credibility and acceptance.
Rapid Fire (Interrogation)	Deploying a barrage of messages, posts, and news stories at an overwhelming pace, saturating media and social networks, creating a challenging environment for discerning reliable information.
False Flag (Interrogation)	Conducting sophisticated false flag operations, impersonating different entities or groups to create confusion, discredit political figures or parties, or subtly manipulate public opinion.

Table 2. AI with Millions of Tokens in 2024 Fictional Election Scenario; Source: Author.

In this scenario, the AI's ability to analyse large datasets, understand human psychology, and generate targeted content would make it highly effective in terms of manipulating public opinion and influencing the election outcome. Using these approaches in a coordinated manner could significantly impact the political landscape of the fictional country.
Table 3 illustrates potential manifestations of HUMINT approaches in the hypothetical scenario where an advanced AI with billions of tokens and 5G/6G broadband infrastructure impacts the outcome of a fictional country's election in 2030 through disinformation/influence operations.

HUMINT Approach	AI-Driven Operations in 2030 Fictional Scenario
Emotional Love	Creating highly personalised content that endears political figures or ideologies to specific demographics, leveraging deep data analysis to resonate with individual values and desires.
Emotional Hate	Identifying and amplifying societal divisions, generating content that exacerbates animosity or contempt towards certain groups or ideologies, using sophisticated targeting based on online behaviour and psychological profiles.
Emotional Fear-Up	Crafting and disseminating scenarios that instil heightened fear about specific outcomes (e.g., national security threats, economic collapse) associated with certain political choices.
Emotional-Pride and Ego-Up	Generating content that boosts the ego of targeted individuals or groups, affirming their beliefs and making them more confident in their political choices aligned with the AI's objectives.
Emotional-Pride and Ego-Down	Subtly undermining the confidence of targeted individuals or groups in their political choices, using tailored content to make them question their decisions or the capabilities of their preferred candidates.
Emotional-Futility	Creating a narrative of inevitability around certain political outcomes, leading to helplessness or apathy among the opposition, reducing their motivation to vote or engage politically.
Repetition (Interrogation)	Repeatedly exposing individuals to specific messages across various platforms reinforces these messages to enhance credibility and acceptance.
Rapid Fire (Interrogation)	Deploying a barrage of messages, posts, and news stories at an overwhelming pace, saturating media and social networks, creating a challenging environment for discerning reliable information.
False Flag (Interrogation)	Conducting sophisticated false flag operations, impersonating different entities or groups to create confusion, discredit political figures or parties, or subtly manipulate public opinion.

Table 3. Advanced AI with Billions of Tokens in 2030 Fictional Election Scenario; Source: Author.

In this scenario, the advanced AI's capabilities, especially in processing and analysing vast amounts of data, would enable it to conduct highly sophisticated and targeted influence operations. Its ability to adapt in real time to changing circumstances and countermeasures would make it a formidable tool in shaping public opinion and electoral outcomes.

Speed and Mass as Qualities

This research investigated the impact of advancements in AI technology on the speed, adaptability, content generation, and sophistication of disinformation campaigns, and compared these aspects with traditional human-operated campaigns. The findings specifically relate to differences in speed and efficiency, content generation and sophistication, as well as adaptability and strategy modification.

In terms of speed and efficiency, human-operated campaigns are relatively slower due to manual data analysis, content creation, and decision-making processes. In contrast, AI-driven operations with millions of tokens conduct faster operations than human-operated campaigns, quickly analysing data and generating content. At the same time, AI-driven operations with billions of tokens are exceptionally fast. They can process vast datasets and complex scenarios almost instantaneously, significantly outpacing human capabilities. Consequently, AI-driven operations, particularly those with billions of tokens, are significantly faster and more efficient than human-operated campaigns, indicating a substantial advancement in the speed and efficiency of disinformation campaigns due to AI technology.

In terms of content generation and sophistication, human-operated campaigns are constrained by human creativity and resources, resulting in potentially more culturally and contextually nuanced but less abundant content. In contrast, AI-driven operations with millions of tokens can rapidly generate large volumes of content, albeit lacking some depth and cultural and contextual understanding compared to humans. However, AI-driven operations with billions of tokens can generate content at a massive scale with high sophistication, potentially matching or surpassing human levels of creativity and contextual awareness. Therefore, AI, particularly with billions of tokens, excels in both the quantity and quality of content generation, surpassing human-operated campaigns. This underscores the significant impact of AI advancements on the sophistication and variety of content in disinformation campaigns.

When it comes to adaptability and strategy modification, human-operated campaigns are slower to adapt to new information and changing circumstances, as the strategies are more rigid and less dynamic. However, AI-driven operations with millions of tokens are more adaptable than humans as they are capable of modifying strategies based on data trends. Nonetheless, they may not capture the full spectrum of human behavioural complexities.

AI-driven operations with billions of tokens, on the other hand, can be highly adaptable and capable of real-time strategy modification based on a comprehensive analysis of emerging trends and nuanced human behaviours. Thus, AI-driven operations, particularly with billions of tokens, offer superior adaptability and dynamic strategy modification compared to human-operated campaigns. This highlights the role of AI in enhancing the flexibility and responsiveness of information campaigns.

To summarise, advancements in AI technology profoundly impact disinformation campaigns, particularly in terms of speed, efficiency, content generation, and adaptability.[22,23,24,25] AI-driven operations, especially those with billions of tokens, demonstrate significant advantages over traditional human-operated campaigns. These advancements allow for more rapid, sophisticated, and adaptable disinformation campaigns, which can be tailored more effectively to specific audiences, and which respond more quickly to changing circumstances.

To this end, as new information and communication technologies such as 5G and 6G are being rolled out, combined with advanced AI models that can generate human-readable text, video, and audio, they are capable of influencing people’s perception of reality in general and elections in particular. Certain actors are likely researching how to develop AI-powered mass surveillance tools that profile individuals in real time, influencing their decision-making and perception of reality. In addition, AI could be used to manipulate the information resources of elections and critical national infrastructure, such as financial systems, communication systems, or supply chains. The consequences of HUMINT-OCO-Disinformation operations could affect voting behaviour, undermine electoral integrity, and lead to polarisation of society, as well as erode public trust in institutions.

Endnotes

[1] Samuel C. Woolley and Douglas R. Guilbeault, “Computational Propaganda in the United States of America: Manufacturing Consensus Online,” 2017, https://ora.ox.ac.uk/objects/uuid:620ce18f-69ed-4294-aa85-184af2b5052e.
[2] Samuel C. Woolley and Philip N. Howard, “Computational Propaganda Worldwide: Executive Summary,” 2017, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/06/Casestudies-ExecutiveSummary.pdf.
[3] Nicholas Confessore, “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far,” 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[4] Katie Harbath and Chris Fernekes, “History of the Cambridge Analytica Controversy,” 2023, https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/.
[5] Alex Hern, “Academic at centre of Cambridge Analytica scandal sues Facebook,” 2019, https://www.theguardian.com/uk-news/2019/mar/18/aleksandr-kogan-cambridge-analytica-scandal-sues-facebook.
[6] Lesley Stahl, “Aleksandr Kogan: The link between Cambridge Analytica and Facebook,” 2018, https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook-60-minutes/.
[7] Wu Youyou, Michal Kosinski, and David Stillwell, “Computer-based personality judgments are more accurate than those made by humans,” PNAS 112, no. 4 (2014): 1036-1040, www.pnas.org/cgi/doi/10.1073/pnas.1418680112.
[8] Michal Kosinski, Yilun Wang, Himabindu Lakkaraju, and Jure Leskovec, “Mining Big Data to Extract Patterns and Predict Real-Life Outcomes,” Psychological Methods 21, no. 4 (2016): 493-506, http://dx.doi.org/10.1037/met0000105.
[9] S.C. Matz, M. Kosinski, G. Nave, and D.J. Stillwell, “Psychological targeting as an effective approach to digital mass persuasion,” PNAS 114, no. 48 (2017): 12714-12719, www.pnas.org/cgi/doi/10.1073/pnas.1710966114.
[10] UZH News, “GPT-3 Informs and Disinforms Us Better,” 2023, https://www.news.uzh.ch/en/articles/media/2023/GPT3.html.
[11] Nature, “Tools such as ChatGPT threaten transparent science; here are our ground rules for their use,” 2023, https://www.nature.com/articles/d41586-023-00191-1.
[12] Department of the Army, “FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations,” 2006, https://www.marines.mil/Portals/1/Publications/FM%202-22.3%20%20Human%20Intelligence%20Collector%20Operations_1.pdf.
[13] Gazmend Huskaj, “The Current State of Research in Offensive Cyberspace Operations,” in 18th European Conference on Cyber Warfare and Security, edited by T. Cruz and P. Simoes, 660-667, 2019.
[14] OpenAI, “Understanding OpenAI GPT Tokens: A Comprehensive Guide,” 2023, https://gpt.space/blog/understanding-openai-gpt-tokens-a-comprehensive-guide.
[15] C. Dunn, “OpenAI tokens and limits,” 2023, https://devblogs.microsoft.com/surface-duo/android-openai-chatgpt-15.
[16] Raf, “What are tokens and how to count them?” 2023, https://help.openai.com/en/articles/4936856-what-are-tokens-and-how-to-count-them.
[17] OpenAI, “New models and developer products announced at DevDay,” 2023, https://openai.com/blog/new-models-and-developer-products-announced-at-devday.
[18] B. Millidge, “The Scale of the Brain vs Machine Learning,” 2022, https://www.beren.io/2022-08-06-The-scale-of-the-brain-vs-machine-learning/.
[19] B.H. Cottman, “How close is GPT-3 to Artificial General Intelligence?” 2021, https://towardsdatascience.com/how-close-is-gpt-3-to-artificial-general-intelligence-cb057a8c503d.
[20] Amandeep Singh-Gill, “A New Arms Race and Global Stability,” 2020, https://www.cigionline.org/articles/new-arms-race-and-global-stability/.
[21] Andrew R. Chow and Billy Perrigo, “The AI Arms Race Is Changing Everything,” 2023, https://time.com/6255952/ai-impact-chatgpt-microsoft-google/.
[22] Rik Ferguson, “Addressing the State of AI’s Impact on Cyber Disinformation/Misinformation,” 2023, https://www.securityweek.com/addressing-the-state-of-ais-impact-on-cyber-disinformation-misinformation.
[23] K. Sedova, C. McNeill, A. Johnson, A. Joshi, and I. Wulkan, “AI and the Future of Disinformation Campaigns: Part 1: The RICHDATA Framework,” 2021, https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns.
[24] K. Sedova, C. McNeill, A. Johnson, A. Joshi, and I. Wulkan, “AI and the Future of Disinformation Campaigns: Part 2: A Threat Model,” 2021, https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns-2.
[25] E. Karinshak and Y. Jin, “AI-driven disinformation: a framework for organisational preparation and response,” Journal of Communication Management 27, no. 4 (2023): 539-562, https://doi.org/10.1108/JCOM-09-2022-0113.

Hybrid Threats – The Chinese Focus On Australia

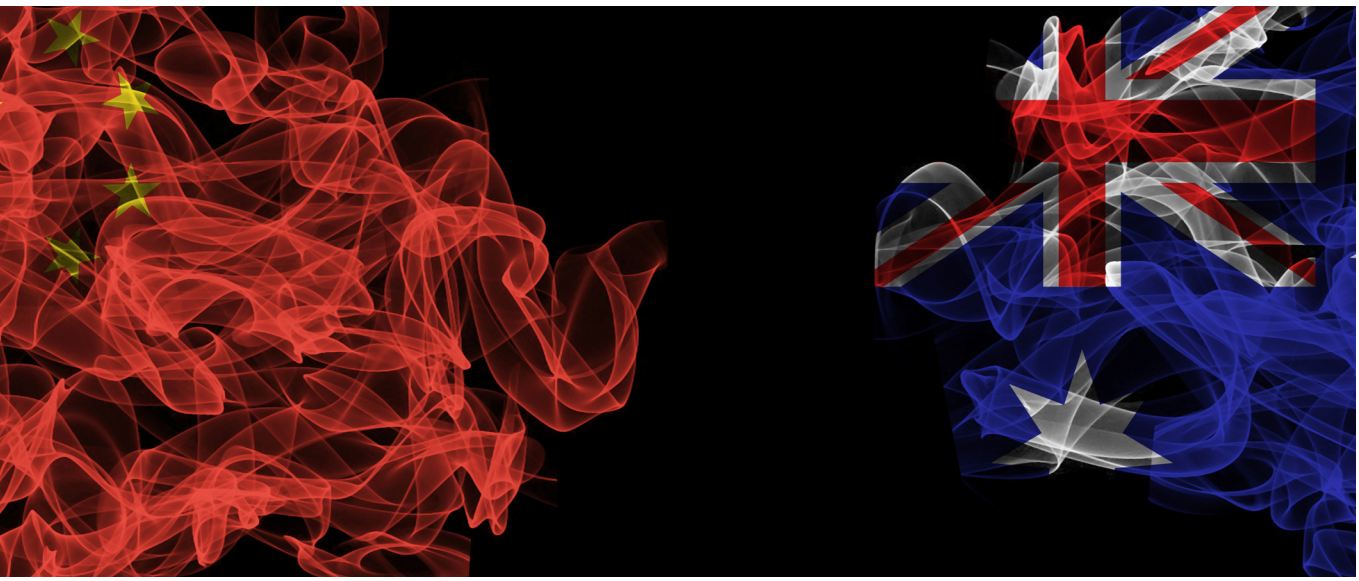
MATTHEW WARREN

Author: Matthew Warren, Centre of Cyber Security Research and Innovation, RMIT University, Melbourne, Australia. The views contained in this article are the author's alone.

Abstract: Cognitive operations affect people's perception of reality and decision-making, guiding groups of people and targeted audiences towards conditions desired by a geopolitical adversary. What we are seeing is the use of social media being used in a disinformation context by authoritarian governments against the West in a direct and indirect way to change societies. But what we are also seeing is those perception approaches being used by authoritarian governments internally and externally. It is difficult to change people's perceptions once they have been altered. This paper explores the hybrid threat relationship between Australia from the People's Republic of China (PRC).

Problem statement: How to understand that dealing with hybrid threats are not standalone but should be part of a greater strategy?

So what?: Understanding that hybrid threats are not standalone but could be part of a greater strategy is vital. This paper will highlight the importance of understanding hybrid threats against Australia from the PRC. Understanding the nature of hybrid threats, how they can be interconnected, and how they have evolved over time.



Source: shutterstock.com/Allexxandar

Coercive and Subversive Activities

In an era of rapid technological advancements and increasing online connectivity, the proliferation of cyber threats, including the spread of new threats such as fake news and disinformation, presents a new significant challenge. According to the European Union (EU), hybrid threats influence and exploit vulnerabilities to inflict damage below the threshold of overt aggression. They are a mixture of coercive and subversive activities, conventional and unconventional methods, used in a coordinated manner across multiple domains.[1]

The European Union Hybrid COE (Centre of Excellence) define hybrid threats as being:[2]

- coordinated and synchronised actions that deliberately target democratic states' and institutions' systemic vulnerabilities through a wide range of means;
- activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international); and
- activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target.

Hybrid attacks usually originate from authoritarian countries such as Russia and the People's Republic of China (PRC) against Western countries.[3]

Defining Hybrid Threats

Defining hybrid threats is challenging due to their complexity and ever evolving nature. Understanding hybrid threats' characteristics is essential to grasp their unique nature. Attackers employ a range of strategies and tactics to achieve their objectives. The EU Hybrid Threat conceptual model is based on 13 key domains.

EU Hybrid Threat Model Domains

The key domains related to this paper's examples are:[4]

Infrastructure

While there is no commonly accepted definition of critical infrastructure (CI), all definitions emphasise the contributing role of CI to society or the debilitating effect in the case of disruption. The EU defines 'critical infrastructure' as "an asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have an impact on society."

Economy

The economy as a domain of hybrid threats is defined as the production, distribution and consumption of all goods and services for a country. It includes its economic development and distribution of wealth. Economic policy instruments such as sanctions, taxation, trade embargoes, trade agreements, asset freezing, sterilised interventions, subsidies, tariffs, sovereign lending and debt forgiveness are all employed in this context.

Information

Weaponising information is used to undermine people's perception of their security by pitting political, social, and cultural identities against one another. The purpose of the action is to exploit identity politics and allegiances, thus dividing influential interest groups and political alliances. Confusion and disorder ensue as people feel more insecure.

Defining Hybrid Threats

The PRC is focused globally on their influence and areas of interest, especially in the Asia Pacific region, and the use of social media for their influence operations. A key aim of their influence campaigns is the long-term acceptance of the PRC's roles and visions of the world, including key political messages, e.g. One China Concept, One Belt-One Road Initiative, South China Expansion.

The paper will look at Hybrid Threat examples related to Australia and PRC, the examples being:

Information Attacks

In 2020, the Australian government released the Breton report, which detailed the death of 39 Afghan civilians and prisoners by Australian special forces soldiers during the Afghanistan War. The then Australian Prime Minister Scott Morrison criticised the PRC's foreign ministry for a Twitter (X) post depicting an image of a grinning Australian soldier slitting the throat of what appears to be an Afghan child.[5]

The Chinese government expressed criticism of Australia in response to the Breton Report for a number of reasons. The key reason was the state of diplomatic relationships between Australia and the PRC. The release of the Breton Report coincided with heightened diplomatic tensions between Australia and the PRC. These tensions were fueled by disagreements over issues such as human rights, territorial disputes, COVID-19 and trade. The example also highlighted

Image posted on Twitter (X) by China's Foreign Ministry

the power of PRC state-controlled media outlets, such as the Global Times, which played a significant role in amplifying the criticism. These government media channels portrayed Australia as being aligned with Western interests and accused it of being part of a broader strategy to contain the PRC's rise. The information attack heightened an already tense situation.

Economic Attacks

Australia's trade ties with the PRC were impacted in 2018 when Australia publicly banned Huawei from its 5G network, and it worsened after Australia called for an enquiry into the origins of COVID-19. The PRC responded by introducing a trade war by banning imports of Australian barley, beef, coal, cotton, seafood and wine imports from Australia, which impacted billions of dollars of Australian exports.[6]

China imposed trade sanctions and tariffs on Australian exports again linked to escalating political tensions. The rationale of the economic actions was that the trade embargoes would have a financial impact on Australia and seriously affect Australia's trade. There was also the political message behind the trade sanctions due to the tense political situation, and the PRC wanted to send a message to Australia of their displeasure of the situation. They wanted Australia to see the error of their ways and stand down from their actions. It is only in 2024 that we are starting to see some normalisation of diplomatic relations between Australia and the PRC.

Infrastructure

One of Australia's key ports in Northern Australia, Darwin Port, was leased to a Chinese-owned company, Landbridge, for a period of 99 years. The concern is that ports form part of Australia's critical infrastructure, and Darwin Port is key to Australia's defence strategy and also U.S. military forces operarting in the area.

The key concern is the national security risk of a PRC company having control of one of Australia's key strategic assets. The arrangement has been controversial and was a key factor in the heightened diplomatic tensions between Australia and the PRC. A key area of tension in Australia was the discussion related to economic gains from leasing the port versus the potential security risks. A future challenge also relates to future Australian investments in Darwin Port when it is controlled by a PRC-owned company.

The new Australian Labour government (2022) has undertaken a security review and decided to put steps in place to monitor Landbridge operations to mitigate any possible security risks.[7] However, there are still ongoing security concerns from some Australian quarters about the agreement and that the new proposed monitoring arrangements

Coercive and Subversive Activities

Developing effective countermeasures is crucial to mitigate the impact of hybrid threats. This paper has highlighted the importance of understanding hybrid threats against Australia from the PRC. Understanding that hybrid threats are not standalone but could be part of a greater strategy is vital. Understanding the nature of hybrid threats, how they can be interconnected, and how they evolve over time is essential.
There are a number of areas where Australia does not fully understand the implications. As an example, the risks in relation to society and democracy are not fully understood, including the risk to Australian democratic institutions, including elections. The awareness and understanding of these threats will help Australia to defend against interference and maintain the integrity of its democratic processes.

Australia's awareness of hybrid threats is essential for protecting its national security, critical infrastructure, democratic institutions, and regional stability in an ever-changing world where authoritarian countries are becoming significant future threats.

Endnotes

[1] European Union, The Landscape of Hybrid Threats: A Conceptual Model Public Version, Publications Office of the European Union, ISBN 978-92-76-29819-9.
[2] European Union Hybrid Threat CoE (Centre of Excellence), Hybrid threats as a concept, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/, last accessed February 16, 2024.
[3] NATO Vilnius Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_217320.htm February 16, 2024.
[4] Graphic and model structure of the domains: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/ February 16, 2024.
[5] Yahoo News, 2020, "PM blasts China for 'truly repugnant' image of Australian soldier," https://au.news.yahoo.com/scott-morrison-slams-china-image-australian-soldier-child-china-025809975.html, November 30, 2023.
[6] New York Times, 2020, "Australia Condemns Lurid Tweet by Chinese Official as 'Disgusting Slur'," https://www.nytimes.com/2020/11/30/world/australia/china-tweet-soldier., November 30, 2023.
[7] Reuters, 2022, "Tension between China and Australia over commodities".
https://www.reuters.com/article/us-australia-trade-china-commodities-tim/timeline-tension-between-china-and-australia-over-commodities-trade-idUSKBN28L0D8/, December 11, 2023.
[8] Reuters, 2023, "Australia says 'not necessary' to cancel Chinese firm's lease on Darwin port," https://www.reuters.com/world/asia-pacific/australia-says-not-necessary-cancel-chinese-firms-lease-darwin-port-2023-10-20/, October 20.

Emerging Hybrid Threats: AI And Microtargeting Disinformation As A Security Threat To The Protection Of International Forces

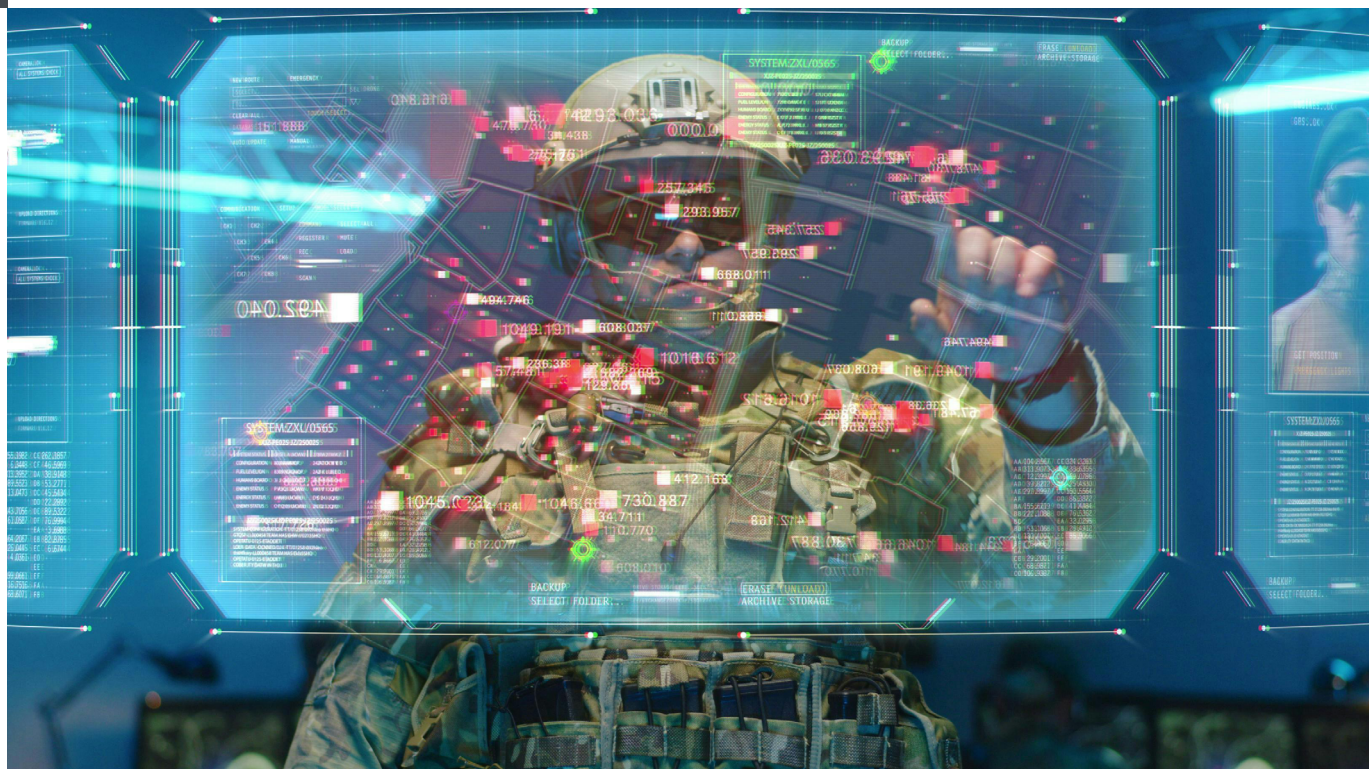
BERNARD SIMAN

Author: Bernard Siman is a Senior Associate Fellow at Egmont Royal Institute for International Relations in Belgium, where he is responsible for hybrid threats and warfare. He teaches at the Royal Military Academy in Belgium, and the European Security and Defence College. He also heads Cyber Diplomacy at the Brussels Diplomatic Academy of the Vrije Universiteit Brussel (VUB). Geographically, he specialises in the Mediterranean and Black Sea regions, including the Middle East, and in global maritime geopolitics. He has authored various publications on hybrid threats and global geopolitics. The views expressed in this article are the author's alone.

Abstract: Disinformation has mainly been viewed as a communication challenge. For entities like the UN, the EU and NATO, it has evolved into a security threat and a Force Protection (FP) challenge, as well as a threat to the well-being of deployed individuals and their families overseas. Feasibly, this threat will only grow with the combination of AI-enabled "deepfakes" and microtargeting.

Problem statement: What role does strategic communication play in ensuring that peacekeeping and EU missions continue to have enhanced protection of their military forces overseas?

So what?: Strategic, emotive communication must urgently become an integral part of the planning and execution of mission security, which should expand in scope to include civil society organisations in the areas where personnel are deployed.



Source: shutterstock.com/Frame Stock Footage

"FIMI" as a Security Threat, Not Just a Communication Challenge

The EU has identified Foreign Information Manipulation and Influence (FIMI) as a key hybrid threat.

'A mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors including their proxies inside and outside of their own territory.'[1]

This is akin to an umbrella description of disinformation, malinformation and other forms of malign operation in both the information and cognitive domains. Disinformation is "the creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public".[2]

Mis-information is unintentionally doing so, whilst mal-information entails deliberately designing and employing dis- and mis-information to cause harm to specific individuals and organisations. It is easy, therefore, to see why FIMI has largely been viewed as a communications threat in the first instance, undermining the soft cornerstones of democratic order, such as trust, legitimacy and cohesion. Whereas this is an accurate description and diagnosis in a broad sense, it does not deal with FIMI as a security threat with consequences on the ground (such as civil disorder and terrorism). These consequences include increased radicalisation, recruitment of terrorists, and incitement to attack. Examples include accusing Western soldiers in the Sahel of abusing the local population. In one case, false photographs were published in Sahel countries purporting to depict a destroyed village due to French Air Force activities. This was deliberate disinformation.

FIMI poses a narrower, more focused and direct military and mission security dimension in the area of force protection, such as in UN operations, EU deployments and NATO missions. It is a force protection threat during deployments, whether civilian or military. In this context, FIMI can take the form of deepfake photos, videos or audio falsely depicting UN peacekeepers, EU or NATO mission personnel torturing or abusing locals. This can have a twofold consequence of increasing the radicalisation and recruitment of terrorists locally, but also creating a backlash in public opinion in the sending countries against deploying troops overseas. Clearly, this is not just a

communication challenge that needs to be resolved by correcting the record and addressing the communication issues in general. It is a direct force protection and mission security threat. As such, Strategic Communications (STRATCOM) should become an integral and more important component of planning UN, EU and NATO deployments beyond tactical "cultural" Strategic Communications and towards formulating and disseminating narratives.

A related strategic threat resulting from FIMI involves undermining public and political support in the countries that participate in sending personnel on these missions, duly undermining their commencement or continuity.

Well-being of Individuals is the Other Face of Maintaining Political Support

Moreover, fake news, as well as deepfakes, are exploited by state and non-state actors to attack the well-being (physical, mental and emotional) and safety of individuals in the field, as well as their families back in their home countries. An AI-generated deepfake video circulated widely just days after the military junta in Burkina Faso ordered French troops to leave the country following the successful coup in 2023. The video urged support for the junta and its leader. A similar video targeting the presence of French troops circulated widely in Mali around the same time. Equally worrying are the "cheap fakes" that are on the other end of the technical specifications spectrum from AI-enabled deepfakes. "Cheap fakes are quicker and less resource-intensive. They can be similarly misleading, though less realistic. Cheap fakes range from videos taken out of context to simple edits such as speeding up or slowing down video or audio to misrepresent events … In Africa, ultra-cheap fakes are more of a problem for disinformation than deepfakes … It is easier to produce large numbers of quick, cheap fakes."[3]

This form of FIMI, in which AI-enabled deepfakes utilize synthetic data coupled with microtargeting, is very likely to become a key hybrid tool in the context of individuals participating in overseas missions and political influence operations, such as elections. In this context and in the broader hybrid threat framework of FIMI, the combination of AI-enabled deepfakes with bot-driven microtargeting will raise the FIMI threat to a totally new, and very dangerous level. Essentially, not knowing not just "what" is true or false but also "who" is real or not, coupled with the emerging phenomenon of developing emotional dependencies and intimacies with bots, will make it extremely challenging to deal with the threat without putting in place very well-resourced concrete institutional and expert structures.

Moreover, a key aim of FIMIs is to whip up resentment against the mission and the individuals participating, both in the recipient and in the sending countries. This latter objective can undermine the physical security of the individuals and their missions as local populations become enraged by fake news and deepfakes. Moreover, the public and political sentiment in the home (sending) countries of the individuals participating in the missions can turn hostile against the individuals, their families, and the missions, including in the local communities where the individuals reside and their families live. At the conference on "75 years of UN peacekeeping: how can UN peacekeeping missions tackle the challenge of disinformation?",[4] it became clear from the various contributions that such activities further undermine the safety and mental well-being of the individuals and their families, as well as budgets, recruitment and support for participation in future missions.

The Anatomy of a Hostile FIMI Operation Using Deepfakes

Deepfakes are video and audio clips that depict individuals doing and saying things they never did or said. They were already being deployed even when the technology and software required actors and considerable time. As technology has rapidly developed, the time, cost, and technical skills required to produce convincing deepfakes have exponentially shrunk. This makes deepfakes more accessible, including the proverbial individual spending time online in their homes. With the emergence of

AI, however, AI-enabled deepfakes are likely to become a key security threat in the hands of malign actors operating in the hybrid domain, particularly given that "within the information environment, the human-centric cognitive dimension remains the most important".[5]

This is mainly the case as deepfakes can currently be produced using completely synthetic data: the faces of people who never existed speaking with voices that never existed in all existing languages and dialects, doing things they never did.

A multi-modal operation has the potential to be both cheap and effective. This kind of operation involves the deliberate combination and coordination of several different hybrid tools to cause damage to an individual, state, group or organisation. For example, a deepfake depicting mission personnel torturing a local individual can be combined with social and traditional media campaigns. The dissemination of this deepfake can also target the deployed individual's family and friends back home.

The deepfake could then cross into the digital sphere, leading to diverse repercussions. These range from security threats related to force protection because of an outraged local population, to concerns about the physical safety of the individuals involved and that of their families. There is also the risk of psychological and mental strain on the families, potentially leading to social ostracisation in their home communities, for example. A snowball effect of incremental tactical security threats can lead to broader malign strategic threats, such as undermining political support for continuing a particular operation.

Developing an Emotive Narrative Key to Defeating FIMI

A key long-term step in preventatively countering FIMI is to stop relying on cold facts alone to defeat and counter emotively formulated FIMI. This became clear during the war against Daesh/ISIS/ISIL. Counter-radicalisation efforts focused on highlighting factual defects in what Daesh was offering. In fact, the motivation for many would-be recruits to Daesh's cause was driven by emotive, idealist, or romantic motivations, or a mixture of the three drivers. These drivers could not be effectively countered by restating cold objective facts without their emotive context.

Europe and the West, in general, have targeted minds for far too long by using blunt facts and, perhaps more often than not, by ignoring hearts. Europe, in particular, needs to deploy a positive emotive narrative and reclaim dominance in the cognitive domain. It has a great story to tell - but facts alone will not win hearts in many regions of the world where missions are deployed. There is currently a sufficiently large space that is being filled with hostile narratives. It is essential to re-occupy this space in the information and cognitive domains through content development and dissemination, which should become an integral part of mission planning.

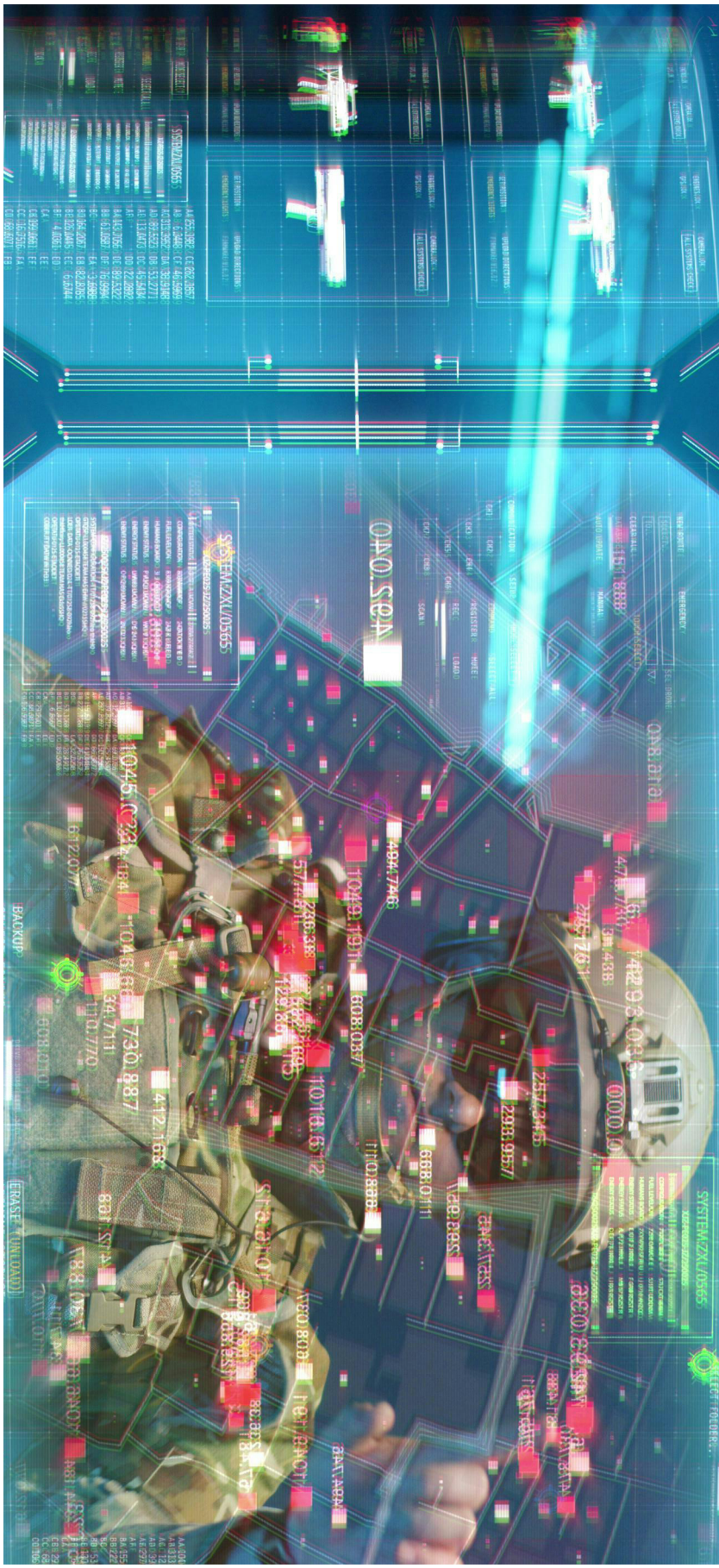
Superiority is Mandatory

FIMI covers a battlefield on which the West must prevail. This war is fought in two domains - information and cognitive, in a quest to influence "What one thinks" and "How one thinks". Whereas facts play a key role in the information domain, the battle in the cognitive domain shapes perceptions, involving emotions as much as it does facts. Narratives also play a crucial role in shaping perceptions. Yet efforts to counter emotive narratives and shape perceptions with cold facts have not yielded the desired results.

It is equally clear that always acting in a defensive mode risks two outcomes. The first is that in order to counter a piece of disinformation, it will need to be repeated first to be able to refute it. In the majority of cases, this simply contributes to the spread and embellishment of the piece of disinformation, not only undermining the effort to counter it, but potentially lending it additional credibility. The second outcome is that the information and cognitive domains will remain in need of proactive and preventive saturation with positive emotive narratives that act as a natural barrier against malign disinformation if the current modus operandi continues to prevail.

Moreover, and from a practical perspective, local civil society organisations can play an important role in countering FIMI and enhancing force protection. To turbo-charge their activities, establishing institutional and structured open-source support (such as a centre) will play an important role in enhancing their ability to defeat FIMI in locally acceptable cultural methods and deliver them in the languages of the deployment locale. This capability will enhance the ability of local civil society organisations and others to defeat FIMI locally.

The need for overseas missions, civilian as well as military (whether the EU or the UN), will continue to grow in importance. There is a clear need to develop an effective set of tactical and strategic responses to FIMI, particularly when it comes to mission security and the continued political support for these missions over and above the generalised responses to FIMI as a communications threat. It is, and will continue to be, a key security threat requiring a commensurate, imaginative and effective set of measures specifically related to STRATCOM.



Endnotes

[1] EEAS, “Strategic Communications, Task Forces and Information Analysis (STRAT.2),” February 2023.
[2] European Court of Auditors, “EU action plans against disinformation,” March 2020.
[3] Kirsten Cosser, “AI-powered disinformation: deepfakes, detection technology and the weaponisation of doubt,” August 07, 2023, https://africacheck.org/fact-checks/blog/ai-powered-disinformation-deepfakes-detection-technology-and-weaponisation-doubt.
[4] “75 years of UN peacekeeping: how can UN peacekeeping missions tackle the challenge of disinformation/misinformation?,” Egmont Institute, June 29, 2023, https://www.egmontinstitute.be/events/75-years-of-un-peacekeeping-how-can-un-peacekeeping-missions-tackle-the-challenge-of-disinformation-misinformation/.
[5] Matthew Fecteau, “The Deep Fakes are coming,” Army War College, The War Room, April 23, 2021, https://warroom.armywarcollege.edu/articles/deep-fakes/.

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

ISBN: 978-3-200-09760-5

THE DEFENCE HORIZON JOURNAL